

Kompletterande bestämmelser till EU:s cyberresiliensförordning

Betänkande av Cyberresiliensutredningen

Stockholm 2025



STATENS OFFENTLIGA
UTREDNINGAR

SOU 2025:115

SOU och Ds finns på [regeringen.se](https://www.regeringen.se) under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2021:1.

Information för dem som ska svara på remiss finns tillgänglig på [regeringen.se/remisser](https://www.regeringen.se/remisser).

Layout: Kommittéservice, Regeringskansliet

Omslag: Åtta45

Tryck och remisshantering: Åtta45, Stockholm 2025

ISBN 978-91-525-1421-4 (tryck)

ISBN 978-91-525-1422-1 (pdf)

ISSN 0375-250X

Till statsrådet Erik Slottner

Regeringen beslutade den 28 november 2024 att tillkalla en särskild utredare med uppgift att analysera behovet av och föreslå åtgärder och kompletterande författningsbestämmelser som behövs i syfte att anpassa svensk rätt till EU:s cyberresiliensförordning. Uppdraget skulle redovisas senast den 15 december 2025.

Som särskild utredare förordnades från och med den 15 december 2024 juristen Annette Norman.

Som huvudsekreterare i utredningen anställdes den seniora rådgivaren Thomas Wallander från och med den 15 december 2024. Som sekreterare i utredningen anställdes från och med den 15 december 2024 juristen Peggy Haase och juristen Camilla Östlund.

Som sakkunniga förordnades den 13 januari 2025 kanslirådet Shafagh Wikner Elhami, Statsrådsberedningen, rättssakkunniga Amanda Arby, Finansdepartementet, departementssekreteraren Harald Fredriksson, Finansdepartementet, departementssekreteraren Rebecca Ideström, Finansdepartementet, kanslirådet Yvonne Stein, Finansdepartementet, departementssekreteraren Jonas Magnusson, Försvarsdepartementet och departementssekreteraren Tobias Walla, Klimat- och näringslivsdepartementet. Amanda Arby entledigades den 15 maj 2025 och rättssakkunniga Malin Söderhjelm, Finansdepartementet, förordnades som sakkunnig samma dag.

Som experter förordnades den 13 januari 2025 enhetschefen Nils Alenius, Försvarets radioanstalt, bedömningsledaren Mattias Andersson, Styrelsen för ackreditering och teknisk kontroll (Swedac), avdelningschefen John Billow, Försvarets materielverk (FMV), juristen Carolina Brånby, Svenskt Näringsliv, cybersäkerhetsstrategen James Christie, Post- och telestyrelsen, strategen Andreas Häll, Myndigheten för samhällsskydd och beredskap (MSB), ämnesrådet Anna Sabelström, Kommerskollegium, juristen Kristina Wallin, Konsumentverket och handläggaren Kristin

Willamo, Energimyndigheten. Kristin Willamo entledigades den 26 augusti 2025 och handläggare Galawesh Sofi, Energimyndigheten, förordnades som expert samma dag. John Billow entledigades den 3 september 2025 och juristen Madelene Skeppar, FMV, förordnades som expert samma dag. Andreas Häll entledigades den 1 september 2025 och seniora rådgivaren Martin Snygg, MSB, förordnades som expert den 26 september 2025.

Utredningen överlämnar härmed betänkandet *Kompletterande bestämmelser till EU:s cyberresiliensförordning*, SOU 2025:115. Utredningens uppdrag är därmed slutfört.

Stockholm i december 2025

Annette Norman

Thomas Wallander
Peggy Haase
Camilla Östlund

Innehåll

Förkortningar	19
Sammanfattning	29
Summary	37
1 Författningsförslag.....	47
1.1 Förslag till lag med kompletterande bestämmelser till EU:s cyberresiliensförordning	47
1.2 Förslag till förordning med kompletterande bestämmelser till EU:s cyberresiliensförordning.....	55
1.3 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)	58
1.4 Förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641)	62
1.5 Förslag till förordning om ändring i förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap	64
2 Uppdraget	65
2.1 Inledning.....	65
2.2 Bakgrund	65
2.3 Uppdraget.....	66
2.4 Utgångspunkter	67
2.5 Definitioner	69

2.6	Utredningsarbetet	69
2.7	Betänkandets disposition	70
3	EU:s cyberresiliensförordning	73
3.1	Inledning	73
3.2	Förordningens innehåll	73
3.2.1	Syfte och tillämpningsområde	73
3.2.2	Allmänna bestämmelser	74
3.2.3	Ekonomiska aktörers skyldigheter och bestämmelser om programvara med fri och öppen källkod	75
3.2.4	Bedömning av överensstämmelse med väsentliga krav på cybersäkerhet	76
3.2.5	Anmälan av organ för bedömning av överensstämmelse	77
3.2.6	Marknadskontroll, skyddsåtgärder och övrig tillsyn	77
3.2.7	Delegerade befogenheter och kommittéförfarande	78
3.2.8	Konfidentialitet och sanktioner	78
3.2.9	Avslutande bestämmelser	78
3.2.10	Rättelser och ändringar i EU:s cyberresiliensförordning	79
3.3	Behov av kompletterande bestämmelser	80
3.3.1	En ny lag och en ny förordning	80
3.3.2	Hänvisningar till EU:s cyberresiliensförordning	81
4	EU:s cyberreglering	83
4.1	Inledning	83
4.2	EU:s strategi för ökad cybersäkerhet	83
4.3	EU:s regelsystem på cyberområdet	85
4.3.1	Förordning (EU) 2019/881 (EU:s cybersäkerhetsakt)	86
4.3.2	Direktiv (EU) 2022/2555 (NIS 2-direktivet)	93

4.3.3	Förordning (EU) 2024/1689 (AI-förordningen)	101
4.3.4	Förordning (EU) 2024/1183 (eIDAS-förordningen)	108
4.3.5	Förordning (EU) 2016/679 (EU:s dataskyddsförordning) och direktiv (EG) 2002/58 (e-dataskyddsdirektivet)	110
4.3.6	Direktiv 2014/53/EU (radioutrustningsdirektivet) och delegerade förordning (EU) 2022/30	114
4.3.7	Förordning (EU) 2023/1230 (maskinförordningen)	115
4.4	Förordning (EU) 2023/988 (förordning om allmän produktsäkerhet)	117
4.4.1	Syfte och tillämpningsområde	117
4.4.2	Krav på cybersäkerhet	117
4.4.3	Artikel 11 i EU:s cyberresiliensförordning och krav på allmän produktsäkerhet	119
4.5	EU:s arbete med regelförenkling på det digitala området	121
4.5.1	EU:s regelförenklingspaket	122
4.5.2	New Legislative Framework (NLF)	125
5	Undantag för nationell säkerhet och försvar	127
5.1	Inledning	127
5.2	Utgångspunkter	127
5.3	Undantag för nationell säkerhet och försvar	128
5.4	Närmare om undantagen	130
5.4.1	Nationell säkerhet och försvarsändamål	130
5.4.2	Produkter som tillverkas eller ändras uteslutande för nationell säkerhet eller försvarsändamål (artikel 2.7)	136
5.4.3	Produkter som utformas specifikt för att behandla säkerhetsskyddsklassificerade uppgifter (artikel 2.7)	137

5.4.4	Undantag från uppgiftsskyldigheten (artikel 2.8)	139
5.5	Remissvar över kommissionen utkast till EU:s cyberresiliensförordning	141
5.6	Produkten tillhandhålls på marknaden.....	145
5.7	Överväganden	148
6	Bestämmelser om bedömning av överensstämmelse	153
6.1	Inledning	153
6.2	Väsentliga cybersäkerhetskrav på produkter med digitala element införs (artikel 6)	153
6.2.1	Presumption om överensstämmelse (artikel 27)...	155
6.2.2	EU-försäkran om överensstämmelse (artikel 28)	156
6.2.3	Allmänna principer för CE-märkning (artikel 29 och 30)	156
6.3	Bedömning av överensstämmelse av de väsentliga cybersäkerhetskraven (artikel 32)	158
6.3.1	Produkter med digitala element som inte förtecknas som viktiga eller kritiska produkter (artikel 32.1)	159
6.3.2	Viktig produkt med digitala element (artikel 32)	159
6.3.3	Kritiska produkter med digitala element (artikel 32.4)	161
6.3.4	Produkter som klassificeras som programvara med fri och öppen källkod (artikel 32.5)	161
6.3.5	AI-system med hög risk (artikel 12)	161
6.4	Närmare om förfaranden för bedömning av överensstämmelse (artikel 32)	163
6.4.1	Intern kontroll baserat på modul A (Bilaga VIII Del 1)	163
6.4.2	EU-typkontroll baserat på modul B (Bilaga VIII Del II)	163

6.4.3	Intern tillverkningskontroll baserat på modul C (Bilaga VIII Del III)	166
6.4.4	Fullständig kvalitetssäkring baserat på modul H (Bilaga VIII Del IV)	166
6.5	Anmälan av organ för bedömning av överensstämmelse....	169
6.5.1	Anmälan (artikel 35)	169
6.5.2	Krav på anmälda organ (artikel 39)	169
6.5.3	Presumption om överensstämmelse för anmälda organ (artikel 40)	169
6.5.4	Ansökan om anmälan (artikel 42)	169
6.5.5	Anmälningsförfarande (artikel 43)	170
6.5.6	De anmälda organens operativa skyldigheter (artikel 47)	172
6.5.7	De anmälda organens informationsskyldighet (artikel 49)	173
6.6	Ackreditering av organ för bedömning av överensstämmelse	174
6.7	Ackreditering bör ligga till grund för anmälan	176
6.8	Anmälände myndighet.....	178
6.9	Tillgång till organ för bedömning av överensstämmelse	180
6.10	Åtgärder vid återkallelse av anmälan av organ för bedömning.....	184
6.11	Övervakning av anmälda organ	186
6.12	Gränsdragningen mellan Swedac och en marknadskontrollmyndighet.....	190
6.13	Överlämnande av förvaltningsuppgifter till privata organ för bedömning av överensstämmelse	191
6.13.1	Överlämnande av förvaltningsuppgift.....	191
6.13.2	Handläggning av ärenden.....	194
6.13.3	Ändring av beslut av ett privatorgan för bedömning av överensstämmelse.....	199
6.14	Överklagande av beslut av anmälda organ och av förvaltningsmyndighet	202

6.14.1	Överklagande av beslut av privat organ för bedömning av överensstämmelse.....	203
6.14.2	Det anmälda organet ska vara motpart	212
6.14.3	Överklagande av förvaltningsmyndighets beslut.....	213
6.14.4	Rätt att överklaga myndighets beslut enligt den nya lagen	214
6.14.5	Förvaltningsmyndighet ska vara motpart	216
6.14.6	Prövningstillstånd i kammarrätt.....	217
7	Standardisering	219
7.1	Inledning	219
7.2	Standardisering i Sverige	220
7.2.1	De tre nationella standardiseringsorganen	220
7.2.2	Standardiseringsorganens finansiering.....	221
7.3	Kommissionens standardiseringsbegäran	222
7.4	Intressenternas roll och fördelar med att delta i standardiseringsarbete.....	223
7.5	Standardiseringsarbete som stöd för EU:s cyberresiliensförordning.....	225
7.5.1	CEN och Cenelec	225
7.5.2	CEN, Cenelec och ETSI	226
7.5.3	Svenskt deltagande i standardiseringsarbetet	227
7.5.4	Utmaningar för standardiseringsarbetet.....	229
7.6	Överväganden	233
8	Sårbarhets- och incidentrapportering	235
8.1	Inledning	235
8.2	Tillverkarens skyldigheter.....	236
8.2.1	Vem ska rapportera vad?.....	236
8.2.2	Till vem ska rapporterna lämnas och hur ska det göras?	237
8.2.3	Vilka uppgifter ska rapporteras och inom vilken tid ska rapporterna lämnas?	239

8.3	CSIRT-enhetens uppgifter	240
8.4	Kompletterande EU-lagstiftning	245
8.5	CSIRT-enhet i Sverige	245
9	Marknadskontroll	247
9.1	Inledning.....	247
9.2	Syftet med marknadskontroll.....	247
9.3	Reglering av marknadskontroll inom EU	248
9.4	Organiseringen av marknadskontroll i Sverige	250
9.5	Utgångspunkter för fördelningen av marknadskontrollansvaret på en eller flera myndigheter	251
9.5.1	EU:s cyberresiliensförordning.....	251
9.5.2	Marknadskontrollmyndighetens uppgifter	253
9.5.3	Kompetensbehov	256
9.5.4	Överväganden	257
9.6	Val av marknadskontrollmyndighet	260
9.6.1	Generella utgångspunkter	260
9.6.2	Statens energimyndighet.....	260
9.6.3	Försvarets materielverk.....	262
9.6.4	Försvarets radioanstalt	266
9.6.5	Konsumentverket	268
9.6.6	Myndigheten för samhällsskydd och beredskap	270
9.6.7	Post- och telestyrelsen	277
9.6.8	Styrelsen för ackreditering och teknisk kontroll.....	283
9.6.9	Post- och telestyrelsen bör ges marknadskontrollansvar för EU:s cyberresiliensförordning	287
9.7	Förbättra kompetensen i en cyberresilient digital miljö	290
9.8	Förslag till kompletterande lagstiftning	291
9.8.1	Upplysningar om marknadskontroll och marknadskontrollmyndigheter	291

9.8.2	Marknadskontrollmyndighetens befogenheter...	293
9.8.3	Beslut om förelägganden	295
9.8.4	Hjälp från Polismyndigheten	296
9.8.5	Bestämmelser om vissa avgifter för marknadskontroll.....	297
9.8.6	Överklagande	298
10	Sanktioner	299
10.1	Inledning	299
10.2	Bestämmelser om sanktionsavgifter.....	299
10.2.1	Det ska vara obligatoriskt att ta ut sanktionsavgift	301
10.2.2	Frågan om strikt ansvar eller uppsåt och vårdslöshet.....	302
10.3	Gemensamma bestämmelser för sanktionsavgift	306
10.3.1	Omständigheter som ska beaktas vid bedömning av sanktionsavgift	307
10.3.2	Sanktionsavgifter kan påföras offentliga myndigheter och offentliga organ.....	309
10.3.3	Anmälade myndighet och marknadskontrollmyndigheten ska besluta om sanktionsavgift	315
10.3.4	Vite och sanktionsavgift för samma överträdelse	320
10.3.5	Undantag	321
10.4	Förfaranderegler och preskription	322
11	Sekretess	325
11.1	Inledning	325
11.2	Bakgrund.....	325
11.3	Bestämmelser om konfidentialitet i EU:s cyberresiliensförordning.....	327
11.4	Bestämmelser om informationsdelning i EU:s cyberresiliensförordning.....	330
11.4.1	CSIRT-enheten	330

11.4.2	Marknadskontrollmyndigheterna.....	332
11.4.3	Den anmälade myndigheten	335
11.4.4	Anmälda organ.....	335
11.5	Offentlighet och sekretess	336
11.6	Sekretess till skydd för sårbarhets- och incident- rapporter med mera	338
11.6.1	Analys av gällande rätt.....	339
11.6.2	En ny sekretessbestämmelse för uppgift i sårbarhets- och incidentrapporter samt en ny sekretessbrytande bestämmelse	342
11.6.3	En ny sekretessbestämmelse för diarium för sårbarhets- och incidentrapporter	349
11.7	Sekretess till skydd för risk- och sårbarhetsanalyser med mera	350
11.8	Sekretess till skydd för enskild vid marknadskontroll och utredning	351
11.9	Sekretess till skydd för enskild inom ramen för regulatoriska sandlådor för cyberresiliens.....	353
11.9.1	Analys av gällande rätt.....	353
11.9.2	En ny sekretessbestämmelse för uppgift om enskild i verksamhet som består i regulatoriska sandlådor för cyberresiliens.....	355
11.10	Sekretess till skydd för enskild i mål och ärenden hos domstol.....	355
11.11	Sekretess till skydd för det internationella samarbetet	356
11.12	Sekretess till skydd för tillsyn samt av straffrättsliga och administrativa förfaranden	359
11.13	Tystnadsplikt.....	360
11.14	Sekretessbrytande bestämmelser och överföring av sekretess (informationsdelning).....	361
11.14.1	Internationell informationsdelning	362
11.14.2	Nationell informationsdelning	362
11.15	Behandling av personuppgifter	365

12	Stöd till företag	369
12.1	Inledning	369
12.2	Företagens utmaningar och behov av stöd	372
12.3	EU:s cyberresiliensförordning.....	375
12.3.1	Anpassningar och kompletterande reglering.....	375
12.3.2	Stöd från ett antal utpekade aktörer	376
12.4	Nuvarande stöd till svenska företag inom cybersäkerhetsområdet	378
12.4.1	Myndigheter som arbetar med cybersäkerhet	379
12.4.2	Andra aktörer och funktioner inom cybersäkerhetsområdet	384
12.5	Stöd till företag gällande regelefterlevnad av EU:s cyberresiliensförordning	388
12.5.1	Stödåtgärder enligt artikel 33.1	390
12.5.2	Regulatoriska sandlådor för cyberresiliens enligt artikel 33.2	393
13	Analys av berörda regelverk.....	397
13.1	Inledning	397
13.2	Lagen (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt	398
13.3	Förslag till ny cybersäkerhetslag (NIS 2-direktivet).....	399
13.4	Dataskyddslagen (2018:218)	4000
13.5	Lagen (2022:482) om elektronisk kommunikation.....	401
13.5.1	Rätt att använda radiosändare	401
13.5.2	Säkerhetsåtgärder och incidentrapportering	403
13.6	Radioutrustningslagen (2016:392)	405
13.7	Produktsäkerhetslagen (2004:451)	406
13.8	Konsumentköplagen (2022:260)	411
13.8.1	EU:s cyberresiliensförordning	411
13.8.2	Närmare om konsumentens rättigheter enligt konsumentköplagen	413

13.8.3	Överväganden	414
13.9	Konsumenttjänstlagen (1985:716)	420
13.9.1	Närmare om konsumentens rättigheter i konsumenttjänstlagen	420
13.9.2	Överväganden	426
14	Övriga frågor	429
14.1	Inledning.....	429
14.2	EU-försäkran om överensstämmelse.....	429
14.3	Gemensam kontaktpunkt för rapportering av sårbarheter och incidenter	430
14.4	Ikraftträdande- och övergångsbestämmelser	432
15	Konsekvensutredning.....	437
15.1	Inledning.....	437
15.1.1	Kommissionens konsekvensbedömning	438
15.1.2	Underlag till konsekvensutredningen	438
15.2	Övergripande om utredningens förslag.....	439
15.3	Vem berörs av förslagen?	440
15.3.1	Uppskattning av antalet ekonomiska aktörer samt förvaltare av programvara med fri och öppen källkod	441
15.4	Ekonomiska konsekvenser för ekonomiska aktörer samt förvaltare av programvara med fri och öppen källkod	443
15.4.1	Ekonomiska konsekvenser för ekonomiska aktörer samt förvaltare av programvara med fri och öppen källkod till följd av EU:s cyberresiliensförordning	443
15.4.2	Ekonomiska konsekvenser för ekonomiska aktörer samt förvaltare av programvara med fri och öppen källkod till följd av utredningens förslag.....	444

15.5	Särskilt om ekonomiska konsekvenser för små och medelstora företag.....	445
15.6	Ekonomiska konsekvenser för Swedac	446
15.7	Ekonomiska konsekvenser för anmälda organ för bedömning av överensstämmelse.....	447
15.8	Ekonomiska konsekvenser för CSIRT-enheten.....	448
15.9	Ekonomiska konsekvenser för Myndigheten för samhällsskydd och beredskap – stöd till företag	453
15.10	Ekonomiska konsekvenser för marknadskontrollmyndigheterna	455
15.10.1	Marknadskontroll.....	456
15.10.2	Ekonomiska konsekvenser för marknadskontrollmyndigheterna – stöd till företag och regulatoriska sandlådor	460
15.10.3	Ekonomiska konsekvenser för Post- och telestyrelsen – förbättra kompetensen i en cyberresilient digital miljö samt öka tillgång på organ för bedömning av överensstämmelse	460
15.11	Ekonomiska konsekvenser för Tullverket	461
15.12	Ekonomiska konsekvenser för Polismyndigheten	461
15.13	Ekonomiska konsekvenser för Sveriges domstolar	462
15.14	Konsekvenser för det kommunala självstyret.....	463
15.15	Konsekvenser med anledning av standardiseringsarbetet ..	463
15.16	Konsekvenser för jämställdhet och den personliga integriteten.....	464
15.17	Särskild hänsyn till tidpunkt för ikraftträdande och behov av speciella informationsinsatser	465
15.18	Utvärdering av konsekvenserna.....	465

16 Författningskommentar 467

16.1 Förslaget till lag med kompletterande bestämmelser till
EU:s cyberresiliensförordning 467

16.2 Förslaget till lag om ändring i offentlighets-
och sekretesslagen (2009:400) 485

Referenser 489**Bilagor**

Bilaga 1 Kommittédirektiv 2024:119 493

Bilaga 2 EU:s cyberresiliensförordning 501

Bilaga 3 Konsultrapport Konsekvenser avseende krav
i EU:s cyberresiliensförordning – Analys på
uppdrag av Cyberresiliensutredningen 585

Förkortningar

Adco	Administrative cooperation
AI-förordningen	Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens)
Beslut nr 768/2008/EG	Europaparlamentets och rådets beslut nr 768/2008/EG av den 9 juli 2008 om en gemensam ram för saluföring av produkter och upphävande av rådets beslut 93/465/EEG
CCCN-förordningen	Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum
CCRA	Common Criteria Recognition Arrangement
CDIS	Centrum för cyberförsvar och informationssäkerhet

CEN	Comité Européen de Normalisation
CER-direktivet	Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG
Cenelec	Comité Européen de Normalisation Electrotechnique
CERT-SE	Sveriges nationella Computer Emergency Response Team
CLC	Cenelec (som referens i dokument)
CSEC	Sveriges Certifieringsorgan för IT-säkerhet
CSIRT-enhet	Computer Security Incident Response Team
Delegerade förordning (EU) 2022/30	Kommissionens delegerade förordning (EU) 2022/30 av den 29 oktober 2021 om komplettering av Europaparlamentets och rådets direktiv 2014/53/EU vad gäller tillämpningen av de väsentliga krav som avses i artikel 3.3 d, e och f i det direktivet
Dora-förordningen	Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011
Digg	Myndigheten för digital förvaltning

E-dataskyddsdirektivet	Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation)
ECCG	Europeiska gruppen för cybersäkerhetscertifiering
eIDAS-förordningen	Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet
Enisa	Europeiska unionens cybersäkerhetsbyrå
ETSI	European Telecommunications Standards Institute
EU	Europeiska unionen
EU:s cyberresiliensförordning	Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen)

EU:s cybersäkerhetsakt	Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten)
EU:s dataskyddsförordning	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
EU:s marknadskontrollförordning	Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011
EU:s maskinförordning	Europaparlamentets och rådets förordning (EU) 2023/1230 av den 14 juni 2023 om maskiner och om upphävande av Europaparlamentets och rådets direktiv 2006/42/EG och rådets direktiv 73/361/EEG

EU:s standardiseringsförordning	Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG
EUCC	European Common Criteria-based Cybersecurity Certification Scheme
EU CyCLONe	European cyber crisis liaison organisation network
EUPCN	European Product Compliance Network
EUSR	European Union Standardisation Request
FL	Förvaltningslagen (2017:900)
FMV	Försvarets Materielverk
FOI	Totalförsvarets forskningsinstitut
FRA	Försvarets radioanstalt
Förordning (EG) nr 765/2008	Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93

Förordning (EU) 2022/2480	Europaparlamentets och rådets förordning (EU) 2022/2480 av den 14 december 2022 om ändring av förordning (EU) nr 1025/2012 vad gäller europeiska standardiseringsorganisationers beslut om europeiska standarder och europeiska standardiseringsprodukter
ICC	Inspektionen för cybersäkerhetscertifiering
ICS	Industriella informations- och styrsystem
ICSMS	Information and Communication System for Market Surveillance
IEC	International Electrotechnical Commission
IKT	Informations- och kommunikationsteknik
IoT	Internet of Things
ISO	International Organization for Standardization
ISO/IEC 17025:2018	SS-EN ISO/IEC 17025:2018 – Allmänna kompetenskrav för provnings- och kalibreringslaboratorier (ISO/IEC 17025:2017)
ISO/IEC 17065:2012	SS-EN ISO/IEC 17065:2012 – Bedömning av överensstämmelse – Krav på organ som certifierar produkter, processer och tjänster (ISO/IEC 17065:2012)
ITS	Svenska Informations- och Telekommunikationsstandardiseringen
ITU	International Telecommunication Union

JTC	Joint Technical Committee
Kommissionen	Europeiska kommissionen
LEK	Lagen (2022:482) om elektronisk kommunikation
LO	Landsorganisationen i Sverige
NCCA	National Cybersecurity Certification Authorities
NCSC	Nationellt cybersäkerhetscenter
NCSC-förordningen	Förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt
NCC-SE	Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet
NIS 2-direktivet	Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet)
NIS-direktivet	Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen
NIS-lagen	Lagen (2018:1174) om informations-säkerhet för samhällsviktiga och digitala tjänster
MSB	Myndigheten för samhällsskydd och beredskap

NLF	New Legislative Framework
OECD	Organisation for Economic Cooperation and Development
OSF	Offentlighets- och sekretess-förordningen (2009:641)
OSL	Offentlighets- och sekretesslagen (2009:400)
OSSE	Organisation för säkerhet och samarbete i Europa
Prop.	Proposition
PTS	Post- och telestyrelsen
Radioutrustnings-direktivet	Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhanda-hållande på marknaden av radio-utrustning och om upphävande av direktiv 1999/5/EG
SACO	Sveriges akademikers central-organisation
SEK	SEK Svensk elstandard
SIS	Svenska Institutet för Standarder
SKA-rådet	Sveriges konsument- och arbetstagarrådet
SOU	Statens offentliga utredningar
SSCD	Secure Signature Creation Device
SSF	Stöldskyddsföreningen
SWEDAC	Styrelsen för ackreditering och teknisk kontroll
TC	Technical Committee
TCO	Tjänstemännens centralorganisation

TK	Teknisk kommitté
WG	Working Group

Sammanfattning

Uppdraget

Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen), här benämnd EU:s cyberresiliensförordning, ska i huvudsak tillämpas från och med den 11 december 2027 (förordningen finns i sin helhet i bilaga 2).

Utredningens uppdrag har varit att analysera behovet av och föreslå åtgärder och kompletterande författningsbestämmelser som behövs i syfte att anpassa svensk rätt till EU:s cyberresiliensförordning och som behöver finnas på plats när förordningens olika bestämmelser börjar tillämpas.

I uppdraget har ingått att överväga och föreslå vilken befintlig myndighet som ska utses till anmälade myndighet med ansvar för att inrätta och genomföra de förfaranden som krävs för bedömning, utseende och anmälan av organ för bedömning av överensstämmelse. I uppdraget har också ingått att föreslå vilken eller vilka befintliga myndigheter som ska utses till nationell marknadskontrollmyndighet. Vidare har ingått att lämna de förslag, inklusive författningsförslag, som är nödvändiga eller annars bedöms lämpliga för att komplettera EU:s cyberresiliensförordning, bland annat om bestämmelser i nationell rätt behöver upphävas eller ändras eller om nya bestämmelser behövs med anledning av förordningen (kommittédirektiven finns i sin helhet i bilaga 1).

EU:s cyberresiliensförordning

EU:s cyberresiliensförordning syftar till att skapa förutsättningar för utvecklingen av säkra produkter med digitala element genom att försäkra att hårdvaru- och programvaruprodukter som släpps ut på marknaden har färre sårbarheter och att tillverkarna tar säkerheten på allvar under produktens hela livscykel. Den syftar också till att skapa förutsättningar för att konsumenter ska få tillräcklig information om cybersäkerheten för de produkter med digitala element som de köper och använder.

EU:s cyberresiliensförordning gäller för produkter inom olika sektorer, inklusive konsumentelektronik, industriell automation och IT-säkerhetslösningar. Förordningen är tillämplig på produkter med digitala element som till exempel smartphones, datorer, IoT-enheter, nätverkskomponenter och programvara för säkerhet. Vissa kategorier av produkter definieras som viktiga eller kritiska, vilket innebär skärpta krav och i vissa fall att produkten blir föremål för tredjepartsbedömning eller certifiering. Viktiga produkter är till exempel lösenordshanterare, operativsystem, routrar, brandväggar samt smarta hemprodukter med säkerhetsfunktioner. Kritiska produkter är hårdvaruenheter med säkerhetsboxar, smarta mätarportar inom smarta mätarsystem och smartkort eller liknande enheter.

EU:s cyberresiliensförordning ställer krav på tillverkare av produkter med digitala element. Tillverkarna åläggs att genomföra riskbedömningar, implementera tekniska och organisatoriska säkerhetsåtgärder samt att dokumentera och redovisa hur de grundläggande cybersäkerhetskraven uppfylls. Tillverkare är skyldiga att rapportera alla aktivt utnyttjade sårbarheter i produkten med digitala element och alla allvarliga incidenter som påverkar säkerheten för produkten med digitala element som tillverkaren får kännedom om till den nationella CSIRT-enheten.

EU:s cyberresiliensförordning ställer också krav på tillverkarens representant, importörer, distributörer samt förvaltare av programvara med fri och öppen källkod.

EU:s cyberresiliensförordning innehåller även bestämmelser om bedömning av överensstämmelse, förfaranden för bedömning om överensstämmelse och anmälan av organ för bedömning av överensstämmelse samt marknadskontroll och verkställighet. Dessutom finns bestämmelser om stödåtgärder för företag och om förbättring av

kompetensen hos olika aktörer i en cyberresilient digital miljö. EU:s cyberresiliensförordning ställer även krav på samverkan mellan berörda aktörer, såväl ekonomiska aktörer som berörda myndigheter.

Tillämpningsområdet

EU:s cyberresiliensförordning är till alla delar bindande och direkt tillämplig i varje medlemsstat. Det innebär att förordningens bestämmelser ska tillämpas av enskilda, myndigheter och domstolar på samma sätt som nationella författningar.

Från förordningens tillämpningsområde finns undantag för produkter och sektorer som redan omfattas av sektorslagstiftning med krav på cybersäkerhet, till exempel vissa medicintekniska produkter, produkter som används inom civil luftfart och fordon.

Vidare undantas från förordningens tillämpningsområde produkter med digitala element som tillverkas uteslutande för nationell säkerhet och försvarsändamål eller specifikt för att hantera säkerhetsskyddsklassificerade uppgifter. Undantag medges även från skyldigheten att lämna information enligt förordningen när informationen berör väsentliga säkerhetsintressen i fråga om nationell säkerhet, allmän säkerhet och försvar.

Utredningens förslag

En ny kompletterande lag och en ny kompletterande förordning

De kompletterande nationella bestämmelser till EU:s cyberresiliensförordning som krävs ska samlas i en ny lag, lagen med kompletterande bestämmelser till EU:s cyberresiliensförordning, och i en ny förordning.

I lagen anges att regeringen får utse anmälande myndighet och marknadskontrollmyndighet. I lagen finns även bestämmelser om marknadskontrollmyndigheternas befogenheter och möjlighet att besluta om sanktioner, även mot myndigheter, för överträdelse av regelverket.

Vidare finns vissa processuella bestämmelser, bland annat införs en rätt att få ett beslut omprövat och att överklaga ett beslut av ett organ för bedömning av överensstämmelse. Rätten till överklagande

begränsas till att omfatta beslut som rör frågor som regleras i EU:s cyberresiliensförordning och anslutande föreskrifter. Ett sådant beslut får överklagas till allmän förvaltningsdomstol. Även ett beslut av anmälade myndighet och en marknadskontrollmyndighet får överklagas. Prövningstillstånd ska krävas vid överklagande av besluten till kammarrätten.

I lagen finns även bestämmelser om att regeringen eller den myndighet regeringen bemyndigar får meddela föreskrifter om anmälan och ackreditering av organ för bedömning av överensstämmelse, avgifter samt regulatoriska sandlådor.

I förordningen finns bland annat bestämmelser om anmälade myndighet, marknadskontrollmyndigheter och en upplysningsbestämmelse om vilken myndighet som är CSIRT-enhet.

Därutöver lämnas förslag om ändring i offentlighets- och sekretesslagen (2009:400) och stöd till företag.

Styrelsen för ackreditering och teknisk kontroll (Swedac) ska vara anmälade myndighet

I EU:s cyberresiliensförordning anges att medlemsstaten ska utse anmälade myndighet. I förordningen finns även bestämmelser om anmälade myndighet. Utredningen föreslår att Styrelsen för ackreditering och teknisk kontroll (Swedac) ska vara anmälade myndighet. Av lagen (2011:791) om ackreditering och teknisk kontroll följer att Swedac utövar tillsyn över anmälda organ för bedömning av överensstämmelse.

Utredningen föreslår även att Swedac ges i uppdrag att föreslå lämpliga åtgärder för att säkerställa att ett anmält organs ärenden i vissa fall kan behandlas av ett annat anmält organ.

Myndigheten för samhällsskydd och beredskap ska vara CSIRT-enhet

I EU:s cyberresiliensförordning finns bestämmelser om den CSIRT-enhet som utsetts till samordnare i respektive medlemsstat. Bland annat är CSIRT-enheten mottagare av sårbarhets- och incidentrapporter.

CSIRT-enheten utses enligt direktiv (EU) 2022/2555¹ (NIS 2-direktivet). NIS 2-direktivet har ännu inte genomförts i svensk rätt. Myndigheten för samhällsskydd och beredskap (MSB) är i dag CSIRT-enhet i Sverige och föreslås, när NIS 2-direktivet genomförs i svensk rätt, fortsatt vara CSIRT-enhet i Sverige.² MSB är således CSIRT-enhet även enligt EU:s cyberresiliensförordning.

Post- och telestyrelsen ska vara marknadskontrollmyndighet

I EU:s cyberresiliensförordning anges att medlemsstaten ska utse en eller flera marknadskontrollmyndigheter. Utredningen föreslår att Post- och telestyrelsen (PTS) ska utses som marknadskontrollmyndighet. Samtidigt regleras i artikel 52.14 i EU:s cyberresiliensförordning att för produkter med digitala element som klassificeras som AI-system med hög risk enligt artikel 6 i förordning (EU) 2024/1689³ (AI-förordningen) ska de marknadskontrollmyndigheter som utsetts enligt AI-förordningen vara de myndigheter som ansvarar för den marknadskontroll som föreskrivs i EU:s cyberresiliensförordning. I betänkande *Anpassningar till AI-förordningen* (SOU 2025:101) lämnas förslag på dessa myndigheter.

Utredningen föreslår vidare att PTS ges i uppdrag att undersöka hur en ordning som bidrar till att säkerställa att det finns en tillräcklig tillgång på organ för bedömning av överensstämmelse kan utformas senast den 11 december 2026.

Befogenheter och sanktioner

Utredningen föreslår kompletterande bestämmelser om befogenheter för marknadskontrollmyndigheterna enligt artikel 14.4 i EU:s marknadskontrollförordning. Dessa befogenheter inkluderar exempelvis

¹ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

² Det finns dock ett förslag att Försvarets radioanstalt ska överta uppgiften att vara CSIRT-enhet från och med den 1 juli 2026, se *Samlade förmågor för ökad cybersäkerhet* (SOU 2025:79).

³ Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

tillhandahållande av handlingar, specifikationer, data eller uppgifter, tillträde till lokaler, mark och transportmedel och möjligheten att införskaffa, inspektera och demontera varuprover.

I EU:s cyberresiliensförordning finns bestämmelser om sanktioner vid överträdelse av förordningens bestämmelser. I den kompletterande lagen finns bestämmelser om att anmälade myndighet respektive en marknadskontrollmyndighet får besluta om sanktioner. Utredningen föreslår även att den anmälade myndigheten och marknadskontrollmyndigheterna får besluta om sanktioner mot en myndighet.

Sekretess och tystnadsplikt

Utredningen föreslår en ny bestämmelse om sekretess till skydd för sårbarhets- och incidentrapporter samt en sekretessbrytande bestämmelse för att möjliggöra informationsdelning enligt vad som föreskrivs i EU:s cyberresiliensförordning. Utredningen föreslår även nya bestämmelser om sekretess till skydd för enskild vid marknadskontroll och utredning samt i verksamhet avseende regulatoriska sandlådor för cyberresiliens enligt EU:s cyberresiliensförordning.

Utredningen föreslår vidare en uppgiftsskyldighet för CSIRT-enheten att lämna vissa uppgifter till en marknadskontrollmyndighet.

Utredningen föreslår slutligen bestämmelser om tystnadsplikt för privata aktörer som deltar i verksamhet som utförs av ett privat organ för bedömning av överensstämmelse, tar befattning med ett ärende som gäller marknadskontroll eller deltar i en regulatorisk sandlåda för cyberresiliens.

Stöd till företag

För att EU:s cyberresiliensförordning inte ska hämma näringslivet och innovation föreslår utredningen stödåtgärder och stödfunktioner för att bistå företag.

Marknadskontrollmyndigheterna och CSIRT-enheten ska enligt EU:s cyberresiliensförordning tillhandahålla stöd till företag. Utredningen föreslår att PTS och MSB ges i uppdrag att redan före ikraftträdandet av EU:s cyberresiliensförordning tillhandahålla detta stöd till företag.

Utredningen föreslår också att MSB ska tillhandahålla och samordna stöd till små och medelstora företag enligt artikel 33.1 i EU:s cyberresiliensförordning och att myndigheten ges i uppdrag att redan före ikraftträdandet av EU:s cyberresiliensförordning tillhandahålla sådant stöd till företag.⁴

Utredningen föreslår vidare att marknadskontrollmyndigheterna får besluta om inrättande och drift av regulatoriska sandlådor för cyberresiliens enligt artikel 33.2 i EU:s cyberresiliensförordning.

Nationell säkerhet

Det finns inget behov av att i kompletterande författning medge undantag från befintliga eller föreslagna bestämmelser med hänsyn till nationell säkerhet eller skydd av andra väsentliga statliga funktioner. EU:s cyberresiliensförordning och nationella regelsystem uppfyller krav på ett högt skydd för den nationella säkerheten och produkter med digitala element.

Konsekvenser

Utredningens förslag syftar till att uppfylla kraven i EU:s cyberresiliensförordning. Förslagen bedöms vara förenliga med EU-rätten.

EU:s cyberresiliensförordning och utredningens förslag berör framför allt ekonomiska aktörer och förvaltare av programvara med fri och öppen källkod, Swedac, PTS och de marknadskontrollmyndigheter som utses enligt AI-förordningen samt MSB. Förslaget berör även anmälda organ, Tullverket, Polismyndigheten och Sveriges domstolar.

EU:s cyberresiliensförordning medför ekonomiska konsekvenser för ekonomiska aktörer samt förvaltare av programvara med fri och öppen källkod. Konsekvenserna är en direkt följd av EU-förordningen i sig och inte av utredningens förslag.

EU:s cyberresiliensförordning och utredningens förslag innebär utökade och delvis nya arbetsuppgifter som bedöms medföra eko-

⁴ Det finns dock förslag att Försvarets radioanstalt ska överta den verksamhet hos MSB som är aktuell för utredningens förslag från och med den 1 juli 2026, se betänkandet *Samlade förslag för ökad cybersäkerhet* (SOU 2025:79).

nomiska konsekvenser för PTS och MSB⁵. Utredningen bedömer att finansieringen bör ske genom ökade anslag.

Ekonomiska konsekvenser till följd av EU:s cyberresiliensförordning och utredningens förslag för övriga offentliga verksamhetsutövare bör enligt utredningen finansieras inom befintlig ram.

Utredningen föreslår att en utvärdering av företags behov av stöd samt berörda myndigheters och domstolarnas resursbehov och finansiering görs 2030 när regelverket som helhet finns på plats och myndigheternas verksamhet kopplad till EU:s cyberresiliensförordning har pågått en period.

Ikraftträdande- och övergångsbestämmelser

Kapitel IV (artiklarna 35–51) i EU:s cyberresiliensförordning om anmälan av organ för bedömning av överensstämmelse ska tillämpas från och med den 11 juni 2026. Vidare ska artikel 14 om rapportering av sårbarheter och allvarliga incidenter tillämpas från och med den 11 september 2026. Övriga bestämmelser i förordningen ska tillämpas från och med den 11 december 2027.

Vissa av utredningens författningsförslag föreslås därför träda i kraft den 11 juni och den 11 september 2026 och i övrigt den 11 december 2027. Det krävs inga övergångsbestämmelser.

⁵ Det finns dock ett förslag att Försvarets radioanstalt ska överta de aktuella uppgifterna från och med den 1 juli 2026, se *Samlade förmågor för ökad cybersäkerhet* (SOU 2025:79).

Summary

Remit

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), referred to hereinafter as the EU Cyber Resilience Act, will mainly apply as of 11 December 2027 (for the Act in its entirety, see Annex 2).

The Inquiry's remit has been to analyse the need for, and to propose, measures and supplementary statutory provisions for the aim of harmonising Swedish law with the EU Cyber Resilience Act, wherein said provisions need to be in place once the Act's various provisions have begun to apply.

The remit has included considering and proposing which existing government agency to designate as notifying authority with responsibility for establishing and implementing the procedures required for assessment, designation and notification of conformity assessment bodies. The remit has also included proposing which existing government agency or agencies to designate as national market surveillance authority or authorities. Moreover, the Inquiry has been tasked with presenting proposals, including statutory proposals, which are necessary or otherwise deemed suitable for supplementing the EU Cyber Resilience Act. This includes determining whether provisions in national law need to be repealed or amended, or if new provisions are needed because of the EU Cyber Resilience Act (for the committee terms of reference, see Annex 1).

EU Cyber Resilience Act

The EU Cyber Resilience Act aims to set the boundary conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufacturers take security seriously throughout a product's lifecycle. It also aims to create conditions for consumers to receive sufficient information about cybersecurity for the products with digital elements that they purchase and use.

The EU Cyber Resilience Act applies to products within various sectors, including consumer electronics, industrial automation and IT security solutions. The Act is applicable to products with digital elements such as smartphones, computers, IoT devices, network components and security software. Certain categories of products are defined as 'important' or 'critical', which entails stricter requirements and in certain cases that a product is subject to third-party conformity assessment or certification. Important products include password managers, operating systems, routers, firewalls and smart home products with security functionalities. Critical products are hardware devices with security boxes, smart meter gateways within smart metering systems and smartcards or similar devices.

The EU Cyber Resilience Act imposes requirements on manufacturers of products with digital elements. Manufacturers are required to carry out risk assessments, implement technical and organisational security measures and document and record how the fundamental cybersecurity requirements have been fulfilled. Manufacturers are obliged to report all actively exploited vulnerabilities in products with digital elements and all severe incidents affecting security for the products with digital elements that they become aware of to the national Computer Security Incident Response Team (CSIRT).

The EU Cyber Resilience Act also imposes requirements on a manufacturer's authorised representatives, importers, distributors and open-source software stewards.

Furthermore, the EU Cyber Resilience Act contains provisions on conformity assessment, procedures for conformity assessment and notification by conformity assessment bodies and market surveillance and enforcement authorities. It also contains provisions

on support measures for businesses and on enhancing skills in a cyber-resilient digital environment. Moreover, the Act imposes requirements on cooperation between relevant actors, which apply to economic actors and government agencies alike.

Scope of application

The EU Cyber Resilience Act in its entirety is binding and directly applicable in all Member States. This means the Act's provisions must be applied by individuals, government agencies and courts in same manner as national statutes.

There are exemptions from the EU Cyber Resilience Act's scope of application for products and sectors that are already covered by sectoral legislation with requirements on cybersecurity, such as certain medical devices and products used for civilian aviation and motor vehicles.

Products with digital elements that are manufactured exclusively for national security and defence purposes or specifically for handling classified information are also exempt from the EU Cyber Resilience Act's scope of application. Moreover, exemptions from the obligation to report information under the Act are granted if the information concerns essential security interests related to national security, public security and defence.

The Inquiry's proposals

A new supplementary act and a new supplementary ordinance

The required national provisions that supplement the EU Cyber Resilience Act should be contained in a new act – the Act on supplementary provisions to the EU Cyber Resilience Act – and in a new ordinance.

The new Act would state that the Government may designate a notifying authority and market surveillance authority. The new Act would also contain provisions on a market surveillance authority's powers and ability to impose administrative fines, including against government agencies, for infringements of the regulatory framework.

There are also certain procedural provisions, including a right to have a decision reviewed and to appeal a decision by a conformity assessment body. The right to appeal is limited to decisions concerning issues regulated under the EU Cyber Resilience Act and associated regulations. Such a decision may be appealed to an independent court or tribunal. A decision by a notifying authority or a market surveillance authority may also be appealed. Appeals of a decision to the administrative court of appeal would only be allowed if leave to appeal had been granted.

The new Act would also contain provisions whereby the Government or the government agency that the Government authorises may enact regulations on notification and accreditation by a conformity assessment body, fees and regulatory sandboxes.

The EU Cyber Resilience Act contains provisions on notifying authorities and market surveillance authorities and a provision specifying which government agency is the CSIRT.

In addition, proposals have been submitted on amending the Public Access to Information and Secrecy Act (2009:400) and support to businesses.

The Swedish Board for Accreditation and Conformity Assessment should be notifying authority

According to the EU Cyber Resilience Act, a Member State must designate a notifying authority. The Act also contains provisions on notifying authorities. The Inquiry proposes that the Swedish Board for Accreditation and Conformity Assessment be designated as notifying authority. Under the Accreditation and Technical Control Act (2011:791), the Swedish Board for Accreditation and Conformity Assessment carries out supervision of notified bodies for conformity assessment.

The Inquiry further proposes that the Swedish Board for Accreditation and Conformity Assessment be tasked with proposing suitable measures to ensure that a notified body's matters can be processed by another notified body.

The Swedish Civil Contingencies Agency should remain CSIRT

The EU Cyber Resilience Act contains provisions on the CSIRT that is designated as coordinator in the relevant Member State. The CSIRT's role includes receiving vulnerability and incident reports.

The CSIRT is appointed under Directive (EU) 2022/2555¹ (NIS 2 Directive). The NIS 2 Directive has not yet been implemented in Swedish law. The Swedish Civil Contingencies Agency is currently the CSIRT in Sweden, and the Inquiry proposes that it remain the CSIRT in Sweden once the NIS 2 Directive has been implemented in Swedish law.² Therefore, the Swedish Civil Contingencies Agency should also be the CSIRT under the EU Cyber Resilience Act.

The Swedish Post and Telecom Authority should be market surveillance authority

According to the EU Cyber Resilience Act, a Member State must designate a market surveillance authority. The Inquiry proposes that the Swedish Post and Telecom Authority be designated as market surveillance authority. At the same time, under Article 52(14) of the EU Cyber Resilience Act, for products with digital elements classified as high-risk AI systems pursuant to Article 6 of Regulation (EU) 2024/1689³ (AI Act), the market surveillance authorities designated for the purposes of the AI Act should be the authorities responsible for the market surveillance activities required under the EU Cyber Resilience Act. Proposals concerning those authorities have been presented in the report 'Amendments in the context of the AI Act' (SOU 2025:101).

The Inquiry further proposes that the Swedish Post and Telecom Authority be tasked with investigating and identifying how a system

¹ Directive (EU) 2022/2555 of the European Parliament and the Council of 14 December 2022 on measures for a high common level of cybersecurity throughout the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

² However, it has been proposed that the National Defence Radio Establishment should take over the CSIRT role as of 1 July 2026; see 'Coordinated capabilities for increased cybersecurity' (SOU 2025:79).

³ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

according to which conformity assessment bodies are ensured sufficient access can be designed by 11 December 2026.

Powers and administrative fines

The Inquiry proposes supplementary provisions on the powers of market surveillance authorities under Article 14(4) of the EU Market Surveillance Act. These powers include gaining access to documents, specifications, data or information, premises, grounds and means of transport, and the possibility of obtaining, inspecting and disassembling samples.

The EU Cyber Resilience Act contains provisions on administrative fines for violating the provisions of the same Act. The supplementary Act would contain provisions whereby notifying authorities and market surveillance authorities may impose administrative fines. The Inquiry also proposes that a notifying authority and market surveillance authorities be empowered to impose sanctions on a government agency.

Secrecy and confidentiality

The Inquiry proposes a new provision on secrecy to protect vulnerability and incident reports and a new provision that overrides secrecy to enable information sharing as provided for in the EU Cyber Resilience Act. The Inquiry also proposes new provisions on secrecy to protect individuals during market surveillance and investigations, and in activities related to regulatory sandboxes for cyber resilience under the EU Cyber Resilience Act.

In addition, the Inquiry proposes a reporting obligation whereby the CSIRT must provide certain information to a market surveillance authority.

Finally, the Inquiry proposes provisions imposing a duty of confidentiality on private actors that take part in activities carried out by a private conformity assessment body, deal with a matter concerning market surveillance or participate in a regulatory sandbox for cyber resilience.

Support to businesses

To ensure that the EU Cyber Resilience Act does not impede the business sector or innovation, the Inquiry proposes introducing support measures and functions to assist businesses.

Under the EU Cyber Resilience Act, market surveillance authorities and the CSIRT must provide support to businesses. The Inquiry proposes that, before the EU Cyber Resilience Act enters into force, the Swedish Post and Telecom Authority and the Swedish Civil Contingencies Agency be tasked with providing this support to businesses.

The Inquiry also proposes that the Swedish Civil Contingencies Agency be tasked with providing and coordinating support to micro-enterprises and small- and medium-sized enterprises, under Article 33(1) of the EU Cyber Resilience Act, and that it be tasked with providing such support to businesses before the EU Cyber Resilience Act enters into force.⁴

The Inquiry further proposes that market surveillance authorities be empowered to establish and operate regulatory sandboxes for cyber resilience, under Article 33(2) of the EU Cyber Resilience Act.

National security

There is no need for supplementary statutes to grant exemptions from existing or proposed provisions in consideration of national security or protection of other essential central government functions. The EU Cyber Resilience Act and national regulatory system fulfil the requirement of a high level of protection for national security and products with digital elements.

⁴ However, it has been proposed that the National Defence Radio Establishment take over the activities of the Swedish Civil Contingencies Agency that are relevant for the Inquiry's proposals as of 1 July 2026; see the report 'Coordinated capabilities for increased cyber-security' (SOU 2025:79).

Impact

The Inquiry's proposals aim to fulfil the requirements under the EU Cyber Resilience Act. The proposals are considered to be compatible with EU law.

The EU Cyber Resilience Act and the Inquiry's proposals primarily concern economic operators and open-source software stewards, the Swedish Board for Accreditation and Conformity Assessment, the Swedish Post and Telecom Authority, the market surveillance authorities that are designated under the AI Act and the Swedish Civil Contingencies Agency. The proposals also concern notified bodies, Swedish Customs, the Swedish Police Authority and the Courts of Sweden.

The EU Cyber Resilience Act will have a financial impact on economic operators and open-source software stewards. This impact stems directly from the EU Act, not from the Inquiry's proposals.

The EU Cyber Resilience Act and the Inquiry's proposals entail expanded and partially new tasks that are expected to have a financial impact on the Swedish Post and Telecom Authority and the Swedish Civil Contingencies Agency⁵. The Inquiry finds that funding should take place through increased appropriations.

The Inquiry finds that the financial impact arising from the EU Cyber Resilience Act and the Inquiry's proposals for other public operators should be funded within existing frameworks.

The Inquiry proposes that an evaluation of the business' need for support and of the need for resources and funding of relevant government agencies and the courts be carried out in 2030 when the regulatory framework is fully in place and the government agency activities related to the EU Cyber Resilience Act have been in progress for some time.

Entry into force and transitional provisions

Chapter IV (Articles 35–51) of the EU Cyber Resilience Act on notification by conformity assessment authorities will apply as of 11 June 2026. Moreover, Article 14 on reporting of vulnerabilities

⁵ However, it has been proposed that the National Defence Radio Establishment take over the relevant tasks as of 1 July 2026; see 'Coordinated capabilities for increased cybersecurity' (SOU 2025:79).

and severe incidents will apply as of 11 September 2026. The remaining provisions of the EU Cyber Resilience Act will apply as of 11 December 2027.

Therefore, the Inquiry proposes that some of its statutory proposals enter into force on 11 June and 11 September 2026, and the remaining proposals on 11 December 2027. No transitional provisions are required.

1 Författningsförslag

1.1 Förslag till lag med kompletterande bestämmelser till EU:s cyberresiliensförordning

Härigenom föreskrivs följande.

Inledande bestämmelser

1 § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen), i denna lag benämnd EU:s cyberresiliensförordning.

Ord och uttryck i denna lag har samma betydelse som i EU:s cyberresiliensförordning.

Anmälande myndighet av organ för bedömning av överensstämmelse

2 § Den myndighet som regeringen bestämmer är anmälande myndighet enligt EU:s cyberresiliensförordning.

3 § I Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och upphävande av förordning (EEG) nr 339/93 och i lagen (2011:791) om ackreditering och teknisk kontroll finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse.

Bestämmelser om ackreditering och anmälan av organ för bedömning av överensstämmelse finns i lagen (2011:791) om ackreditering

och teknisk kontroll och i föreskrifter som har meddelats i anslutning till den lagen.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om förfarandena vid bedömning, utseende och anmälan av organ för bedömning och för övervakning av dessa enligt artikel 39–43 samt anmälda organs informationsskyldighet enligt artikel 49 och deltagande i sektorsövergripande grupp enligt artikel 51 i EU:s cyberresiliensförordning.

Marknadskontroll

4 § Bestämmelser om marknadskontroll finns i Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011.

Marknadskontrollmyndighet

5 § Den myndighet eller de myndigheter som regeringen bestämmer är marknadskontrollmyndighet.

Av artikel 52.14 i EU:s cyberresiliensförordning framgår att för produkter med digitala element som omfattas av EU:s cyberresiliensförordning och som klassificeras som AI-system med hög risk enligt artikel 6 i Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) ska de marknadskontrollmyndigheter som utsetts enligt förordning (EU) 2024/1689 vara de myndigheter som ansvarar för den marknadskontroll som föreskrivs i EU:s cyberresiliensförordning.

Marknadskontrollmyndighetens befogenheter

6 § Vid marknadskontroll enligt förordning (EU) 2019/1020 har en marknadskontrollmyndighet befogenhet att enligt

1. artikel 14.4 a–14.4 c kräva att ekonomiska aktörer eller förvaltare av programvara med fri och öppen källkod ska tillhandahålla handlingar, specifikationer, data eller uppgifter,

2. artikel 14.4 d utföra oanmälda inspektioner på plats och fysiska kontroller av produkter,

3. artikel 14.4 e få tillträde till lokaler, mark eller transportmedel,

4. artikel 14.4 f inleda undersökningar på eget initiativ,

5. artikel 14.4 g kräva att ekonomiska aktörer eller förvaltare av programvara med fri och öppen källkod ska vidta lämpliga åtgärder för att få en bristande överensstämmelse att upphöra eller att eliminera en risk,

6. artikel 14.4 h själv vidta åtgärder,

7. artikel 14.4 j införskaffa, inspektera och demontera varuprover, och

8. artikel 14.4 k kräva att innehåll på ett onlinegränssnitt ska avlägsnas, att en varning ska visas eller att åtkomsten ska begränsas.

Befogenheten enligt första stycket 8 gäller inte i fråga om databaser som omfattas av tryckfrihetsförordningens eller yttrandefrihetsgrundlagens skydd.

När ändrade förhållanden ger anledning till det, ska en marknadskontrollmyndighet besluta att åtgärder enligt första stycket 8 inte längre behöver gälla.

7 § En marknadskontrollmyndighet får införskaffa ett varuprov under dold identitet enligt artikel 14.4 j i förordning (EU) 2019/1020 endast om det är nödvändigt för att syftet med kontrollen ska uppnås. Myndigheten ska underrätta den ekonomiska aktören eller förvaltaren av programvara med fri och öppen källkod om att införskaffandet har skett under dold identitet, så snart det går utan att syftet med åtgärden går förlorat.

Förelägganden och vite

8 § En marknadskontrollmyndighet får besluta de förelägganden som behövs i ett enskilt fall för att EU:s cyberresiliensförordning, denna lag, anslutande föreskrifter och förordning (EU) 2019/1020 ska följas.

Ett beslut om föreläggande enligt första stycket eller 6 § får förenas med vite.

Omedelbar verkställighet

9 § En marknadskontrollmyndighet får när den fattar beslut enligt 6 eller 8 §§ bestämma att beslutet ska gälla omedelbart.

Hjälp av Polismyndigheten

10 § Polismyndigheten ska på begäran av marknadskontrollmyndigheten lämna den hjälp som behövs när myndigheten vidtar åtgärder enligt 6 §.

Hjälp enligt första stycket får begäras endast om

1. det på grund av särskilda omständigheter kan befaras att åtgärden inte kan utföras utan att en polismans särskilda befogenheter enligt 10 § polislagen (1984:387) behöver tillgripas, eller
2. det annars finns synnerliga skäl.

Föreskrifter om regulatoriska sandlådor

11 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om regulatoriska sandlådor för cyberresiliens.

Tystnadsplikt

12 § Den som deltar i verksamhet som utförs av ett privat organ för bedömning av överensstämmelse enligt EU:s cyberresiliensförordning får inte obehörigen röja eller utnyttja det som han eller hon fått kännedom om under det att uppgifterna utfördes.

Den som har tagit befattning med ett ärende som gäller marknadskontroll eller deltar i en regulatorisk sandlåda för cyberresiliens enligt EU:s cyberresiliensförordning får inte obehörigen röja eller utnyttja vad han eller hon har fått veta om någons affärs- eller driftförhållanden.

I det allmännas verksamhet tillämpas bestämmelserna i offentlighets- och sekretesslagen (2009:400).

Avgifter

13 § Av lagen (2014:140) med bemyndigande att meddela vissa föreskrifter om marknadskontroll av varor och annan närliggande tillsyn framgår att föreskrifter för avgifter för kontroll enligt förordning (EU) 2019/1020 får meddelas.

Ändring av beslut av privata organ för bedömning av överensstämmelse

14 § Ett privat organ för bedömning av överensstämmelse ska ändra ett beslut som det har meddelat, om

1. organet anser att beslutet är uppenbart felaktigt i något väsentligt hänseende på grund av att det har tillkommit nya omständigheter eller av någon annan anledning, och

2. beslutet kan ändras snabbt och enkelt och utan att det blir till nackdel för någon enskild.

Sanktionsavgift

15 § En marknadskontrollmyndighet ska besluta att ta ut sanktionsavgift vid överträdelse av artikel 13 och 14 samt väsentliga cybersäkerhetskrav i bilaga I i EU:s cyberresiliensförordning och anslutande föreskrifter.

Avgiftens storlek ska bestämmas med tillämpning av artikel 64.5 i EU:s cyberresiliensförordning.

Sanktionsavgiften ska bestämmas till högst 15 000 000 euro eller, om överträdelsen begås av ett företag, till 2,5 procent av dess totala

globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

Sanktionsavgiften för en myndighet ska bestämmas till högst 10 000 000 kronor.

16 § En marknadskontrollmyndighet ska besluta att ta ut en sanktionsavgift vid överträdelse av artikel 18–23, 28, 30.1–30.4, 31.1–31.4, 32.1–32.3, 33.5 och 53 i EU:s cyberresiliensförordning och anslutande föreskrifter.

Avgiftens storlek ska bestämmas med tillämpning av artikel 64.5 i EU:s cyberresiliensförordning.

Sanktionsavgiften ska bestämmas till högst 10 000 000 euro eller, om överträdelsen begås av ett företag, upp till 2 procent av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

Sanktionsavgiften för en myndighet ska bestämmas till högst 5 000 000 kronor.

17 § Den anmälade myndigheten ska besluta att ta ut en sanktionsavgift vid överträdelse av artikel 39, 41, 47 och 49 i EU:s cyberresiliensförordning och anslutande föreskrifter.

Avgiftens storlek ska bestämmas med tillämpning av artikel 64.5 i EU:s cyberresiliensförordning.

Sanktionsavgiften ska bestämmas till högst 10 000 000 euro eller, om överträdelsen begås av ett företag, upp till 2 procent av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

Sanktionsavgiften för en myndighet ska bestämmas till högst 5 000 000 kronor.

18 § En marknadskontrollmyndighet ska besluta att ta ut en sanktionsavgift vid överträdelse av artikel 64.4 i EU:s cyberresiliensförordning och anslutande föreskrifter.

Avgiftens storlek ska bestämmas med tillämpning av artikel 64.5 i EU:s cyberresiliensförordning.

Sanktionsavgiften ska bestämmas till högst 5 000 000 euro eller, om överträdelsen begås av ett företag, upp till 1 procent av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

Sanktionsavgiften för en myndighet ska bestämmas till högst 2 500 000 kronor.

19 § Den anmälade myndigheten och en marknadskontrollmyndighet får avstå från att ta ut en sanktionsavgift när överträdelsen bedöms som ringa eller ursäktlig, eller om det annars med hänsyn till omständigheterna vore oskäligt att besluta om en sanktion.

20 § Sanktionsavgiften ska betalas till den anmälade myndigheten eller marknadskontrollmyndigheten inom 30 dagar från det att beslutet om att ta ut sanktionsavgift fick laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas i tid, ska den anmälade myndigheten och marknadskontrollmyndigheten lämna den obetalda avgiften för indrivning.

Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

En sanktionsavgift tillfaller staten.

21 § Innan den anmälade myndigheten och marknadskontrollmyndigheten beslutar om sanktionsavgift ska den som avgiften ska tas ut av få tillfälle att yttra sig. Om så inte har skett inom två år från det att överträdelsen ägde rum får någon sanktionsavgift inte beslutas.

Ett beslut om sanktionsavgift ska delges.

22 § En beslutad sanktionsavgift ska falla bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

23 § En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande vid vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

Överklagande

24 § Ett beslut av en förvaltningsmyndighet eller ett anmält organ enligt EU:s cyberresiliensförordning, denna lag och anslutande föreskrifter får överklagas till allmän förvaltningsdomstol.

En myndighet får överklaga en förvaltningsmyndighets eller ett anmält organs beslut.

Förvaltningsmyndigheten eller det anmälda organet ska vid överklagande vara motpart i domstolen.

Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Denna lag träder i kraft i fråga om 2 §, 3 §, 12 § första stycket och 24 § den 11 juni 2026 och i övrigt den 11 december 2027.

1.2 Förslag till förordning med kompletterande bestämmelser till EU:s cyberresiliensförordning

Härigenom föreskrivs följande.

1 § Denna förordning kompletterar Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen), i denna förordning benämnd EU:s cyberresiliensförordning, samt lagen med kompletterande bestämmelser till EU:s cyberresiliensförordning.

I denna förordning avses med *CSIRT-enhet*: Den CSIRT-enhet som utsetts till samordnare enligt definitionen i artikel 3.51 i EU:s cyberresiliensförordning. Ord och uttryck i denna förordning har i övrigt samma betydelse som i EU:s cyberresiliensförordning.

Anmälade myndighet

2 § Styrelsen för ackreditering och teknisk kontroll är anmälade myndighet enligt artikel 36 i EU:s cyberresiliensförordning.

CSIRT-enhet

3 § I [föreslagna] 27 § förordningen (2025:000) om cybersäkerhet¹ finns bestämmelser om vilken myndighet som är CSIRT-enhet.

Marknadskontrollmyndigheter

4 § Post- och telestyrelsen är marknadskontrollmyndighet.

5 § I [föreslagna] förordningen (2025:000) med kompletterande bestämmelser till EU:s förordning om artificiell intelligens² finns bestämmelser om vilka myndigheter som är marknadskontrollmyndigheter enligt Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelli-

¹ Se delbetänkandet *Nya regler om cybersäkerhet* (SOU 2024:18).

² Se betänkandet *Anpassningar till AI-förordningen* (SOU 2025:101).

gens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

Regulatoriska sandlådor

6 § En marknadskontrollmyndighet får besluta om inrättande och drift av regulatoriska sandlådor för cyberresiliens enligt artikel 33.2 i EU:s cyberresiliensförordning.

Uppgiftsskyldighet

7 § CSIRT-enheten ska lämna de uppgifter som behövs för att en marknadskontrollmyndighet ska kunna fullgöra sina uppgifter enligt EU:s cyberresiliensförordning och anslutande föreskrifter.

EU-försäkrans om överensstämmelse

8 § En EU-försäkrans om överensstämmelse eller en förenklad EU-försäkrans om överensstämmelse som avses i artikel 28 i EU:s cyberresiliensförordning ska vara skriven på svenska eller engelska.

Rätt att meddela föreskrifter

9 § Styrelsen för ackreditering och teknisk kontroll får meddela föreskrifter om förfarandena vid bedömning, utseende och anmälan av organ för bedömning och för övervakning av dessa enligt artikel 39–43 samt anmälda organs informationsskyldighet enligt artikel 49 och deltagande i sektorsövergripande grupp enligt artikel 51 i EU:s cyberresiliensförordning.

10 § En marknadskontrollmyndighet får meddela föreskrifter om avgifter för marknadskontroll enligt Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direk-

tiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011.

11 § En marknadskontrollmyndighet får meddela föreskrifter om regulatoriska sandlådor för cyberresiliens.

Denna förordning träder i kraft i fråga om 2 och 9 §§ den 11 juni 2026, i fråga om 1 § andra stycket och 3 § den 11 september 2026 samt i övrigt den 11 december 2027.

1.3 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400)

dels att 18 kap. 19 § ska ha följande lydelse,

dels att det ska införas tre nya paragrafer, 18 kap. 8 d, 18 kap. 8 e och 31 kap. 25 b §§, och nya rubriker närmast före 18 kap. 8 d, 18 kap. 8 e och 31 kap. 25 b §§ av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

18 kap.

*Sårbarhets- och
incidentrapporter enligt
förordning (EU) 2024/2847*

8 d §

Sekretess gäller för uppgift i en sårbarhets- eller incidentrapport enligt artikel 14 eller 15 i Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyber-resiliensförordningen) samt för uppgift om vilka åtgärder som har vidtagits till följd av cyberhotet, tillbudet, sårbarheten eller incidenten om det inte står klart att uppgiften kan röjas utan skada för tillverkaren av produkten med digitala element eller för förvaltaren av programvara med fri och öppen källkod i den mån denne deltar i utveck-

lingen av produkter med digitala element, för den som ingett rapporten, för användaren eller för den verksamhet där den aktuella produkten används eller för de åtgärder som tillverkaren eller förvaltare av programvara med fri och öppen källkod vidtagit motverkas.

För uppgift i en allmän handling gäller sekretessen i högst fyrtio år.

Sekretessbrytande bestämmelse

8 e §

Sekretess enligt 18 kap. 8 d § hindrar inte CSIRT-enheten att underrätta användarna av produkter med digitala element enligt vad som anges i artikel 14.8 i förordning (EU) 2024/2847 eller att informera allmänheten enligt vad som anges i artikel 17.2 i förordning (EU) 2024/2847.

Nuvarande lydelse

Föreslagen lydelse

18 kap.

19 §¹

Den tystnadsplikt som följer av 5–7, 8, 9 och 10 §§, 11 § första stycket, 12, 12 a och 13 §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 5–7, 8, 8 d, 9 och 10 §§, 11 § första stycket, 12, 12 a och 13 §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

¹ Senaste lydelse 2024:477.

Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol, undersökningsledare eller åklagare eller inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Den tystnadsplikt som följer av 17 § inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol eller åklagare.

Att den tystnadsplikt som följer av 1–3 §§ i vissa fall inskränker rätten att meddela och offentliggöra uppgifter utöver det som anges i andra stycket följer av 7 kap. 10 §, 12–18 §§, 20 § 3 och 22 § första stycket 1 och andra stycket tryckfrihetsförordningen samt 5 kap. 1 § och 4 § första stycket 1 och andra stycket yttrandefrihetsgrundlagen.

Nuvarande lydelse

Föreslagen lydelse

31 kap.

Regulatorisk sandlåda för cyberresiliens

25 b §

Sekretess gäller i verksamhet avseende regulatorisk sandlåda för cyberresiliens enligt artikel 33 i förordning (EU) 2024/2847 för uppgift om en enskilds affärs- eller driftförhållanden, uppfinningar eller forskningsresultat om det kan antas att den enskilde lider avsevärd skada om uppgiften röjs.

För uppgift i en allmän handling gäller sekretessen i högst tjugo år.

Denna lag träder i kraft i fråga om 31 kap. 25 b § den 11 december 2027 och i övrigt den 11 september 2026.

1.4 **Förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641)**

Häriigenom föreskrivs i fråga om offentlighets- och sekretessförordningen (2009:641)

 dels att 3 § ska ha följande lydelse,

 dels att bilagan till offentlighets- och sekretessförordningen (2009:641) ska ha följande lydelse.

3 §¹ Följande myndigheter ska i den utsträckning som framgår nedan inte tillämpa 5 kap. 2 § andra stycket offentlighets- och sekretesslagen (2009:400).

Myndighet	Register
<i>Den myndighet som är CSIRT-enhet enligt [föreslagna] 27 § förordningen (2025:000) om cybersäkerhet², en marknadskontrollmyndighet samt en myndighet som rapporterar sårbarheter eller incidenter enligt artikel 14 eller 15 i Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen).</i>	<i>Diarium över sårbarhets- och incidentrapporter enligt artikel 14 och 15 i Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen).</i>

¹ Senaste lydelse 2024:1184.

² Se delbetänkandet *Nya regler om cybersäkerhet* (SOU 2024:18).

Bilaga³

Verksamheten består i	Särskilda begränsningar i sekretessen
173. marknadskontroll och utredning enligt förordning (EU) 2024/2847 och anslutande föreskrifter.	sekretessen gäller inte beslut i ärenden sekretessen enligt 9 § första stycket 1 gäller inte om intresset av allmän kännedom om förhållande som rör människors hälsa och säkerhet, miljön eller redligheten i handeln eller ett liknande allmänintresse har sådan vikt att uppgiften bör lämnas ut

Denna förordning träder i kraft i fråga om 3 § den 11 september 2026 och i övrigt den 11 december 2027.

³ Senaste lydelsen 2023:637.

1.5 Förslag till förordning om ändring i förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap

Härigenom föreskrivs i fråga om förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap att det ska införas en ny paragraf, 18 m §, av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

18 m §

Myndigheten för samhällsskydd och beredskap ska tillhandahålla och samordna stöd till små och medelstora företag enligt artikel 33.1 i Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen).

Denna förordning träder i kraft den 11 december 2027.

2 Uppdraget

2.1 Inledning

I detta kapitel redogörs inledningsvis för bakgrunden till utredningsuppdraget (avsnitt 2.2). Därefter redogörs för utredningens direktiv och uppdraget (avsnitt 2.3), utgångspunkter för arbetet (avsnitt 2.4), definitioner (avsnitt 2.5), arbetets bedrivande (avsnitt 2.6) och betänkandets disposition (avsnitt 2.7).

2.2 Bakgrund

Sverige står som många andra länder inför en dynamisk och föränderlig hotbild och cyberhot där aktörer kontinuerligt utvecklar nya metoder och ny teknik. Sveriges cybersäkerhet påverkas av sårbarheter som kan ha olika ursprung och manifestera sig inom många områden. Dessa sårbarheter kan var för sig eller samlat utgöra strategiska sårbarheter och riskera att påverka samhällsviktig verksamhet och ytterst Sveriges säkerhet. Sårbarheter som är vanligt förekommande kan bland annat röra organisatoriska, tekniska, infrastrukturrella och mänskliga faktorer.

Sveriges cybersäkerhetspolitik påverkas av internationell reglering, styrande dokument, policyer och standarder. Det nationella cybersäkerhetsarbetet och reglering på området styrs därför delvis nationellt men också i ökande grad av den internationella kontexten.

Frågor som rör ökad cybersäkerhet är ett område som sträcker sig över flera politikområden och samhällssektorer. På lagstiftningsområdet styrs utvecklingen främst av EU-samarbetet där unionen har tagit flera initiativ till reglering och normgivning inom digitala frågor och cybersäkerhet (se kapitel 4). Samtidigt har Nato ett växande fokus på strategiska cybersäkerhets- och teknikfrågor, och inom organisationen bedrivs ett omfattande arbete med strategiska

tekniker och cyberförsvar. Den civil-militära kopplingen inom cybersäkerhetsfrågor understryker betydelsen av ett samordnat utvecklingsarbete inom cybersäkerhet och cyberförsvar.

För att åstadkomma ökad cybersäkerhet krävs därför ett tvärsektoriellt arbete utifrån en rad olika kompetenser, bland annat när det gäller ett systematiskt cybersäkerhetsarbete där skyddsåtgärder systematiskt prioriteras utifrån en bedömning av vilka risker som är mest sannolika och har störst potentiell påverkan. Ett systematiskt och riskbaserat cybersäkerhetsarbete hos samhällets alla organisationer utgör, tillsammans med säkerhetsskydd och cyberförsvar, Sveriges nationella motståndskraft på cybersäkerhetsområdet.

Förordning (EU) 2024/2847¹ (EU:s cyberresiliensförordning) syftar till att öka tillverkares och andra ekonomiska aktörers ansvar för cybersäkerhet och att produkter med digitala element placeras på inre marknaden med färre sårbarheter. I kapitel 3 finns en översiktlig redogörelse för EU:s cyberresiliensförordning.

EU:s cyberresiliensförordning som helhet ska tillämpas från och med den 11 december 2027. Artiklarna 35–51 (kapitel IV) som rör anmälan av organ för bedömning ska dock tillämpas från och med den 11 juni 2026 och artikel 14 som rör sårbarhets- och incidentrapportering ska tillämpas från och med den 11 september 2026.

2.3 Uppdraget

Regeringen beslutade om kommittédirektiven till utredningen den 28 november 2024 (bilaga 1). Utredningens uppdrag är att analysera behovet av och föreslå åtgärder och kompletterande författningsbestämmelser som behövs i syfte att anpassa svensk rätt till EU:s cyberresiliensförordning.

¹ Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen).

Utredningen ska bland annat:

- föreslå vilken befintlig myndighet som ska utses till anmälände myndighet med ansvar för att bland annat inrätta och genomföra de förfaranden som krävs för bedömning, utseende och anmälan av organ för bedömning av överensstämmelse,
- föreslå vilken befintlig myndighet eller vilka befintliga myndigheter som ska utses till marknadskontrollmyndighet,
- analysera om befintliga bestämmelser i nationell rätt behöver upphävas eller ändras eller om nya bestämmelser behövs med anledning av förordningen och
- lämna de förslag, inklusive författningsförslag, i övrigt som är nödvändiga eller annars bedöms lämpliga för att komplettera förordningen.

Direktiven finns i sin helhet i bilaga 1.

2.4 Utgångspunkter

I kommittédirektiven anges att utredaren vid utformningen av sina förslag noga ska beakta skyddet för grundläggande fri- och rättigheter, däribland yttrande- och informationsfriheten samt äganderätten, behovet av att upprätthålla ett högt skydd för den nationella säkerheten och för produkter som har utvecklats uteslutande för ändamål som rör nationell säkerhet eller försvarsändamål. Utredarens förslag ska även utformas utifrån kostnadseffektivitet och så att företagens och myndigheternas totala regelbörda och kostnader inte ökar mer än nödvändigt. Utredaren ska i detta sammanhang ta medborgarnytta, effektivitet och konkurrenskraft i beaktning.

Utöver i direktiven angivna utgångspunkter uppkommer även ett antal andra utgångspunkter som utredningen har att förhålla sig till i utredningsarbetet och som behandlas nedan.

EU-rättsliga utgångspunkter

EU:s cyberresiliensförordning är en del av EU:s bredare strategi för cybersäkerhet² och kompletterar flera andra centrala EU-lagar inom cyberområdet. Införandet av EU:s cyberresiliensförordning har beröringspunkter med frågor och verksamheter som behandlas i såväl andra EU-rättsliga regleringar som i nationella strategier och författningar på angränsande cyberområden, bland annat vad avser samverkan mellan berörda aktörer och rapportering av sårbarheter. Det finns därför behov av att belysa de andra EU-rättsliga regleringarna i de delar de har beröringspunkter med EU:s cyberresiliensförordning och berörda nationella regelsystem på cyberområdet (se kapitel 4).

Nationell strategi för cybersäkerhet

Regeringen framhåller i en ny nationell strategi för cybersäkerhet 2025–2029³ vikten av en hög nivå av cybersäkerhet och att samhällsviktig verksamhet kan upprätthållas även vid cybersäkerhetsincidenter.⁴ Den nationella strategin och den tillhörande handlingsplanen berör hela samhället och alla typer av organisationer, såväl deras ledningar som de funktioner som arbetar med cybersäkerhet.⁵ Strategins primära målgrupp är myndigheterna med särskilt ansvar för verksamhet som bedrivs inom ramen för Nationellt cybersäkerhetscenter (NCSC), och tillsynsmyndigheter inom den samlade cybersäkerhetsregleringen samt andra organisationer som ingår i beredskaps- och NIS 2-sektorerna.

Vad som anges i strategin har beröring med flera av de frågor som regleras i EU:s cyberresiliensförordning och som ingår i utredningsuppdraget, bland annat vad gäller uppgifter till och organisering av myndigheter, rapportering av sårbarheter och incidenter, stöd till organisationer, med mera. Vad som anges i strategin beaktas i de delar som det berör utredningsarbetet.

² The EU's Cybersecurity Strategy for the Digital Decade, 2020.

³ *En ny era av cybersäkerhet, Nationell strategi för cybersäkerhet 2025–2029*, skr. 2024/25:121 Regeringskansliet (Försvarsdepartementet) 2025.

⁴ Strategin ersätter den tidigare strategin *Nationell strategi för samhällets informations- och cybersäkerhet* (Skr. 2016/17:213).

⁵ I strategins bilaga 2 ges en nulägesbeskrivning av de centrala aktörer som har särskilda roller och ansvar att bedriva tillsyn, stötta och samordna arbetet med cybersäkerhet.

Nationell säkerhet

I EU:s cyberresiliensförordningen anges att regleringen inte påverkar medlemsstaternas befogenheter i fråga om verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på straffrättens område. Samtidigt kan konstateras att många av de produkter som omfattas av förordningens tillämpningsområde också kommer att användas i verksamheter som berör samhällsviktiga tjänster och i verksamhet som berör säkerhetskänslig verksamhet och det svenska totalförsvaret, såväl det civila som militära försvaret. En utgångspunkt i arbetet har därför varit, i enlighet med direktiven, att noga beakta behovet av att upprätthålla ett högt skydd för den nationella säkerheten och för produkter som har utvecklats uteslutande för ändamål som rör nationell säkerhet eller försvarsändamål. Dessa frågor behandlas vidare i kapitel 5.

2.5 Definitioner

EU:s cyberresiliensförordning, som är en unionsrättslig författning, är direkt tillämplig i medlemsstaterna och innehåller definitioner av olika begrepp, eller hänvisar till definitioner i andra rättsakter av de olika begrepp som förekommer i förordningen, bland annat cybersäkerhet. Eftersom EU:s cyberresiliensförordning är direkt tillämplig på nationell nivå bör förekommande begrepp ges samma innebörd och mening när de förekommer i den kompletterande nationella lagstiftningen. Dock kan vissa begrepp och bestämmelser som förekommer i förordningen och som berör effektiva rättsmedel, sanktioner och den nationella processordningen behöva anpassas till nationella förhållanden.

2.6 Utredningsarbetet

Utredningen började sitt arbete i december 2024. Utredningen har inledningsvis inhämtat underlag i form av offentliga utredningar, propositioner, faktapromemorior, nationella strategier, med mera. Arbetet har bedrivits på sedvanligt sätt med sex sammanträden med sakkunniga och experter. Sekretariatet har haft enskilda möten med olika experter i utredningen i syfte att inhämta fördjupad kunskap

inom vissa av de sakområden som behandlas i uppdraget. Utredningen har även haft möte med Marknadskontrollrådet och Implementeringsrådet.

Utredningen har därutöver haft möten med representanter för berörda myndigheter för att informera sig om förutsättningar för dessa myndigheter att kunna ansvara för en eller flera av de uppgifter och verksamheter som utredningen har i uppdrag att analysera och lämna förslag om, bland annat den myndighet som föreslås som marknadskontrollmyndighet, dvs. Post- och telestyrelsen. Utredningen har också träffat representanter för Trafikverket och järnvägsindustrins branschorganisation SWED'TRAIN.

Utredningen har hållit sig informerad om och beaktat relevant arbete som bedrivs inom Regeringskansliet, bland annat AI-utredningens arbete och vad gäller uppdraget åt en sakkunnig att analysera behovet av kompletterande bestämmelser till EU-förordningen om allmän produktsäkerhet. Utredningen har också hållit sig informerad om och beaktat arbetet i internationella forum med anledning av genomförandet av EU:s cyberresiliensförordning. Utredningen har hållit sig informerad om arbetet i Europeiska unionens cybersäkerhetsbyrå (Enisa) och högnivåforumet för europeisk standardisering.

Utredningen har löpande hållit företrädare för Finansdepartementet informerade om utredningsarbetet.

2.7 Betänkandets disposition

I detta kapitel presenteras bakgrund, uppdraget, utgångspunkter, definitioner, utredningsarbetets genomförande och betänkandets utformning. I kapitel 3 finns en övergripande beskrivning av EU:s cyberresiliensförordning och en redogörelse för behovet av kompletterande nationell lagstiftning. I kapitel 4 redogörs översiktligt för EU:s övergripande strategi på cyberområdet och för mer centrala EU-rättsliga författningar som syftar till ökad cybersäkerhet och där det finns en direkt koppling till EU:s cyberresiliensförordning. I kapitel 5 behandlas frågor som rör behovet av att upprätthålla ett högt skydd för den nationella säkerheten och för produkter som har utvecklats uteslutande för ändamål som rör nationell säkerhet eller försvarsändamål. I kapitel 6 behandlas bestämmelser i EU:s

cyberresiliensförordning som gäller för förfaranden för bedömning av överensstämmelse av produkter med digitala element, ackreditering och anmälan av organ för bedömning av överensstämmelse och anmälande myndighet. Vidare lämnas förslag som rör omprövning och överklagande av beslut av organ för bedömning överensstämmelse samt instansordning vid överklagande av sådana beslut och beslut av anmälande myndighet och marknadskontrollmyndighet. I kapitel 7 redogörs för standardiseringsarbetet som utförs till stöd för EU:s cyberresiliensförordning. I kapitel 8 behandlas sårbarhets- och incidentrapportering enligt EU:s cyberresiliensförordning. I kapitel 9 redogörs för marknadskontroll samt lämnas förslag på marknadskontrollmyndighet och på en marknadskontrollmyndighets befogenheter. I kapitel 10 redogörs för bestämmelser om sanktioner i EU:s cyberresiliensförordning och lämnas förslag på kompletterande bestämmelser om sanktioner. I kapitel 11 behandlas frågan om sekretess och informationsdelning samt lämnas förslag på kompletterande bestämmelser om sekretess. Vidare behandlas frågan om behandling av personuppgifter. I kapitel 12 redogörs för behov av och lämnas förslag på stödåtgärder till företag i syfte att förbereda dessa att efterleva kraven i EU:s cyberresiliensförordning. Vidare redogörs för behovet och regleringen av regulatoriska sandlådor. I kapitel 13 redogörs för bestämmelser i nationella författningar som berörs av EU:s cyberresiliensförordning och om de behöver upphävas, ändras eller om nya bestämmelser behövs med anledning av förordningen. I kap. 14 behandlas frågan om språk i EU-försäkran och om gemensam kontaktpunkt. Därefter behandlas och lämnas förslag på ikraftträdande- och övergångsbestämmelser för den kompletterande lagen och förordningen. I kapitel 15 finns en konsekvensutredning. I kapitel 16 finns författningskommentarer.

Det finns därutöver tre bilagor till betänkandet. I bilaga 1 finns kommittédirektiven. I bilaga 2 finns EU:s cyberresiliensförordning. I bilaga 3 finns konsultrapporten *Konsekvenser avseende krav i EU:s cyberresiliensförordning – Analys på uppdrag av Cyberresiliensutredningen* (Fi 2024:07).

3 EU:s cyberresiliensförordning

3.1 Inledning

Detta kapitel innehåller en övergripande beskrivning av förordning (EU) 2024/2847¹ (EU:s cyberresiliensförordning) och en redogörelse för behovet av kompletterande nationell lagstiftning.

3.2 Förordningens innehåll

3.2.1 Syfte och tillämpningsområde

EU:s cyberresiliensförordning syftar till att skapa förutsättningar för utveckling av säkra produkter med digitala element genom att försäkra att hård- och mjukvara släpps ut på marknaden med färre sårbarheter och att tillverkare tar större ansvar för produkters cybersäkerhet genom deras livscykel. Förordningen syftar även till att konsumenter ska få tillräcklig information om cybersäkerheten för de produkter med digitala element som de köper och använder.

EU:s cyberresiliensförordning är tillämplig på alla produkter med digitala element som tillhandahålls på marknaden och vars avsedda ändamål eller rimligen förutsebara användning omfattar en direkt eller indirekt logisk eller fysisk dataanslutning till en enhet eller ett nät. EU:s cyberresiliensförordning är bland annat tillämplig på smartphones, datorer, IoT-enheter, nätverkskomponenter och programvara för säkerhet. Förordningen gäller för produkter inom olika sektorer, inklusive konsumentelektronik, industriell automation och IT-säkerhetslösningar. Vissa produkter med digitala element faller utanför tillämpningsområdet för EU:s cyberresi-

¹ Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen).

liensförordning, eftersom de omfattas av andra unionsregler som uppställer cybersäkerhetskrav, till exempel medicinsk utrustning, motorfordon och flygsystem.

EU:s cyberresiliensförordning gäller således för alla produkter med digitala element. De risker olika produkter kan ha från ett cybersäkerhetsperspektiv varierar dock. Förordningen innehåller därför olika regler för olika kategorier av produkter, på ett sätt som reflekterar deras olika nivåer av säkerhetsrisk och samhällspåverkan. Förordningen kategoriserar vissa produkter med digitala element som viktiga produkter med digitala element, klasserna I eller II, eller kritiska produkter med digitala element. Viktiga produkter är bland annat lösenordshanterare, operativsystem, routrar, brandväggar samt smarta hemprodukter såsom smarta dörrlås, babyövervakningssystem och larmsystem. Kritiska produkter är hårdvaruenheter med säkerhetsboxar, smarta mätarportar inom smarta mätarsystem och smartkort eller liknande enheter.

Bestämmelserna i förordningen innebär i stora delar en anpassning till ett horisontellt ramverk för produktlagstiftning i EU, den så kallade nya lagstiftningsramen (New Legislative Framework, NLF).

3.2.2 Allmänna bestämmelser

I kapitel I i EU:s cyberresiliensförordning finns vissa allmänna bestämmelser. Till en början anges förordningens innehåll, tillämpningsområde och vissa definitioner (artiklarna 1–3). EU:s cyberresiliensförordning omfattar, med vissa undantag som anges i artikel 2, produkter med digitala element, dvs. programvaru- eller hårdvaruprodukter och dess lösningar för fjärrbehandling av data, inbegripet programvaru- eller hårdvarukomponenter som släpps ut på marknaden separat. Det finns en allmän bestämmelse om fri rörlighet (artikel 4) och en bestämmelse om upphandling eller användning av produkter med digitala element (artikel 5).

I kapitlet finns vidare de centrala bestämmelserna om att produkter med digitala element ska uppfylla de väsentliga cybersäkerhetskraven avseende egenskaper hos produkter med digitala element och krav på sårbarhetshantering (artikel 6). Vissa produkter med digitala element kategoriseras som tidigare nämnts som viktiga pro-

dukter med digitala element, klasserna I och II samt kritiska produkter med digitala element (artikel 7 och 8).

Kapitlet innehåller också bestämmelser om samråd med berörda parter när kommissionen utarbetar åtgärder för genomförandet av EU:s cyberresiliensförordning (artikel 9) och krav på olika parter att förbättra kompetensen i en cyberresilient digital miljö (artikel 10).

Det finns även bestämmelser som reglerar relationen till förordning (EU) 2023/988² när det gäller produkter med digitala element avseende risker eller riskkategorier som inte omfattas av EU:s cyberresiliensförordning (artikel 11) och relationen till förordning (EU) 2024/1689³ när det gäller produkter med digitala element som utgör AI-system med hög risk (artikel 12).

3.2.3 Ekonomiska aktörers skyldigheter och bestämmelser om programvara med fri och öppen källkod

I kapitel II finns bestämmelser om skyldigheter för de ekonomiska aktörerna, dvs. tillverkare, tillverkarens representant, importör och distributör, samt förvaltare av programvara med fri och öppen källkod (artiklarna 13, 14, 18, 19, 20 och 24). Bestämmelserna innehåller detaljerade regler bland annat om vilket ansvar respektive aktör har och vilka åtgärder som ska vidtas när det gäller riskbedömning, teknisk dokumentation, bedömning av överensstämmelse, EU-försäkran om överensstämmelse, märkning, olika typer av skadeförebyggande arbete och tillhandahållande av bruksanvisning och annan information som ska anges på eller följa med produkter med digitala element.

Tillverkaren är skyldig att rapportera alla aktivt utnyttjade sårbarheter i produkten med digitala element och alla allvarliga incidenter som påverkar säkerheten för produkten med digitala element (artikel 14). Det finns vidare bestämmelser om frivillig rapportering av eventuella sårbarheter i en produkt med digitala element och cyber-

² Europaparlamentets och rådets förordning (EU) 2023/988 av den 10 maj 2023 om allmän produktsäkerhet, ändring av Europaparlamentets och rådets förordning (EU) nr 1025/2012 och Europaparlamentets och rådets direktiv (EU) 2020/1828 och om upphävande av Europaparlamentets och rådets direktiv 2001/95/EG och rådets direktiv 87/357/EEG.

³ Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

hot som kan påverka riskprofilen för en produkt med digitala element som gäller för tillverkare och andra fysiska eller juridiska personer (artikel 15). För de anmälningar som avses i artikel 14 och 15 och för att förenkla tillverkarens rapporteringsskyldigheter ska Enisa inrätta en gemensam rapporteringsplattform (artikel 16). Andra bestämmelser avseende rapportering finns i artikel 17.

Kommissionen ges befogenheter att anta delegerade akter för att inrätta frivilliga program för säkerhetsintyg för programvara med fri och öppen källkod (artikel 25). För att underlätta genomförandet av EU:s cyberresiliensförordning och säkerställa ett konsekvent genomförande ska kommissionen dessutom utarbeta och tillhandahålla vägledning som ska vara till hjälp för de ekonomiska aktörerna (artikel 26).

3.2.4 Bedömning av överensstämmelse med väsentliga krav på cybersäkerhet

I kapitel III finns bestämmelser om bedömning av produkter med digitala elements överensstämmelse med de väsentliga cybersäkerhetskraven. Produkter med digitala element som överensstämmer med harmoniserade standarder, eller delar av sådana, vilka har offentliggjorts i Europeiska unionens officiella tidning, med gemensamma specifikationer eller en EU-försäkran om överensstämmelse eller ett certifikat som har utfärdats enligt förordning (EU) 2019/881⁴ ska i den utsträckning de överensstämmer med sådana förutsättas överensstämma med de väsentliga kraven i EU:s cyberresiliensförordning (artikel 27).

Kapitlet innehåller även detaljerade bestämmelser om förfaranden för bedömning av överensstämmelse. Det regleras vilka förfaranden som kan tillämpas för olika typer av produkter med digitala element, inklusive viktiga produkter med digitala element, klasserna I och II och kritiska produkter med digitala element (artikel 32).

Vidare finns bestämmelser om upprättande av EU-försäkran om överensstämmelse (artikel 28), om CE-märkning (artiklarna 29 och 30), om upprättande av teknisk dokumentation (artikel 31), om

⁴ Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

stödåtgärder för mikroföretag och små och medelstora företag, inbegripet uppstarts företag (artikel 33) samt om avtal om ömsesidigt erkännande med tredjeländer, för att främja och underlätta internationell handel (artikel 34).

3.2.5 Anmälan av organ för bedömning av överensstämmelse

I kapitel IV finns bestämmelser om anmälan av organ för bedömning av överensstämmelse (artiklarna 35–51). Det finns bland annat bestämmelser om skyldighet att anmäla vilka organ som utför bedömning av överensstämmelse, om de myndigheter som gör sådana anmälningar (artiklarna 36–38), om krav på de anmälda organen (artiklarna 39–41), om ansökan om anmälan och om anmälningsförfarandet (artiklarna 42 och 43), om identifikationsnummer och förteckning över anmälda organ (artikel 44), om ändringar i anmälan och ifrågasättande av de anmälda organens kompetens (artiklarna 45 och 46) och om de anmälda organens operativa skyldigheter (artiklarna 47–51).

Bestämmelserna i kapitlet överensstämmer i allt väsentligt med de referensbestämmelser på området som finns i beslut nr 768/2008/EG.⁵

3.2.6 Marknadskontroll, skyddsåtgärder och övrig tillsyn

I kapitel V finns bestämmelser om marknadskontroll och kontroll av produkter med digitala element på unionsmarknaden (artikel 52). I fråga om sådan kontroll ska förordning (EU) 2019/1020⁶ (EU:s marknadskontrollförordning) tillämpas. Varje medlemsstat ska utse en eller flera marknadskontrollmyndigheter för att säkerställa ett effektivt genomförande av EU:s cyberresiliensförordning. Det regleras även samarbete med de myndigheter som tar emot sårbarhets- och incidentrapporter, Enisa, de nationella myndigheter för cybersäkerhetscertifiering, de myndigheter som utövar tillsyn över unionens dataskyddsrätt och de myndigheter som är ansvariga för andra krav som rör en produkt med digitala element. Det finns

⁵ Europaparlamentets och rådets beslut nr 768/2008/EG av den 9 juli 2008 om en gemensam ram för saluföring av produkter och upphävande av rådets beslut 93/465/EEG.

⁶ Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011.

även en bestämmelse om marknadskontrollmyndigheternas tillgång till data och dokumentation (artikel 53).

Vidare finns det bestämmelser om förfaranden för att hantera produkter med digitala element som utgör en betydande cybersäkerhetsrisk på nationell nivå och om ett unionsförfarande i fråga om skyddsåtgärder (artiklarna 54–56). Det finns också ett förfarande för att hantera den situation att produkter med digitala element överensstämmer med kraven men utgör en betydande cybersäkerhetsrisk (artikel 57). Vidare finns regler om åtgärder avseende formell bristande överensstämmelse (artikel 58). Slutligen finns det bestämmelser om marknadskontrollmyndigheternas gemensamma aktiviteter och samordnade tillsynsåtgärder (artikel 59 och 60).

3.2.7 Delegerade befogenheter och kommittéförfarande

I kapitel VI regleras kommissionens befogenheter att anta delegerade akter och förfarandet för den kommitté som ska biträda kommissionen vid framtagande av genomförandeakter (artikel 61 och 62).

3.2.8 Konfidentialitet och sanktioner

I kapitel VII finns bestämmelser om konfidentialitet (artikel 63). Det regleras också skyldigheter för medlemsstaterna att fastställa sanktioner för överträdelser av bestämmelserna i EU:s cyberresiliensförordning och att vidta de åtgärder som krävs för att säkerställa att de tillämpas (artikel 64). I artikel 64 fastställs även sanktionsbelopp för olika typer av bristande efterlevnad av kraven i EU:s cyberresiliensförordning och vilka aspekter som ska beaktas vid beslut om sanktionsavgiftens storlek. Vidare finns en bestämmelse om grupp-talan om ekonomiska aktörers överträdelser av EU:s cyberresiliensförordning skadar konsumenternas kollektiva intressen.

3.2.9 Avslutande bestämmelser

I kapitel VIII regleras ändringar av tre unionsrättsakter (artiklarna 66–68), bland annat ändras bilaga I till EU:s marknadskontrollförordning. I kapitlet finns övergångsbestämmelser (artikel 69), regler

om rapportering, utvärdering och översyn (artikel 70) samt om ikraftträdande och tillämpning (artikel 71).

3.2.10 Rättelser och ändringar i EU:s cyberresiliensförordning

Genom rättelse⁷ och ändring⁸ av EU:s cyberresiliensförordning i dess ursprungliga lydelse har artikel 13.4⁹, artikel 31.3,¹⁰ artikel 32,¹¹ artikel 64¹² och artikel 67¹³ fått delvis ny lydelse.

⁷ Rättelse 2025/90555 och 2025/90828, se bilaga 2.

⁸ Europaparlamentets och rådets förordning (EU) 2025/327 av den 11 februari 2025 om det europeiska hälsodataområdet och om ändring av direktiv 2011/24/EU och förordning (EU) 2024/2847.

⁹ Artikel 13.4 ska ersättas med följande: ”4. När en produkt med digitala element släpps ut på marknaden ska tillverkaren inkludera den bedömning av cybersäkerhetsrisker som avses i punkt 3 i denna artikel i den tekniska dokumentation som krävs enligt artikel 31 och bilaga VII. För de produkter med digitala element som avses i artiklarna 12 och 32.5a och som också omfattas av andra unionsrättsakter får bedömningen av cybersäkerhetsriskerna ingå i den riskbedömning som krävs enligt dessa unionsrättsakter. I de fall då vissa väsentliga cybersäkerhetskrav inte är tillämpliga på produkten med digitala element ska tillverkaren inkludera en tydlig motivering till detta i den tekniska dokumentationen.”

¹⁰ Artikel 31.3 ska ersättas med följande: ”3. För de produkter med digitala element som avses i artiklarna 12 och 32.5a vilka även omfattas av andra unionsrättsakter som föreskriver teknisk dokumentation ska en enda serie teknisk dokumentation upprättas med den information som avses i bilaga VII och den information som föreskrivs i andra unionsrättsakter.”

¹¹ I artikel 32 ska följande punkt införas: ”5a. Tillverkare av produkter med digitala element som klassificeras som elektroniska hälsodokumentationssystem enligt Europaparlamentets och rådets förordning (EU) 2025/327 ska visa överensstämmelse med de väsentliga kraven i bilaga I till den här förordningen genom att använda det relevanta förfarande för bedömning av överensstämmelse som föreskrivs i kapitel III i förordning (EU) 2025/327.”

¹² Artikel 64.10, inledningsfrasen: I stället för: ”Genom undantag från punkterna 3–9 ska de administrativa sanktionsavgifter som avses i dessa punkter inte tillämpas på följande:” ska det stå: ”Genom undantag från punkterna 2–9 ska de administrativa sanktionsavgifter som avses i dessa punkter inte tillämpas på följande:”

¹³ Artikel 67: I stället för: ”69. Europaparlamentets och rådets förordning (EU) 2024/2847.” ska det stå: ”72. Europaparlamentets och rådets förordning (EU) 2024/2847.”

3.3 Behov av kompletterande bestämmelser

3.3.1 En ny lag och en ny förordning

Utredningens förslag: Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen), i denna lag benämnd EU:s cyberresiliensförordning.

Utredningens bedömning: Denna förordning kompletterar Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen), i denna förordning benämnd EU:s cyberresiliensförordning, samt lagen med kompletterande bestämmelser till EU:s cyberresiliensförordning.

EU-förordningar är i alla delar bindande och direkt tillämpliga i varje medlemsstat. De ska tillämpas av domstolar och myndigheter i medlemsstaterna som direkt gällande rätt och de kan åberopas av enskilda. En EU-förordning får inte inkorporeras eller transformeras till nationell rätt och medlemsstaterna får inte utfärda bestämmelser i sådana frågor som regleras i förordningen. Det är dock vanligt att EU-förordningar innehåller bestämmelser som medför en skyldighet att införa regler av verkställande karaktär. Exempelvis kan det behövas nationella regler som anger myndigheter som ansvarar för tillsyn och marknadskontroll.

Medlemsstaterna är vidare skyldiga att se till att det finns bestämmelser som gör att en EU-förordning kan tillämpas i praktiken och få effektivt genomslag. EU:s cyberresiliensförordning behöver kompletteras med sådana regler. De kompletterande nationella bestämmelser till EU:s cyberresiliensförordning som krävs ska samlas i en ny kompletterande lag, lagen med kompletterande bestämmelser till EU:s cyberresiliensförordning, och i en ny kompletterande förordning.

3.3.2 Hänvisningar till EU:s cyberresiliensförordning

Hänvisningar till unionsrättsakter i svensk författning kan göras antingen statiska eller dynamiska. En statisk hänvisning avser unionsrättsakten i en viss angiven lydelse. En följd av denna hänvisningsteknik är att den nationella författningen normalt behöver ändras varje gång unionsrättsakten ändras. En dynamisk hänvisning innebär att hänvisningen avser unionsrättsakten i den vid varje tidpunkt gällande lydelse.

Den föreslagna lagen med kompletterande bestämmelser innehåller bestämmelser om sanktionsavgifter. Bestämmelserna om beslut om sanktionsavgift bör innehålla en statisk hänvisning till EU:s cyberresiliensförordning, dvs. avse förordningen i den ursprungliga lydelsen, med hänsyn till behovet av förutsebarhet i fråga om när en sanktionsavgift kan bli följden av överträdelser.

Övriga bestämmelser i den föreslagna lagen med kompletterande bestämmelser till EU:s cyberresiliensförordning har däremot en sådan karaktär att eventuella ändringar bör få omedelbart genomslag i regleringen. Dessa bestämmelser bör därför innehålla dynamiska hänvisningar till EU:s cyberresiliensförordning.

4 EU:s cyberreglering

4.1 Inledning

Förordning (EU) 2024/2847¹ (EU:s cyberresiliensförordning) är en del av EU:s bredare strategi och åtgärder för ökad cybersäkerhet och kompletterar flera andra centrala EU-författningar inom detta område. Förordningen utgör även en del i det EU-rättsliga regelverket som syftar till att stärka produktsäkerheten generellt på den inre marknaden.

I detta kapitel redogörs inledningsvis översiktligt för EU:s övergripande strategi på cyberområdet (avsnitt 4.2) och därefter för de mer centrala EU-rättsliga författningar som syftar till ökad cybersäkerhet och där det finns en direkt koppling till EU:s cyberresiliensförordning (avsnitt 4.3). I avsnitt 4.4 behandlas bestämmelser om cybersäkerhet i förordning (EU) 2023/988² (förordning om produktsäkerhet) i de delar som berör EU:s cyberresiliensförordning. I avsnitt 4.5 behandlas EU:s arbete med regelförenkling med koppling till EU:s cyberresiliensförordning.

4.2 EU:s strategi för ökad cybersäkerhet

EU:s senaste strategi för ökad cybersäkerhet³ är formulerad för att hantera den alltmer komplexa hotbild som följer av digitaliseringen. Strategin betonar att EU ska bygga upp en gemensam motstånds-

¹ Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen).

² Europaparlamentets och rådets förordning (EU) 2023/988 av den 10 maj 2023 om allmän produktsäkerhet, ändring av Europaparlamentets och rådets förordning (EU) nr 1025/2012 och Europaparlamentets och rådets direktiv (EU) 2020/1828 och om upphävande av Europaparlamentets och rådets direktiv 2001/95/EG och rådets direktiv 87/357/EEG.

³ The EU's Cybersecurity Strategy for the Digital Decade, 2020.

kraft mot cyberattacker och säkerställa att medborgare och företag kan använda tillförlitliga digitala tjänster. Strategin framhåller särskilt att samhällsviktiga funktioner måste skyddas mot en ny och komplex hotbild.

Strategins huvudmål är:

- att stärka cyberresiliens och teknologiskt självbestämmande,
- öka operativ förmåga att förebygga och hantera attacker, samt
- fördjupa internationellt samarbete.

I strategin framhålls genomförandet av direktiv (EU) 2022/2555⁴ (NIS 2-direktivet) och direktiv (EU) 2022/2557⁵ (CER-direktivet) som viktiga delar att uppnå ökad cybersäkerhet och motståndskraft i samhällsviktiga verksamheter. NIS 2-direktivet omfattar fler sektorer och verksamheter av samhällskritisk betydelse, med skärpta säkerhetskrav, rapporteringsskyldigheter och harmoniserade sanktioner i syfte att förbättra informationsdelning och krisberedskap över gränserna.

Strategin innehåller också initiativ för att förebygga och hantera cyberangrepp operativt, till exempel behovet av att bygga ett nätverk av säkerhetsoperationscenter (SOC) med AI-baserade verktyg, som ska fungera som en gemensam cybersköld genom tidig upptäckt av attacker. För att samordna insatser mellan EU-institutioner och medlemsstater föreslås en ny gemensam cybersäkerhetsenhet (Joint Cyber Unit) som omfattar både civila myndigheter, rättsväsende och militära cyberförband. Vidare betonar strategin behovet av att säkra kompetensförsörjning och innovation inom cybersäkerhet, bland annat genom stöd till små och medelstora företag samt utbildningssatsningar och forskning på området. På EU-nivå föreslås också stärkta samarbetsstrukturer.

Strategin erkänner också den avgörande roll som privata aktörer har och uppmuntrar myndigheter och företag att dela information om hot och samverka kring säkerhetsåtgärder, samtidigt som särskilt små företag bör få stöd för att höja sin egen säkerhetsnivå.

⁴ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

⁵ Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

Slutligen understryker strategin EU:s globala roll. EU ska arbeta med partners som FN och NATO samt likasinnade länder för att driva på rättsbaserade normer och samarbete samt bekämpa gränsöverskridande cyberbrott.

För att strategins åtgärder ska kunna genomföras mobiliserar EU betydande resurser genom program som ett Digitalt Europa⁶, Horisont Europa⁷ och återhämtningsfonden⁸. Detta stöder medlemsstaternas satsningar och syftar till att stärka EU:s gemensamma skyddsnivå mot cyberhot och teknologiska självbestämmande.

4.3 EU:s regelsystem på cyberområdet

Utredningens bedömning: EU har antagit flera centrala regelsystem som syftar till ökad cybersäkerhet i unionen. Flera av regelverken föreskriver skyldigheter för berörda aktörer att genomföra åtgärder för att minimera cyberhot, sårbarheter och risker i produkter, tjänster och verksamheter. Det finns beröringspunkter mellan EU:s cyberresiliensförordning och flera av regelverken. Flera av regelsystemen är fortsatt under utveckling. Utredningens analys och förslag får utgå från vad som är känt om respektive regelsystem under utredningsarbetet. Denna osäkerhet innebär också att det kan behövas kompletterande åtgärder i det fortsatta nationella lagstiftningsarbetet.

EU:s cyberresiliensförordning är en viktig del i unionens åtgärder att öka cybersäkerheten. Förordningen har en horisontell ansats och gäller alla produkter med digitala element som är uppkopplade (direkt eller indirekt) mot en annan enhet eller ett nätverk.

Samtidigt kan noteras att EU har antagit flera andra centrala regelsystem som syftar till ökad cybersäkerhet i unionen. Även om regelsystemen har delvis olika utgångspunkter och syften så utgör

⁶ Programmet för ett digitalt Europa (DIGITAL) är ett EU-program för att driva den digitala omställningen. Programmet finansierar projekt inom bland annat AI, cybersäkerhet och superdatorer.

⁷ Horisont Europa är EU:s forsknings- och innovationsprogram och som stöder bland annat grundforskning och innovation.

⁸ Återhämtningsfonden (Next Generation EU) är en temporär återhämtningsfond efter covid-19-pandemin som syftar till att bland annat bygga ett mer digitalt och motståndskraftigt EU. Återhämtningsfonden är en bredare finansieringsmekanism som bidrar till många EU-initiativ, inklusive ovan angivna program.

respektive regelsystem en del av de samlade åtgärderna för att öka cybersäkerheten i unionen. Flera av regelsystemen föreskriver bland annat skyldighet för berörda aktörer att genomföra riskhanteringsåtgärder för att minimera hot, sårbarheter och risker i själva produkten, tjänsten eller verksamheten. Berörda aktörer har även skyldighet att rapportera olika former av hot, sårbarheter och angrepp i produkter, tjänster och verksamheter.

I detta avsnitt redogörs översiktligt för de mer centrala EU-rättsliga regelsystem som berör eller har koppling till regelverket i EU:s cyberresiliensförordning och där regelverken ska samverka och tillämpas parallellt när förutsättningar för detta föreligger.

4.3.1 Förordning (EU) 2019/881 (EU:s cybersäkerhetsakt)

Förordning (EU) 2019/881⁹ (EU:s cybersäkerhetsakt) antogs den 17 juni 2019. Den innehåller bestämmelser som dels definierar och reglerar Europeiska unionens cybersäkerhetsbyrås (Enisa) roll och uppgifter, dels upprättar ett europeiskt certifieringsramverk för cybersäkerhet IKT-produkter, -tjänster och -processer. Förordningen fördelar också ansvar mellan EU-nivån (kommissionen och Enisa), nationella myndigheter i medlemsländerna, samt expert- och intressentgrupper vid framtagande av certifieringsordningar och tillsyn. I förordningen framhålls att en harmonisering av regler för certifiering inom hela EU bidrar till att öka cybersäkerheten och förtroendet för IKT-produkter, -tjänster och -processer samt undviker att tillverkare behöver uppfylla olika, ibland motstridiga, nationella certifieringskrav.

EU:s cybersäkerhetsakt möjliggör att certifieringar även kan användas för att påvisa efterlevnad av andra EU-rättsliga regelverk med krav på cybersäkerhet, till exempel EU:s cyberresiliensförordning, NIS 2-direktivet (avsnitt 4.3.2) förordning (EU) 2024/1689¹⁰ (AI-

⁹ Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

¹⁰ Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

förordningen) (avsnitt 4.3.3) och förordning (EU) 2024/1183¹¹ (eIDAS-förordningen) (avsnitt 4.3.4), med mera.

Certifiering på säkerhetsnivåer (assurans)

EU:s cybersäkerhetsakt anger att certifiering av en IKT-produkt, -tjänst eller -process kan ske på tre säkerhetsnivåer (assuransnivåer), dvs. på grundläggande, betydande eller hög nivå.¹² Dessa nivåer motsvarar den bedömda risken och motståndskraften hos den certifierade produkten eller tjänsten. En certifiering enligt någon av angivna nivåer utgår från gemensamma säkerhetsmål som anges i artikel 51 i EU:s cybersäkerhetsakt. Säkerhetsnivån (assuransnivån) avgör hur noggrant produkten granskas för sårbarheter innan certifikat utfärdas. Resultatet blir att ju högre säkerhetsnivå (assuransnivå), desto mindre sannolikt är det att certifierade produkter har okända sårbarheter och om sårbarheter uppdagas senare ska de hanteras och åtgärdas genom föreskrivna rapporteringsmekanismer. Som utgångspunkt är certifiering enligt certifieringsramverket frivillig.

Krav att rapportera sårbarheter

Certifikatsinnehavaren, dvs. normalt tillverkaren av produkten eller leverantören av tjänsten, ska enligt artikel 56.8 i EU:s cybersäkerhetsakt informera certifieringsorganet eller, i vissa fall, den berörda myndigheten, om alla sårbarheter eller oegentligheter som upptäcks i efterhand och som kan påverka den certifierade IKT-produktens eller -tjänstens överensstämmelse med kraven för certifieringen. Det innebär att om en ny sårbarhet upptäcks i en certifierad IKT-produkt, ska tillverkaren utan onödigt dröjsmål meddela det certifieringsorgan som utfärdade certifikatet. Certifieringsorganet ska i vissa fall även vidarebefordra informationen till den nationella myndigheten för cybersäkerhetscertifiering. Denna ordning bidrar till att säkerställa att sårbarheter åtgärdas och ger möjlighet till att

¹¹ Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet.

¹² Se skäl 82.

eventuellt uppdatera eller återkalla certifikat om säkerhetskraven inte längre uppfylls.

Enligt artikel 55 i EU:s cybersäkerhetsakt ska tillverkaren av certifierade IKT-produkter även tillhandahålla vägledning och rekommendationer för säker konfiguration, installation, drift och underhåll av IKT-produkten. Även uppgift om hur länge säkerhetsuppdateringar och stöd kommer att erbjudas ska lämnas, dvs. cybersäkerhetsrelaterade uppdateringar. När det gäller sårbarhetsrapportering ska kontaktuppgifter och angivna metoder för att ta emot sårbarhetsinformation från slutanvändare och säkerhetsforskare finnas. Detta innebär att tillverkaren ska ha en kontaktpunkt hos certifieringsorganet för rapportering av sårbarheter. Vidare ska det finnas hänvisning till online-förteckningar över kända sårbarheter som gäller produkten samt relevanta säkerhetsråd. Det kan till exempel vara en referens till en databas som EU:s databas för sårbarheter som är under införande eller en CVE¹³-databas där publika sårbarheter för produkten listas. Denna information ska finnas elektroniskt tillgänglig och uppdateras vid behov under hela certifikatets giltighetstid. Syftet är att användare ska kunna hålla produkten säker och informeras om kända sårbarheter eller uppdateringar.

Enisa har en central roll i att stödja certifieringsramverket och har bland annat offentliggjort riktlinjer för sårbarhetshantering och rapportering inom ramen för certifieringsordningar. I januari 2025 publicerade Enisa *EUCC Scheme – Guidelines on Vulnerability Management and Disclosure* som vägleder certifikatinnehavare i hur de ska etablera processer för att ta emot, analysera och åtgärda sårbarhetsrapporter på ett standardiserat sätt.¹⁴ Enisa fungerar även som ett nav för att sprida information om sårbarheter och byrån utvecklar och underhåller en europeisk sårbarhetsdatabas.

¹³ Common Vulnerabilities and Exposures.

¹⁴ Enisa riktlinjer bygger på internationella standarder, bland annat ISO/IEC 30111:2019 (processer för hantering av sårbarheter) och ISO/IEC 29147:2018 (sårbarhetsrapportering). Tillverkare uppmanas även införa rutiner för "koordinated vulnerability disclosure" (CVD) – det vill säga att samarbeta med forskare och CERT/CSIRT-enheter för ansvarsfullt offentliggörande först efter att en uppdatering ("patch") finns tillgänglig.

Krav på säkerhet i komponenter från tredje part

Moderna IKT-produkter bygger ofta på tredjepartskomponenter, till exempel öppna programbibliotek som integreras i den egna produkten. I skäl 11 i EU:s cybersäkerhetsakt konstateras att detta medför risker i leverantörskedjan eftersom sårbarheter i komponenter från tredje part riskerar att påverka säkerheten i den slutliga produkten. Enligt artikel 51 d ska man som ett av säkerhetsmålen identifiera och dokumentera kända beroenden för IKT-produkten. Kraven vid certifiering av en IKT-produkt på nivå betydande och hög innebär att den inte innehåller kända sårbarheter eller innefattar sårbarheter i de inbäddade komponenterna från tredje part. Därför ställs krav på att certifierade produkter undersöks avseende beroenden och leverantörer på ett sätt som minimerar riskerna. Genom dokumentation av komponenter och versioner kan både utvärderare och slutanvändare bättre förstå potentiella sårbarheter kopplade till dessa beroenden samt användare och kunder vidta åtgärder för riskhantering, till exempel tillämpa uppdateringar när en sårbarhet i en viss komponent blir känd.

Vidare ställs krav på leverantörskedjans säkerhet. I EU:s cybersäkerhetsakt anges i första hand tekniska krav på cybersäkerhet i produkten. Samtidigt ska tillverkaren utöva kontroll över sina leverantörer och underleverantörers produkter för att uppfylla certifieringskraven. I artikel 51 ställs som mål att kunna återställa systemets säkerhet och funktion efter incidenter, vilket förutsätter att leverantören har en beredskap att hantera även brister som härrör från tredjepartsdelar. För certifierade produkter på nivå hög blir hanteringen av säkerheten i leverantörskedjan särskilt viktig. Certifieringsorganet kan här behöva granska utvecklingsprocessen och hur tillverkaren arbetar med leverantörsrisker. Under certifikatets giltighet måste förändringar i komponenter hanteras kontrollerat. Om en sårbarhet upptäcks i en tredjepartskomponent efter certifiering gäller samma rapporteringskrav som nämnts tidigare, dvs. sårbarheten ska meddelas till certifieringsorganet och åtgärdas. I vissa fall kan certifikatet återkallas om inte sårbarheten i komponenten kan åtgärdas och den allvarligt underminerar produktens cybersäkerhet.

Enisa har tagit fram riktlinjer för leverantörskedjans cybersäkerhet. Dessa riktlinjer kan stödja tillverkare som till exempel ansöker om ett certifikat enligt EU:s cybersäkerhetsakt.¹⁵

Samverkan och tillsyn

För att genomföra certifieringsramverket har EU:s cybersäkerhetsakt etablerat en styr- och tillsynsstruktur med tydlig rollfördelning. Kommissionen får begära att en certifieringsordning tas fram, efter samråd med medlemsstater och experter. Enisa utarbetar därefter förslag på certifieringsordning utifrån kommissionens begäran. Enisa leder även tekniska arbetsgrupper med experter från näringslivet och samverkar med nationella myndigheter i arbetet med att ta fram en certifieringsordning. Kommissionen ansvarar slutligen för att anta europeiska certifieringsordningar som formella genomförandeakter. Enisa tillhandahåller en offentlig portal där man kan finna information om gällande certifieringsordningar och utfärdade certifikat.

Vidare ska varje medlemsstat utse en eller flera nationella myndigheter för cybersäkerhetscertifiering (nationella cybersäkerhetscertifieringsmyndigheter, NCCA). Dessa myndigheter, i Sverige är Försvarets materielverk (FMV) en sådan myndighet, samverkar med andra myndigheter och utövar tillsyn inom sitt territorium. De nationella myndigheterna ska också samverka med andra berörda aktörer inom EU.

Den europeiska gruppen för cybersäkerhetscertifiering (ECCG) utgörs av representanter för medlemsstaternas nationella myndighet för cybersäkerhetscertifiering (NCCA). ECCG har i uppgift att bland annat bistå och ge råd till kommissionen för att säkerställa enhetlig tillämpning av EU:s cybersäkerhetsakt och ge synpunkter på utkast till certifieringsordningar. ECCG samarbetar även med Enisa i framtagandet av certifieringsordningar och utbyter information om nya cybercertifieringsbehov och bästa praxis mellan länderna.

Intressentgruppen för cybersäkerhetscertifiering (SCCG) är en grupp med experter från industrin, standardiseringsorgan, akademi, med flera. Syftet är att involvera privata sektorns perspektiv i arbetet med att bland annat ta fram certifieringsordningar. SCCG bi-

¹⁵ Enisa rapport: *Good practices for supply chain cybersecurity*, June, 2003.

drar med rekommendationer och expertis under arbetet med att ta fram och uppdatera certifieringsordningar. Tillsammans utgör dessa aktörer en flernivåstyrning där Enisa fungerar som navet som håller samman processen.

EU:s cybersäkerhetsakt kompletterar och samverkar med övriga centrala unionsrättsliga regelverk som bland annat utgörs av EU:s cyberresiliensförordning och NIS 2-direktivet. Kommissionen har i uppgift att övervaka att regelverken utvecklas koordinerat och ges en ändamålsenlig och kostnadseffektiv tillämpning för ökad cybersäkerhet i medlemsstaterna och unionen.

Genomförandeförordning (EU) 2024/482 (EUCC)

Kommissionen beslutade den 31 januari 2024 att anta den första europeiska certifieringsordningen enligt EU:s cybersäkerhetsakt, den Common Criteria-baserade europeiska ordningen för cybersäkerhetscertifiering (EUCC).¹⁶ EUCC började tillämpas fullt ut 2025. EUCC syftar till att stärka cybersäkerheten inom informations- och kommunikationsteknik genom gemensamma krav och metoder för certifiering av IKT-produkter. Certifiering kan ske på assurancesnivåerna betydande och hög, där den högre nivån kräver att det certifierande organet, utöver ackreditering, även har bemyndigande från den nationella myndigheten för cybersäkerhetscertifiering. Swedac ansvarar för att ackreditera de organ som ansöker om att få verka inom EUCC-systemet i Sverige (se kapitel 6). Ackreditering sker bland annat enligt relevanta internationella standarder, exempelvis ISO/IEC 17065¹⁷ och ISO/IEC 17025¹⁸, beroende på certifieringsorganets verksamhet.

¹⁶ Kommissionens genomförandeförordning (EU) 2024/482 av den 31 januari 2024 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller antagande av den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC).

¹⁷ SS-EN ISO/IEC 17065:2012 – Bedömning av överensstämmelse – Krav på organ som certifierar produkter, processer och tjänster (ISO/IEC 17065:2012).

¹⁸ SS-EN ISO/IEC 17025:2018 – Allmänna kompetenskrav för provnings- och kalibreringslaboratorier (ISO/IEC 17025:2017).

Förordning (EU) 2025/37 om utlokaliserade säkerhetstjänster.

Förordning (EU) 2025/37¹⁹, som trädde i kraft den 15 januari 2025, utsträcker tillämpningsområdet för EU:s cybersäkerhetsakt även till certifiering av så kallade hanterade/utlokaliserade säkerhetstjänster. Förordningen syftar till att säkerställa unionens motståndskraft mot cyberattacker och för att förebygga sårbarheter på den inre marknaden. Förordningen är avsedd att komplettera det övergripande regelverket med övergripande cybersäkerhetskrav för produkter med digitala element i EU:s cyberresiliensförordning, och föreskriver säkerhetsmålsättningar för utlokaliserade säkerhetstjänster, samt tillämpning och tillförlitlighet av de tjänsterna.

Definitionen av utlokaliserade säkerhetstjänster i förordningen överensstämmer med den för utlokaliserade säkerhetstjänster i artikel 6.40 i NIS 2-direktivet. De tjänsterna består i att utföra, eller tillhandahålla stöd för, verksamhet som rör deras kunders hantering av cybersäkerhetsrisker, och har blivit allt viktigare när det gäller att förhindra och mildra incidenter. Leverantörerna av dessa tjänster betraktas därför vara väsentliga eller viktiga entiteter som tillhör en högkritisk sektor enligt NIS 2-direktivet. Såsom anges i skäl 86 i det direktivet har leverantörer av utlokaliserade säkerhetstjänster på områden som incidenthantering, penetrationstester, säkerhetsrevisioner och konsulttjänster en särskilt viktig roll när det gäller att bistå entiteter i deras arbete med att förebygga, upptäcka, reagera på eller återhämta sig från incidenter. Leverantörer av utlokaliserade säkerhetstjänster har dock också själva varit mål för cyberattacker och utgör en särskild risk, eftersom de är nära integrerade i sina kunders verksamhet. Det anses därför viktigt att väsentliga och viktiga entiteter i den mening som avses i NIS 2-direktivet visar större noggrannhet vid valet av leverantörer av utlokaliserade säkerhetstjänster.

Förordningen ger en juridisk grund för att EU ska kunna utveckla och anta certifieringsordningar för leverantörer av angivna säkerhetstjänster. Detta innebär att exempelvis företag som erbjuder incidenthantering eller penetrationstestning ges möjlighet certifiera sina tjänster enligt en europeisk certifieringsordning. Arbetet med

¹⁹ Europaparlamentets och rådets förordning (EU) 2025/37 av den 19 december 2024 om ändring av förordning (EU) 2019/881 vad gäller utlokaliserade säkerhetstjänster.

att utveckla ett sådan certifieringsordning har påbörjats av Enisa under 2025.

Sammanfattning

EU:s cyberresiliensförordning knyter an till det europeiska ramverket för cybersäkerhetscertifiering på flera punkter. På ett mer övergripande plan kan noteras att cyberresiliensförordningen integrerar certifieringsramverket enligt EU:s cybersäkerhetsakt i systemet för bedömning av överensstämmelse. Harmoniserade standarder, gemensamma specifikationer och erkända certifikat är tre parallella sätt för tillverkaren att visa att man uppfyller kraven på cybersäkerhet i en produkt. En av de tydligaste kopplingarna mellan EU:s cybersäkerhetsakt och EU:s cyberresiliensförordning är reglerna för hur certifiering enligt cybersäkerhetsakten kan användas inom cyberresiliensförordningens tillämpningsområde. Syftet med kopplingen mellan cyberresiliensförordningen och cybersäkerhetsakten är bland annat att undvika dubbelreglering och dubbla kontroller samt att utnyttja befintliga (frivilliga) verktyg för att underlätta efterlevnad av de nya obligatoriska kraven i cyberresiliensförordningen. Kopplingen mellan regelverken har också en utvecklingsdimension. Om nya hot och cybersäkerhetsrisker uppkommer kan EU genom cybersäkerhetsakten ta fram nya certifieringsordningar, som kan tillämpas för certifiering för till exempel vissa kritiska produkter under cyberresiliensförordningen.

Kommissionen har även under 2025 inlett ett offentligt samråd för att samla in synpunkter inför en bredare utvärdering och översyn av EU:s cybersäkerhetsakt. Översynen kan medföra ytterligare ändringar eller justeringar av cybersäkerhetsakten, grundat på erfarenheterna från de första åren med det nya ramverket.

4.3.2 Direktiv (EU) 2022/2555 (NIS 2-direktivet)

Direktiv (EU) 2022/2555 (NIS 2-direktivet) antogs den 14 december 2022, och ska vara implementerat i medlemsstaterna senast den 17 oktober 2024. I NIS 2-direktivet uppmanas medlemsstaterna att fastställa nationella strategier för ökad cybersäkerhet och samarbeta med EU för gränsöverskridande insatser och verkställighet. Genom

NIS 2-direktivet inrättas en enhetlig rättslig ram för att upprätthålla cybersäkerheten i 18 kritiska sektorer i hela EU. Direktivet kräver att medlemsstaterna förbättrar sin cybersäkerhetskapacitet samtidigt som de inför riskhanteringsåtgärder och rapporteringskrav för verksamhetsutövare inom fler sektorer och fastställer bland annat regler för incidentrapportering, informationsutbyte, samarbete och tillsyn. Både väsentliga och viktiga verksamhetsutövare som tillhandahåller samhällskritiska tjänster ingår, även mindre aktörer kan omfattas om de är särskilt kritiska. Alla verksamhetsutövare som avses i bilaga 1 eller 2 i NIS 2-direktivet och som inte är väsentliga ska betraktas som viktiga verksamhetsutövare.

Vissa sektorer, bland annat finanssektorn som omfattas av förordning (EU) 2022/2554²⁰ undantas från NIS 2-direktivet.

Krav på riskhanteringsåtgärder (artikel 21)

NIS 2-direktivet innefattar krav på skärpta åtgärder för högre cybersäkerhet och krav på styrning och rapportering av incidenter samt myndighetstillsyn. Alla berörda verksamheter åläggs att införa riskbaserade åtgärder för ökad cybersäkerhet och rapporteringsskyldigheter för att skydda nätverk och informationssystem. I artikel 21 i NIS 2-direktivet anges bland annat att medlemsstaterna ska säkerställa att väsentliga och viktiga verksamheter (entiteter) vidtar lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster för att förhindra eller minimera incidenters påverkan på mottagarna av deras tjänster och på andra tjänster. NIS 2-direktivet kräver att verksamheter har en plan för att hantera säkerhetsincidenter, till exempel hantering och uppföljning av kända sårbarheter och på incidenter som drabbar driften av samhällsviktiga tjänster.

²⁰ Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1).

Rapportering av incidenter

Under NIS 2-direktivet ska berörd verksamhet utan onödigt dröjsmål rapportera varje incident som har en betydande påverkan på tillhandahållandet av den berörda tjänsten. En betydande incident definieras som en händelse som orsakar eller riskerar orsaka allvarlig driftsstörning eller stora ekonomiska förluster för verksamheten, eller som påverkar många människor med betydande skada. Sådana incidenter kan utgöras av till exempel angrepp och dataintrång som slår ut nätverks- och informationssystem eller som medför driftbortfall av kritiska plattformar. Av artikel 23 framgår rapporteringskraven som sker i olika steg. Rapportmottagare nationellt är antingen den nationella CSIRT-enheten eller den behöriga myndigheten. Myndigheterna har en skyldighet att bekräfta, återkoppla och inom 24 timmar från tidig varning ge en initial respons med eventuella råd om åtgärder. Om incidenten kan röra andra medlemsstater ska myndigheten dela information utan dröjsmål med berörda CSIRT-enheter och med Enisa. Den drabbade verksamhetsutövaren är skyldig att rapportera och hantera incidenten internt, medan CSIRT-enheten ansvarar för att samordna och stödja, till exempel ge teknisk hjälp om verksamheten begär det, informera allmänheten om det är nödvändigt för att förhindra vidare skada, samt eventuellt uppmärksamma brottsbekämpande myndigheter vid misstanke om brott.

Myndigheternas roll i detta sammanhang är att koordinera och eventuellt vidta ytterligare åtgärder. Enisa kan bland annat delge varningar om ett akut hot och sårbarheter till alla medlemsstater, en nationell CSIRT-enhet kan stödja tillverkaren med teknisk rådgivning och informera nationella tillsynsmyndigheter.

Krav på tredjepartsbedömning

Frågan om eventuella krav på tredjepartsbedömning för att ytterligare öka cybersäkerheten behandlas i artikel 24 i NIS 2-direktivet. I artikel 24.1 anges att för att visa att vissa krav enligt artikel 21 är uppfyllda får medlemsstaterna ålägga väsentliga och viktiga verksamhetsutövare (entiteter) att använda särskilda IKT-produkter, IKT-tjänster och IKT-processer, som har utvecklats av den väsentliga eller viktiga verksamhetsutövaren (entiteten) eller upphandlats

från tredje parter, och som är certifierade enligt en europeisk ordning för cybersäkerhetscertifiering som antagits i enlighet med artikel 49 i EU:s cybersäkerhetsakt.

Vidare anges i artikel 24.2 att kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 38 för att komplettera NIS 2-direktivet genom att ange vilka kategorier av väsentliga eller viktiga verksamhetsutövare (entiteter) som ska vara skyldiga att använda vissa certifierade IKT-produkter, IKT-tjänster och IKT-processer eller erhålla ett certifikat enligt en europeisk ordning för cybersäkerhetscertifiering som har antagits enligt artikel 49 i EU:s cybersäkerhetsakt. Dessa delegerade akter ska antas om det har fastställts att cybersäkerhetsnivån är otillräcklig och ska omfatta en genomförandeperiod. NIS 2-direktivet ställer således inte några formella krav på att produkter med digitala element som omfattas av EU:s cyberresiliensförordning ska ha blivit föremål för tredjepartsgranskning eller vara certifierade enligt EU:s cybersäkerhetsakt. Befogenheten att ställa sådana krav har överlämnats till medlemsstaterna respektive kommissionen när förutsättningar och behov av att ställa sådana krav föreligger.

Krav på säkerhet i leveranskedjan

NIS 2-direktivet uppmanar verksamhetsutövaren att införa policys för säker utveckling och anskaffning av bland annat IKT-produkter. Krav på cybersäkerhet ska vägas in vid inköp, upphandling av system och tjänster. Exempelvis kan en verksamhetsutövare ställa krav på att en leverantör av en programvara följer vissa standarder. Vidare kan leverantörens leveransförmåga och säkerhet behöva följas upp över tid. Som anges ovan ska väsentliga och viktiga verksamheter (entiteter) integrera leverantörsrisker i sin riskhantering. Artikel 21.2 d i NIS 2-direktivet anger att säkerhetsåtgärderna ska omfatta leverantörskedjans säkerhet, inklusive säkerhetsaspekter i relationerna med varje direkt leverantör eller tjänsteleverantör.

Organisering av tillsyn

Enligt NIS 2-direktivet ska varje medlemsland utse en eller flera behöriga tillsynsmyndigheter med uppdrag att övervaka efterlevnaden av direktivet. Dessa myndigheter har rätt att göra inspektioner, begära information och utfärda sanktioner. De ska också stödja verksamhetsutövare genom vägledning och bästa praxis. För väsentliga verksamhetsutövare, dvs. större aktörer inom kritiska sektorer, föreskrivs både proaktiv och reaktiv tillsyn genom till exempel regelbundna säkerhetsrevisioner och andra kontroller. Viktiga verksamhetsutövare, dvs. mindre kritiska, övervakas i första hand reaktivt vid indikation på brister. Tillsynsmyndigheterna har befogenhet att kräva information och genomföra inspektioner, samt utfärda bindande förelägganden om åtgärder vid bristande säkerhet. Vid allvarlig underlåtenhet kan kännbara sanktioner utgå.²¹ Även andra påföljder kan bli aktuella, till exempel temporär avstängning av ledande personer eller av verksamheten vid grova överträdelser.

Samverkan mellan berörda aktörer

NIS 2-direktivet ställer även krav på ökat samarbetet mellan medlemsstaterna. Varje land ska utse en kontaktpunkt för att koordinera gränsöverskridande incidenter, och information om incidenter med påverkan i flera länder ska delas med andra stater och Enisa utan dröjsmål. Det finns också mekanismer för ömsesidig hjälp och utbyte av varningar. Enisa och det befintliga CSIRT-nätverket får en viktig roll i att höja den kollektiva beredskapen inom EU. På EU-nivå samordnas olika åtgärder och verksamheter enligt NIS 2-direktivets via tre huvudsakliga mekanismer (se nedan).

European Union Agency for Cybersecurity (Enisa)

Under NIS 2-direktivet fungerar Enisa som sekretariat och stöd för NIS 2-samarbetsgrupp. Enisa utvecklar riktlinjer, utbildningsmaterial och främjar informationsutbyte. Enisa spelar även en nyckelroll i CSIRT-nätverket och hjälper till att sammanställa lägesbilder över

²¹ NIS 2-direktivet ställer krav på effektiva och avskräckande sanktionsavgifter på upp till 10 miljoner euro eller 2 procent global omsättning (vilket som är högst) för väsentliga enheter, respektive upp till 7 miljoner euro eller 1,4 procent för viktiga enheter.

cyberhot i Europa. Enisa är även sammankallande för CSIRT-nätverket och bidrar med verktyg och expertis för incidenthantering mellan medlemsstaterna.

Under EU:s cyberresiliensförordning får Enisa även en ny roll att ta emot och analysera inkommande rapporter om sårbarheter och incidenter från tillverkare av produkter med digitala element. Enisa kommer även att ansvara för och driva den tekniska infrastrukturen (gemensam rapportplattform) och upprätthålla en sårbarhetsdatabas. Enisa kan härigenom agera som tidig varningscentral på EU-nivå, dvs. om Enisa noterar flera rapporter om angrepp mot eller sårbarheter i produkter, kan de delge varningar eller rekommendationer. Enisa ska även stödja kommissionen i standardiseringsarbete genom att identifiera var det behövs standarder och samarbeta med standardiseringsorgan. Vidare deltar Enisa sedan tidigare i arbetet att utveckla europeiska certifieringsordningar och även anpassa befintliga eller föreslå nya certifieringsordningar för att stödja kraven i EU:s cyberresiliensförordning.

NIS 2 – samarbetsgrupp

NIS 2 – samarbetsgrupp är en grupp med representanter från EU-kommissionen, Enisa och medlemsstaterna. Gruppen träffas regelbundet för att diskutera genomförandet av NIS 2-direktivet, ta fram rekommendationer, identifiera gemensamma utmaningar och vid behov utarbeta samordnade riskbedömningar för bland annat leverantörskedjor. Samarbetet syftar till att öka likformigheten i tillsynen och främja informationsdelning mellan medlemsstaterna.

Computer Security Incident Response Team (CSIRT-nätverket)

Computer Security Incident Response Teams (CSIRT)-nätverket är ett nätverk som sammankopplar nationella CSIRT-enheter. Dessa är tekniska expertenheter som utbyter teknisk information om cyberincidenter och hanterar gränsöverskridande incidentkoordinering. Under NIS 2-direktivet ska CSIRT-nätverket, med Enisa som koordinator, till exempel stödja vid större incidenter som drabbar flera länder samt dela varningar i realtid.

Genomförandeförordning (EU) 2024/2690

Genomförandeförordning (EU) 2024/2690²² antogs den 17 oktober 2024. I förordningen fastställs bland annat de tekniska och metodologiska kraven för de åtgärder som avses i NIS 2-direktivet med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för innehållsleverans, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster, leverantörer av onlinemarknadsplatser, sökmotorer och plattformar för sociala nätverkstjänster samt leverantörer av betrodda tjänster (de relevanta enheterna).

Regeringens proposition (2025/26:28) Ett starkt skydd för nätverks- och informationssystem

Regeringen beslutade den 9 oktober 2025 om proposition (2025/26:28) *Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag* i syfte att genomföra NIS 2-direktivet i svensk rätt. I propositionen föreslår regeringen att det ska införas en ny cybersäkerhetslag. Den nya lagen innebär att offentliga och enskilda verksamhetsutövare inom vissa utpekade sektorer bland annat ska vidta åtgärder för att skydda sina nätverks- och informationssystem samt rapportera betydande incidenter. Den nya lagen innehåller också regler om tillsyn och ingripandemöjligheter mot verksamhetsutövare som inte följer lagens bestämmelser. Därutöver föreslås ändringar i andra lagar som rör elektronisk kommunikation, toppdomäner och sekretess. Den nya lagen och övriga lagändringar föreslås träda i kraft den 15 januari 2026.

²² Kommissionens genomförandeförordning (EU) 2024/2690 av den 17 oktober 2024 om fastställande av regler för tillämpningen av direktiv (EU) 2022/2555 vad gäller tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet och närmare angivelse av i vilka fall en incident ska anses vara betydande med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade drifttjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster.

Direktiv (EU) 2018/1972 (kodexen)

Genom direktiv (EU) 2018/1972²³ (kodexen) inrättades ett harmoniserat ramverk för elektroniska kommunikationsnät, elektroniska kommunikationstjänster, tillhörande faciliteter, tillhörande tjänster och vissa aspekter av terminalutrustning.

Direktivet är genomfört i lagen (2022:482) om elektronisk kommunikation, se vidare avsnitt 13.5. Direktivet innehåller bland annat bestämmelser om säkerhetsåtgärder och incidentrapportering (artikel 40 och 41).

Det finns beröringspunkter mellan EU:s cyberresiliensförordning och kodexen. Båda regelverken innehåller bestämmelser om cybersäkerhet och incidentrapportering. Kodexen gäller dock för tillhandahållare av elektroniska kommunikationsnät och -tjänster. Till skillnad från EU:s cyberresiliensförordning gäller således bestämmelserna i kodexen inte tillverkare men vid tillhandahållandet av elektroniska kommunikationsnät och -tjänster kan produkter med digitala element som omfattas av EU:s cyberresiliensförordning användas.

NIS 2-direktivet upphäver bestämmelserna om säkerhetsåtgärder och incidentrapportering i kodexen och ersätter dem med bestämmelserna som följer av NIS 2-direktivet genom att artikel 43 i NIS 2-direktivet föreskriver att artikel 40 och 41 i kodexen ska utgå med verkan från och med den 18 oktober 2024. Som ovan angetts är NIS 2-direktivet emellertid ännu inte genomfört i svensk rätt. Regeringen beslutade den 9 oktober 2025 om en proposition i syfte att genomföra direktivet i svensk rätt genom en ny cybersäkerhetslag som föreslås träda i kraft den 15 januari 2026. Bestämmelserna i LEK som genomför artikel 40 och 41 i kodexen gäller därför till dess att den nya cybersäkerhetslagen träder i kraft.

²³ Europaparlamentets och rådets direktiv (EU) 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation.

4.3.3 Förordning (EU) 2024/1689 (AI-förordningen)

Förordning (EU) 2024/1689²⁴ (AI-förordningen) antogs den 13 juni 2024. AI-förordningen är det första regelverket för artificiell intelligens inom EU. Syftet med förordningen är att främja användningen av människocentrerad och tillförlitlig artificiell intelligens (AI) och förbättra den inre marknadens funktion. Samtidigt ska en hög skyddsnivå säkerställas för bland annat hälsa, säkerhet och grundläggande rättigheter som fastställs i stadgan mot skadliga effekter av AI-system i unionen (artikel 1). I förordningen fastställs bland annat särskilda krav för AI-system med hög risk och skyldigheter för operatörer av sådana system (artikel 1). För produkter med digitala element och som innehåller vad som betraktas som ett AI-system med hög risk ställs även krav på att produkten och AI-systemet möter ställda krav på cybersäkerhet.

Ett AI-system kategoriseras efter vilken risk det kan innebära, och kraven ökar med risknivån. För varje nivå ställer förordningen olika krav och begränsningar. Nedan ges en översikt över AI-förordningens bestämmelser i de delar som berör utredningens uppdrag, bland annat vad gäller krav på cybersäkerhet i AI-system med hög risk.

Förbjudna AI-områden

I artikel 5 i AI-förordningen anges AI-områden (AI-system) som är förbjudna, bland annat förbjuds utsläppande på marknaden, ibruktagande eller användning av ett AI-system som omfattas av förbudet i bestämmelsen.

²⁴ Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens). Förordningen (EU) 2024/1689 benämns i denna lag AI-förordningen.

AI-system med hög risk och krav på cybersäkerhet

I artikel 6 i AI-förordningen finns klassificeringsregler för AI-system med hög risk. Med ett sådant system avses:

- a) AI-systemet är avsett att användas som en säkerhetskomponent i en produkt, eller AI-systemet är i sig en produkt, som omfattas av unionens harmoniseringslagstiftning som förtecknas i bilaga I.
- b) Den produkt vars säkerhetskomponent enligt led a är AI-systemet, eller själva AI-systemet som en produkt, omfattas av krav på att genomgå en tredjepartsbedömning av överensstämmelse för att produkten ska kunna släppas ut på marknaden eller tas i bruk enligt unionens harmoniseringslagstiftning som förtecknas i bilaga I.

Utöver de AI-system med hög risk som avses i punkt 1 ska också AI-system som avses i bilaga III betraktas som AI-system med hög risk.

I AI-förordningen finns vidare bestämmelser som bland annat ställer krav på risk- och sårbarhetshantering (artikel 9), krav på robust konstruktion och försvar mot manipulation (artikel 15), krav på loggning och spårbarhet (artikel 12) och krav på incidenthantering inklusive rapportering (artikel 73 och relaterade bestämmelser). Dessa bestämmelser syftar till att säkerställa att AI-system med hög risk är tekniskt motståndskraftiga mot fel och attacker, och att det finns organisatoriska processer för att hantera uppkommande risker över systemets hela livslängd. I efterföljande avsnitt behandlas AI-system med hög risk och kraven på cybersäkerhet i dessa system.

Risk- och sårbarhetshantering genom livscykeln (artikel 9)

I AI-förordningen finns regler om riskhantering genom hela AI-systemets livscykel. Artikel 9 anger att leverantören ska inrätta ett riskhanteringssystem för AI-system med hög risk, som ska etableras, genomföras, dokumenteras och underhållas löpande under hela livscykeln. Riskhanteringssystemet ska också inkludera att hämta in och analysera data från eftermarknadsövervakning (artikel 72)

för att identifiera nya risker som uppstår efter att systemet tagits i bruk. På så vis integreras livscykelperspektivet genom att drifts-erfarenheter och incidenter ska leda till uppdaterad riskanalys.

Riskhanteringsåtgärderna ska leda till att kvarstående riskbedöms som acceptabel innan systemet släpps ut på marknaden. Artikel 9 betonar också att testning av AI-systemet är en del av riskhanteringen, systemet ska testas under utveckling och innan driftsättning för att verifiera att det uppfyller kraven och fungerar pålitligt för sitt syfte. Leverantören får inte tillhandhålla ett AI-system med hög risk utan en grundlig riskbedömning och tester som visar att riskerna är under kontroll. En viktig del av riskhanteringen är sårbarhetshantering, dvs. att identifiera och åtgärda säkerhetsbrister. AI-förordningen integrerar sårbarhetsperspektivet på flera sätt. Dels under artikel 15.5 som anger att systemet ska konstrueras för att minimera utnyttjbara sårbarheter och motstå attacker, dels genom riskhanteringsprocessen där kända sårbarheter i mjukvara eller modell utgör risker som ska analyseras och åtgärdas via design eller kontroller. Vidare kräver förordningen att leverantören håller sig informerad om tekniska framsteg, dvs. om nya sårbarheter upptäcks genom forskningsrön eller incidentrapporter måste riskhanterings-systemet uppdateras för att hantera dem. Här finns en parallell till EU:s cyberresiliensförordning (se nedan), som uttryckligen kräver att tillverkare åtgärdar sårbarheter via uppdateringar.

Riktighet, robusthet och cybersäkerhet (artikel 15)

I artikel 15.1 i AI-förordningen föreskrivs att AI-system med hög risk ska utformas och utvecklas på ett sådant sätt att de uppnår en lämplig nivå avseende riktighet, robusthet och cybersäkerhet under hela sin livscykel. Av punkten 4 följer att AI-system med hög risk ska vara så resilienta som möjligt mot felaktigheter, funktionsfel eller inkonsekvenser som kan uppstå inom det system eller den miljö där systemet är i drift, särskilt på grund av deras interaktion med fysiska personer eller andra system, varför även tekniska och organisatoriska åtgärder ska vidtas i detta avseende. AI-system med hög risk ska vara resilienta mot försök av obehöriga tredje parter att ändra deras användning, utdata eller prestanda genom att utnyttja systemets sårbarheter. De tekniska lösningar som syftar till

att säkerställa cybersäkerhet i AI-system med hög risk ska vara anpassade till de relevanta omständigheterna och riskerna. De tekniska lösningarna för att hantera AI-specifika sårbarheter ska inbegripa åtgärder för att förebygga, upptäcka, reagera på, komma till rätta med och bekämpa attacker som försöker manipulera träningsdatasetet (dataförgiftning) eller förtränade komponenter som används i träningen (modellförgiftning), indata som är utformade för att få AI-modellen att göra ett misstag (antagonistiska exempel eller modellkringgående), sekretessangrepp eller modellfel.

Sammantaget ställer artikel 15 omfattande säkerhetskrav, bland annat ska systemet vara robust internt, stå emot attacker och noggrant i sina beslut, för att på så sätt maximera säkerheten och tilliten till AI-system med hög risk genom hela dess användning.

Presumtion om överensstämmelse med vissa krav på cybersäkerhet (artikel 42)

I artikel 42 i AI-förordningen anges närmare vad som gäller för att visa presumtion om överensstämmelse med vissa krav på cybersäkerhet i AI-förordningen. Av punkten 2 följer att AI-system med hög risk som har certifierats, eller för vilka en försäkran om överensstämmelse har utfärdats inom ramen för en ordning för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt ska förutsättas uppfylla de cybersäkerhetskrav som anges i artikel 15 i AI-förordningen, förutsatt att cybersäkerhetscertifikatet eller försäkran om överensstämmelse eller delar därav omfattar dessa krav.

Roller och ansvarsfördelning enligt AI-förordningen

AI-förordningen definierar olika aktörers roller och fördelar ansvaret för att kraven efterlevs. Leverantören (tillverkare/utvecklare) är den aktör som utvecklar ett AI-system eller låter tillverka det och släpper ut det på den inre marknaden under sitt namn eller varumärke. Leverantören har huvudansvaret för att systemet uppfyller AI-förordningens alla relevanta krav, särskilt om det är ett AI-system med hög risk. Leverantören ska låta göra en konformitetsbedömning av systemet innan det släpps ut, upprätta en EU-försäkran om överensstämmelse (artikel 47) och CE-märka AI-systemet (arti-

kel 48). För AI-system med hög risk innebär konformitetsbedömningen antingen intern kontroll med eget ansvar eller, i vissa fall, bedömning av ett anmält organ (beroende på om harmoniserade standarder följts eller om AI-systemet även omfattas av sektorslagstiftning). Leverantören ska dessutom registrera AI-system med hög risk (artikel 51 och 60).

Om en tillverkare bygger in ett AI-system med hög risk som säkerhetskomponent i en produkt så har den tillverkaren också ansvar att AI-komponenten uppfyller AI-förordningen. Artikel 25 behandlar ansvarsfördelning längs värdekedjan och klargör att om en tillverkare integrerar ett redan existerande AI-system i sin produkt på ett sätt som inte bara innebär normal användning utan ändrar ett ändamål eller gör en väsentlig förändring, då betraktas denne som ny leverantör för AI-systemet. Det betyder att produkttillverkaren måste uppfylla relevanta leverantörskrav för AI-delen.

Sammanfattningsvis kan noteras att leverantören/utvecklaren har det primära ansvaret att AI-systemet är säkert och följer reglerna, medan användaren ansvarar för korrekt och ansvarsfull användning. Importörer och distributörer fungerar som kontrollstationer för att inga icke-kompatibla AI-system finns på marknaden. Genom denna rollfördelning skapas ett delat ansvar längs hela kedjan, vilket ökar chanserna att krav på robusthet och säkerhet upprätthålls i praktiken.

Tillsyn över AI-system

För att övervaka och genomdriva AI-förordningen inrättas en flernivåstruktur av tillsynsorgan på både EU-nivå och nationell nivå. Syftet är att skapa en enhetlig tillämpning i hela unionen, liknande hur förordning (EU) 2016/679²⁵ (EU:s dataskyddsförordning) övervakas av både nationella myndigheter och ett europeiskt dataskyddsråd.²⁶

²⁵ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

²⁶ Enligt AI-förordningen inrättas följande huvudorgan för styrning och tillsyn: – AI-kontoret (European AI Office) är ett nytt kontor inom EU-kommissionen med ansvar att samordna och genomdriva de gemensamma AI-reglerna i hela EU. AI-kontoret blir en central kontaktpunkt och har en operativ roll i att övervaka efterlevnaden, särskilt för övergripande frågor som rör generella AI-modeller och gränsöverskridande ärenden. I praktiken

AI-förordningens ikraftträdande

AI-förordningen är formellt antagen men träder i kraft gradvis. Förordningen trädde i kraft den 1 augusti 2024. Detta markerar startpunkten för en övergångsperiod innan alla nya regler blir tillämpliga. Full efterlevnad kommer att krävas 2026.

Betänkandet Anpassningar till AI-förordningen – Säker användning, effektiv kontroll och stöd för innovation (SOU 2025:101)

Regeringen beslutade den 19 september 2024 att tillkalla en särskild utredare med uppdrag att se över behovet av nationella anpassningar till följd av AI-förordningen. AI-utredningen lämnade sitt betänkande *Anpassningar till AI-förordningen – Säker användning, effektiv kontroll och stöd för innovation* (SOU 2025:101) i oktober 2025. I betänkandet anges att ansvarsfördelningen för marknadskontroll bör göras med utgångspunkt från att ansvaret behöver centraliseras samtidigt som sektorsspecifik kunskap behöver säkerställas vad gäller vissa produkter och områden. Därför föreslås ett system för marknadskontroll som består av flera marknadskontrollmyndigheter och där Post- och telestyrelsen (PTS) ska vara marknadskontrollmyndighet med huvudsakligt ansvar för AI-förordningen. Vidare föreslås att PTS, Integritetsskyddsmyndigheten (IMY) och Finansinspektionen ska få ett delat ansvar för marknadskontroll över AI-system med hög risk som avses i bilaga III

är "AI-kontoret" en funktion inom EU-kommissionen, men det betecknas separat i lagen för att signalera dess särskilda fokus på AI-tillsyn.

– Varje medlemsland ska utse en eller flera nationella behöriga myndigheter som ansvarar för att lokalt övervaka AI-förordningens efterlevnad. Dessa myndigheter ska hantera marknadskontroll, ta emot klagomål och utföra tillsyn av AI-system inom sitt territorium. De samarbetar med AI-kontoret och med varandra, bland annat genom det europeiska AI-styrelsen.

– AI-styrelsen (European AI Board) är ett europeiskt råd/forum bestående av representanter från alla medlemsstaters tillsynsmyndigheter och kommissionen. AI-styrelsens roll är att stötta en enhetlig och konsekvent tillämpning av AI-förordningen genom att utfärda rekommendationer, främja samarbete och ge råd till kommissionen och medlemsländerna.

– En vetenskaplig panel inrättas som är en oberoende expertpanel knuten till AI-kontoret som består av forskare och tekniska experter inom AI.

– Ett rådgivande forum för intressenter inrättas och utgör en forumgrupp för berörda parter att kunna ge teknisk expertis och perspektiv till AI-styrelsen och kommissionen.

Utöver dessa nya organ kommer befintliga EU-institutioner och organ att bidra inom sina respektive ansvarsområden, till exempel kommer Enisa stödja arbetet med cybersäkerhet i AI-systemen och EDPB (Europeiska dataskyddsstyrelsen) kan involveras i frågor där AI och dataskydd möts.

till AI-förordningen. Nio befintliga marknadskontrollmyndigheter föreslås ska få ansvar för marknadskontroll över AI-system med hög risk som är relaterade till den harmoniserade unionslagstiftningen i bilaga IA till AI-förordningen. IMY föreslås ska vara huvudsakligt ansvarig för marknadskontroll över de förbjudna AI-användningsområdena i artikel 5. För området i artikel 5 föreslås även PTS och Finansinspektionen få ett visst ansvar.

Anmälade myndigheter enligt AI-förordningen

I SOU 2025:101 lämnas förslag på att Swedac och Läkemedelsverket ska vara anmälade myndigheter enligt AI-förordningen. Swedac föreslås ansvara för anmälda organ inom alla områden med undantag för anmälda organ för AI-system med hög risk som är relaterade till produkter som omfattas av EU:s förordningar om medicintekniska produkter, för vilka Läkemedelsverket föreslås ansvara.

Samordning och samverkan

I betänkandet görs vidare bedömningen att det finns ett stort behov av samordning och samverkan inom AI-förordningen samt att marknadskontrollmyndigheternas samordning och samverkan i vissa avseenden bör regleras särskilt. Mot den bakgrunden föreslås att en myndighet, PTS i egenskap av marknadskontrollmyndighet med huvudsakligt ansvar för AI-förordningen, ska vara samordnande marknadskontrollmyndighet och att den myndigheten också ska vara gemensam kontaktpunkt. PTS ska leda en samordningsfunktion där marknadskontrollmyndigheterna ska samverka och utbyta information. Vidare föreslås att PTS ska samordna ett marknadskontrolluppdrag, om ett enskilt marknadskontrollärende berör flera marknadskontrollmyndigheters ansvarsområden. Att utöva marknadskontroll över AI-system kan förväntas bli komplicerat. Mot den bakgrunden föreslås att PTS i komplicerade ärenden ska stödja vissa av marknadskontrollmyndigheterna med expertkunskap. PTS ska även ansvara för den huvudsakliga kontakten med allmänheten, ansvara för åtgärderna i artikel 62.1 b–d i AI-förordningen och för att lämna generell vägledning om AI-förordningen.

En kompletterande lag och förordning

I betänkandet lämnas vidare förslag på bestämmelser som behöver komplettera AI-förordningen och som föreslås ska samlas i en ny lag och en ny förordning. I betänkandet lämnas kompletterande bestämmelser om sekretess, tystnadsplikt, uppgiftsskyldighet och sekretessbrytande bestämmelser. Kompletteringslagen, kompletteringsförordningen och övriga författningsändringar föreslås träda i kraft den 2 augusti 2026.

4.3.4 Förordning (EU) 2024/1183 (eIDAS-förordningen)

Genom förordning (EU) 2024/1183²⁷ (eIDAS-förordningen) uppdateras förordning (EU) nr 910/2014²⁸ vad gäller inrättandet av ett europeiskt ramverk för digital identitet. Förordning (EU) nr 910/2014 har sedan 2014 reglerat elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden. Genom eIDAS-förordningen, som trädde i kraft 20 maj 2024, har regelverket utvidgats och moderniserats, bland annat genom införandet av ett europeiskt ramverk för digital identitet.

Krav på cybersäkerhet

I skäl 15 i eIDAS-förordningen anges att förordningen fastställer harmoniserade villkor för inrättandet av ett ramverk för europeiska digitala identitetsplånböcker som ska tillhandahållas av medlemsstaterna. Alla unionsmedborgare och invånare i unionen bör på ett säkert sätt kunna begära, välja, kombinera, lagra, radera, dela och visa identitetsuppgifter och begära att deras personuppgifter raderas under användarens egen kontroll, samtidigt som selektivt utlämnande av personuppgifter möjliggörs. De tekniker som används för att uppnå dessa mål bör utformas för att uppnå högsta möjliga nivå av säkerhet, integritet, användarvänlighet, tillgänglighet, användbar-

²⁷ Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet.

²⁸ Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

het och sömlös interoperabilitet. Den europeiska digitala identitetsplånboken ska kunna användas för att identifiera sig elektroniskt och logga in hos både offentliga och privata e-tjänster i hela EU.

Plånboken möjliggör även kvalificerade elektroniska underskrifter i högsta tillitsnivå (kvalificerade e-underskrifter) samt kan integreras i system för stark kundautentisering. En viktig ny aspekt är att plånboken inte bara kan användas för elektronisk identifiering innehåller personens elektroniska ID-handling, utan även olika attribut. Ett attribut definieras som en egenskap, en kvalitet, en rättighet eller ett tillstånd för en fysisk eller juridisk person eller ett föremål. och intyg och den fungerar som en gemensam struktur för att utfärda, lagra och validera elektroniska intyg om personliga uppgifter och kvalifikationer.

Förordningen innebär ett obligatorisk erkännande av digitala plånböcker i alla EU-länder med striktare säkerhetskrav, särskilt för identitetsplånböcker och betrodda tjänster.

Förordningen innebär ett obligatorisk erkännande av digitala plånböcker i alla EU-länder. Plånboken möjliggör även kvalificerade elektroniska underskrifter samt kan integreras i system för stark kundautentisering. En viktig ny aspekt är att plånboken inte bara kan användas för elektronisk identifiering, utan även olika attribut. Ett attribut definieras som en egenskap, en kvalitet, en rättighet eller ett tillstånd för en fysisk eller juridisk person eller ett föremål.

Vidare införs ett tekniskt ramverk och gemensamma specifikationer ska fastställas via genomförandeakter. En gemensam arkitektur- och referensram (ARF) En gemensam arkitektur- och referensram (ARF) tas fram med medlemsstaternas experter och som ligger till grund för hur plånböckerna tekniskt ska fungera och interagera, till exempel vilka dataformat som ska stödjas för identitetsintyg. Hur säkerhetskomponenter samspelar har tagits fram med stöd av medlemsstaternas experter och ligger till grund för hur plånböckerna tekniskt ska fungera och interagera, till exempel vilka dataformat som ska stödjas för identitetsintyg och hur säkerhetskomponenter samspelar.

EU:s cyberresiliensförordning ställer cybersäkerhetskrav på produkter med digitala delar, vilket omfattar komponenter som används i plånboken, som utgör en produkt med digitala element enligt cyberresiliensförordningen och måste därför uppfylla kraven på väsentliga cybersäkerhetskrav enligt bilaga I.

För särskilt kritiska plånbokskomponenter, till exempel kryptomoduler, kan tredjepartscertifiering enligt europeiska cybersäkerhetscertifieringsordningar krävas. Om produkten är certifierad enligt EU:s cybersäkerhetsakt kan detta ge presumtion om överensstämmelse med cyberresiliensförordningens krav och därigenom förenkla godkännandeprocessen.

När det gäller certifiering av komponenter i plånboken kan noteras att kommissionen och Enisa för närvarande arbetar med att ta fram en certifieringsordning. Certifiering enligt cybersäkerhetsakten möjliggör att en komponent kan återanvändas gränsöverskridande i flera medlemsstater, vilket har betydelse eftersom interoperabilitet krävs för plånboken inom hela EU. Även medlemsstaterna arbetar med att ta fram nationella certifieringsordningar för plånboken.

4.3.5 Förordning (EU) 2016/679 (EU:s dataskyddsförordning) och direktiv (EG) 2002/58 (e-dataskyddsdirektivet)

EU:s dataskyddsförordning och direktiv (EG) 2002/58²⁹ (e-dataskyddsdirektivet) innehåller bestämmelser om skydd för personuppgifter.

EU:s dataskyddsförordning fastställer bestämmelser om skydd för fysiska personer med avseende på behandlingen av personuppgifter och om det fria flödet av personuppgifter. Förordningen skyddar fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Genom e-dataskyddsdirektivet harmoniseras medlemsstaternas bestämmelser för att säkerställa ett likvärdigt skydd av de grundläggande fri- och rättigheterna, i synnerhet rätten till integritet, när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation.

Både EU:s dataskyddsförordning och e-dataskyddsdirektivet innehåller bestämmelser om krav på säkerhetsåtgärder och incidentrapportering. Den som behandlar uppgifter (personuppgiftsansvarige respektive tillhandahållare elektroniska kommunikationsnät och -tjänster) är enligt bestämmelserna skyldig att vidta åtgärder för att hantera risken för händelser som kan leda till oavsiktlig eller otill-

²⁹ Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation).

låten utplåning, förlust eller ändring eller otillåtet avslöjande av eller otillåten åtkomst till de uppgifter som behandlas.

Även EU:s cyberresiliensförordning syftar till att säkerställa skydd för personuppgifter. Produkter med digitala element får tillhandahållas på marknaden endast om de uppfyller de väsentliga cybersäkerhetskraven i bilaga I i EU:s cyberresiliensförordning. Kraven innebär bland annat att tillverkare ska säkerställa skydd mot obehörig åtkomst, skydda riktigheten hos och konfidentialiteten för behandlade uppgifter samt endast behandla uppgifter som är nödvändigt i förhållande till syftet med produkten ("uppgiftsminimering").

Skäl 32 i EU:s cyberresiliensförordning anger att cyberresiliensförordningen inte bör påverka tillämpningen av EU:s dataskyddsförordning inbegripet när det gäller bestämmelser om inrättandet av certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd som syftar till att visa att personuppgiftsansvarigas och personuppgiftsbiträdens databehandling uppfyller kraven i den förordningen. Sådan behandling kan vara inbyggd i en produkt med digitala element. Inbyggt dataskydd och dataskydd som standard samt allmän cybersäkerhet är viktiga aspekter av EU:s dataskyddsförordning. Genom att skydda konsumenter och organisationer från cybersäkerhetsrisker bidrar de väsentliga cybersäkerhetskrav som fastställs i EU:s cybersäkerhetsförordning till att förbättra skyddet av personuppgifter och individers personliga integritet. När det gäller både standardiseringen och certifieringen av cybersäkerhetsaspekter bör synergier övervägas genom samarbete mellan kommissionen, europeiska standardiseringsorganisationer, Enisa, Europeiska dataskyddsstyrelsen, som inrättats genom EU:s dataskyddsförordning, och de nationella tillsynsmyndigheterna med ansvar för dataskydd. Synergier mellan EU:s cyberresiliensförordning och unionens dataskyddsrätt bör också skapas på områdena marknadskontroll och kontroll av efterlevnaden. Därför bör de nationella marknadskontrollmyndigheter som utses enligt EU:s cyberresiliensförordning samarbeta med de myndigheter som utövar tillsyn över tillämpningen av unionens dataskyddsrätt. De sistnämnda bör också ha tillgång till information av relevans för utförandet av deras uppgifter.

EU:s dataskyddsförordning

EU:s dataskyddsförordning innehåller bestämmelser om skydd för fysiska personer med avseende på behandlingen av personuppgifter och om det fria flödet av personuppgifter. Förordningen innehåller även bestämmelser om krav på säkerhet och incidentrapportering. Kompletterande svenska bestämmelser finns i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning, se vidare avsnitt 13.4.

Enligt artikel 25 i EU:s dataskyddsförordning ska den personuppgiftsansvarige, med beaktande av bland annat den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter genomföra lämpliga tekniska och organisatoriska åtgärder, så att kraven i förordningen uppfylls och den registrerades rättigheter skyddas. Den personuppgiftsansvarige ska säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Åtgärderna ska säkerställa att personuppgifter inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer. En godkänd certifieringsmekanism i enlighet med artikel 42 får användas för att visa att kraven i punkterna 1 och 2 i den här artikeln följs.

Enligt artikel 32 ska den personuppgiftsansvarige och personuppgiftsbiträdet, med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. Vid en personuppgiftsincident ska den personuppgiftsansvarige enligt artikel 33 i EU:s dataskyddsförordning anmäla personuppgiftsincidenten till tillsynsmyndigheten.

E-dataskyddsdirektivet

I e-dataskyddsdirektivet finns bestämmelser som preciserar och kompletterar EU:s dataskyddsförordning inom sektorn elektronisk kommunikation. Direktivet är framför allt genomfört i lagen (2022:482) om elektronisk kommunikation, se vidare avsnitt 13.5.

Artikel 4 i e-dataskyddsdirektivet reglerar säkerhet i samband med behandlingen av uppgifter. Leverantören av en allmänt tillgänglig elektronisk kommunikationstjänst ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa säkerheten i sina tjänster, om nödvändigt tillsammans med leverantören av det allmänna kommunikationsnätet när det gäller nätsäkerhet. Dessa åtgärder ska säkerställa en säkerhetsnivå som är anpassad till den risk som föreligger, med beaktande av dagens tillgängliga teknik och kostnaderna för att genomföra åtgärderna. Utan att det påverkar tillämpningen av EU:s dataskyddsförordning ska dessa åtgärder minst säkerställa att endast auktoriserad personal, och endast i lagligen tillåtna syften, får tillgång till personuppgifter, att skydda personuppgifter som lagrats eller överförts mot oavsiktlig eller olaglig förstörelse, oavsiktlig förlust eller ändring samt mot icke auktoriserad eller olaglig lagring och behandling eller icke auktoriserat eller olagligt tillträde eller offentliggörande samt säkerställa införandet av en säkerhetsstrategi för behandling av personuppgifter.

Om det föreligger särskilda risker för brott mot nätsäkerheten, ska leverantören av en allmänt tillgänglig elektronisk kommunikationstjänst informera abonnenterna om sådana risker och, om risken ligger utanför tillämpningsområdet för de åtgärder som tjänsteleverantören ska vidta, om hur de kan avhjälpas, inbegripet en uppgift om de sannolika kostnader som detta kan medföra.

Vid ett personuppgiftsbrott ska leverantören av de allmänt tillgängliga elektroniska kommunikationstjänsterna utan onödigt dröjsmål anmäla personuppgiftsbrottet till den behöriga nationella myndigheten.

Om personuppgiftsbrottet kan antas inverka menligt på en abonnents eller en enskild persons personuppgifter eller integritet ska leverantören också underrätta abonnenten eller den enskilda personen om detta brott utan onödigt dröjsmål.

Det ska inte vara ett krav att underrätta den berörda abonnenten eller enskilda personen om personuppgiftsbrottet om leverantören

tillfredsställande har visat för den behöriga myndigheten att den har genomfört lämpliga tekniska skyddsåtgärder och att dessa åtgärder tillämpats på de uppgifter som berördes av säkerhetsöverträdelser. Sådana tekniska skyddsåtgärder ska göra uppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till uppgifterna.

Utan att det påverkar leverantörens skyldighet att underrätta drabbade abonnenter och enskilda personer får den behöriga nationella myndigheten, efter att ha beaktat brottets sannolika negativa effekter, kräva att leverantören meddelar abonnenten eller den enskilda personen om personuppgiftsbrottet, om så inte redan har skett.

Anmälan till abonnenten eller den enskilda personen ska minst omfatta en beskrivning av arten av personuppgiftsbrottet och de kontaktpunkter där ytterligare information kan erhållas, och den ska innehålla rekommendationer till åtgärder som mildrar eventuella negativa följder av personuppgiftsbrottet. Anmälan till den behöriga nationella myndigheten ska dessutom beskriva konsekvenserna av personuppgiftsbrottet och de åtgärder som leverantören föreslagit eller vidtagit för att avhjälpa det.

Leverantörerna ska föra förteckningar över personuppgiftsbrott som omfattar faktauppgifterna kring brotten, deras följder och vilka motåtgärder som vidtagits.

Ytterligare bestämmelser om incidentrapporteringen finns i kommissionens förordning 611/2013.³⁰

4.3.6 Direktiv 2014/53/EU (radioutrustningsdirektivet) och delegerade förordning (EU) 2022/30

Genom direktiv 2014/53/EU³¹ (radioutrustningsdirektivet) upprättas en rättslig ram för tillhandahållandet på marknaden och ibruktagandet av radioutrustning i unionen. Radioutrustningsdirektivet har i svensk rätt genomförts genom radioutrustningslagen (2016:392), radioutrustningsförordningen (2016:394) samt Post- och telesty-

³⁰ Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation.

³¹ Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG.

relsen föreskrifter (PTSFS 2023:2) om radioutrustning, se vidare avsnitt 13.6.

Artikel 3.3 i radioutrustningsdirektivet innehåller en förteckning av ett antal väsentliga krav som radioutrustning inom vissa kategorier eller klasser ska uppfylla, bland annat finns här cybersäkerhetskrav. Kommissionen ges genom artikeln befogenhet att anta delegerade akter som anger vilka kategorier eller klasser av radioutrustning som berörs av vart och ett av kraven i artikel 3.3.

Kommissionen har med stöd av artikeln antagit delegerade förordning (EU) 2022/30³². Genom förordningen ska krav vad gäller skydd av nät, personlig integritet och skydd mot bedrägeri i artikel 3.3 d, e och f i radioutrustningsdirektivet tillämpas på viss radioutrustning. Artikel 3 i delegerad förordning (EU) 2022/30 föreskriver att bestämmelserna ska tillämpas från och med den 1 augusti 2025.

De produkter som omfattas av delegerade förordning (EU) 2022/30 omfattas även av EU:s cyberresiliensförordning. De cybersäkerhetskrav som anges i EU:s cyberresiliensförordning omfattar alla aspekter av de väsentliga krav som avses i artikel 3.3 d, e och f i radioutrustningsdirektivet. För att undvika dubbelreglering när EU:s cyberresiliensförordning ska börja tillämpas avser kommissionen att upphäva delegerad förordning (EU) 2022/30.³³

4.3.7 Förordning (EU) 2023/1230 (maskinförordningen)

Förordning (EU) 2023/1230³⁴ (EU:s maskinförordning) är ett nytt regelverk som ersätter direktiv 2006/42/EG³⁵ för att höja säkerhetsnivån för maskiner på EU:s inre marknad och gäller från den 20 januari 2027.

Förordningen syftar till att hantera risker relaterade till digitalisering, cybersäkerhet och artificiell intelligens (AI), och inför nya

³² Kommissionens delegerade förordning (EU) 2022/30 av den 29 oktober 2021 om komplettering av Europaparlamentets och rådets direktiv 2014/53/EU vad gäller tillämpningen av de väsentliga krav som avses i artikel 3.3 d, e och f i det direktivet.

³³ Kommissionen har den 26 maj 2025 tagit fram ett utkast till förslag på delegerad förordning som avser att upphäva delegerade förordning (EU) 2022/30 från och med den 11 december 2027, se <https://circabc.europa.eu/ui/group/43315f45-aaa7-44dc-9405-a86f639003fe/library/12166519-54dd-4466-991b-7012d258f9d1/details>.

³⁴ Europaparlamentets och rådets förordning (EU) 2023/1230 av den 14 juni 2023 om maskiner och om upphävande av Europaparlamentets och rådets direktiv 2006/42/EG och rådets direktiv 73/361/EEG.

³⁵ Europaparlamentets och rådets direktiv 2006/42/EG av den 17 maj 2006 om maskiner och om ändring av direktiv 95/16/EG.

krav på tillverkare, importörer och distributörer, inklusive att en tredje part ska bedöma vissa säkerhetsfunktioner som självutvecklande system. Andra risker i samband med ny digital teknik är sådana som orsakas av tredje parter och som påverkar säkerheten för produkter som omfattas av förordningen. Tillverkarna åläggs att vidta proportionerliga åtgärder som är begränsade till skyddet av säkerheten för produkten som omfattas av förordningen. Detta utesluter inte att andra unionsrättsakter som specifikt behandlar cybersäkerhetsaspekter tillämpas på produkter som omfattas av denna förordning.³⁶

I förordningen framhålls att utvecklingen inom maskinsektorn har lett till en ökad användning av digitala hjälpmedel, och programvara spelar en allt viktigare roll vid utvecklingen av maskiner. Definitionen av maskiner bör därför anpassas och även definitionen av säkerhetskomponenter till att inte bara omfatta fysiska apparater utan även digitala enheter. För att ta hänsyn till den ökande användningen av programvara som en säkerhetskomponent, bör programvara som utför en säkerhetsfunktion och släpps ut på marknaden separat betraktas som en säkerhetskomponent.³⁷ För att säkerställa att maskiner eller relaterade produkter, när de släpps ut på marknaden eller tas i bruk, inte medför hälso- och säkerhetsrisker för människor eller husdjur och inte skadar egendom och i tillämpliga fall miljön, behöver grundläggande hälso- och säkerhetskrav fastställas som måste vara uppfyllda för att maskinerna eller de relaterade produkterna ska få släppas ut på marknaden eller tas i bruk.³⁸

I artikel 20.9 i förordningen anges att maskiner och relaterade produkter som har certifierats eller för vilka en försäkran om överensstämmelse har utfärdats enligt en ordning för cybersäkerhetscertifiering som antagits i enlighet med EU:s cybersäkerhetsakt,³⁹ ska förutsättas överensstämma med de grundläggande hälso- och säkerhetskraven i punkterna 1.1.9 och 1.2.1 i bilaga III vad gäller skydd mot förvanskning och säkerhet och tillförlitlighet i styrsystem i den mån dessa krav omfattas av cybersäkerhetscertifikatet eller försäkran om överensstämmelse eller delar av dem.

³⁶ Skäl 25.

³⁷ Skäl 19.

³⁸ Skäl 26.

³⁹ Skäl 51.

4.4 Förordning (EU) 2023/988 (förordning om allmän produktsäkerhet)

4.4.1 Syfte och tillämpningsområde

Förordning (EU) 2023/988⁴⁰ (förordning om allmän produktsäkerhet) började tillämpas den 13 december 2024. Det övergripande syftet med förordningen om allmän produktsäkerhet är att säkerställa en hög konsumentskyddsnivå och förbättra den inre marknadens funktion. I förordningen fastställs grundläggande regler om säkerheten hos konsumentprodukter som släpps ut eller tillhandahålls på marknaden. Förordningen ska tillämpas på produkter som levereras eller tillhandahålls, och som är avsedda för konsumenter eller som, under rimligen förutsebara förhållanden, sannolikt kommer att användas av konsumenter. För produkter som omfattas av *särskilda säkerhetskrav enligt unionsrätten är förordningen tillämplig endast i fråga om de aspekter, risker eller riskkategorier som inte omfattas av de kraven*. Vissa produktkategorier är dock helt undantagna från tillämpningsområdet. Medlemsstaterna får enligt förordningen om allmän produktsäkerhet inte förhindra att produkter tillhandahålls som omfattas av direktiv 2001/95/EG⁴¹ och uppfyller kraven i det direktivet samt släpptes ut på marknaden före den 13 december 2024. Bestämmelserna om tillsyn på produktsäkerhetsområdet anpassas även till förordning (EU) 2019/1020 (EU:s marknadskontrollförordning).

4.4.2 Krav på cybersäkerhet

Förordningen om allmän produktsäkerhet innehåller bestämmelser om *allmänt säkerhetskrav* som innebär att ekonomiska aktörer endast får tillhandahålla säkra produkter. Det finns en presumtion för att en produkt är säker om produkten överensstämmer med relevanta krav i europeiska standarder eller, när det saknas europeiska standarder, nationella krav avseende hälsa och säkerhet i den med-

⁴⁰ Europaparlamentets och rådets förordning (EU) 2023/988 av den 10 maj 2023 om allmän produktsäkerhet, ändring av Europaparlamentets och rådets förordning (EU) nr 1025/2012 och Europaparlamentets och rådets direktiv (EU) 2020/1828 och om upphävande av Europaparlamentets och rådets direktiv 2001/95/EG och rådets direktiv 87/357/EEG.

⁴¹ Europaparlamentets och rådets direktiv 2001/95/EG av den 3 december 2001 om allmän produktsäkerhet.

lemsstat där produkten tillhandahålls på marknaden. Om det varken finns unionslagstiftning om harmonisering, europeiska standarder eller hälso- och säkerhetskrav i nationell lagstiftning ska vissa aspekter beaktas vid bedömningen av om en produkt är säker, bland annat produktens egenskaper, dess inverkan på andra produkter och andra produkters inverkan på produkten.

I artikel 6.1 g i förordningen anges att när det krävs på grund av produktens art ska den innehålla lämpliga cybersäkerhetsegenskaper som är nödvändiga för att skydda produkten mot yttre påverkan, inbegripet tredje parter med avsikt att vålla skada, när en sådan påverkan kan inverka på produktens säkerhet, inbegripet eventuell förlust av sammankoppling.

I skäl 25 framhålls att ny teknik kan innebära nya risker för konsumenters hälsa och säkerhet eller ändra det sätt på vilket befintliga risker kan realiseras, såsom ett externt angrepp som medför att produkten hackas eller att dess egenskaper ändras. Ny teknik kan väsentligen ändra den ursprungliga produkten, till exempel genom programvaruuppdateringar, som då bör bli föremål för en ny riskbedömning om den väsentliga ändringen påverkar produktens säkerhet. I skäl 26 anges samtidigt att specifika cybersäkerhetsrisker som påverkar konsumenters säkerhet samt protokoll och certifiering kan hanteras genom sektorsspecifik lagstiftning. Det bör emellertid säkerställas att relevanta ekonomiska aktörer och nationella myndigheter, i de fall sektorsspecifik lagstiftning inte är tillämplig, beaktar de risker som är kopplade till ny teknik när produkterna utformas respektive bedöms, i syfte att säkerställa att de ändringar som tillförts produkten inte äventyrar dess säkerhet.

Om kommissionen får kännedom om en produkt, produktkategori eller produktgrupp som kan utgöra en allvarlig risk för människors hälsa och säkerhet kan den på eget initiativ, eller efter förfrågan från medlemsstaterna, under vissa villkor anta genomförandeakter med lämpliga åtgärder. Dessa kan till exempel innebära förbud mot att släppa ut eller tillhandahålla sådana produkter på marknaden eller särskilda villkor för marknadsföringen.

4.4.3 Artikel 11 i EU:s cyberresiliensförordning och krav på allmän produktsäkerhet

I skäl 50 i EU:s cyberresiliensförordning anges att förordningen är avgränsad till cybersäkerhetsrisker och att produkter med digitala element ”kan dock utgöra andra säkerhetsrisker som inte alltid rör cybersäkerheten”. Dessa övriga risker ska regleras av annan relevant unionslagstiftning, och om sådan saknas ska produkten omfattas av förordningen om allmän produktsäkerhet.

Artikel 11 i EU:s cyberresiliensförordning reglerar förhållandet mellan den förordningen och förordningen om allmän produktsäkerhet. Enligt artikel 11 i den först nämnda förordningen ska vissa delar av förordningen om allmän produktsäkerhet tillämpas för de *aspekter* och *risker* eller *riskkategorier* som inte omfattas av EU:s cyberresiliensförordning, under förutsättning att produkten inte redan omfattas av särskilda säkerhetskrav i annan harmoniserad unionslagstiftning. Detta innebär att den förordningen gäller för produkter med digitala inslag inom tillämpningsområde för EU:s cyberresiliensförordning vad gäller alla säkerhetsaspekter som faller utanför cyberresiliensförordningens egna väsentliga krav på cybersäkerhet. Syftet med regleringen är att undvika att det uppkommer säkerhetsluckor för en produkt med digitala element. Eftersom en sådan produkt även kan innefatta andra risker än enbart sådana som är cyberrelaterade, ska dessa fortsatt omfattas av generell produktsäkerhetsreglering om inte sektorsspecifika regler täcker dem.

Artikel 11 utgör således en lagteknisk koppling som säkerställer att produkter med digitala element uppfyller också generella säkerhetskrav för till exempel fysisk och kemisk säkerhet, utöver de nya kraven på cybersäkerhet i EU:s cyberresiliensförordning.

Närmare om begreppen ”aspekter”, ”risker” och ”riskkategorier” i artikel 11 i EU:s cyberresiliensförordning

I artikel 11 i EU:s cyberresiliensförordning anges att förordningen om allmän produktsäkerhet ska tillämpas för ”aspekter och risker eller riskkategorier som inte omfattas” av den förstnämnda förordningen. Dessa begrepp ska förstås i ljuset av den senare förordningens terminologi och produktlagstiftningens systematik.

Aspekter syftar här på säkerhetsaspekter hos produkten, dvs. olika dimensioner av produktsäkerhet. En produkt med digitala element kan ha flera säkerhetsaspekter, till exempel elektrisk säkerhet, fysisk säkerhet, kemisk säkerhet, brand- och termisk säkerhet. EU:s cyberresiliensförordning adresserar uttryckligen cybersäkerhetsaspekten hos produkten, men inte andra typer av säkerhet. De ”aspekter ... som inte omfattas” syftar således på andra relevanta säkerhetsområden utanför cybersäkerhetsområdet. I skäl 8 i förordningen om allmän produktsäkerhet anges att även om sektorsspecifik lagstiftning finns för vissa produkters säkerhetsaspekter, är det omöjligt att täcka alla produkter, och därför måste ett generellt produktsäkerhetskrav fylla igen luckor för risktyper som inte omfattas av specifik lagstiftning.

Risker definieras i den angivna förordningen som ”kombinationen av sannolikheten för att en farlig situation som kan orsaka skada ska uppkomma och skadans allvar”. Det handlar alltså om en bedömd fara, dels hur trolig en skada är, dels hur allvarliga konsekvenserna kan bli. I produktsäkerhetssammanhang avser ”risk” typiskt en konkret säkerhetsrisk för konsumentens hälsa eller säkerhet. EU:s cyberresiliensförordning introducerar på sin sida i artikel 3.37 ”cybersäkerhetsrisker”, som definieras som risk för förlust eller störning orsakad av en incident, som ska uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att incidenten inträffar. Dessa utgör en egen kategori av risk som avses i EU:s cyberresiliensförordning. Artikel 11 anger risker ”som inte omfattas”, vilket syftar på övriga typer av säkerhetsrisker för konsumenter utanför cyberområdet. Riskkategorier avser bredare grupperingar av besläktade risker, till exempel elektriska risker, kemiska risker, mekaniska risker, strålningsrisker, med mera. Termen ”riskkategorier” i artikel 11 anger att inte bara individuella risker utan hela kategorier av risk omfattas av hänvisningen till förordningen om allmän produktsäkerhet.

Sammantaget kan noteras att EU:s cyberresiliensförordning täcker i princip en riskkategori i form av cybersäkerhetsrelaterade risker, till exempel att en produkt med digitala element blir angripen digitalt med negativa följder. Alla andra riskkategorier, till exempel fysisk skaderisk eller brandrisk utgör kategorier som inte omfattas av och faller därmed under förordningen om allmän produktsäkerhet om ingen sektorslagstiftning kan tillämpas. Artikel 11

säkerställer att dessa aspekter och risktyper regleras även om de ligger utanför tillämpningsområdet för EU:s cyberresiliensförordning.

Slutligen aktualiseras ansvarsfördelningen mellan olika marknadskontrollmyndigheter. I och med att artikel 11 anger förordningen om allmän produktsäkerhet för vissa risker, kommer det att krävas samverkan och samarbete mellan berörda marknadskontrollmyndigheter. Den myndighet som övervakar efterlevnad av EU:s cyberresiliensförordning behöver samverka med den eller de marknadskontrollmyndigheter som hanterar övrig produktsäkerhet. Frågan om samverkan mellan marknadskontrollmyndigheter behandlas i kapitel 9.

Utredningen om Kompletterande bestämmelser till EU-förordningen om allmän produktsäkerhet, med mera.

Regeringskansliet (Finansdepartementet) beslutade den 18 oktober 2024 att ge en utredare i uppdrag att analysera behovet av kompletterande bestämmelser till förordningen om allmän produktsäkerhet.⁴² Utredaren ska bland annat analysera vilka ändringar som är nödvändiga och lämpliga för att anpassa svensk rätt till förordningen och lämna nödvändiga författningsförslag. Utredaren ska redovisa uppdraget senast den 18 november 2025.

4.5 EU:s arbete med regelförenkling på det digitala området

I detta avsnitt behandlas EU:s arbete med regelförenkling med koppling till det digitala området och som har beröringspunkter med regelverket i EU:s cyberresiliensförordning.

⁴² Regeringskansliets (Finansdepartementet) beslut 2024-10-18. Direktiv: *Kompletterande bestämmelser till EU-förordningen om allmän produktsäkerhet och reglering av säkerhetskrav för produkter som inte omfattas av förordningen.*

4.5.1 EU:s regelförenklingspaket

Den 21 maj 2025 presenterade EU-kommissionen en ny strategi för den inre marknaden i form av meddelandet *Ett enklare och snabbare Europa: Meddelande om genomförande och förenkling*.⁴³ Strategin är ett led i genomförandet av kommissionens konkurrenskraftskompass och syftar till att ta bort kvarstående hinder, stärka innovationskraften, samt främja tillväxt och investeringar. I meddelandet presenterade kommissionen en översyn och anpassning av lagstiftningen som ska leda till snabba och synliga förbättringar för människor och företag.

Bland de förenklingsinitiativ som nämns ingår en serie så kallade "Omnibuspaket" för ett antal prioriterade områden som identifierats tillsammans med berörda parter under de senaste åren. I samband med publiceringen av strategin presenterade EU-kommissionen det fjärde förenklingspaketet, Omnibus IV, som inkluderar förslag kopplat till digitalisering och gemensamma specifikationer. Förslagen innehåller ett antal ändringar i sektorsspecifik produktlagstiftning. De ändringar som föreslås kan generellt sett delas in i två kategorier.

Den första kategorin avser ändringar som syftar till att främja digitalisering och minska de administrativa bördorna för företag genom att ta bort krav på rapportering i pappersformat. Förslaget innehåller bland annat krav på digitalisering av EU-försäkran om överensstämmelse och andra dokument som är nödvändiga för företag att tillhandahålla för att intyga att en produkt uppfyller relevant EU-lagstiftning. Förslaget innehåller även en skyldighet att tillhandahålla informationen i EU-försäkran om överensstämmelse i de digitala produktpassen (DPP).

Det föreslås också att företag ska införa en "digital kontakt" för att underlätta kommunikationen mellan företagen och de nationella myndigheterna.

Den andra kategorin av ändringar som föreslås avser så kallade gemensamma specifikationer som alternativ till harmoniserade standarder. I harmoniserad EU-lagstiftning fastställs olika grundläggande krav, till exempel avseende hälsa och säkerhet, för pro-

⁴³ Meddelande från kommissionen till Europaparlamentet, rådet, europeiska ekonomiska och sociala kommittén samt regionkommittén *Ett enklare och snabbare Europa: Meddelande om genomförande och förenkling* COM (2025) 47 final 2025.

dukter som släpps ut på den inre marknaden. Harmoniserade standarder är det vanligaste sättet för företag att visa att en produkt överensstämmer med de grundläggande hälso- och säkerhetskraven. Överensstämmelse med harmoniserade standarder skapar en presumtion om att produkten uppfyller de väsentliga kraven i relevant lagstiftning. Om harmoniserade standarder inte finns tillgängliga kan företagen inte dra nytta av presumtionen om överensstämmelse. De måste då visa överensstämmelse på andra sätt, ofta med kostsamma och komplexa förfaranden för bedömning av överensstämmelse. Gemensamma specifikationer är bestämmelser om tekniska krav som ger ett alternativ till en standard att uppfylla de krav som gäller för en produkt.

Syftet med de föreslagna ändringarna är att införa gemensamma specifikationer i de 20 EU-rättsakter som listas i förslaget och som nu inte erbjuder ett sådant alternativ i sin nuvarande version. Bakgrunden till kommissionens förslag om gemensamma specifikationer är att det under det senaste året förekommit situationer där de europeiska standardiseringsorganen inte har tillhandahållit kommissionen de begärda harmoniserade standarderna. Genom förslaget införs gemensamma specifikationer som föreslås antas av kommissionen med stöd av genomförandeakter.

En central del av Omnibus IV är införandet av en ny definitionskategori för företag kallade ”small mid-caps” (SMC), som ett komplement till den gällande EU-definitionen av små och medelstora företag (SME). Företag som inte uppfyller kraven för SME möter strängare regler och rapporteringskrav. Omnibus IV adresserar detta genom att formellt definiera företag som en mellankategori mellan SME och stora företag. Så kallade ”Small mid-cap-företag” föreslås omfatta företag med färre än 750 anställda samt en årsomsättning på högst 150 miljoner euro eller totala tillgångar upp till 129 miljoner euro.

EU har även initierat ett arbete för att samordna och förenkla den digitala lagstiftningen.⁴⁴ Arbetet syftar till att skapa en mer samlad så kallad ”Digital Act” eller en gemensam digital regelbok

⁴⁴ 1. Kommissionens arbetsprogram 2025: *Gemensamma framsteg: En djärvare, enklare och snabbare union*, bilagorna 1–5, COM(2025) 45, 11.2.2025. 2. *Ett enklare och snabbare EU: Meddelande om genomförande och förenkling*, 11.2.2025. 3. *Översyn av EU:s cybersäkerhetsakt*, offentligt samråd, 11 april 2025. 4. *Strategin för den europeiska dataunionen*, offentligt samråd, 23 maj 2025. 5. *Den digitala belåten – digital omnibus, uppmaning att inkomma med synpunkter*, 16 september 2025.

för unionen. Syftet med denna samlade ansats är att säkerställa att de olika digitala regelverken är konsekventa och lätta att tillämpa i praktiken, utan onödig byråkrati. Kommissionen vill öka förutsebarheten och rättssäkerheten för digitala tjänster och företag, sänka kostnaderna för efterlevnad och undanröja eventuella motstridigheter mellan lagar. Samtidigt betonas att förenklingarna inte ska sänka skyddsnivån för till exempel data- och konsumentskydd, och fokus ligger på att göra reglerna mer klargörande och proportionerliga. Kommissionen aviserade hösten 2024 att digitala regler skulle ses över ur ett förenklingsperspektiv och i september 2025 lanserades en öppen konsultation (Call for Evidence) för ett ”Digitalt förenklingspaket” (Digital Omnibus), med målet att kunna presentera ett förslag redan i november 2025. Förslaget som väntas bestå av både en förordning och ett direktiv är planerat att offentliggöras 19 november 2025. Det digitala förenklingspaketet väntas innehålla förslag på ändringar i ett flertal befintliga lagar inom cybersäkerhet, data, och AI. Enligt kommissionens inriktning kommer bland annat EU:s cyberresiliensförordning att ses över och eventuellt justeras. Vissa rapporteringskrav i EU:s cyberresiliensförordning och i NIS 2-direktivet kan komma att förenklas för att minska överlappande incidentrapportering och dokumentationsbörda. Även EU:s cybersäkerhetsakt kan komma att justeras för att förenkla certifieringsramverket och undvika dubbla krav. EU:s ambition är att det digitala regelverket på sikt ska bli integrerat och enklare att tillämpa. Genom en samordnad digital lagstiftning är ambitionen både att göra det enklare för företag att följa reglerna och upprätthålla ett högt skydd för användare och konsumenter i det digitala samhället.

Utredningen kan notera att det ovan angivna arbetet mot en samlad Digital Act befinner sig i ett tidigt skede. Omnibuspaketet för digital förenkling under 2025 blir första steget. Därefter väntar en period av utvärdering och eventuellt nya lagförslag eller konsolideringar under 2026–2027.

Eftersom de frågor som behandlas i bland annat Omnibuspaketet fortfarande är föremål för behandling och förhandling mellan EU-instanser och medlemsstaterna är det i dagsläget inte möjligt att bedöma vilken påverkan eller vilka ändringar som kan komma att göras och som kan komma att påverka utformningen av andra berörda EU-rättsliga regelverk på det digitala området. Det kan noteras att EU:s cyberresiliensförordning finns bland de rättsakter

som anges vara föremål för översyn, även om förordningen inte formellt finns i förslagen i det fjärde Omnibuspaketet.

Utredningen bedömer att det i dagsläget är svårt att bedöma vilken påverkan på tillämpningen av EU:s cyberresiliensförordning som förslagen kan medföra. Den fortsatta utvecklingen av EU:s förenklingsarbete behöver dock bevakas i det fortsatta lagstiftningsarbetet i anslutning till EU:s cyberresiliensförordning.

4.5.2 New Legislative Framework (NLF)

New Legislative Framework (NLF) antogs 2008 genom beslut 768/2008/EG⁴⁵ och förordning 765/2008/EG⁴⁶. Syftet var att skapa ett enhetligt ramverk för EU:s produktlagstiftning, inklusive regler för ackreditering, överensstämmelsebedömning, CE-märkning och marknadskontroll. Sedan dess har digitalisering, globalisering och hållbarhetskrav förändrat produktmarknaden. NLF har bidragit till ökad enhetlighet i lagstiftningen och förbättrade förfaranden för bedömning av överensstämmelse av krav på produkter, men teknisk utveckling inom digitalisering och cirkulär ekonomi har – enligt EU-kommissionen – gjort det nödvändigt att analysera om ramverket fortfarande är ändamålsenligt.⁴⁷

Kommissionen inledde därför en utvärdering av NLF under 2020. *Roadmapen* för utvärderingen var öppen för synpunkter under 2020 och fokuserade på att bedöma hur NLF kunde anpassas till bland annat den digitala omställningen. En expertgrupp⁴⁸ analyserade ramverket och uppmärksammade att bland annat bestämmelserna om marknadskontroll i förordning (EU) 765/2008 hade moderniserats genom förordning (EU) 2019/1020⁴⁹ och framhöll att utvärder-

⁴⁵ Europaparlamentets och rådets beslut nr 768/2008/EG av den 9 juli 2008 om en gemensam ram för saluföring av produkter och upphävande av rådets beslut 93/465/EEG.

⁴⁶ Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93.

⁴⁷ Meddelande från kommissionen till Europaparlamentet, rådet, europeiska ekonomiska och sociala kommittén samt regionkommittén: *Den inre marknaden: vår europeiska hemmamarknad i en osäker värld En strategi för att göra den inre marknaden enkel, sömlös och stark*, COM (2025) 500 final.

⁴⁸ Fit for Future (F4F) Plattform är en expertgrupp som lämnar råd till kommissionen. Plattformen har avgett ett yttrande 2021 som föreslår att utvärderingen ska breddas till att inkludera harmoniserade standarder, digitalisering och marknadskontroll.

⁴⁹ Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011.

ingen skulle omfatta frågor såsom programvaruuppdateringar, artificiell intelligens (AI) och anmälda organs kompetens.

Kommissionen publicerade år 2022 ett utvärderingsdokument⁵⁰ som bygger på samråd med medlemsstater, industrin, konsumentorganisationer och standardiseringsorgan. I utvärderingen konstaterades att NLF varit ändamålsenligt och effektivt, men att ramverket har svagheter vad gäller anpassning till digitalisering, komplexa värdekedjor och cirkulär ekonomi. Utvärderingen rekommenderade att man undersöker hur NLF kan moderniseras för att bland annat hantera digitala produktpass och digital CE-märkning. Kommissionen gav i juli 2025 berörda aktörer möjlighet att lämna synpunkter på ett dokument om behovet av revidering av NLF. Dokumentet identifierar problem såsom långsam informationsöverföring om produkters överensstämmelse, och begränsad konsumentkunskap om CE-märkning. I dokumentet behandlas policyalternativ, inklusive obligatoriskt digitalt produktpass, och frågor om översyn av anmälda organ och harmonisering med marknadskontrollförordningen.

Efter utvärderingen ingår revideringen av NLF i kommissionens *Single Market Strategy 2025*.⁵¹ I strategin betonas att NLF och reglerna för harmoniserade produkter behöver moderniseras för att utnyttja digitalisering och förbättra marknadskontroll. I strategin föreslås bland annat inrättandet av en EU-myndighet under 2025 för att samordna marknadskontroll och lagstiftningsförslag om revidering av NLF under 2026.

⁵⁰ Commission Staff Working Document Executive Summary of the Evaluation of the New Legislative Framework {SWD (2022) 364 final}.

⁵¹ Single Market Strategy (COM (2025) 500).

5 Undantag för nationell säkerhet och försvar

5.1 Inledning

I kommittédirektiven anges att utredningen ska ta ställning till behovet av undantag från befintliga eller föreslagna bestämmelser med hänsyn till nationell säkerhet eller skydd av andra väsentliga statliga funktioner. Vidare ska utredningen vid utformningen av förslag bland annat noga beakta behovet av att upprätthålla ett högt skydd för den nationella säkerheten och för produkter som har utvecklats uteslutande för ändamål som rör nationell säkerhet eller försvarsändamål. Även i detta sammanhang ska förslagen utformas utifrån kostnadseffektivitet och att företagens och myndigheternas totala regelbörda och kostnader inte ökar mer än nödvändigt.

5.2 Utgångspunkter

En utgångspunkt för utredningens analys och övervägande i denna del av arbetet är att införandet och tillämpningen av regelverket i EU:s cyberresiliensförordning inte medför risker som kan påverka den nationella säkerheten. Det behöver därför klarläggas hur förordningen i detta avseende kan komma att tillämpas och vilken påverkan som tillämpningen kan få för nationell säkerhet samt även för de aktörer som berörs av förordningen, dvs. myndigheter och berörda ekonomiska aktörer. Frågan om den närmare innebörden av begreppen nationell säkerhet, allmän säkerhet och försvar behöver därför initialt belysas, särskilt mot bakgrund av att undantag från förordningens tillämpningsområde får ske för bland annat produkter med digitala element som tillverkas uteslutande för nationell

säkerhet och försvarsändamål eller specifikt för att hantera säkerhetsskyddsklassificerade uppgifter (artikel 2.7).

Vidare medges undantag från skyldigheten att lämna information enligt förordningen när informationen berör väsentliga säkerhetsintressen i fråga nationell säkerhet, allmän säkerhet och försvar (artikel 2.8).

Frågan är hur de unionsrättsliga begreppen nationell säkerhet, allmän säkerhet och försvar kan tolkas i belysning av syftet med EU:s cyberresiliensförordning.

Utgångspunkten för analysen av hur man kan upprätthålla ett högt skydd för den nationella säkerheten, skydd av andra väsentliga statliga funktioner och skydd för produkter med digitala element som har utvecklats uteslutande för ändamål som rör nationell säkerhet eller försvarsändamål bör därför även beröra säkerhetsskyddsregleringens tillämpningsområde, eftersom produkter med digitala element som används i säkerhetskänslig verksamhet faller inom säkerhetsskyddslagens tillämpningsområde och får undantas från förordningens tillämpningsområde.

Vidare omfattas alla produkter med digitala element som tillhandahålls på den inre marknaden av förordningens tillämpningsområde, även produkter som tillhandahålls myndigheter som verkar på områdena för allmän säkerhet och försvar, om inte undantag från tillämpningsområdet kan ske med stöd av bestämmelserna i förordningen. Det behöver därför även belysas när ett tillhandahållande på marknaden kan anses föreligga och i vilken utsträckning angivna myndigheter kan beröras av regelverket.

5.3 Undantag för nationell säkerhet och försvar

I artikel 2.7 i EU:s cyberresiliensförordning anges att förordningen inte ska tillämpas på produkter med digitala element som utvecklats eller ändrats uteslutande för ändamål som rör nationell säkerhet eller försvarsändamål eller på produkter som utformats specifikt för att behandla säkerhetsskyddsklassificerade uppgifter.

Vidare anges i artikel 2.8 att de skyldigheter som fastställs i förordningen får inte medföra tillhandahållande av information vars utlämnande skulle strida mot väsentliga intressen i fråga om medlemsstaternas nationella säkerhet, allmänna säkerhet eller försvar.

I skäl 14 anges att förordningen inte bör påverka medlemsstaternas ansvar att skydda den nationella säkerheten i enlighet med unionsrätten. Medlemsstaterna bör kunna låta produkter med digitala element som är upphandlade eller används för ändamål som rör nationell säkerhet eller försvar omfattas av ytterligare åtgärder, förutsatt att sådana åtgärder är förenliga med medlemsstaternas skyldigheter enligt unionsrätten.

Vidare anges i skäl 26 att produkter med digitala element som utvecklas eller ändras uteslutande för ändamål som rör nationell säkerhet eller försvar eller produkter som är särskilt utformade för att behandla säkerhetsskyddsklassificerade uppgifter inte bör omfattas av förordningens tillämpningsområde. Medlemsstaterna uppmanas samtidigt att säkerställa samma eller en högre skyddsnivå för dessa produkter som för de produkter som omfattas av förordningens tillämpningsområde.

I artikel 5.1 anges att förordningen inte ska hindra medlemsstaterna från att införa ytterligare cybersäkerhetskrav för produkter med digitala element när det gäller upphandling eller användning av dessa produkter för specifika ändamål, inbegripet när dessa produkter upphandlas eller används för ändamål som rör nationell säkerhet eller försvarsändamål, förutsatt att kraven är förenliga med medlemsstaternas skyldigheter enligt unionsrätten och att de är nödvändiga och proportionella för att uppnå dessa ändamål. Av artikel 5.2 framgår att utan att det påverkar tillämpningen av direktiven 2014/24/EU¹ och 2014/25/EU² ska medlemsstaterna, när produkter med digitala element som omfattas av förordningens tillämpningsområde upphandlas, säkerställa att överensstämmelse med de väsentliga cybersäkerhetskraven i bilaga I till förordningen, inbegripet tillverkarnas förmåga att ändamålsenligt hantera sårbarheter, beaktas i upphandlingsprocessen.

Vidare anges i artikel 63.1.c att alla parter som deltar i tillämpningen av förordningen ska respektera konfidentialiteten för den information och de data som de erhåller när de utför sina uppgifter och sin verksamhet på ett sådant sätt att de skyddar bland annat intressen som rör nationell och allmän säkerhet. I artikel 63.2 anges

¹ Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EG.

² Europaparlamentets och rådets direktiv 2014/25/EU av den 26 februari 2014 om upphandling av enheter som är verksamma på områdena vatten, energi, transporter och posttjänster och om upphävande av direktiv 2004/17/EG.

att utan att det påverkar tillämpningen av artikel 63.1 får information som utbyts på konfidentiell basis mellan marknadskontrollmyndigheterna och mellan marknadskontrollmyndigheter och kommissionen inte lämnas ut utan föregående samtycke från den marknadskontrollmyndighet som ursprungligen lämnat informationen. Av artikel 63.3 följer att punkterna 1 och 2 påverkar inte kommissionens, medlemsstaternas och de anmälda organens rättigheter och skyldigheter när det gäller att utbyta information och utfärda varningar och inte heller de berörda personernas skyldighet att lämna information enligt medlemsstaternas straffrätt.

Vidare får enligt artikel 63.4 kommissionen och medlemsstaterna vid behov utbyta känslig information med berörda myndigheter i tredjeländer med vilka de har slutit bilaterala eller multilaterala avtal om konfidentialitet som garanterar en tillräcklig skyddsnivå.

5.4 Närmare om undantagen

För att kunna analysera tillämpningsområdet för undantagen i artikel 2.7 och 2.8 måste den närmare innebörden av begreppen nationell säkerhet, allmän säkerhet, försvar, väsentliga säkerhetsintressen och säkerhetsskyddsklassificerade uppgifter belysas. Vad som avses med och den närmare innebörden av de EU-rättsliga begreppen nationell säkerhet, allmän säkerhet och försvarsändamål (försvar) behandlas i nästa avsnitt. Därefter behandlas vad som avses med begreppet säkerhetsskyddsklassificerade uppgifter. I efterföljande avsnitt behandlas vad som inryms i begreppet väsentliga intressen i fråga om medlemsstaternas nationella säkerhet, allmänna säkerhet eller försvar.

5.4.1 Nationell säkerhet och försvarsändamål

EU:s befogenhet framgår av EU:s grundfördrag. Ett av dem är fördraget om Europeiska unionen (FEU). Av det framgår att unionen ska bara handla inom ramen för de befogenheter som medlemsstaterna har tilldelat unionen i fördragen för att nå de mål som fastställs där. Varje befogenhet som inte har tilldelats unionen i fördragen ska tillhöra medlemsstaterna (artikel 5 FEU). En av de frågor som inte anges i uppräkningsen av unionens befogenhetskategorier

och befogenhetsområden är frågan om nationell säkerhet. Av artikel 4.2 FEU framgår att unionen ska respektera medlemsstaternas väsentliga statliga funktioner, särskilt funktioner vars syfte är att hävda deras territoriella integritet, upprätthålla lag och ordning och skydda den nationella säkerheten. I synnerhet ska den nationella säkerheten vara varje medlemsstats eget ansvar. Uttrycket nationell säkerhet (national security) är som nämnts ett EU-rättsligt begrepp. Eftersom det vid tillämpningen av artikel 4.2 FEU handlar om områden där beslutanderätten redan har överlämnats till EU, tillämpas bestämmelsen av EU-domstolen i de här sammanhangen genom en avvägning mellan de olika intressen som är aktuella i de enskilda målen.

Frågan om åtgärder som en medlemsstat vidtar för att skydda nationell säkerhet omfattas av unionsrättens tillämpningsområde har aktualiserats i EU-domstolen i målen C-623/17, C-511/18, C-512/18 och C-520/18. Målen rörde statliga myndigheters, bland annat underrättelseorgans och brottsbekämpande myndigheters, tillgång till uppgifter om elektronisk kommunikation och åtgärder som tillhandahållare av elektroniska kommunikationstjänster vidtar i enlighet med nationell lagstiftning för att möjliggöra detta. En fråga i målen var om sådana åtgärder, som syftar till att upprätthålla nationell säkerhet, faller inom unionsrättens tillämpningsområde och i så fall hur unionsrätten ska tolkas. Av EU-domstolens avgöranden får anses framgå att medlemsstaternas åtgärder inte helt kan undantas unionsrätten enbart på grund av att åtgärderna vidtas med hänvisning till den allmänna säkerheten eller det nationella försvaret. Det har då rört situationer där den övergripande frågan avsett den inre marknadens funktion.³ Som anges i artikel 4.2 har varje medlemsstat samtidigt ett eget ansvar att upprätthålla den nationella säkerheten och varje medlemsstat har rätt att skydda sina väsentliga säkerhetsintressen i enlighet med artikel 346 i fördraget om EU:s funktionssätt (EUF-fördraget).⁴ Bedömningen av en stats

³ Se även målen C-387/05, C-186/01 och C-72/83.

⁴ Artikel 346 i Fördraget om EU:s funktionssätt:

1. Bestämmelserna i fördragen ska inte hindra tillämpningen av följande regler:

a) Ingen medlemsstat ska vara förpliktad att lämna sådan information vars avslöjande den anser strida mot sina väsentliga säkerhetsintressen.

b) Varje medlemsstat får vidta åtgärder, som den anser nödvändiga för att skydda sina väsentliga säkerhetsintressen i fråga om tillverkning av eller handel med vapen, ammunition och krigsmateriel; sådana åtgärder får inte försämma konkurrensvillkoren på den inre marknaden vad gäller varor som inte är avsedda speciellt för militärändamål.

2. Rådet får på förslag från kommissionen genom enhälligt beslut ändra den lista som rådet den 15 april 1958 fastställde över varor på vilka bestämmelserna i punkt 1 b ska tillämpas.

utrymme för nationella åtgärder kan därför påverkas av det enskilda medlemsstatens förhållanden, särskilt när det gäller vilka åtgärder som kan anses nödvändiga ur nationell säkerhetssynpunkt.

Som ovan framgår är begreppet nationell säkerhet ett EU-rättsligt begrepp som avgränsar EU:s befogenhet gentemot medlemsstaterna. I svensk nationell lagstiftning används ofta uttrycket Sveriges säkerhet eller rikets säkerhet (se nedan). Uttrycket rikets säkerhet har under de senaste åren utmönstrats ur flera författningar till förmån för uttrycket Sveriges säkerhet. Den justeringen är dock bara språklig och avser ingen ändring av begreppets betydelse.

Begreppet nationell säkerhet har använts i viss utsträckning i svensk nationell lagstiftning. Författningar där uttrycket nationell säkerhet används bygger ofta på EU-rättsakter där national security anges som ett undantag från EU-rättsaktens omfattning. Uttrycket har då översatts till nationell säkerhet i samband med att den aktuella EU-rättsakten genomförts. Exempel på det är radioutrustningslagen (2016:392) och brottsdatalagen (2018:1177) vilka genomför direktiv 2014/53/EU⁵ respektive direktiv (EU) 2016/680⁶. När brottsdatalagen infördes uttalade regeringen att den inte såg någon motsättning i att använda det EU-rättsliga begreppet i brottsdatalagen, samtidigt som begreppet Sveriges säkerhet används för att ur ett nationellt perspektiv beskriva tillämpningsområdet för annan lagstiftning. När det gäller definitionen av begreppet nationell säkerhet bedömde regeringen att en definition visserligen skulle kunna underlätta att avgöra om lagen är tillämplig eller inte, men att det inte var lämpligt att göra det eftersom det i förlängningen är upp till EU-domstolen att avgöra begreppets närmare innebörd.⁷ Uttrycket har, på motsvarande sätt som begreppet Sveriges säkerhet, därför ingen tydlig definition.

När säkerhetsskyddslagen (2018:585) infördes övervägdes om man borde konkretiseras vad uttrycket Sveriges säkerhet kan avse. Regeringen bedömde dock att uttrycket skulle användas för att av-

⁵ Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG.

⁶ Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

⁷ Prop. 2017/18:232 s. 104.

gränsa tillämpningsområdet i den nya lagen, utan att det behövde definieras närmare. Regeringen konstaterade samtidigt att det finns en viss osäkerhet kring uttryckets innebörd och att förklaringen till det delvis är att de förhållanden som är av betydelse för Sveriges säkerhet kan förändras över tiden, bland annat i takt med samhällsutvecklingen. Innebörden av uttrycket måste därför bedömas i det ljuset vilket medför ett fokus på skydd av grundläggande samhällsfunktioner.⁸

Regeringen uttalade vidare:⁹

Uttrycket "Sveriges säkerhet" tar i enlighet med vad som uttalades i propositionen *Förstärkt skydd mot främmande macts underrättelseverksamhet* (prop. 2013/14:51 s. 36) sikte på förhållanden av grundläggande betydelse för Sverige. Det innebär att lagens krav på säkerhetsskydd på samma sätt som tidigare gäller för såväl militär som civil verksamhet. Vilka verksamheter som är av betydelse för att upprätthålla Sveriges säkerhet måste bedömas i ljuset av samhällsutvecklingen. Vad som behöver skyddas för att förebygga hot mot Sveriges säkerhet kan därför i viss utsträckning förändras över tid. Tidigare var uttrycket starkt förknippat med Försvarsmaktens verksamhet, eftersom det främsta hotet mot rikets säkerhet ansågs vara ett militärt angrepp. I dag är samhället och hotbilden mer komplex och föränderlig, vilket i sin tur har fört med sig att uppgifter som rör förhållanden inom andra samhällssektorer också kan vara av betydelse för den nationella säkerheten. Det kan exempelvis gälla uppgifter om viktig civil infrastruktur såsom flygplatser, energianläggningar och förmedlingsstationer för telekommunikation. Även inom sådana områden som typiskt sett domineras av enskilda aktörer kan det finnas uppgifter som behöver skyddas enligt bestämmelserna i denna lag. Här kan nämnas olika former av elektronisk utrustning som används i syfte att skydda information eller informationssystem eller uppgifter om bl.a. tillverkningsätt och konstruktion av produkter inom telekommunikationsområdet.

Med uttrycket "som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd" avses uppgifter som är säkerhetskänsliga för andra stater och mellanfolkliga organisationer och som Sverige genom säkerhetsskyddsöverenskommelser har åtagit sig att skydda. Sådana överenskommelser gäller i dag i förhållande till ett trettioital stater och vissa mellanfolkliga organisationer, bl.a. EU och Nato. Bestämmelsen ger även stöd för säkerhetsskyddsåtgärder som följer av folkrättsliga förpliktelser i övrigt, bl.a. EU-rättsliga bestämmelser inom t.ex. luftfartsskyddsområdet.

Alla delar i en verksamhet som har betydelse för Sveriges säkerhet omfattas av paragrafen. Det kan t.ex. röra sig om uppgifter som är hemliga med hänsyn till Sveriges säkerhet och som kan finnas i informa-

⁸ Prop. 2017/18:89 s. 41.

⁹ Prop. 2017/18:89 s. 133 f.

tionssystem eller fysiska handlingar. Det kan också röra sig om personal, fastigheter och andra anläggningar samt informationssystem som inte i första hand behöver skyddas för att de innehåller hemliga uppgifter utan för att de är vitala för förmågan att upprätthålla kritiska samhällsfunktioner, t.ex. för Sveriges demokratiska statsskick, rättsväsende eller brottsbekämpande förmåga.

I regeringens proposition (2025/26:28) *Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag* med anledning av NIS 2-direktivet¹⁰ noteras att direktivet inte är tillämpligt på offentliga förvaltningsentiteter som bedriver verksamhet inom områdena nationell säkerhet, allmän säkerhet, försvar och brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott. Regeringen konstaterar samtidigt att det inte utvecklas närmare i direktivet vad som avses med uttrycken och för att genomföra direktivet på korrekt sätt i nationell rätt krävs därför en tolkning av vad de avser för slags verksamhet i Sverige. Regeringen noterar samtidigt att uttrycket nationell säkerhet är ett vedertaget begrepp inom unionsrätten men som saknar en tydlig definition i densamma. Regeringen noterar vidare att i Sverige används uttrycket Sveriges säkerhet i olika sammanhang och att innebörden av uttrycket har behandlats i flera lagstiftningsärenden de senaste åren.¹¹ Regeringen framhåller att uttrycket tar sikte på förhållanden av grundläggande betydelse för Sverige och att det kan handla om både militär och civil verksamhet, så länge verksamheten har en sådan betydelse. Uttrycket används exempelvis i 1 kap. 1 § säkerhetsskyddslagen, som gäller bland annat för den som till någon del bedriver verksamhet som är av betydelse Sveriges säkerhet. En slutsats av det anförda är – enligt regeringen – att direktivet bland annat inte är tillämpligt på säkerhetskänslig verksamhet. Regeringen framhåller vidare att uttrycket allmän säkerhet i direktivet bör anses omfatta det som avses med uttrycket i EUF-fördraget, dvs allmän säkerhet avser skydd av en medlemsstats institutioner, dess väsentliga offentliga tjänster och dess invånares överlevnad. Regeringen konstaterar samtidigt att vilken verksamhet som uttrycket försvar avser i direktivet bör inte kräva någon närmare analys.

¹⁰ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

¹¹ Se till exempel regeringens proposition (2022/23:116) *Ett granskningssystem för utländska direktinvesteringar till skydd för svenska säkerhetsintressen*, s. 21.

Utredningen kan för sin del notera att begreppet försvar i EU-rätt och svensk rätt avser främst militärt försvar och de försvarsrelaterade funktioner som skyddar staten mot yttre hot. Inom EU-samarbetet är säkerhet och försvar fortfarande till övervägande del nationella kompetenser eftersom medlemsstaterna behåller kontrollen över sina respektive försvarsmakter och militära resurser. Detta återspeglas också i EU-rätten genom till exempel artikel 346 i EUF som medger undantag för försvarsmateriel och väsentliga säkerhetsintressen kopplade till försvaret, och sekundärrätt, till exempel direktiv 2009/81/EG¹², som erkänner medlemsstaternas behov av att skydda hemlig försvarsinformation och strategiska intressen inom försvaret. All verksamhet som rör utveckling och anskaffning av försvarsmateriel som är av betydelse för Sveriges försvarskapacitet bör därför som betraktas som verksamhet som rör försvarsändamål. När artikel 2.7 undantar produkter för ”försvarsändamål” avses i denna artikel dock endast sådana produkter som uteslutande utvecklas eller ändras för användning inom bland annat försvarsverksamheten. Produkterna kommer då i stället att omfattas av nationella försvars- och säkerhetskrav. Genom Försvarsmaktens föreskrifter och krav för it-system, och genom internationella försvarssamarbeten, till exempel genom Nato-standarder, säkerställs att dessa produkter får en hög säkerhet och ett högt skydd.

Sammanfattningsvis erkänns i både EU-rätt och svensk rätt medlemsstaternas möjlighet att förfoga över sin egen försvarsmakt och den EU-rättsliga lagstiftningen är utformad för att inte inkräkta på det området annat än i samordnande eller stödjande syfte. Därutöver finns det flera förbehåll i EU-fördragen kopplade till frågor som rör medlemsstatens allmänna ordning och säkerhet. Som ovan framgår anger regeringen att med allmän säkerhet avses omfatta det som avses med uttrycket i EUF-fördraget. Allmän säkerhet gäller skydd av en medlemsstats institutioner, dess väsentliga offentliga tjänster och dess invånares överlevnad. Den fria rörligheten kan till exempel begränsas med hänsyn till allmän ordning och säkerhet.

Sammantaget bedömer utredningen att vad som innefattas i uttrycken nationell säkerhet, allmän säkerhet och försvar sedan tidi-

¹² Europaparlamentets och rådets direktiv 2009/81/EG av den 13 juli 2009 om samordning av förfarandena vid tilldelning av vissa kontrakt för byggtreprenader, varor och tjänster av upphandlande myndigheter och enheter på försvars- och säkerhetsområdet och om ändring av direktiven 2004/17/EG och 2004/18/EG.

gare är tillräckligt klarlagda och bör i sig inte medföra tillämpningsproblem när begreppen tillämpas i anslutning till undantagen i artikel 2.7 och artikel 2.8. i EU:s cyberresiliensförordning.

5.4.2 Produkter som tillverkas eller ändras uteslutande för nationell säkerhet eller försvarsändamål (artikel 2.7)

För att omfattas av undantaget i artikel 2.7 krävs att produkten tillverkas eller ändras uteslutande för nationell säkerhet eller försvarsändamål. Produkten ska således tillverkas eller ändrats uteslutande för angivna ändamål vilket innebär att om produkten samtidigt tillhandhålls på marknaden för även för andra ändamål är undantaget inte tillämpligt. Om en produkt inte är framtagen uteslutande för nationell säkerhet och försvar, utan exempelvis har en civil variant eller potentiell civil användning, så kan den betraktas som en marknadsprodukt. Om produkten har dubbla användningsområden, dvs. kan användas såväl för angivna ändamål som för annan verksamhet är undantaget inte tillämpligt. Det är tillverkaren som ska visa att förutsättningar för undantaget är tillämpligt. Avgörande är således produktens karaktär och avsedda användning. Om produkten är utvecklad eller ändrad uteslutande för verksamhet som rör nationell säkerhet, allmän säkerhet eller försvarsändamål talar det för att produkten omfattas av undantaget i artikel 2.7. Om produkten däremot inte uteslutande utvecklats för angivna ändamål, till exempel ett IKT- eller kommunikationssystem som även kan användas för andra ändamål som faller utanför de i artikel 2.7 angivna ändamålen, kan den inte anses vara uteslutande utvecklad för dessa ändamål och då kvarstår kraven i förordningen på produkten. Avgörande är således syftet med produkten, inte vilken myndighet eller annan aktör som anskaffar den. Om till exempel en försvarsmyndighet köper servrar, datorprogram eller liknande som även tillhandhålls på marknaden, faller produkten utanför undantaget i artikel 2.7. Om en myndighet beställer ett system som uteslutande är utvecklat eller anpassat för allmän säkerhet eller försvarsändamål och som inte tillhandhålls på marknaden överhuvudtaget, torde produkten enligt utredningens bedömning omfattas av undantaget.

5.4.3 Produkter som utformas specifikt för att behandla säkerhetsskyddsklassificerade uppgifter (artikel 2.7)

Undantaget i artikel 2.7 i EU:s cyberresiliensförordning omfattar även produkter som utformats specifikt för att behandla säkerhetsskyddsklassificerade uppgifter.¹³ I unionsrätten förekommer begreppet säkerhetsskyddsklassificerade uppgifter bland annat i rådets beslut 2013/488/EU av den 23 september 2013 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade uppgifter.¹⁴ Beslutet inrättar ett övergripande säkerhetssystem för skydd av säkerhetsskyddsklassificerade uppgifter, som omfattar Europeiska unionens råd, dess generalsekretariat och EU-länderna, för att man ska kunna utveckla rådets verksamhet på alla områden som kräver hantering av säkerhetsskyddsklassificerade uppgifter. Genom beslutet anges de grundläggande principerna och miniminormer för skyddet av säkerhetsskyddsklassificerade EU-uppgifter. Dessa principer och normer gäller för rådet och generalsekretariatet och ska iakttas av EU-länderna i enlighet med deras nationella lagar för att säkerställa att var och en av dem ger säkerhetsskyddsklassificerade EU-uppgifter en motsvarande skyddsnivå.

Begreppet säkerhetsskyddsklassificerade uppgifter definieras nationellt i säkerhetsskyddslagen (2018:585) som uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) (OSL) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig (1 kap. 2 § andra stycket).¹⁵ Andra ledet i bestämmelsen tar sikte på verksamheter som inte formellt omfattas av bestämmelserna i OSL, till exempel företag och andra enskilda aktörer. Av bestämmelsen följer att även uppgifter som finns hos

¹³ I den engelska språkversionen anges i skäl 26: "Products with digital elements that are developed or modified exclusively for national security or defence purposes or products that are specifically designed to process classified information fall outside the scope of this Regulation. Member States are encouraged to ensure the same or a higher level of protection for those products as for those falling within the scope of this Regulation." Vidare anges i artikel 2.7: This Regulation does not apply to products with digital elements developed or modified exclusively for national security or defence purposes or to products specifically designed to process classified information."

¹⁴ Även Europeiska kommissionen och Europaparlamentet har antagit bestämmelser för behandling av säkerhetsskyddsklassificerade EU-uppgifter. Se Kommissionens beslut (EU, Euratom) 2015/444 av den 13 mars 2015 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (EUT L 72, 17.3.2015, s. 53) och Beslut av Europaparlamentets presidium av den 15 april 2013 om bestämmelserna för Europaparlamentets hantering av sekretessbelagd information (EUT C 96, 1.4.2014, s. 1).

¹⁵ Prop. 2017/18:89, bet. 2017/18:Ju U21, rskr. 2017/18:289.

sådana aktörer är säkerhetsskyddsklassificerade fastän OSL formellt inte gäller för aktören, förutsatt uppgiften skulle ha omfattats av sekretess, om OSL hade varit tillämplig. Det är tillräckligt att uppgiften till sin natur är sådan att den materiellt sett kan hänföras till en bestämmelse om sekretess med hänsyn till antingen Sveriges säkerhet eller Sveriges förbindelser med en annan stat eller mellanfolklig organisation.

I 2 kap. 5 § första stycket säkerhetsskyddslagen anges att säkerhetsskyddsklassificerade uppgifter ska delas in i säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet. Av 2 kap. 5 § andra stycket följer att säkerhetsskyddsklassificerade uppgifter som omfattas av ett internationellt åtagande om säkerhetsskydd på motsvarande sätt ska delas in i säkerhetsskyddsklass, om de inte redan har klassificerats av en annan stat eller en mellanfolklig organisation. Indelningen i säkerhetsskyddsklass ska i sådant fall göras utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges förhållande till annan stat eller mellanfolklig organisation.

I förordning eller myndighetsföreskrifter konkretiseras det vilka specifika åtgärder som ska vidtas för att skydda de säkerhetsskyddsklassificerade uppgifterna.

Säkerhetspolisen har i detta sammanhang framhållit att det engelska begreppet ”classified information” har översatts till säkerhetsskyddsklassificerad information i den svenska versionen av förordningsförslaget. Detta undantag bör dock, enligt myndigheten, kunna tillämpas inte endast i förhållande till säkerhetsskyddsklassificerade uppgifter utan även för andra typer av sekretessbelagda uppgifter, inklusive sådana som omfattas av förundersökningssekretess (se nedan).

Artikel 2.7 anger vidare att produkten ska vara specifikt utformad för att behandla säkerhetsskyddsklassificerade uppgifter. Det kan noteras att artikel 2.7 inte definierar vilka tekniska specifikationer som krävs för att en produkt med digitala element ska omfattas av artikels tillämpningsområde. Att en produkt är specifikt utformad för att specifikt behandla säkerhetsskyddsklassificerade uppgifter innebär normalt att produkten är avsedd för hantering av sådan information som omfattas av undantaget, dvs. att den är konstruerad med funktioner och säkerhetsmekanismer för att uppfylla krav för hantering av sådan information, till exempel dokumenta-

tionskontroll, åtkomstbegränsningar, fysisk och logisk säkerhet, kryptografi och spårbarhet.

5.4.4 Undantag från uppgiftsskyldigheten (artikel 2.8)

När det gäller skyldigheter att tillhandahålla information vars utlämnande skulle strida mot medlemsstatens väsentliga intressen när det gäller nationell säkerhet, allmän säkerhet eller försvar finns undantag från cyberresiliensförordningens tillämpningsområde i artikel 2.8. Vad som avses med begreppen nationell säkerhet och försvar har behandlats ovan i avsnitt 5.4.1.

I artikel 2.8 nämns även allmän säkerhet och det slås fast att ingen informationsskyldighet enligt EU:s cyberresiliensförordning ska medföra risk för att väsentliga intressen avseende allmän säkerhet åsidosätts. Allmän säkerhet (eng. public security) avser skyddet för samhället och allmänheten i stort mot allvarliga hot, faror eller störningar. Inom EU-rätten förekommer begreppet allmän säkerhet som ett legitimt intresse som kan motivera undantag eller inskränkningar i exempelvis de fria rörligheterna och andra rättigheter, vid sidan av allmän ordning. Det handlar typiskt sett om medlemsstatens inre säkerhet och allmänna ordning, såsom att förebygga eller hantera terrorism, grov organiserad brottslighet, större katastrofer eller andra hot mot befolkningens liv och hälsa.

I NIS 2-direktivet återfinns liknande bestämmelser, och i direktivet anges att det inte ska tillämpas på offentliga organ som bedriver verksamhet inom allmän säkerhet.

I svensk rätt används termen allmän säkerhet ofta tillsammans med allmän ordning för att beteckna den offentliga tryggheten och ordningen i samhället. Att något utgör ett hot mot allmän säkerhet och ordning kan syfta på risk för allvarlig brottslighet, upplopp eller fara för medborgarnas säkerhet i stort. Även om allmän säkerhet inte är exakt definierat i en särskild lag är det ett etablerat begrepp som täcker in den generella säkerheten för allmänheten till skillnad från nationell säkerhet som rör statens vitala intressen. I praktiken inkluderar allmän säkerhet bland annat civil säkerhet, krishantering och den bredare brottsbekämpningens syfte att upprätthålla trygghet i samhället. Begreppet har en viss elasticitet och

vilken reglering som behövs till stöd för vad som krävs för att upprätthålla allmän säkerhet får bedömas från fall till fall.

För att ett undantag ska kunna ske med stöd av artikel 2.8 krävs även att informationen rör ett väsentligt intresse som avser nationell säkerhet, allmän säkerhet och försvar. Medlemsstaten har rätt att bedöma när informationen rör ett väsentligt intresse i angivna avseende.

Begreppet väsentligt intresse återfinns även i artikel 346 i EUF-fördraget. I artikeln ges medlemsstaterna rätt att göra undantag från EU-regler med hänvisning till sina väsentliga nationella säkerhetsintressen.¹⁶ Artikeln består av två huvudpunkter: (a) att ingen medlemsstat är skyldig att lämna ut information om den anser att utlämnandet strider mot dess väsentliga säkerhetsintressen, och (b) att varje stat får vidta de åtgärder den anser nödvändiga för att skydda sina väsentliga säkerhetsintressen i fråga om tillverkning av eller handel med vapen, ammunition och krigsmateriel, under förutsättning att dessa åtgärder inte försämrar konkurrensvillkoren för varor som inte specifikt är avsedda för militärt bruk.

Artikel 346 i EUF har generell räckvidd inom EU-rätten och är ett uttryck för att nationell säkerhet är varje medlemsstats eget ansvar, något som även framgår av artikel 4.2 FEU. Artikel 346 i EUF säkerställer att EU-regler inte hindrar en medlemsstat från att vidta nödvändiga åtgärder för att skydda medlemsstatens väsentliga säkerhetsintressen. EU-domstolen har i praxis betonat att undantag som artikel 346 i EUF måste tolkas restriktivt. Det är medlemsstaten som åberopar undantaget som måste visa att åtgärden eller undantaget håller sig inom det nödvändiga för att skydda statens väsentliga säkerhetsintressen och att undantaget endast får användas i vissa situationer.

Artikel 2.8 i EU:s cyberresiliensförordning ger stöd för undantag från skyldigheter att tillhandahålla information vars utlämnande skulle strida mot Sveriges väsentliga säkerhetsintressen inom angivna områden. Det kan till exempel avse skyldigheten att rapportera sårbarheter i en produkt med digitala element enligt artikel 14 och 16 i EU:s cyberresiliensförordning. I det enskilda fallet kan noteras att artikel 16 medger att information om sårbarheter och incidenter kan underlåtas när i artikeln angivna förutsättningar före-

¹⁶ Se till exempel SOU 2022:24 – *Materielförsörjningsstrategi*.

ligger bland annat när ett utlämnande skulle strida mot Sveriges väsentliga intressen.

5.5 Remissvar över kommissionen utkast till EU:s cyberresiliensförordning

Utredningen kan notera att flera myndigheter som yttrat sig i remissförfarandet över kommissionens utkast till EU:s cyberresiliensförordning, bland annat Försvarmakten, Försvarets materielverk (FMV), Försvarets radioanstalt (FRA) Säkerhetspolisen och Polismyndigheten anser att uttrycket nationell säkerhet i artikel 4.2 FEU och undantaget för nationell säkerhet i artikel 2.7 behöver förtydligas i förordningen. Vidare har några myndigheter efterfrågat ett förtydligande av begreppet tillhandahållande av en produkt på den inre marknaden.

Försvarmakten noterar att enligt artikel 4.2 FEU ska medlemsstaternas suveräna rättigheter avseende nationell säkerhet respekteras. Enligt förordningsförslaget ska den inte tillämpas på sådana produkter med digitala element som utvecklats uteslutande för ändamål som rör nationell säkerhet eller militära ändamål eller på produkter som utformats specifikt för att behandla säkerhetsskyddsklassificerade uppgifter. Myndigheten menar att det uppstår tolkningssvårigheter gällande samhällsviktiga funktioner som är en del av totalförsvaret och därmed av betydelse för Sveriges säkerhet. Undantaget för nationell säkerhet behöver därför förtydligas i förordningen. Vidare innebär förslaget att produkter med dubbla användningsområden kommer att omfattas av förordningens tillämpningsområde. Vissa produkter som används av myndigheten, eller i annan verksamhet som rör nationell säkerhet, skulle alltså omfattas av förordningen. Det innebär bland annat att en incident som ska rapporteras in till Enisa samtidigt kan utgöra en incident som rör Sveriges säkerhet och därmed bör tillkännages myndigheten inom ramen för dess uppgifter inom säkerhetsskyddslagstiftningen. Därutöver har myndighetens cyberförsvaret ett behov av att skyndsamt få rapporter om sårbarheter i produkter som används inom det militära försvaret, i syfte att snabbt kunna vidta nödvändiga skyddsåtgärder. Myndigheten anser därför att incidenter som rör nationell säkerhet i första hand ska hanteras nationellt i stället för genom Enisa.

Försvarsmakten förutsätter att myndigheten inte kan anses som en sådan ekonomisk aktör som ikläds skyldigheter enligt förordningen, när myndigheten själv utvecklar eller importerar produkter för eget bruk. Om det råder några tveksamheter kring detta bör det förtydligas i förordningstexten.

FMV framhåller att av artikel 4.2 FEU framgår att den nationella säkerheten är varje medlemsstats eget ansvar och faller utanför EU-rättens område. Medlemsstaterna ska, när det gäller nationella säkerhetsintressen, kunna köpa och utveckla produkter som inte ska omfattas av förordningens krav. Medlemsstaterna ska, med hänvisning till nationell säkerhet, fritt kunna tillföra ytterligare krav på produkter som omfattas av förordningen. FMV anser att det inte återspeglas i förslagen till undantag i förordningen. Förslagen till undantag är alltför snävt formulerade och innebär tolknings-svårigheter avseende vilka produkter, med användningsområde inom nationell säkerhet, som kan tänkas omfattas av undantaget. Formuleringar som ”utvecklats uteslutande för ändamål som rör nationell säkerhet” och ”produkter som utformats specifikt för att behandla säkerhetsskyddsklassificerade uppgifter” lämnar få produkter utanför den föreslagna förordningens tillämpningsområde och myndigheten anser att regleringen ska ha en skrivning som är samma eller liknande som finns i artikel 1.2 i EU:s cybersäkerhetsakt där det anges att den förordningen påverkar inte medlemsstaternas befogenheter i fråga om verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på straffrättens område. FMV påpekar även att artikel 11 i förordningsförslaget föreskriver ett mycket omfattande och detaljerat rapporteringskrav för tillverkare. Det finns därmed en risk med att det föreslagna förfarandet genererar stora mängder känslig information och att rapportera och samla all denna känsliga information i sig kan utgöra en risk. En insamling av kunskap om sårbarheter i samtliga produkter som omfattas av förordningen, dvs. kommersiell mjuk- och hårdvara med digitala element, skulle göra Enisa till ett mål för många olika hotaktörer och skulle då kunna utgöra ett hot även mot enskilda medlemsstats nationella säkerhet. FMV anser att en sådan inrapportering till Enisa inte bör genomföras på det sätt som föreslås och föreslår att till exempel bör den nationella CSIRT-enhetens roll övervägas i sammanhanget.

Även *FRA* bedömer att förslaget till förordning är mycket omfattande och det är avgörande att det tydligt framgår att nationell säkerhet inte omfattas av förordningens tillämpningsområde. *FRA* anser att det förslag till undantag som framgår av artikel 2.5 är alltför snävt formulerat. Det avgörande bör vara produktens användningsområde inom nationell säkerhet, inte i vilket syfte produkten har utvecklats. Formuleringen av ett undantag för nationell säkerhet och andra områden som faller utanför EU-rättens område bör samordnas med motsvarande bestämmelse i förslaget till förordning om harmoniserade regler för artificiell intelligens (AI-förordningen).

FRA pekar också på att det finns risker med den alltför detaljerade rapporteringen av sårbarheter som föreslås gälla för tillverkare. Information om en produkts sårbarheter och vilka korrigerande eller riskreducerande åtgärder som har vidtagits är i sig känslig information och att samla sådan information i den omfattning som förslaget innebär medför sårbarheter. Om det blir aktuellt att hantera sådan information digitalt i ett it-system måste stora krav ställas på säkerheten och tillräckligt med resurser måste avsättas för detta ändamål. Åtgärder för att motverka cyberangrepp och sårbarheter i en produkt handlar även om nationell säkerhet, varför det föreslagna rapporteringskravet måste analyseras noga i förhållande till undantaget för nationell säkerhet. Risken är annars att ett undantag för nationell säkerhet urholkas om förordningens rapporteringskrav är alltför långtgående för de produkter som omfattas.

Säkerhetspolisen noterar att förordningens avsikt kan sägas vara att skydda i första hand konsumenter och andra aktörer som inte har möjlighet att själva kravställa och identifiera brister i uppkopplade produkters cybersäkerhet. Myndigheten menar att produkter som utvecklats i syfte att användas i verksamheter som ligger utanför EU:s kompetens, inklusive på området nationell säkerhet, inte ska omfattas av förordningen. Undantaget bör således inte vara begränsat till varor som utvecklats uteslutande för sådan användning, utan formuleras på bredare sätt.

Säkerhetspolisen påpekar vidare att det engelska uttrycket "classified information" har översatts till säkerhetsskyddsklassificerad information i den svenska versionen av förordningsförslaget. Detta undantag bör dock kunna tillämpas inte endast i förhållande till säkerhetsskyddsklassificerade uppgifter utan även för andra typer av sekretessbelagda uppgifter, inklusive sådana som omfattas av

förundersökningssekretess. Vilka typer av information och klassificeringar som bör omfattas av undantaget behöver därför analyseras närmare.

Säkerhetspolisen noterar även att enligt definitionen i artikel 3.23 i förordningsförslaget omfattas ”varje leverans av en produkt med digitala element för distribution eller användning på unionsmarknaden i samband med kommersiell verksamhet, antingen mot betalning eller kostnadsfritt”. Myndigheten är av uppfattningen att enligt definitionen bör en myndighet som till exempel själv ombesörjer import en viss produkt från ett tredjeland för eget bruk inte kunna anses utgöra en importör eller av annan anledning omfattas av skyldigheterna i förordningen, eftersom agerandet inte har samband med kommersiell verksamhet. Myndigheten har dock uppfattat att vissa svenska marknadskontrollmyndigheter menar att en myndighet eller annan organisation som importerar en produkt för sitt eget bruk ska anses tillhandahålla produkten på unionsmarknaden. En sådan syftestolkning görs med argumentet att produkten även i sådant fall får viss utbredning i samhället. Myndigheten anser att förordningsförslaget behöver förtydligas så att det inte råder några oklarheter om att privat import och andra typer av leveranser som har samband med offentlig verksamhet inte ska anses utgöra ett tillhandahållande.

Polismyndigheten framhåller att det är angeläget att med ett förtydligande kring förordningsförslaget tillämpningsområde när det gäller vilka som är ekonomiska aktörer i förordningen mening. Om det är så att myndigheten i något avseende skulle anses omfattas av förordningen så anser myndigheten att det bör införas undantag. Myndigheten noterar vidare att den föreslagna förordningen uppställer krav på rapporteringsskyldighet och transparens. Exempelvis ska tillverkare anmäla vissa sårbarheter till EU:s cybersäkerhetsbyrå Enisa som i sin tur ska vidarebefordra information till nationella CSIRT-enheter. Myndigheten anser att det är viktigt att det säkerställs att inga för myndigheten skyddsvärda metoder och förmågor röjs. Ett exempel är om en produkt tagits fram exklusivt för myndigheten och den visar sig utgöra en betydande cybersäkerhetsrisk. Enligt myndighetens uppfattning torde det då till exempel inte finnas anledning för marknadskontrollmyndigheten att informera om det publikt. Det kan vidare befaras att artikel 52 som behandlar konfidentialitet inte ger ett tillräckligt skydd mot röjande av känslig infor-

mation. Samtidigt kan myndigheten ha behov av att kunna ta del av material från marknadskontrollmyndigheten inom ramen för den brottsförebyggande och brottsutredande verksamheten på cyberområdet varför båda dessa intressen bör beaktas.

Säkerhets- och försvarsföretagen (SOFF) noterar att definitionen av begreppet nationell säkerhet är ett brett begrepp som förekommer i flera förordningar och oftast med referensen att det faller utanför EU:s kompetens (artikel 4.2). I Sverige finns ingen vedertagen definition och det förekommer olika begreppsanvändning inom olika områden, bland annat allmän säkerhet och ordning, Sveriges säkerhet samt väsentliga säkerhetsintressen. Att begreppet tolkats olika i nationell lagstiftning ställer större krav på att det är tydlig med vad begreppet innebär i förordningsförslaget och att förslaget tydliggör nationell säkerhet. I fråga om it-produkter och -tjänster är det sällan Sveriges säkerhet som avses, utan mer av dess förmåga och den tekniska karaktären. SOFF vill samtidigt understryka att civila komponenter och produkter, som har dubbla användningsområden, kan användas för även för militära ändamål. Dessa har sällan utvecklats uteslutande för militära ändamål, men antalet civila produkter som har militära ändamål är omfattande. Antalet produkter som utvecklats uteslutande för militära ändamål är samtidigt mycket begränsat i antal.

Teknikföretagen anser att i detta sammanhang bör det säkerställas att definitionen av begreppet nationell säkerhet är tydlig och överensstämmer med andra relevanta lagstiftningar.

5.6 Produkten tillhandhålls på marknaden

I remissomgången över utkastet till EU:s cyberresiliensförordning har några av myndigheterna påtalat behov av förtydliganden om en produkt med digitala element som anskaffas av en myndighet i vissa fall inte kan anses tillhandhållen på marknaden. Utredningen bedömer att det därför kan finnas skäl att belysa regleringen i detta avseende.

Inom EU-rätten avser begreppet marknadstillträde i grunden rätten och möjligheten att släppa ut produkter på EU-marknaden, förutsatt att de uppfyller gällande krav i harmoniserad lagstiftning. Termen är nära kopplad till utsläppande på marknaden, vilket in-

träffar när en produkt för första gången görs tillgänglig i EU. För att en produkt ska få marknadsstillträde måste den vid utsläppandet uppfylla tillämpliga hälso-, säkerhets- och prestandakrav enligt harmoniserad lagstiftning. Syftet är att endast produkter som överensstämmer med dessa krav ska cirkulera fritt inom unionen. Det innebär att produkten med digitala element får tillhandhållas på den inre marknaden när den uppfyller krav på cybersäkerhet i EU:s cyberresiliensförordning och övriga tillämpliga krav på produkten enligt harmoniserad unionsrätt. Marknadsstillträdet är således villkorat av överensstämmelse med angivna krav, dvs. om en produkt inte uppfyller kraven får den inte tillhandhållas på marknaden. Det innebär att produkter med digitala element måste uppfylla kraven i EU:s cyberresiliensförordning för att kunna tillhandhållas på marknaden.

Både EU:s cyberresiliensförordning och i många fall EU:s produktlagstiftning i övrigt medger samtidigt att produkter för nationell säkerhet och försvarsändamål inte ska omfattas av de vanliga marknadskrav som gäller civila produkter. Detta undantag speglar en etablerad princip i EU-rätten att skyddet av väsentliga säkerhetsintressen enligt bland annat artikel 346 i EUF-fördraget kan motivera undantag från harmoniserade regler¹⁷, vilket till exempel kommer till uttryck i de tidigare angivna undantagen i artikel 2.7 och artikel 2.8. I dessa fall är produkten undantagen från förordningen tillämpningsområde och kraven för tillhandhållande på marknaden är inte tillämpliga i dessa fall.

Tillhandahållande på marknaden

I kommissionens vägledning *Meddelande från kommissionen 2022 års blåbok om genomförandet av EU:s produktbestämmelser* anges att varje utbudande eller överlåtelse som kan leda till att en produkt övergår till en ny användare utgör ett tillhandahållande på marknaden. Efterföljande överlåtelser, till exempel från distributör till slutanvändare, är fortsatta tillhandahållanden. Enligt EU:s harmoniserade terminologi som används i både EU:s cyberresiliensförordning och EU:s marknadskontrollförordning omfattar bestäm-

¹⁷ Flera andra EU-förordningar och direktiv har liknande klausuler. Till exempel undantas radioutrustning "som uteslutande används för verksamhet som rör allmän säkerhet, försvar eller statens säkerhet" från det ordinarie regelverket. Sådan utrustning hanteras utanför de civila produktkraven.

melserna alla former av överlåtelse av produkten från en ekonomisk aktör till en annan, exempelvis försäljning eller uthyrning, så länge det sker i ett affärsmässigt sammanhang. Det avser varje enskild produkt och varje enskild transaktion, inte huruvida produkten marknadsförs brett eller till allmänheten. I praktiken innebär detta att om en tillverkare eller leverantör avtalar om att leverera en produkt till en kund inom EU, till exempel en försvarsmyndighet, så sker ett tillhandahållande på marknaden. Det saknas i sammanhanget betydelse om köparen är en myndighet, eftersom en sådan leverans räknas som att produkten tillhandahålls på unionsmarknaden, under förutsättning att leveransen sker som del av en kommersiell affär.

Tillhandahållandet anses äga rum när produkten ställs till mottagarens förfogande efter tillverkning. Även en begränsad spridningen till en enda myndighet ändrar inte det faktum att produkten gjorts tillgänglig på marknaden i lagens mening. I det fall där till exempel en försvarsmyndighet får produkten direkt från tillverkaren/leverantören, sker utsläppandet och tillhandahållandet samtidigt i och med leveransen. Myndigheten fungerar som slutlig användare, om ingen vidaredistribution är avsedd, vilket bekräftar att produkten är avsedd för slutanvändning på unionsmarknaden, som är ett kriterium för att produkten ska omfattas av begreppet tillhandahållande. Den aktuella produkten betraktas således som tillhandahållen på marknaden enligt de rättsliga definitionerna. Att den upphandlas genom direktavtal av en enda myndighet, till exempel en försvarsmyndighet, utan att finnas allmänt tillgänglig, påverkar inte detta eftersom en kommersiell leverans på den inre marknaden har ägt rum, vilket uppfyller kriteriet för tillhandahållande på marknaden. Produkten måste därmed i princip uppfylla relevanta krav i harmoniserad lagstiftning vid leveransen, bland annat kraven i EU:s cyberresiliensförordning, för att lagligen få släppas ut på marknaden om inte angivna undantag från förordningen är tillämpligt på den berörda produkten.

Utredningen bedömer att det behov av förtydliganden som efterfrågas av några av remissinstanserna när det gäller tillämpningsområdet för ovan angivna EU-förordningar inte kan göras i form av ändring eller komplettering i form av nationell författningsreglering utan eventuella oklarheter i dessa frågor bör lämpligen få sin lösning i rättstillämpningen.

5.7 Överväganden

Utredningens bedömning: Det finns inget behov av att i författning medge undantag från befintliga eller föreslagna bestämmelser med hänsyn till nationell säkerhet eller skydd av andra väsentliga statliga funktioner. EU:s cyberresiliensförordning och nationella regelsystem uppfyller krav på ett högt skydd för den nationella säkerheten och produkter med digitala element.

Utredningen har enligt direktiven att ta ställning till behovet av undantag från befintliga eller föreslagna bestämmelser med hänsyn till nationell säkerhet eller skydd av andra väsentliga statliga funktioner och vid utformningen av förslag noga beakta behovet av att upprätthålla ett högt skydd för den nationella säkerheten och för produkter som har utvecklats uteslutande för ändamål som rör nationell säkerhet eller försvarsändamål. Utredningen har i utredningsarbetet bland annat tagit del av ovan angivna myndigheters synpunkter över utkastet till EU:s cyberresiliensförordning.

Utredningen bedömer att de förslag som utredningen lämnar i den kompletterande lagen eller i övrigt lämnar inte föranleder något behov av författningsändring eller komplettering av författning. Utredningens har till stöd för denna slutsats gjort följande överväganden och bedömning.

Av artikel 2.1 i EU:s cyberresiliensförordning framgår att alla produkter med digitala element som omfattas av förordningen och som uppfyller de angivna väsentliga kraven på cybersäkerhet får tillhandhållas på den inre marknaden. Det innebär att ett stort antal produkter med digitala element får tillhandhållas offentliga och privata användare, till exempel myndigheter och andra aktörer. Produkter som utvecklas eller ändras uteslutande för användning i verksamhet som avser nationell säkerhet eller försvarsändamål får med stöd av artikel 2.7 undantas från förordningens tillämpningsområde. Motsvarande gäller för en produkt med digitala element som utformats specifikt för att behandla säkerhetsskyddsklassificerade uppgifter. Begreppet säkerhetsskyddsklassificerade uppgifter (eng. classified information) i artikel 2.7 omfattar sådana uppgifter som definieras i 1 kap. 2 § säkerhetsskyddslagen (2018:585), men kan även som Säkerhetspolisen framhållit i det ovan angivna yttrandet omfatta fler uppgifter. En produkt som omfattas av angivna undantag kan

tillhandhållas utan att tillverkaren behöver efterleva de skyldigheter som följer av förordningen. Eftersom produkten är avsedd uteslutande för verksamhet som rör nationell säkerhet eller försvarsändamål eller för att behandla säkerhetsskyddsklassificerade uppgifter torde den i detta fall även omfattas av informationssäkerhets- och rapporteringskraven i den nationella säkerhetsskyddslagstiftningen. Utredningen bedömer att den regleringen i de fall den är tillämplig ger ett högt skydd för produkter med digitala element.

I sammanhanget har uppkommit frågan om den närmare innebörden av uttrycket nationell säkerhet (artikel 4.2 FEU) och även uttrycket väsentliga intressen i artikel 346 i EUF. Bland annat har Försvarsmakten och FMV påtalat utmaningen att tolka den närmare innebörden av detta uttryck. Utredningen kan notera att frågan om hur detta uttryck kan förstås har varit föremål för överväganden i flera olika lagstiftningsärenden under åren och regeringen har uttalat att uttrycket nationell säkerhet är ett EU-rättsligt begrepp och den närmare innebörden av begreppet ska därför fastställas av EU-domstolen. Samtidigt ska noteras att artikel 4.2 ger medlemsstaterna rätt att själva definiera vad som avses med medlemsstatens nationella säkerhet. För svenskt vidkommande har regeringen uttalat att i nationell säkerhet inryms uttrycket Sveriges säkerhet, ett uttryck som också behandlas i flera olika lagstiftningsärenden under senare år och som kommer till uttryck i säkerhetsskyddslagstiftningen.

Utredningen bedömer att det i detta sammanhang, även om myndigheternas önskemål om ett förtydligande kan vinna viss förståelse, inte nu finns skäl att föreslå ett avsteg från den princip som kommit till uttryck i angivna lagstiftningsärenden om hur uttrycket kan förstås och tillämpas, eftersom den närmare innebörden av uttrycket, som regeringen också framhållit, inte lämpar sig för fattningsreglering. Det ska samtidigt noteras att verksamhet som har betydelse för Sveriges säkerhet, dvs. säkerhetskänslig verksamhet som omfattas av den nationella säkerhetsskyddsregleringen, får anses röra Sveriges nationella säkerhet i den meningen som avses med begreppet nationell säkerhet i artikel 4.2 FEU.

Utredningen bedömer att det blir därför en fråga för rättstillämpningen att med stöd av EU-domstolens praxis, nationell rättspraxis på säkerhetsskyddsområdet, uttalanden i lagförarbeten samt myndigheternas föreskrifter och allmänna råd bedöma tillämpningsområdet för artikel 4.2 FEU och hur de angivna undantagen i arti-

kel 2.7 och 2.8 i EU:s cyberresiliensförordning kan tillämpas på produkter med digitala element.

Som ovan framgår krävs för ett sådant undantag för en produkt att den utvecklats eller ändrats uteslutande för nationell säkerhet eller för försvarsändamål. Det innebär enligt utredningens bedömning att om produkten även tillhandhålls på marknaden för andra syften än de i artikel 4.2 FEU angivna ändamålen, dvs. utgör produkter med dubbla användningsområden, är undantagen inte tillämpliga på produkten utan tillverkaren ska då följa de bestämmelser som anges i EU:s cyberresiliensförordning. I denna situation kan det uppkomma en skyldighet för tillverkaren att rapportera aktivt utnyttjade sårbarheter produkten enligt artikel 14 i EU:s cyberresiliensförordning till den nationella CSIRT-enheten, och även till Enisa, samtidigt som produkten används i verksamhet som rör Sveriges nationella säkerhet. Som bland annat Försvarsmakten påpekar kan information om sårbarheten röra nationell säkerhet och det kan uppkomma behov av att den inte sprids innan berörda myndigheter kan vidta åtgärder för att reducera riskerna för skador.

I detta sammanhang kan noteras att artikel 16.2 ger den CSIRT-enhet som utsetts till samordnare som först tog emot anmälan möjlighet att under vissa förutsättningar underlåta att sprida anmälan via den gemensamma rapporteringsplattformen till övriga CSIRT-enheter. Under exceptionella omständigheter, särskilt på begäran av tillverkaren och mot bakgrund av känslighetsnivån hos den anmälda information som tillverkaren angett i enlighet med artikel 14.2 a får spridningen av anmälan skjutas upp på grundval av motiverade cybersäkerhetsrelaterade skäl under en tidsperiod som är absolut nödvändig, inbegripet när en sårbarhet är föremål för ett förfarande för samordnad delgivning av information om sårbarheter som avses i artikel 12.1 i direktiv (EU) 2022/2555 (NIS 2).

Vidare anges att under särskilt exceptionella omständigheter, om tillverkaren i den anmälan som avses i artikel 14.2 b anger att

- a) den anmälda sårbarheten aktivt har utnyttjats av en fientlig aktör och att den, enligt tillgänglig information, inte har utnyttjats i någon annan medlemsstat än den där den CSIRT-enhet som utsetts till samordnare finns till vilken tillverkaren har anmält sårbarheten, eller

- b) all omedelbar ytterligare spridning av den anmälda sårbarheten sannolikt skulle leda till tillhandahållande av information vars utlämnande skulle strida mot den medlemsstatens väsentliga intressen, eller
- c) den anmälda sårbarheten utgör en överhängande hög cyber-säkerhetsrisk till följd av den fortsatta spridningen,

ska endast information om att tillverkaren har gjort en anmälan, allmän information om produkten, den allmänna karaktären av utnyttjandet och information om att säkerhetsrelaterade skäl angetts göras tillgänglig samtidigt för Enisa till dess att den fullständiga anmälan sprids till de berörda CSIRT-enheterna och Enisa. Om Enisa på grundval av denna information anser att det finns en systemrisk som påverkar säkerheten på den inre marknaden ska Enisa rekommendera den mottagande CSIRT-enheten att sprida den fullständiga anmälan till de andra CSIRT-enheter som utsetts till samordnare och till Enisa själv.

Utredningen bedömer att regleringen i artikel 16 gäller i de fall artikel 2.8 inte är tillämpliga. Som ovan framgår får ett utlämnande av information om en sårbarhet eller incident i det enskilda fallet underlåtas om det skulle strida mot väsentliga intressen som rör Sveriges nationella säkerhet, allmänna säkerhet eller försvar. Den närmare innebörden av vad som avses med uttrycken nationell säkerhet, allmän säkerhet och försvar har berörts ovan. Sammantaget bedömer utredningen att artikel 2.8 och artikel 16 i EU:s cyberresiliensförordning i förening med den nationella säkerhetsskyddsregleringen medför ett tillräckligt skydd för att uppgifter inte lämnas ut om det strider mot Sveriges väsentliga intressen avseende nationell säkerhet, allmän säkerhet och försvar. Utredningen bedömer att regelsystemet för säkerhetsskydd sammantaget uppfyller kraven på ett högt skydd för den nationella säkerheten och för produkter med digitala element. Det finns därför inget behov av att medge undantag från befintliga eller föreslagna bestämmelser eller ändra befintlig lagstiftning med hänsyn till nationell säkerhet eller skydd av andra väsentliga statliga funktioner.

6 Bestämmelser om bedömning av överensstämmelse

6.1 Inledning

I detta kapitel behandlas bestämmelser i EU:s cyberresiliensförordning som gäller för förfaranden för bedömning av överensstämmelse av produkter med digitala element (avsnitt 6.2–4), anmälan av organ för bedömning av överensstämmelse (avsnitt 6.5), ackreditering av organ för bedömning av överensstämmelse (avsnitt 6.6 och 7), anmälade myndighet (avsnitt 6.8), tillgång till organ för bedömning av överensstämmelse (avsnitt 6.9), åtgärder vid återkallelse av anmälan av organ för bedömning (avsnitt 6.10), övervakning av anmälda organ (avsnitt 6.11) och gränsdragningen mellan Swedac och en marknadskontrollmyndighet (avsnitt 6.12). Vidare behandlas vissa processuella frågor som rör överlämnande av förvaltningsuppgifter till privata organ för bedömning av överensstämmelse (avsnitt 6.13) samt överklagande av beslut av organ för bedömning av överensstämmelse och förvaltningsmyndighet (avsnitt 6.14).

6.2 Väsentliga cybersäkerhetskrav på produkter med digitala element införs (artikel 6)

I artikel 6 i EU:s cyberresiliensförordning föreskrivs att produkter med digitala element som omfattas av förordningens tillämpningsområde får tillhandahållas på marknaden endast om

- a) de uppfyller de väsentliga cybersäkerhetskraven i bilaga I del I, förutsatt att de är korrekt installerade och underhållna och används för avsett ändamål eller under förhållanden som rimligen

kan förutses och, i tillämpliga fall, att de nödvändiga säkerhetsuppdateringarna har installerats, och

- b) de processer som införs av tillverkaren uppfyller de väsentliga cybersäkerhetskrav som fastställs i bilaga I del II.

I artikel 3.1 definieras en produkt med digitala element som en programvaru- eller hårdvaruprodukt och dess lösningar för fjärrbehandling av data, inbegripet programvaru- eller hårdvarukomponenter som släpps ut på marknaden separat.

I skäl 2 i förordningen framhålls att förordningen syftar till att fastställa randvillkor för utvecklingen av säkra produkter med digitala element genom att säkerställa att hårdvaru- och programvaruprodukter som släpps ut på marknaden har färre sårbarheter och att tillverkarna tar säkerheten på allvar under produktens hela livscykel. Den syftar också till att skapa förutsättningar för att användarna ska kunna ta hänsyn till cybersäkerheten när de väljer och använder produkter med digitala element, exempelvis genom att öka transparensen när det gäller stödperioden för produkter med digitala element som släpps ut på marknaden.¹

I bilaga I del I anges produkter med digitala element ska utformas, utvecklas och produceras på ett sådant sätt att de säkerställer en lämplig cybersäkerhetsnivå baserat på riskerna. Vidare anges att på grundval av den bedömning av cybersäkerhetsrisker som avses i artikel 13.2 ska produkter med digitala element uppfylla de krav som anges i bilaga I del I a–m. Tillverkare av produkterna ska också uppfylla de krav på sårbarhetshantering som anges i bilaga I del II 1–8.

När det gäller frågan hur många produkter och tillverkare som berörs av förordningens tillämpningsområde är en sådan bedömning förenad med stor osäkerhet. Frågan behandlas mer ingående i kapitel 15.

¹ I skäl 6 anges att kommissionen bör ge vägledning för att hjälpa ekonomiska aktörer, särskilt mikroföretag och små och medelstora företag, vid tillämpningen av förordningen. Sådan vägledning bör bland annat omfatta dess tillämpningsområde, särskilt distansbehandling av data och dess konsekvenser för utvecklare av programvara med fri och öppen källkod, tillämpningen av de kriterier som används för att fastställa stödperioder för produkter med digitala element, samspelet mellan denna förordning och annan unionsrätt och begreppet väsentlig ändring.

6.2.1 Presumtion om överensstämmelse (artikel 27)

Av artikel 27.1 i EU:s cyberresiliensförordning följer att produkter med digitala element, och processer som införts av tillverkaren, som överensstämmer med harmoniserade standarder, eller delar av sådana, vilka har offentliggjorts i Europeiska unionens officiella tidning, ska förutsättas överensstämma med de väsentliga cybersäkerhetskrav i bilaga I som omfattas av dessa standarder eller delar av dem.²

Vidare följer av artikel 27.8 att produkter med digitala element och processer som har införts av tillverkaren för vilka en EU-försäkran om överensstämmelse eller ett certifikat har utfärdats enligt förordning (EU) 2019/881³ (EU:s cybersäkerhetsakt), ska förutsättas överensstämma med de väsentliga cybersäkerhetskraven i bilaga I i den mån som EU-försäkran om överensstämmelse eller det europeiska cybersäkerhetscertifikatet, eller delar av dessa, täcker dessa krav.

Kommissionen ges i artikel 27.9 befogenhet att anta delegerade akter för att komplettera EU:s cyberresiliensförordning genom att specificera vilka europeiska ordningar för cybersäkerhetscertifiering inom ramen för cybersäkerhetsakten som kan användas för att visa att produkter med digitala element överensstämmer med de väsentliga cybersäkerhetskrav som fastställs i bilaga I till denna förord-

² Kommissionen ska i enlighet med artikel 10.1 i förordning (EU) nr 1025/2012 begära att en eller flera europeiska standardiseringsorganisationer utarbetar harmoniserade standarder för de väsentliga cybersäkerhetskraven i bilaga I till cyberresiliensförordningen. När kommissionen utarbetar begäranden om en sådan standardisering ska den sträva efter att beakta befintliga europeiska och internationella standarder för cybersäkerhet som införts eller håller på att tas fram, i syfte att förenkla utvecklingen av harmoniserade standarder, i enlighet med förordning (EU) nr 1025/2012. Kommissionen får anta genomförandeakter om fastställande av gemensamma specifikationer som omfattar tekniska krav som gör det möjligt att uppfylla de väsentliga cybersäkerhetskraven i bilaga I för produkter med digitala element som omfattas av cyberresiliensförordningens tillämpningsområde. Om en harmoniserad standard antas av en europeisk standardiseringsorganisation och föreslås för kommissionen i syfte att offentliggöra hänvisningen till den i Europeiska unionens officiella tidning, ska kommissionen bedöma den harmoniserade standarden i enlighet med förordning (EU) nr 1025/2012. När en hänvisning till en harmoniserad standard offentliggörs i Europeiska unionens officiella tidning ska kommissionen upphäva de genomförandeakter som avses i punkt 2, eller delar av dem som omfattar samma väsentliga cybersäkerhetskrav som de som omfattas av denna harmoniserade standard. Om en medlemsstat anser att en gemensam specifikation inte helt uppfyller de väsentliga cybersäkerhetskraven i bilaga I ska den underrätta kommissionen om detta genom att lämna en detaljerad förklaring. Kommissionen ska bedöma denna detaljerade förklaring och får vid behov ändra genomförandeakten om fastställande av den gemensamma specifikationen i fråga.

³ Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

ning, eller delar av dessa. Utfärdandet av ett europeiskt cybersäkerhetscertifikat inom ramen för sådana system, med lägst assurancesnivån ”betydande”, befriar tillverkaren från skyldigheten att utföra en tredjepartsbedömning av överensstämmelse för de motsvarande kraven, i enlighet med artikel 32.2 a och b och 32.3 a och b i EU:s cyberresiliensförordning.

6.2.2 EU-försäkran om överensstämmelse (artikel 28)

I artikel 28.1 i EU:s cyberresiliensförordning anges att en EU-försäkran om överensstämmelse ska upprättas av tillverkarna i enlighet med artikel 13.12 och som ska ange att de tillämpliga väsentliga cybersäkerhetskraven i bilaga I uppfylls för produkten med digitala element.

EU-försäkran om överensstämmelse ska enligt artikel 28.2 utformas i enlighet med mallen i bilaga V och ska innehålla de uppgifter som anges i de relevanta förfaranden för bedömning av överensstämmelse som fastställs i bilaga VIII⁴. Om en produkt med digitala element omfattas av mer än en unionsrättsakt där det ställs krav på EU-försäkran om överensstämmelse ska en enda EU-försäkran om överensstämmelse upprättas med avseende på alla dessa unionsrättsakter. I denna försäkran ska det anges vilka unionsrättsakter som berörs, inbegripet publikationshänvisningarna till dem. Genom att EU-försäkran om överensstämmelse upprättas ska tillverkaren ta ansvar för att produkten överensstämmer med digitala element.⁵

6.2.3 Allmänna principer för CE-märkning (artikel 29 och 30)

Allmänna principer för CE-märkning fastställs i förordning (EG) nr 765/2008⁶. Närmare bestämmelser för hur CE-märkningen ska fästas på produkter med digitala element anges i artiklarna 29 och 30 i EU:s cyberresiliensförordning. CE-märkningen ska vara den

⁴ En sådan försäkran ska uppdateras när så är lämpligt. Den ska tillhandahållas på de språk som krävs av den medlemsstat där produkten med digitala element släpps ut på marknaden eller tillhandahålls på marknaden (se kapitel 14).

⁵ Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 61 för att komplettera cyberresiliensförordningen genom att lägga till uppgifter till det minimiinnehåll för EU-försäkran om överensstämmelse som fastställs i bilaga V, för att ta hänsyn till den tekniska utvecklingen (punkten 5).

⁶ Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93.

enda märkning som garanterar överensstämmelse med kraven i cyberresiliensförordningen för produkter med digitala element. CE-märkningen visar att en produkt uppfyller kraven och utgör det synliga resultatet av en process som omfattar en bedömning av överensstämmelse med kraven.

Regler och villkor för anbringande av CE-märkning (artikel 30)

I artikel 30 föreskrivs att CE-märkningen ska fästas på produkten med digitala element så att den är synlig, läsbar och outplånlig. Om detta inte är möjligt eller inte är lämpligt på grund av produktens art, ska den fästas på förpackningen och på den EU-försäkran om överensstämmelse enligt artikel 28 som medföljer produkten med digitala element.⁷

CE-märkningen ska fästas innan produkten med digitala element släpps ut på marknaden. Den får åtföljas av ett piktogram eller annan märkning som anger en särskild cybersäkerhetsrisk eller användning som fastställs i genomförandeakter. Medlemsstaterna ska utgå från befintliga mekanismer för att säkerställa att bestämmelserna om CE-märkning tillämpas korrekt och vidta lämpliga åtgärder i händelse av otillbörlig användning av märkningen.⁸

Teknisk dokumentation (artikel 31)

Av artikel 31 framgår att den tekniska dokumentationen ska omfatta alla relevanta data eller uppgifter om de metoder som tillverkaren använt för att säkerställa att produkter med digitala element och de processer som införts av tillverkaren uppfyller de väsentliga

⁷ För produkter med digitala element i form av programvara ska CE-märkningen fästas antingen på EU-försäkran om överensstämmelse enligt artikel 28 eller på den webbplats som åtföljer programvaruprodukten. I det sistnämnda fallet ska det relevanta avsnittet på webbplatsen kunna nås enkelt och direkt av konsumenterna.

⁸ I de fall då en produkt med digitala element omfattas av annan unionsharmoniseringslagstiftning än cyberresiliensförordningen som också föreskriver CE-märkning ska CE-märkningen visa att produkten även uppfyller kraven som anges i sådan annan unionsharmoniseringslagstiftning. Kommissionen får genom delegerade akter fastställa tekniska specifikationer för etiketter, piktogram eller andra märkningar som rör säkerheten för produkter med digitala element, deras stödperioder och mekanismer för att främja användningen av sådana och öka allmänhetens medvetenhet om säkerheten hos produkter med digitala element.

cybersäkerhetskrav som fastställs i bilaga I. Den ska minst omfatta de aspekter som fastställs i bilaga VII (punkten 1).⁹

Förenklad dokumentation för mikroföretag och små företag (artikel 33)

Mikroföretag och små företag får tillhandahålla alla delar av den tekniska dokumentation som anges i bilaga VII med användning av ett förenklat formulär. För detta ändamål ska kommissionen genom genomförandeakter specificera det förenklade formuläret för teknisk dokumentation med hänsyn till mikroföretagens och småföretagens behov, inbegripet hur de uppgifter som anges i bilaga VII ska tillhandahållas. Om ett mikroföretag eller ett småföretag väljer att tillhandahålla den information som anges enligt bilaga VII på ett förenklat sätt ska det använda angivna formulär och anmälda organ ska godta detta formulär för bedömning av överensstämmelse.

6.3 Bedömning av överensstämmelse av de väsentliga cybersäkerhetskraven (artikel 32)

I beslut nr 768/2008/EG¹⁰ fastställs moduler för bedömning av överensstämmelse, som står i proportion till risknivån och den säkerhetsnivå som krävs. För att säkerställa enhetlighet mellan olika sektorer och undvika ad hoc-varianter baseras förfarandena för bedömning av överensstämmelse på dessa moduler.

Av artikel 32 följer att tillverkaren ska visa överensstämmelse med de väsentliga cybersäkerhetskraven genom att använda

- a) förfarandet för intern kontroll (baserat på modul A) enligt bilaga VIII,
- b) förfarande enligt EU-typkontroll (baserat på modul B) i bilaga VIII, följt av förfarandet för överensstämmelse med EU-typ grundat på intern tillverkningskontroll (baserat på modul C) enligt bilaga VIII,

⁹ Den tekniska dokumentationen ska upprättas innan produkten med digitala element släpps ut på marknaden och ska uppdateras kontinuerligt, vid behov, under åtminstone stödperioden.

¹⁰ Europaparlamentets och rådets beslut nr 768/2008/EG av den 9 juli 2008 om en gemensam ram för saluföring av produkter och upphävande av rådets beslut 93/465/EEG.

- c) överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H) enligt bilaga VIII, eller
- d) i tillämpliga fall förfaranden enligt en europeisk ordning för cybersäkerhetscertifiering enligt artikel 27.9.

Förfarandena för bedömning av överensstämmelse omfattar granskning och kontroll av både produkten och processrelaterade krav som omfattar hela livscykeln för produkter med digitala element, inbegripet dplanering, utformning, utveckling eller produktion, testning och underhåll av produkten med digitala element.

6.3.1 Produkter med digitala element som inte förtecknas som viktiga eller kritiska produkter (artikel 32.1)

Bedömningen av överensstämmelse för produkter med digitala element som inte förtecknas som viktiga eller kritiska produkter med digitala element i EU:s cyberresiliensförordning kan utföras av tillverkaren på eget ansvar i enlighet med förfarandet för intern kontroll baserat på modul A i beslut nr 768/2008/EG i enlighet med cyberresiliensförordningen.¹¹ Inom ramen för det interna kontrollförfarandet säkerställer och försäkrar tillverkaren på eget ansvar att produkten med digitala element och tillverkarens processer uppfyller de tillämpliga väsentliga cybersäkerhetskrav som fastställs i cyberresiliensförordningen.¹² Tillverkaren kan även välja ett striktare förfarande för bedömning av överensstämmelse som involverar tredje part.

6.3.2 Viktig produkt med digitala element (artikel 32)

Viktig produkt med digitala element som omfattas av klass I (artikel 32.2)

Av artikel 32.2 följer att vid bedömningen av om en viktig produkt med digitala element som omfattas av klass I som anges i bilaga III, och de processer som införts av dess tillverkare överensstämmer med

¹¹ Detta förfarande är också tillämpligt i fall där en tillverkare väljer att delvis eller inte alls tillämpa en tillämplig harmoniserad standard, gemensam specifikation eller en tillämplig europeisk ordning för cybersäkerhetscertifiering.

¹² Skäl 91.

de väsentliga cybersäkerhetskraven i bilaga I, gäller att om tillverkaren inte har tillämpat, eller endast delvis har tillämpat, harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering på minst assurancesnivå ”betydande” enligt artikel 27 ska den berörda produkten med digitala element och de processer som införts av tillverkaren genomgå något av följande förfaranden med avseende på dessa väsentliga cybersäkerhetskrav, vilket även gäller om sådana harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering saknas:

- a) EU-typkontroll (baserat på modul B) som anges i bilaga VIII, följd av förfarandet för överensstämmelse med EU-typ grundat på intern tillverkningskontroll (baserat på modul C) enligt bilaga VIII, eller
- b) bedömning av överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H) enligt bilaga VIII.

Viktig produkt med digitala element som omfattas av klass II (artikel 32.3)

Av artikel 32.3 följer att om produkten är en viktig produkt med digitala element som omfattas av klass II enligt bilaga III ska tillverkaren visa överensstämmelse med de väsentliga cybersäkerhetskraven i bilaga I genom att använda något av följande förfaranden:

- a) EU-typkontroll (baserat på modul B) enligt bilaga VIII, följd av förfarandet för överensstämmelse med EU-typ grundat på intern tillverkningskontroll (baserat på modul C) enligt bilaga VIII,
- b) överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H) enligt bilaga VIII, eller
- c) en europeisk ordning för cybersäkerhetscertifiering enligt artikel 27.9 i EU:s cyberresiliensförordning på minst assurancesnivå ”betydande” i enligt EU:s cybersäkerhetsakt, om sådan finns och i tillämpliga fall.

6.3.3 Kritiska produkter med digitala element (artikel 32.4)

I artikel 32.4 anges att kritiska produkter med digitala element som förtecknas i bilaga IV ska visa överensstämmelsen med de väsentliga cybersäkerhetskraven i bilaga I genom:

- a) en europeisk ordning för cybersäkerhetscertifiering i enlighet med artikel 8.1, eller
- b) om villkoren i artikel 8.1 inte är uppfyllda, något av de förfaranden som avses i artikel 32.3.

6.3.4 Produkter som klassificeras som programvara med fri och öppen källkod (artikel 32.5)

Tillverkare av produkter med digitala element som klassificeras som programvara med fri och öppen källkod¹³ och som omfattas av de kategorier som anges i bilaga III ska kunna visa överensstämmelse med de väsentliga cybersäkerhetskraven i bilaga I genom att använda ett av de förfaranden som avses i artikel 32.1, förutsatt att den tekniska dokumentation som avses i artikel 31 görs tillgänglig för allmänheten när dessa produkter släpps ut på marknaden.

6.3.5 AI-system med hög risk (artikel 12)

I artikel 12 i EU:s cyberresiliensförordning anges att produkter med digitala element vilka omfattas av denna förordning och även klassificeras som AI-system med hög risk enligt artikel 6 i förordning (EU) 2024/1689¹⁴ (AI-förordningen) anses överensstämma med de cybersäkerhetskrav som fastställs i artikel 15 i AI-förordningen om:

- a) dessa produkter uppfyller de väsentliga cybersäkerhetskrav som fastställs i bilaga I del I i EU:s cyberresiliensförordning,

¹³ Med programvara med fri och öppen källkod avses programvara vars källkod delas öppet och som tillhandahålls inom ramen för en licens med fri och öppen källkod som ger alla rättigheter att göra den fritt tillgänglig att användas, modifieras och vidare distribueras.

¹⁴ Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

- b) de processer som tillverkaren infört uppfyller de väsentliga cybersäkerhetskrav som fastställs i bilaga I del II i EU:s cyberresiliensförordning, och
- c) uppnåendet av den nivå av cybersäkerhetsskydd som krävs enligt artikel 15 i AI-förordningen visas genom en EU-försäkran om överensstämmelse som utfärdats enligt EU:s cyberresiliensförordning.

För produkter med digitala element och cybersäkerhetskrav som avses i artikel 12.1 ska det relevanta förfarande för bedömning av överensstämmelse som föreskrivs i artikel 43 i AI-förordningen tillämpas. Vid denna bedömning ska anmälda organ som är behöriga att kontrollera överensstämmelsen för AI-system med hög risk inom ramen för AI-förordningen också vara behöriga att kontrollera överensstämmelsen med kraven i bilaga I till EU:s cyberresiliensförordning för AI-system med hög risk inom ramen för cyberresiliensförordningen, förutsatt att dessa anmälda organ uppfyller kraven i artikel 39 i cyberresiliensförordningen och detta har bedömts i samband med anmälningsförfarandet inom ramen för AI-förordningen (punkten 2).

Genom avvikelse från artikel 12.2 i EU:s cyberresiliensförordning ska

- *viktiga produkter* med digitala element som förtecknas i bilaga III till denna förordning, och som omfattas av de förfaranden för bedömning av överensstämmelse som avses i artikel 32.2 a och b och 32.3 i denna förordning, och
- *kritiska produkter* med digitala element som förtecknas i bilaga IV till denna förordning, vilka klassificeras som AI-system med hög risk enligt artikel 6 i AI-förordningen, och som omfattas av förfarandet för bedömning av överensstämmelse som grundar sig på intern kontroll enligt bilaga VI till AI-förordningen,

genomgå de förfaranden för bedömning av överensstämmelse som föreskrivs i EU:s cyberresiliensförordning i den mån som de väsentliga cybersäkerhetskrav som anges i den förordningen berörs.¹⁵

¹⁵ Tillverkare av produkter med digitala element som avses i punkt 1 i denna artikel får delta i de regulatoriska sandlådor för AI som avses i artikel 57 i förordning (EU) 2024/1689 (punkten 4).

6.4 Närmare om förfaranden för bedömning av överensstämmelse (artikel 32)

I detta avsnitt redogörs för förfaranden för bedömning av överensstämmelse som anges i artikel 32 i EU:s cyberresiliensförordning och som beskrivs närmare i bilaga VIII till förordningen.

6.4.1 Intern kontroll baserat på modul A (Bilaga VIII Del 1)

Intern kontroll baserat på modul A är ett förfarande för bedömning av överensstämmelse genom vilket tillverkaren säkerställer och försäkrar på eget ansvar att produkter med digitala element uppfyller alla de väsentliga cybersäkerhetskraven i del I i bilaga I och att tillverkaren uppfyller de väsentliga cybersäkerhetskraven i del II i bilaga I.

Tillverkaren ska upprätta en skriftlig EU-försäkran om överensstämmelse för varje produkt med digitala element i enlighet med artikel 28 och ska kunna uppvisa den tillsammans med den tekniska dokumentationen för de berörda nationella myndigheterna under en period på 10 år efter det att produkten med digitala element har släppts ut på marknaden eller under stödperioden, beroende på vilken period som är längst.¹⁶

6.4.2 EU-typkontroll baserat på modul B (Bilaga VIII Del II)

Tillverkaren får lämna in ansökan om EU-typkontroll till ett valfritt anmält organ för bedömning av överensstämmelse. EU-typkontroll baserat på modul B är den del av ett förfarande för bedömning av överensstämmelse genom vilken ett anmält organ för bedömning av överensstämmelse undersöker den tekniska utformningen och utvecklingen hos produkten med digitala element och de processer för sårbarhetshantering som tillverkaren infört och intygar att en produkt med digitala element uppfyller de väsentliga cybersäkerhetskraven i del I i bilaga I och att tillverkaren uppfyller de väsentliga cybersäkerhetskraven i del II i bilaga I.

¹⁶ I EU-försäkran om överensstämmelse ska det anges för vilken produkt med digitala element den har upprättats. En kopia av EU-försäkran om överensstämmelse ska på begäran göras tillgänglig för berörda myndigheter.

Det anmälda organet ska bland annat granska den tekniska dokumentationen och underlaget för att bedöma om den tekniska utformningen och utvecklingen av produkten med digitala element uppfyller de väsentliga cybersäkerhetskraven i bilaga I del I och om de processer för sårbarhetshantering som tillverkaren infört uppfyller de väsentliga cybersäkerhetskraven i del II.¹⁷

Det anmälda organet ska därefter utarbeta en bedömningsrapport i vilken de åtgärder som utförts och resultatet av dem redovisas.¹⁸ Om typen och även processerna för sårbarhetshantering uppfyller de väsentliga cybersäkerhetskraven i bilaga I ska det anmälda organet utfärda ett EU-typintyg till tillverkaren¹⁹ eller, i annat fall, avslå ansökan om EU-typintyg och informera sökanden om detta samt utförligt motivera avslaget.

Det anmälda organet ska vidare följa med i den tekniska utvecklingen, och om denna tyder på att den godkända typen och processerna för sårbarhetshantering inte längre uppfyller de tillämpliga väsentliga cybersäkerhetskraven i bilaga I ska organet fastställa om det krävs ytterligare undersökningar och underrätta tillverkaren om detta.

Tillverkaren ska å sin sida underrätta det anmälda organ som innehåller den tekniska dokumentationen för EU-typintyget om alla ändringar av den godkända typen och processerna för sårbarhetshantering som kan påverka överensstämmelsen med de väsentliga cybersäkerhetskraven i bilaga I eller villkoren för intygets giltighet. För sådana ändringar krävs ytterligare godkännande i form av ett tillägg till det ursprungliga EU-typintyget.

¹⁷ Det anmälda organet för bedömning av överensstämmelse ska även utföra lämpliga undersökningar och provningar för att, i de fall där tillverkaren har valt att tillämpa lösningarna i de relevanta harmoniserade standarderna eller de tekniska specifikationerna för de krav som anges i bilaga I, kontrollera att de lösningarna har tillämpats på rätt sätt eller, om dessa inte har tillämpats, kontrollera om de lösningar som tillverkaren använt uppfyller de väsentliga cybersäkerhetskraven

¹⁸ Utan att det påverkar det anmälda organets skyldigheter gentemot de anmälade myndigheterna får organet endast offentliggöra hela eller delar av innehållet i rapporten med tillverkarens samtycke.

¹⁹ Intyget ska innehålla tillverkarens namn och adress, slutsatserna av undersökningen, eventuella giltighetsvillkor och de uppgifter som krävs för identifiering av den godkända typen och processerna för sårbarhetshantering. Intyget kan ha en eller flera bilagor. Intyget och bilagorna ska innehålla all information som behövs för att bedöma om de tillverkade eller utvecklade produkterna med digitala element överensstämmer med den undersökta typen och processerna för sårbarhetshantering och för att kontrollera produkter i bruk.

Det anmälda organet ska även regelbundet genomföra revisioner för att säkerställa att processerna för sårbarhetshantering enligt bilaga I del II genomförs på föreskrivet sätt.

Underrättelse till anmälade myndigheter (punkt 9)

Ett anmält organ för bedömning av överensstämmelse ska underrätta sina anmälade myndigheter om de EU-typintyg och tillägg till dessa som det har utfärdat eller återkallat, och det ska periodiskt återkommande eller på begäran ge den anmälade myndigheten tillgång till förteckningen över de intyg och eventuella tillägg till dessa som det har avslagit, tillfälligt återkallat eller på annat sätt belagt med restriktioner.

Varje anmält organ för bedömning av överensstämmelse ska även underrätta de övriga anmälda organen om de EU-typintyg och eventuella tillägg till dessa som det har vägrat utfärda, återkallat eller på annat sätt belagt med restriktioner och, på begäran, om de intyg och tillägg till dessa som det har utfärdat.

Kommissionen, medlemsstaterna och de övriga anmälda organen har rätt att på begäran få en kopia av EU-typkontrollintyget och alla tillägg till det. Kommissionen och medlemsstaterna har också rätt att på begäran få en kopia av den tekniska dokumentationen och av resultaten från de undersökningar som utförts av det anmälda organet.²⁰

Tillverkaren ska för de nationella myndigheterna kunna uppvisa en kopia av EU-typintyget med bilagor och tillägg tillsammans med den tekniska dokumentationen under tio år efter det att produkten med digitala element släpptes ut på marknaden eller under stödperioden, beroende på vilken period som är längst.

²⁰ Det anmälda organet ska spara en kopia av EU-typintyget med bilagor och tillägg samt av den tekniska dokumentationen, inklusive dokumentation från tillverkaren, så länge som intyget är giltigt.

6.4.3 Intern tillverkningskontroll baserat på modul C (Bilaga VIII Del III)

Överensstämmelse med typ som grundar sig på intern tillverkningskontroll baserat på modul C är den del av ett förfarande för bedömning av överensstämmelse genom vilken tillverkaren fullgör föreskrivna skyldigheter i denna del samt säkerställer och försäkrar att de berörda produkterna med digitala element överensstämmer med typen enligt beskrivningen i EU-typintyget och uppfyller de väsentliga cybersäkerhetskraven i bilaga I del I och att tillverkaren uppfyller de väsentliga cybersäkerhetskraven i del II.

Tillverkaren ska i detta fall vidta alla nödvändiga åtgärder för att produktionen och övervakningen av den ska leda till att de tillverkade produkterna med digitala element överensstämmer med den godkända typen enligt beskrivningen i EU-typintyget, med de väsentliga cybersäkerhetskraven i del I i bilaga I och säkerställer att tillverkaren uppfyller de väsentliga cybersäkerhetskraven i del II i bilaga I.

Tillverkaren ska även i dessa fall fästa CE-märkningen på varje enskild produkt med digitala element som överensstämmer med typen enligt beskrivningen i EU typintyget och som uppfyller de föreskrivna kraven. Tillverkaren ska även upprätta en skriftlig försäkran om överensstämmelse för en produktmodell och kunna uppvisa den för de nationella myndigheterna under en period på tio år efter det att produkten med digitala element har släppts ut på marknaden eller under stödperioden, beroende på vilken period som är längst. En kopia av försäkran om överensstämmelse ska på begäran göras tillgänglig för de behöriga myndigheterna.

6.4.4 Fullständig kvalitetssäkring baserat på modul H (Bilaga VIII Del IV)

En bedömning av överensstämmelse med krav som grundar sig på fullständig kvalitetssäkring baserat på modul H är ett förfarande genom vilket tillverkaren fullgör föreskrivna skyldigheter samt säkerställer och försäkrar på eget ansvar att de berörda produkterna med digitala element eller produktkategorierna uppfyller de väsentliga cybersäkerhetskraven i del I i bilaga I och att de processer för sårbarhetshantering som tillverkaren infört uppfyller kraven i del II i bilaga I.

Tillverkaren ska i detta fall tillämpa ett godkänt kvalitetssystem för utformning, utveckling, slutlig produktkontroll och provning av de berörda produkterna med digitala element och för hantering av sårbarheter. Tillverkaren ska även upprätthålla dess effektivitet under hela stödperioden och ska stå under övervakning. Kvalitetssystemet ska säkerställa att produkterna med digitala element uppfyller de väsentliga cybersäkerhetskraven i del I i bilaga I och att de processer för sårbarhetshantering som tillverkaren infört uppfyller kraven i del II i bilaga I. Alla de faktorer, krav och bestämmelser som tillverkaren tagit hänsyn till ska dokumenteras på ett systematiskt och överskådligt sätt i form av skriftliga riktlinjer, förfaranden och anvisningar. Denna dokumentation av kvalitetssystemet ska möjliggöra en enhetlig tolkning av rutiner och kvalitetsåtgärder, såsom program, planer, manualer och protokoll.

Tillverkaren får hos ett valfritt anmält organ för bedömning av överensstämmelse ansöka om att få kvalitetssystemet för de berörda produkterna med digitala element bedömt. Det anmälda organet ska bedöma om kvalitetssystemet uppfyller kraven och ska förutsätta att kraven är uppfyllda i fråga om de delar av kvalitetssäkringssystemet som uppfyller motsvarande specifikationer i den nationella standard genom vilken den relevanta harmoniserade standarden eller de tekniska specifikationerna genomförs.

Det anmälda organet ska genomföra en revision som ska omfatta ett bedömningsbesök i tillverkarens anläggning, om en sådan anläggning finns. Revisionsgruppen ska granska den tekniska dokumentationen för att kontrollera att tillverkaren känner till de tillämpliga kraven som anges i cyberresiliensförordningen och kan utföra de undersökningar som krävs för att säkerställa att produkten med digitala element överensstämmer med kraven. Utöver erfarenhet av kvalitetsledningssystem ska även minst en av revisionsgruppens deltagare ha erfarenhet av bedömning av det aktuella produktområdet och den berörda produkttekniken, och känna till de tillämpliga kraven som anges i cyberresiliensförordningen.

Tillverkaren eller tillverkarens representant ska meddelas beslutet av det anmälda organet. Meddelandet ska innehålla slutsatserna från revisionen och det motiverade bedömningsbeslutet.

Tillverkaren ska åta sig att fullgöra de skyldigheter som är förknippade med det godkända kvalitetssystemet och att upprätthålla det så att det förblir ändamålsenligt och effektivt. Tillverkaren ska även

informera det anmälda organ som har godkänt kvalitetssystemet om alla planerade ändringar av systemet. Det anmälda organet ska bedöma de föreslagna ändringarna och avgöra om ett ändrat kvalitetssystem fortfarande uppfyller de föreskrivna kraven eller om en ny bedömning är nödvändig. Det ska meddela tillverkaren sitt beslut. Meddelandet ska innehålla slutsatserna från undersökningen och det motiverade bedömningsbeslutet.

Anmälda organ för bedömning av överensstämmelse har övervakningsansvar (punkt 4 och 7)

Det anmälda organet för bedömning av överensstämmelse ska övervaka att tillverkaren fullgör de skyldigheter som är förenade med det godkända kvalitetssystemet. Det anmälda organet ska därför regelbundet genomföra revisioner för att säkerställa att tillverkaren vidmakthåller och tillämpar kvalitetssystemet, samt överlämna en revisionsrapport till tillverkaren. För att möjliggöra en bedömning ska tillverkaren ge det anmälda organet tillträde till lokaler för utformning, utveckling, produktion, kontroll, provning och lagring och tillhandahålla all nödvändig information.

Varje anmält organ ska vidare underrätta sin anmälade myndighet om de godkännanden av kvalitetssystem som det har utfärdat eller återkallat och ska regelbundet eller på begäran ge den anmälade myndigheten tillgång till förteckningen över godkännanden som det har vägrat att utfärda, tillfälligt återkallat eller på annat sätt belagt med restriktioner. Varje anmält organ ska även underrätta de övriga anmälda organen för bedömning av överensstämmelse om de godkännanden av kvalitetssystem som det har vägrat utfärda eller tillfälligt eller slutgiltigt återkallat och, på begäran, om de godkännanden av kvalitetssystem som det har utfärdat.

6.5 Anmälan av organ för bedömning av överensstämmelse

6.5.1 Anmälan (artikel 35)

Av artikel 35.1 EU:s cyberresiliensförordning följer att medlemsstaterna ska anmäla vilka organ som fått i uppdrag att utföra bedömningar av överensstämmelse i enlighet med denna förordning till kommissionen och övriga medlemsstater.

6.5.2 Krav på anmälda organ (artikel 39)

I artikel 43.1 EU:s cyberresiliensförordning anges att de anmälade myndigheterna ska endast anmäla de organ för bedömning av överensstämmelse som har uppfyllt kraven i artikel 39.2–12. Av dessa bestämmelser följer att ett organ för bedömning av överensstämmelse bland annat ska vara inrättat i enlighet med nationell rätt och vara juridisk person och vara ett tredjepartsorgan som är oberoende av den organisation eller produkt med digitala element som den bedömer.

6.5.3 Presumtion om överensstämmelse för anmälda organ (artikel 40)

Av artikel 40 i EU:s cyberresiliensförordning framgår att för ett organ för bedömning av överensstämmelse som kan visa att det uppfyller kriterierna i de relevanta harmoniserade standarderna eller delar av dem till vilka hänvisningar har offentliggjorts i Europeiska unionens officiella tidning ska en presumtion om överensstämmelse med kraven i artikel 39 gälla, i den mån som dessa krav omfattas av de tillämpliga harmoniserade standarderna.

6.5.4 Ansökan om anmälan (artikel 42)

I artikel 42 EU:s cyberresiliensförordning anges att ett organ för bedömning av överensstämmelse ska lämna in en ansökan om anmälan till den anmälade myndigheten i den medlemsstat där det är etablerat. Ansökan ska åtföljas av en beskrivning av de bedömningar av överensstämmelse, det eller de förfaranden för bedömning av överens-

stämmelse och den eller de produkter med digitala element som organet anser sig ha kompetens för samt ett ackrediteringsintyg, om det finns ett sådant, som utfärdats av ett nationellt ackrediteringsorgan och där det intygas att organet för bedömning av överensstämmelse uppfyller kraven i artikel 39 i förordningen. Om organet för bedömning av överensstämmelse inte kan uppvisa något ackrediteringsbevis ska det ge den anmälade myndigheten alla de underlag som krävs för kontroll, erkännande och regelbunden tillsyn av att det uppfyller kraven i artikel 39.

Den anmälade myndigheten ska fatta beslut om att anmäla ett organ för bedömning om detta uppfyller kraven för ett sådant organ. Om den anmälade myndigheten avslår en ansökan om anmälan från ett organ för bedömning av överensstämmelse enligt EU:s cyberresiliensförordning, till exempel om det inte kan visa på förekomst av föreskriven kompetens, får beslutet överklagas enligt den nationella ordning som gäller för myndighetens beslut om anmälan av organ för bedömning, dvs. enligt lagen (2011:791) om ackreditering och teknisk kontroll.

6.5.5 Anmälningförfarande (artikel 43)

I artikel 43.1 och 43.2 i EU:s cyberresiliensförordning anges att den anmälade myndigheten ska endast anmäla de organ för bedömning av överensstämmelse som har uppfyllt kraven i artikel 39 i förordningen. Den anmälade myndigheten ska underrätta kommissionen och de andra medlemsstaterna via databasen Nando som utvecklats och förvaltas av kommissionen. Nando är ett elektroniskt anmälningssverktyg som utvecklas och förvaltas av kommissionen och där en förteckning kan hittas över alla anmälda organ.²¹

Anmälan ska innehålla detaljerade uppgifter om bedömningarna av överensstämmelse, modulerna för bedömning av överensstämmelse och de berörda produkterna med digitala element samt ett relevant intyg om kompetens. Om en anmälan inte grundar sig på ett sådant ackrediteringsintyg som avses i artikel 42.2 ska den anmälade myndigheten ge kommissionen och de andra medlemsstaterna de skriftliga underlag som styrker att organet för bedömning av överensstämmelse har erforderlig kompetens och att de system

²¹ Skäl 103.

som behövs för att se till att organet övervakas regelbundet och fortsätter att uppfylla kraven i artikel 39 har inrättats. Det berörda organet får bedriva verksamhet som anmält organ endast om kommissionen eller de andra medlemsstaterna inte har rest några invändningar inom två veckor från anmälan, i de fall då ett ackrediteringsintyg används, eller inom två månader från anmälan, i de fall då ingen ackreditering används. Endast ett sådant organ ska anses vara ett anmält organ vid tillämpning av cyberresiliensförordningen. Kommissionen och övriga medlemsstater ska underrättas om eventuella relevanta senare ändringar av anmälan.

Förteckningar över anmälda organ (artikel 44)

Kommissionen ska tilldela varje anmält organ ett identifikationsnummer. Organet ska tilldelas ett enda sådant nummer även om det anmälts enligt unionsrättsakter. Kommissionen ska offentliggöra förteckningen över de organ som anmälts, inklusive de identifikationsnummer som de har tilldelats och den verksamhet som de har anmälts för. Kommissionen ska säkerställa att denna förteckning hålls aktuell.

Utbyte av erfarenhet (artikel 50)

Kommissionen ska se till att det förekommer utbyte av erfarenhet mellan de myndigheter i medlemsstaterna som ansvarar för riktlinjerna för anmälan av organ för bedömning av överensstämmelse (artikel 50).

Samordning av anmälda organ (artikel 51)

Av konkurrensskäl är det av avgörande betydelse att de anmälda organen tillämpar förfarandena för bedömning av överensstämmelse utan att belasta de ekonomiska aktörerna i onödan. Av samma skäl och för att säkerställa likabehandling av de ekonomiska aktörerna måste en enhetlig teknisk tillämpning av förfarandena för bedömning av överensstämmelse säkerställas. Detta bör bäst uppnås genom lämp-

lig samordning och lämpligt samarbete mellan de anmälda organen.²² Kommissionen ska säkerställa att lämplig samordning och samarbete mellan de anmälda organen införs och att samordningen och samarbetet bedrivs på ett tillfredsställande sätt genom en sektorsövergripande grupp av anmälda organ.

Medlemsstaterna ska säkerställa att de organ som de har anmält deltar i gruppens arbete direkt eller genom utsedda företrädare.

Utredningen bedömer att den anmälade myndigheten bör ha i uppgift att inom ramen för myndighetens ansvarsområde verka för att anmälda organ eller utsedda företrädare deltar i det angivna arbetet (se avsnitt 6.7 och 6.8).

6.5.6 De anmälda organens operativa skyldigheter (artikel 47)

Av artikel 47.1 EU:s cyberresiliensförordning följer att anmälda organ för bedömning av överensstämmelse ska utföra bedömningar av överensstämmelse i enlighet med förfarandena i artikel 32 och bilaga VIII.

Av artikel 47.2 följer att ett organ för bedömning av överensstämmelse även ska utöva sin verksamhet med vederbörlig hänsyn till ett företags storlek, särskilt i fråga om mikroföretag och små och medelstora företag. Vidare ska beaktas bransch, struktur, komplexitet och cybersäkerhetsrisknivån hos produkterna med digitala element och den berörda tekniken samt om produktionsprocessen karaktäriseras som mass- eller serietillverkning. Bedömningar av överensstämmelse ska också utföras på ett proportionellt sätt så att de inte blir onödigt betungande för de ekonomiska aktörerna.

Om ett anmält organ konstaterar att en tillverkare inte uppfyller de krav som anges i bilaga I eller motsvarande harmoniserade standarder eller gemensamma specifikationer som avses i artikel 27, ska det begära att tillverkaren vidtar lämpliga korrigerande åtgärder innan ett intyg om överensstämmelse utfärdas eller, i annat fall, ska ansökan avslås. Om ett anmält organ efter det att ett intyg har utfärdats konstaterar att en produkt med digitala element inte längre uppfyller kraven ska det kräva att tillverkaren vidtar lämpliga korrigerande åtgärder, och vid behov ska intyget tillfälligt eller slutgiltigt återkallas. Om korrigerande åtgärder inte vidtas eller inte får önskad

²² Skäl 105.

effekt ska det anmälda organet, beroende på vad som är lämpligt, begränsa eller tillfälligt, alternativt slutgiltigt, återkalla alla intyg (artikel 47.4).

6.5.7 De anmälda organens informationsskyldighet (artikel 49)

Av artikel 49 i EU:s cyberresiliensförordning följer att de anmälda organen ska underrätta den anmälade myndigheten om följande:

- a) Avslag på ansökan om intyg, eller begränsning, tillfälligt tillbakadragande eller återkallelse av ett intyg.
- b) Omständigheter som inverkar på räckvidden och villkoren för anmälan.
- c) Begäran från marknadskontrollmyndigheterna om information om bedömningar av överensstämmelse.
- d) På begäran, bedömningar av överensstämmelse som gjorts inom ramen för anmälan och all annan verksamhet, inklusive gränsöverskridande verksamhet och underentreprenad.

De anmälda organen ska även ge de andra organ som anmälts, och som utför liknande bedömningar av överensstämmelse som täcker samma produkter med digitala element, relevant information om frågor som rör negativa och, på begäran, positiva resultat av bedömningar av överensstämmelse.

Avgifter för bedömning av överensstämmelse

I artikel 32.6 anges att organ för bedömning av överensstämmelse ska, när de fastställer avgifterna för bedömning av överensstämmelse, ta hänsyn till mikroföretags och små och medelstora företags, inbegripet uppstarts företags, särskilda intressen och behov. Vidare framgår av skäl 96 i EU:s cyberresiliensförordning även att organ för bedömning av överensstämmelse bör tillämpa det relevanta granskningsförfarande och den testning som föreskrivs i förordningen endast när så är lämpligt och enligt en riskbaserad metod.

6.6 Ackreditering av organ för bedömning av överensstämmelse

I artikel 39 i EU:s cyberresiliensförordning finns bestämmelser om vilka krav som organ för bedömning av överensstämmelse som önskar bli anmälda som organ för bedömning ska uppfylla.

I artikel 42 anges att ett organ för bedömning av överensstämmelse ska lämna in en ansökan om anmälan till den anmälade myndigheten i den medlemsstat där det är etablerat. Ansökan ska åtföljas av en beskrivning av de bedömningar av överensstämmelse, det eller de förfaranden för bedömning av överensstämmelse och den eller de produkter med digitala element som organet anser sig ha kompetens för samt ett ackrediteringsintyg, om det finns ett sådant, som utfärdats av ett nationellt ackrediteringsorgan och där det intygas att organet för bedömning av överensstämmelse uppfyller kraven i artikel 39. Om organet för bedömning av överensstämmelse inte kan uppvisa något ackrediteringsbevis ska det ge den anmälade myndigheten alla de underlag som krävs för kontroll, erkännande och regelbunden tillsyn av att det uppfyller kraven i artikel 39.

I skäl 101 i EU:s cyberresiliensförordning framhålls att de nationella myndigheterna bör betrakta öppen ackreditering som föreskrivs i förordning (EG) nr 765/2008 som det bästa sättet att styrka den tekniska kompetensen hos organen för bedömning av överensstämmelse och för att säkerställa den nödvändiga nivån av förtroendet för intyg om överensstämmelse.

EU har antagit gemensamma regler för ackreditering genom EU:s förordning (EG) nr 765/2008 om ackreditering och beslut nr 768/2008/EG av den 9 juli 2008 om en gemensam ram för saluföring av produkter. Vid införandet av EU:s förordning om ackreditering²³ konstaterade kommissionen att ackreditering användes i samtliga medlemsstater, men att det inte hade reglerats på gemenskapsnivå. Bristen på gemensamma bestämmelser hade enligt kommissionen lett till olika tillvägagångssätt och system inom gemenskapen, vilket fått till följd att olika medlemsstater har varit olika strikta vid ackreditering. Kommissionen konstaterade mot den bak-

²³ Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93

grunden att det var nödvändigt att utveckla en heltäckande ram för ackreditering och att på gemenskapsnivå fastställa principer för hur ackrediteringen ska organiseras och genomföras.²⁴

Ackreditering är en kompetensprövning som görs enligt europeiska och internationella standarder. För att bli ackrediterad provas kompetens, rutiner och metoder så att alla kvalitetskrav uppfylls enligt en standard. Syftet med ackreditering är att kunna säkerställa att certifiering, validering, verifiering, kalibrering, kontroll och provning görs med hög kvalitet och god säkerhet för liv, hälsa och miljö. Ackrediteringen innebär kontroller av att uppdragen utförs opartiskt, korrekt och grundas på internationellt erkända standarder.²⁵

Enligt förordning (EG) nr 765/2008 ska varje medlemsstat utse ett enda nationellt ackrediteringsorgan. Av artikel 5 i den angivna förordningen följer att ett nationellt ackrediteringsorgan på begäran av ett organ för bedömning ska utvärdera huruvida organet är kompetent att utföra specifik bedömning av överensstämmelse. Om organet har konstaterats vara kompetent, ska det nationella ackrediteringsorganet utfärda ett ackrediteringsintyg om detta. När en medlemsstat beslutar att inte använda ackreditering ska den förse kommissionen och övriga medlemsstater med de handlingar som krävs för att intyga kompetensen hos de anmälda organ som den utser för genomförandet av relevant harmoniserad gemenskapslagstiftning. Nationella ackrediteringsorgan ska utöva tillsyn över de anmälda organ som de har utfärdat ackrediteringsintyg för. Den nationella ackrediteringen ska generellt vara fri från kommersiell konkurrens och bedrivs som en icke-vinstdrivande aktivitet. Detta gäller oberoende av om ackrediteringen sker på harmoniserade eller icke-harmoniserade områden. Ackrediteringsorganen får inte bedriva verksamhet som konkurrerar med de organ som ackrediteras. Inte heller ska olika länders nationella ackrediteringsorgan aktivt konkurrera med varandra. Kraven på de organ som ackrediterats har också fastställts i standarder.

I Sverige är Swedac utsedd till nationellt ackrediteringsorgan. Det finns i dagsläget ca 1 300 ackrediterade verksamheter i Sverige, varav knappt 40 anmälda organ är kompetensbedömda genom ackreditering. Dessutom är två organ anmälda av Läkemedelsverket en-

²⁴ Skäl 10 i EU:s förordning om ackreditering.

²⁵ <https://www.swedac.se/tjanster/ackreditering/> (hämtad 2025-10-10).

ligt regelverket för medicintekniska produkter och därmed inte ackrediterade.²⁶

6.7 Ackreditering bör ligga till grund för anmälan

Utredningens förslag: I Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och upphävande av förordning (EEG) nr 339/93 och i lagen (2011:791) om ackreditering och teknisk kontroll finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse.

Bestämmelser om ackreditering och anmälan av organ för bedömning av överensstämmelse finns i lagen (2011:791) om ackreditering och teknisk kontroll och i föreskrifter som har meddelats i anslutning till den lagen.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om förfarandena vid bedömning, utseende och anmälan av organ för bedömning och för övervakning av dessa enligt artikel 39–43 samt anmälda organs informations-skyldighet enligt artikel 49 och deltagande i sektorsövergripande grupp enligt artikel 51 i EU:s cyberresiliensförordning.

I förordning (EG) nr 765/2008 och lagen (2011:791) om ackreditering och teknisk kontroll finns bestämmelser inom det område som EU:s cyberresiliensförordning tillämpas. I den senare lagen följer att organ för bedömning ska vara ackrediterade om inte annat föreskrivs.

Av artikel 36.2 i EU:s cyberresiliensförordning framgår att medlemsstaterna får bestämma att den bedömning, utseende och övervakning som avses i artikel 36.1 ska utföras av ett nationellt ackrediteringsorgan i den mening som avses i, och i enlighet med, förordning (EG) nr 765/2008.

I och med att EU:s cyberresiliensförordning förordar en öppen ackreditering och att organen för bedömning av överensstämmelse bör vara ackrediterade enligt förordning (EG) nr 765/2008 ska en sådan ordning i första hand övervägas. Utredningen behöver därför

²⁶ Betänkande *Anpassningar till AI-förordningen Säker användning, effektiv kontroll och stöd för innovation* (SOU 2025:101), s. 311.

ta ställning till om Sverige ska använda sig av ackreditering för anmälan av organ enligt EU:s cyberresiliensförordning.

I sammanhanget kan noteras att i Sverige är nuvarande huvudregel att bedömning och övervakning av anmälda organ sker av Swedac genom ackreditering för de områden där Swedac är anmälande myndighet. Vid anmälningsförfaranden enligt samtliga av dessa rättsakter, förutom beträffande EU:s förordningar om medicintekniska produkter, bedöms och övervakas anmälda organ genom ackreditering. Bedömning genom ackreditering har således använts nationellt under lång tid och regeringen konstaterade även i samband med att svensk lag anpassades till EU:s förordning om ackreditering att det svenska systemet var anpassat till de krav som ställdes på ackreditering i förordningen.²⁷ De regler som behövs för att ackreditera organ enligt EU:s cyberresiliensförordning finns också på plats, vilket utgör ytterligare skäl för att använda ackreditering.²⁸

Utredningen bedömer sammantaget att det är lämpligt att ackreditering används för att bedöma och övervaka de organ som ska anmälas enligt EU:s cyberresiliensförordning. Denna ordning följer även direkt av bestämmelserna i 7–9 §§ lagen (2011:791) om ackreditering och teknisk kontroll. Någon ytterligare reglering i detta avseende behövs därför inte.

Det kan dock finnas behov av att i lagen med kompletterande bestämmelser till EU:s cyberresiliensförordning införa en upplysningsbestämmelse som anger att bestämmelser om ackreditering och anmälan finns i förordning (EG) nr 765/2008 och i lagen (2011:791) om ackreditering och teknisk kontroll.

Vidare bör regeringen eller den myndighet regeringen utser bemyndigas att meddela de ytterligare föreskrifter om ackreditering och anmälan som kan behövas samt om anmälda organs informationskyldighet enligt artikel 49 och deltagande i sektorsövergripande grupp enligt artikel 51 i EU:s cyberresiliensförordning.

²⁷ Prop. 2010/11:80 s. 51.

²⁸ I Europaparlamentets och rådets beslut 768/2008/EG fastställs gemensamma principer och referensbestämmelser som kan användas för harmoniserad unionsslagstiftning. Bestämmelser i EU:s cyberresiliensförordning om anmälande myndigheter, anmälda organ och förfaranden för bedömning av överensstämmelse har mycket stora likheter med referensbestämmelserna i beslutet. De är också i princip identiska med bestämmelserna i EU:s marknadskontrollförordning. EU:s marknadskontrollförordningen kompletteras genom lagen om ackreditering och teknisk kontroll och den tillhörande förordningen samt genom de föreskrifter och allmänna råd som Swedac har utfärdat.

6.8 Anmälade myndighet

Utredningens förslag: Den myndighet som regeringen bestämmer är anmälade myndighet enligt EU:s cyberresiliensförordning.

Utredningens bedömning: Styrelsen för ackreditering och teknisk kontroll är anmälade myndighet enligt artikel 36 i EU:s cyberresiliensförordning.

Styrelsen för ackreditering och teknisk kontroll får meddela föreskrifter om förfarandena vid bedömning, utseende och anmälan av organ för bedömning och för övervakning av dessa enligt artikel 39–43 samt anmälda organs informationsskyldighet enligt artikel 49 och deltagande i sektorsövergripande grupp enligt artikel 51 i EU:s cyberresiliensförordning.

I skäl 99 till EU:s cyberresiliensförordning anges att det system som fastställs i förordningen bör kompletteras av ackrediterings-systemet enligt förordning (EG) nr 765/2008. Vidare anges att eftersom ackreditering är ett viktigt verktyg för att kontrollera kompetensen hos organen för bedömning av överensstämmelse bör det också användas för anmälningssyften. För att säkerställa en enhetlig kvalitetsnivå vid bedömning av överensstämmelse för produkter med digitala element måste också krav fastställas för de anmälade myndigheterna och andra organ som är involverade i bedömningen, anmälan och övervakningen av anmälda organ.

Av artikel 36.1 framgår att varje medlemsstat ska utse en anmälade myndighet med ansvar för att inrätta och genomföra de förfaranden som krävs vid bedömning, utseende och anmälan av organ för bedömning av överensstämmelse och vid kontroll, inklusive överensstämmelse med artikel 41. Vidare följer av artikel 36.2 att medlemsstaterna får besluta att den bedömning och övervakning som ska utföras får ske av ett nationellt ackrediteringsorgan i enlighet med förordning (EG) nr 765/2008.

I artikel 37 i EU:s cyberresiliensförordning anges de krav som en anmälade myndighet ska uppfylla. Om den anmälade myndigheten delegerar eller på annat sätt överlåter den bedömning, anmälan eller övervakning till ett organ som inte är offentligt, ska detta organ vara en juridisk person och i tillämpliga delar följa artikel 37. Detta organ ska dessutom ha vidtagit åtgärder för att täcka det an-

svar som följer av dess verksamhet. Den anmälade myndigheten ska ta fullt ansvar för de uppgifter som utförs av ett sådant organ.

Swedac är i dagsläget anmälade myndighet inom samtliga områden utom för det medicintekniska området. Swedac anmäler således i princip alla organ och det gäller oberoende av vilken sakkunskap som krävs.

Med hänsyn till de kriterier som EU:s cyberresiliensförordning ställer upp på organisationen hos den anmälade myndigheten (se artikel 37) är det i och för sig möjligt att överväga även andra myndigheter än Swedac, till exempel en myndighet som i andra avseenden får ett större ansvar enligt EU:s cyberresiliensförordning.

Utredningen föreslår i kapitel 9 att Post- och telestyrelsen (PTS) ska utses till ansvarig marknadskontrollmyndighet enligt EU:s cyberresiliensförordning. Med utgångspunkten att koncentrera och samla nödvändig kunskap om cybersäkerhet och EU:s cyberresiliensförordning på så få myndigheter som möjligt kan även PTS övervägas som anmälade myndighet. Även med utgångspunkt i verksamheten i det nationella cybersäkerhetscentret vid Försvarets radioanstalt och Försvarets materielverks roll som nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt skulle dessa myndigheter kunna komma i fråga som anmälade myndighet. Det finns dock enligt utredningen flera skäl som talar emot en sådan lösning, bland annat har ingen av dessa myndigheter tidigare bedrivit verksamhet som anmälade myndighet av ackrediterade organ och skulle behöva bygga upp en sådan kompetens. Vidare har antalet anmälade myndigheter i Sverige hittills begränsats till två, och Swedac har organisation och kunskap om såväl anmälandeförfaranden som tillämpning av unionsrättslig reglering.

Utredningen föreslår dessutom att bedömningen av om ett organ för bedömning av överensstämmelse uppfyller kraven för anmälan som huvudregel bör ske genom ackreditering (se ovan avsnitt 6.7). Det förfarande för bedömning, utseende och anmälan som ska ske enligt EU:s cyberresiliensförordning skiljer sig dessutom inte nämnvärt från den uppgift Swedac redan utför på andra områden. Swedac har även i dag i uppgift att ansvara för ackreditering av organ för bedömning av överensstämmelse enligt EU:s cybersäkerhetsakt. Utredningen bedömer att Swedac i sin verksamhet redan möter de krav som ställs på en myndighet som utses till anmälade myndighet enligt artikel 37 i EU:s cyberresiliensförordning.

Sammantaget bedömer utredningen mot bakgrund av den kunskap och erfarenhet Swedac besitter som anmälände myndighet, att Swedac är lämplig myndighet och har förutsättningar att vara anmälände myndighet även enligt EU:s cyberresiliensförordning, vilket talar för att myndigheten bör utses att vara anmälände myndighet.

Utredningen föreslår därför att Swedac bör vara anmälände myndighet enligt EU:s cyberresiliensförordning och ansvara för att utse och anmäla alla anmälda organ enligt den förordningen.

I den kompletterande lagen till EU:s cyberresiliensförordning bör därför anges att den myndighet som regeringen bestämmer ska vara anmälände myndighet enligt cyberresiliensförordningen.

Regeringen bör i den kompletterande förordningen till lagen ange att Swedac ska vara anmälände myndighet. Medlemsstaterna ska enligt artikel 38.1 informera kommissionen om sina förfaranden för bedömning och anmälan av organ för bedömning av överensstämmelse och för övervakning av anmälda organ samt om eventuella ändringar. Det följer av uppgiften som anmälände myndighet att Swedac fullgör uppgiften att informera kommissionen. Kommissionen ska offentliggöra informationen.

Swedac bör ges möjlighet att meddelas kompletterande föreskrifter om förfarandena vid bedömning, utseende och anmälan av organ för bedömning och för övervakning av dessa enligt artikel 39–43 samt anmälda organs informationsskyldighet enligt artikel 49 och deltagande i sektorsövergripande grupp enligt artikel 51 i EU:s cyberresiliensförordning.

6.9 Tillgång till organ för bedömning av överensstämmelse

Utredningens bedömning: Hur tillgång till nationella organ för bedömning av överensstämmelse kan säkerställas och att organen har tillgång till cybersäkerhetskompetens behöver utredas närmare.

Utredningens förslag: Post-och telestyrelsen ska ges i uppdrag att undersöka hur en ordning som bidrar till att säkerställa tillgången på organ för bedömning av överensstämmelse senast den senast den 11 december 2026 kan utformas.

Av artikel 35.2 i EU:s cyberresiliensförordning framgår att medlemsstaterna ska sträva efter att senast den 11 december 2026 säkerställa att det finns ett tillräckligt antal anmälda organ i unionen för att utföra bedömningar av överensstämmelse, i syfte att undvika flaskhalsar och hinder för marknadstillträde. Kommissionen bör sträva efter att hjälpa medlemsstaterna och andra berörda parter i detta arbete.²⁹

I detta sammanhang väcks även frågan om hur Sverige nationellt kan säkerställa att det finns tillgängliga anmälda organ för bedömning av överensstämmelse även när tillgången till sådana organ på den inre marknaden skulle begränsas eller helt upphöra, till exempel under kris och höjd beredskap.

I det uppdrag som utredningen gett till företaget Governo AB har ingått att analysera vissa frågor kring det nuvarande läget och de utmaningar som finns vad avser nationell tillgång på organ för bedömning av överensstämmelse enligt EU:s cyberresiliensförordning. I uppdraget har ingått att beskriva och analysera vilka typer av organ för bedömning av överensstämmelse som kan behövas i Sverige för att möta kommande behov, vad en eventuell brist på organ skulle innebära för svenska tillverkare och om det finns ett behov av statliga insatser för att stimulera fler aktörer att bli organ för bedömning av överensstämmelse.

Sammantaget framkommer av rapporten bland annat följande.

Organ för bedömning av överensstämmelse spelar en avgörande roll i att säkerställa att produkter, främst viktiga produkter i klass två och kritiska produkter, uppfyller de cybersäkerhetskrav som ställs enligt lagstiftningen. För att kunna bedriva verksamhet som organ för bedömning av överensstämmelse måste företagen bland annat ha personal med tillräcklig teknisk kunskap och kännedom om de väsentliga cybersäkerhetskraven och tillämpliga harmoniserade standarder på området.

Många tillverkare kommer inledningsvis, sannolikt samtidigt, att behöva genomföra bedömning av överensstämmelse och anlita anmälda organ. Efterfrågan på sådana organ bedöms därför inledningsvis vara stor, vilket kan leda till flaskhalsar och längre väntetider, främst vad avser viktiga produkter i klass två och kritiska produkter, som kräver bedömning av överensstämmelse. Samtidigt kommer det inte finnas en skyldighet för tillverkare att genomföra en tredjeparts-

²⁹ Skäl 95.

bedömning av överensstämmelse om ett europeiskt cybersäkerhetscertifikat har utfärdats enligt europeiska ordningar för cybersäkerhetscertifiering, på åtminstone assurancesnivån betydande, i de fall produktkategorin har pekats ut i en delegerad akt. Detta skulle möjligen kunna minska behovet av organ för bedömning av överensstämmelse på marknaden på sikt. Detsamma gäller för tillverkare som tillämpar harmoniserade standarder, samtidigt som avsaknad av standarder medför att tillverkare, som annars endast hade behövt genomföra en bedömning av överensstämmelse enligt modul A, i detta fall måste tillämpa andra moduler på samma sätt som viktiga produkter i klass två. Tidpunkten för när harmoniserande standarder är på plats blir därmed också avgörande för behovet av organ för bedömning av överensstämmelse, när bestämmelserna träder i kraft. Vidare påverkas frågan om anmälda organ av hur EU:s cyberresiliensförordning förhåller sig till AI-förordningen. Anmälda organ som är behöriga att bedöma överensstämmelse för AI-system med hög risk inom ramen för cyberresiliensförordningen kommer även vara behöriga att bedöma överensstämmelser enligt den senare förordningen, vilket bör kunna minska behovet av organ för bedömning av överensstämmelse enligt EU:s cyberresiliensförordning, även om tillgången till sådana organ enligt AI-förordningen är under utveckling.

I rapporten identifieras tre svenska ackrediterade organ för bedömning av överensstämmelse med kompetens inom cybersäkerhet. Det finns indikationer på att fler svenska företag kan antas vara intresserade av att ta sig an uppgiften att vara organ för bedömning av överensstämmelse enligt EU:s cyberresiliensförordning.³⁰ Det finns även andra svenska företag inom cyberområdet med tillräckliga kompetens och resurser för att vara intresserade av rollen som anmält organ för bedömning av överensstämmelse enligt EU:s cyberresiliensförordning.

Utbudet av organ för bedömning av överensstämmelse kan antas öka eftersom det med största sannolikhet kommer finnas en efterfrågan på deras tjänster. Ett flertal företag som i dag har kom-

³⁰ Ett exempel som anges är RISE (RISE Research Institutes of Sweden), som är ett statligt ägt forskningsinstitut och innovationspartner, och som i sitt remissyttrande avseende EU:s cybersäkerhetsakt bedömde att bolaget kan spela en central roll när olika certifieringsordningar ska implementeras. RISE såg då en möjlighet att agera som organ för bedömning av överensstämmelse på både lägre och högsta assurancesnivå och som utvärderare/granskare genom tillgången till institutets testlaboratorier. RISE är även ett ackrediterat organ inom ramen för EU:s radioutrustningsdirektiv (2014/53/EU) och kan vara intresserad av att behålla den rollen.

petens inom cybersäkerhet eller inom närliggande områden kan antas vara intresserade av att utveckla sin verksamhet för att kunna genomföra bedömningar av överensstämmelse. Det finns exempelvis i dag sju ackrediterade svenska organ inom området "Ledningssystem för informationssäkerhet", vilket visar på en kompetens inom närliggande områden. Även redan existerande organ på marknaden som har väletablerade processer för modulförfaranden liknande de som krävs inom ramen för EU:s cyberresiliensförordning kan vara intresserade av att utveckla en kompetens inom cybersäkerhet. Genom att bygga på sina befintliga styrkor och anpassa sig till de nya krav som ställs kan dessa organ positionera sig för att bättre tillgodose marknadens behov i framtiden.

I rapporten görs samtidigt bedömningen att det är komplicerat att uppskatta i vilken utsträckning företag kommer anpassa sin verksamhet för att ta en roll som organ för bedömning av överensstämmelse. Med största sannolikhet kommer det att finnas en efterfrågan på tjänster från både svenska tillverkare och företag från andra EU-länder, vilket rimligtvis bör utgöra ett starkt incitament för dessa aktörer. Men att bygga upp kompetens, system och processer är både resurskrävande och innebär ett risktagande. Kontakter som tagits inom ramen för uppdraget visar att många företag i dagsläget är osäkra på hur marknaden kan utvecklas, bland annat då harmoniserade standarder behöver tas fram på området, och därför avvaktar med sina investeringsbeslut. Om staten ser behov av att öka tillgången på svenska organ för bedömning av överensstämmelse så skulle en tänkbar åtgärd för att komplettera marknadens utbud möjligen kunna vara att etablera ett organ för bedömning av överensstämmelse hos en svensk myndighet, till exempel Försvarets materielverk (FMV) eller PTS, dock har dessa möjligheter inte närmare undersökts och vilka förutsättningar som finns för en sådan lösning, och FMV har för sin del angett att myndigheten är tveksam till om det vore en lämplig lösning.

I rapporten görs bedömningen att den tid det tar för ett företag att bli ackrediterat spelar en central roll. Avsaknaden av standarder och etablerad praxis för ackreditering inom nya områden kan innebära en tidskrävande bedömningsprocess, vilket kan fördröja ett växande utbud av organ för bedömning av överensstämmelse på den svenska marknaden.

I rapporten görs vidare bedömningen att konsekvenserna av en potentiell brist på svenska organ för bedömning av överensstämmelse kan innebära att anmälda organ tvingas prioritera vissa produktgrupper, att tillverkare riskerar förseningar i marknadstillträde och att mindre aktörer hamnar i underläge om de inte är ute i god tid. En annan möjlig konsekvens av ett initialt stort behov av organ för bedömning av överensstämmelse är att svenska tillverkare kommer att vända sig till organ i andra EU-länder.

Sammantaget framkommer av rapporten att det vid ikraftträdande av EU:s cybersäkerhetsförordning sannolikt kommer att finnas ett underskott av organ för bedömning av överensstämmelse på den svenska marknaden. Det kommer därför att behövas informationsinsatser från statliga aktörer för att stimulera fler aktörer att bli organ för bedömning av överensstämmelse.

Utredningen bedömer mot bakgrund av det ovan angivna att PTS som föreslagen marknadskontrollmyndighet är den myndighet som är lämpligast för att undersöka vilka åtgärder som bör vidtas som bidrar till att säkerställa tillgången på organ för bedömning av överensstämmelse. Myndigheten ska därför ges ett sådant uppdrag, som bör redovisas senast den 11 december 2026.

Utredningen behandlar i avsnitt 9.7 även frågan om hur vilka åtgärder som kan behövas för att säkra tillgång på cybersäkerhetskompetens hos organ för bedömning av överensstämmelse.

6.10 Åtgärder vid återkallelse av anmälan av organ för bedömning

Utredningens bedömning: Kravet att medlemsstaten ska vidta lämpliga åtgärder för att säkerställa att ett anmält organs ärenden kan behandlas av ett annat anmält organ behöver utredas.

Utredningens förslag: Styrelsen för ackreditering och kontroll ska ges i uppdrag att föreslå lämpliga åtgärder för att säkerställa att ett anmält organs ärenden kan behandlas av ett annat anmält organ.

Av artikel 46.1 i EU:s cyberresiliensförordning framgår att kommissionen ska undersöka alla fall där den hyser tvivel, eller där den upplysts om sådana tvivel, om ett anmält organs kompetens eller ett anmält organs fortsatta uppfyllande av de krav och skyldigheter som det omfattas av. Den anmälade medlemsstaten ska på begäran ge kommissionen all information om grunderna för anmälan eller det berörda organets fortsatta kompetens.

Kommissionen ska säkerställa att all känslig information som den erhåller under sina undersökningar behandlas konfidentiellt. Om kommissionen konstaterar att ett anmält organ inte uppfyller eller inte längre uppfyller kraven för anmälan ska den meddela detta till den anmälade medlemsstaten och anmoda medlemsstaten att vidta erforderliga korrigerande åtgärder, till exempel vid behov återta anmälan.

Om en anmälade myndighet har konstaterat eller har informerats om att ett anmält organ inte längre uppfyller de krav som anges i artikel 39 eller att det underlåter att fullgöra sina skyldigheter ska myndigheten i förekommande fall, beroende på hur allvarlig underlåtenheten att uppfylla kraven eller fullgöra skyldigheterna är, begränsa anmälan eller återkalla den tillfälligt eller slutgiltigt. Den ska omedelbart informera kommissionen och de andra medlemsstaterna om detta (artikel 45.1).

I händelse av begränsning eller tillfällig eller slutgiltig återkallelse av anmälan eller om det anmälda organet har upphört med verksamheten ska den anmälade medlemsstaten vidta lämpliga åtgärder för att säkerställa att det anmälda organets ärenden antingen behandlas av ett annat anmält organ eller hålls tillgängliga för de ansvariga anmälade myndigheterna och marknadskontrollmyndigheterna på deras begäran (artikel 45.2).

Utredningen bedömer att kravet att den anmälade medlemsstaten ska vidta lämpliga åtgärder för att säkerställa att det anmälda organets ärenden antingen behandlas av ett annat anmält organ eller hålls tillgängliga för de ansvariga anmälade myndigheterna och marknadskontrollmyndigheterna väcker ett antal rättsliga frågeställningar. Kravet att angivna ärenden hålls tillgängliga för berörda myndigheter bedöms kunna mötas inom ramen för den befintlig författningsregleringen.

Däremot väcker kravet att medlemsstaten ska vidta lämpliga åtgärder för att säkerställa att det anmälda organets ärenden be-

handlas av ett annat anmält organ ett antal frågor, bland annat hur medlemsstaten ska kunna säkerställa ett annat anmält organ behandlar ett sådant ärende.

En sådan ordning förutsätter att det redan finns ett befintligt organ för bedömning av överensstämmelse med motsvarande kompetensområde som angivna ärenden avser. Vidare måste organet för bedömning frivillig åta sig angivna ärenden eftersom det i dag saknas rättsliga förutsättningar för en tvingande överföring av sådana ärenden.

Utredningen bedömer att frågan om en nationell ordning för att få organ för bedömning av överensstämmelse att på frivillig väg möta angivna krav behöver utredas, bland annat om det finns någon begränsning i att organet för bedömning till vilket ett ärende överlämnas ska vara svenskt eller inte. Även formerna för hur ett överlämnande till ett sådant organ kan ske kan variera beroende på de förutsättningar som råder, till exempel om det förutsätter ett offentligt upphandlingsförfarande eller beslut i annan form. Även formerna för ett hur ett beslut om överlämnande ska fattas bör utredas, dvs. vilken myndighet eller annan aktör som bör besluta i dessa fall. Utredningen bedömer att dessa frågeställningar bör analyseras av Swedac, som bör få i uppdrag att undersöka hur en sådan ordning skulle kunna utformas.

6.11 Övervakning av anmälda organ

Utredningens bedömning: I lagen (2011:791) om ackreditering och teknisk kontroll finns nationell författningsreglering om tillsyn och sanktioner som kompletterar förordning (EG) nr 765/2008. Det finns därför inte behov av att införa någon ny kompletterande reglering på detta område.

I artikel 36.1 anges att anmälande myndighet ska ha ansvar för att inrätta och genomföra de förfaranden som krävs vid bedömning, utseende och anmälan av organ för bedömning av överensstämmelse och vid kontroll av dessa organ.

I 1 § lagen (2011:791) om ackreditering och teknisk kontroll anges att denna lag kompletterar förordning (EG) nr 765/2008, när det gäller ackreditering och CE-märkning. Denna lag tillämpas

också bland annat beträffande organ som anmäls till Europeiska kommissionen och de andra medlemsstaterna för uppgifter i samband med bedömning av överensstämmelse enligt harmoniserad unionslagstiftning. Enligt 2 § ska vid tillämpningen av denna lag gälla de definitioner som finns i förordning (EG) nr 765/2008.

Lagen (2011:791) om ackreditering och teknisk kontroll innebär att svensk rätt anpassas till förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter när det gäller ackreditering och CE-märkning.

I 3 § anges att bedömning av överensstämmelse och annan teknisk kontroll utförs enligt denna lag av eller under medverkan av ackrediterade organ eller organ som avses i 1 § andra stycket 1 och 2 om kontrollen (1) är föreskriven i lag eller annan författning, (2) har ålagts någon genom beslut av en myndighet, eller (3) efter slutförandet har särskilda rättsverkningar enligt lag eller annan författning.

I 4 § anges att Swedac, som utsetts att vara nationellt ackrediteringsorgan, ansvarar för ackreditering enligt förordning (EG) nr 765/2008.

Av 5 § följer att Swedac beslutar i fråga om ackreditering enligt artikel 5.1 i förordning (EG) nr 765/2008. Ackreditering beviljas genom utfärdande av ackrediteringsintyg. Ackrediteringsintyg gäller för viss tid eller tills vidare och ska innehålla de villkor som gäller för ackrediteringen.

I 6 § anges att Swedac beslutar om begränsning eller återkallelse av ett ackrediteringsintyg enligt artikel 5.4 i förordning (EG) nr 765/2008. Swedac får bestämma att ett beslut om begränsning eller återkallelse av ackrediteringsintyg ska gälla med omedelbar verkan. Organ som ska anmälas till Europeiska kommissionen och de andra medlemsstaterna.

Av 7 § följer att om ett organ för bedömning av överensstämmelse begär att få bli utsett och anmält för uppgifter i samband med bedömning av överensstämmelse, ska Swedac i samråd med berörda myndigheter avgöra om organet uppfyller kraven för den uppgift som anmälan avser enligt bland annat harmoniserad unionslagstiftning. I dessa fall ska Swedacs bedömning ske genom ackreditering, om inget annat är föreskrivet.

Enligt 8 § ska Swedac fatta beslut att utse organ för anmälan som uppfyller förutsättningarna enligt 7 §.

När ett organ har utsetts enligt 8 § för uppgifter enligt 7 § första stycket 1, ska Swedac anmäla organet till Europeiska kommissionen

och de andra medlemsstaterna, samt underrätta Europeiska kommissionen och de andra medlemsstaterna om ändringar i anmälan (9 §).

Swedac får besluta att begränsa eller, tillfälligt eller helt, återkalla en anmälan enligt 9 § om det anmälda organet inte längre uppfyller kraven för att få utföra de uppgifter som det anmälts för, eller allvarligt har underlåtit att fullgöra sina skyldigheter. Swedac får bestämma att ett beslut om begränsning eller återkallelse av en anmälan av ett organ ska gälla med omedelbar verkan (10 §).

Av 14 § framgår att bestämmelser om CE-märkning finns i artikel 30.1–30.5 i förordning (EG) nr 765/2008 och rättsakter som har utformats för vissa produkter i enlighet med rådets resolution av den 7 maj 1985 om en ny metod för teknisk harmonisering och standarder.³¹

I 18 § anges att Swedac utövar tillsyn över de organ som avses i denna lag eller i de föreskrifter som har meddelats med stöd av lagen.

Av 19 § följer att Swedac har rätt att hos de organ som omfattas av tillsynen på begäran få tillträde till lokaler samt få tillgång till upplysningar och handlingar i den utsträckning som behövs för tillsynen.

I 21 § anges att ackrediterade organ eller organ som bedöms enligt 7 § ska betala avgift till Swedac för att täcka kostnaderna för ackreditering, tillsyn och bedömning.

I 22 § föreskrivs att den som befattar sig med ett ärende enligt denna lag får inte obehörigen röja eller utnyttja vad han eller hon därvid fått veta om någons affärs- eller driftförhållanden. I det allmännas verksamhet tillämpas i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400).

I 23 § föreskrivs att Swedac får besluta att ta ut en sanktionsavgift av den som oriktigt har uppgett sig vara ackrediterad eller

³¹ Av 15 § framgår att CE-märkning av en produkt får göras endast

1. om märkningen står i överensstämmelse med de i 14 § angivna rättsakterna, och
2. om, när rättsakten utgörs av direktiv, föreskrifter om märkningen finns i lag eller annan författning som genomför direktivet.

Skyldighet att vidta rättelse

16 § Om en produkt har CE-märkts trots att den inte överensstämmer med de krav som gäller för CE-märkning, ska den som ansvarar för CE-märkningen omedelbart vidta rättelse så att överträdelsen upphör.

Ansvar

17 § Den som med uppsåt eller av oaktsamhet bryter mot 15 § döms till böter, om gärningen inte är belagd med straff enligt annan författning.

Den som har åsidosatt ett vitesföreläggande som meddelats med stöd av annan författning, ska inte dömas till ansvar enligt första stycket för en gärning som omfattas av föreläggandet.

anmäld av styrelsen för uppgifter i samband med bedömning av överensstämmelse. Sanktionsavgiften får tas ut även om överträdelsen inte har skett uppsåtligt eller av oaktsamhet.

Av 24 § följer att Swedac får besluta att ta ut sanktionsavgift av någon endast om denne har delgetts en underrättelse om att myndigheten överväger att fatta ett sådant beslut inom fem år från det att överträdelsen skett.

Sanktionsavgift får dock inte tas ut för en överträdelse som omfattas av ett vitesföreläggande eller en sanktion enligt annan författning. Sanktionsavgift får inte heller tas ut för en överträdelse för vilken straff har ådömts enligt annan författning (25 §).

I 26 § anges att sanktionsavgift får tas ut med ett belopp som bestäms med hänsyn till överträdelsens art och omfattning, vad som är känt om den avgiftsskyldiges ekonomiska förhållanden och omständigheterna i övrigt. Regeringen får meddela föreskrifter om hur sanktionsavgiften ska bestämmas.

I 27 § anges att om en överträdelse är ursäktlig eller det av någon annan anledning skulle vara oskäligt att ta ut sanktionsavgift, ska den som avses i 23 § helt eller delvis befrias från sanktionsavgift. Detta gäller även om det inte har framställts något yrkande om befrielse från sanktionsavgift.

Av 28 § följer att Swedac ska genast informera tillsynsmyndigheter om beslut som fattats att ta ut sanktionsavgift. Styrelsen ska även informera andra som också har möjlighet att vidta sanktioner mot överträdelsen.

I 33 § anges att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om ackreditering. Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter i fråga om organ som ska anmälas enligt 9 §.

I 34 § anges att beslut enligt 5, 6 och 8 §§, 10 § första stycket, 19, 21 och 23 §§ får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Ett organ som vill bli ackrediterat måste lämna en ansökan till Swedac som prövar och bedömer om organet uppfyller de krav som ställs i förordning (EG) nr 765/2008, lagen och förordningen om ackreditering och teknisk kontroll och de föreskrifter som Swedac har utfärdat för det aktuella området. Organet måste även uppfylla de sektorsspecifika myndighetsföreskrifter eller andra krav som organet ska arbeta i enlighet med. Efter att en verksamhet ackredi-

terats genomför Swedac regelbundet granskningar av att kraven som ställs på kompetens och arbetsrutiner uppfylls.

Utredningen gör bedömningen att den nationella författningsreglering som nu finns på området för ackreditering och anmälan ger den nationella ackrediteringsmyndigheten möjlighet att utöva tillsyn över anmälda ackrediterade organ för bedömning av överensstämmelse och vid behov fatta beslut om sanktionsavgift vid överträdelse av regelsystemet, utom i de fall när en överträdelse faller under bestämmelserna i EU:s cyberresiliensförordning, då ska förordningens bestämmelser tillämpas (se kap. 10). Någon ytterligare kompletterande nationell lagstiftning i denna behövs därför inte.

6.12 Gränsdragningen mellan Swedac och en marknadskontrollmyndighet

Utredningens bedömning: Swedacs uppgifter och ansvar för såväl ackreditering som anmälan och tillsyn av organ för bedömning av överensstämmelse framgår av gällande reglering om ackreditering och anmälan i förening med de ytterligare krav som anges i EU:s cyberresiliensförordning och kommande anslutande unionsrättsliga författningar

Motsvarande gäller för marknadskontrollmyndigheterna enligt EU:s cyberresiliensförordning och övrig reglering på området för marknadskontroll.

Det behövs inte någon nationell kompletterande reglering för att närmare ange myndigheternas ansvarsområden.

Utredningen bedömer att när det gäller Swedacs uppgifter och ansvar för såväl ackreditering som anmälan och tillsyn av organ för bedömning av överensstämmelse framgår detta av gällande reglering om ackreditering och anmälan i förening med de ytterligare krav som anges i EU:s cyberresiliensförordning och kommande anslutande unionsrättsliga författningar.

Motsvarande gäller för den eller de myndigheter för marknadskontroll enligt EU:s cyberresiliensförordning och övrig reglering på området för marknadskontroll. Det behövs därför inte någon nationell kompletterande reglering för att närmare ange myndigheternas ansvarsområden. Berörda myndigheter bör emellertid

samverka och samråda vid tillsyn över ett tillsynsobjekt för att undvika att oklarhet uppstår om vad tillsynen av respektive myndighet omfattar och för att reducera kostnaderna för tillsynsobjektet. Det är viktigt att i detta arbete beakta de kostnader, den tid och andra aspekter som en överlappande granskning av såväl Swedac som marknadskontrollmyndigheterna kan innebära för den som blir granskad. Frågan om marknadskontroll behandlas i kapitel 9.

6.13 Överlämnande av förvaltningsuppgifter till privata organ för bedömning av överensstämmelse

Utredningens bedömning: Den verksamhet som enligt EU:s cyberresiliensförordning utförs av privata organ för bedömning av överensstämmelse i fråga om EU-typkontroll (modul B) och beslut om godkännande av kvalitetssystem (modul H) utgör ett överlämnande av förvaltningsuppgift till enskild som innefattar myndighetsutövning. EU:s cyberresiliensförordning är att likställa med lag och innebär att det inte behövs kompletterande nationella bestämmelser till stöd för att överlämna dessa förvaltningsuppgifter till sådana organ.

6.13.1 Överlämnande av förvaltningsuppgift

Enligt 12 kap. 4 § andra stycket regeringsformen får överlämnande av en förvaltningsuppgift som innefattar myndighetsutövning ske endast med stöd av lag.

Enligt kapitel IV i EU:s cyberresiliensförordning får privaträttsliga subjekt i form av anmält organ för bedömning av överensstämmelse genomföra bedömning i enlighet med de angivna förfarandena i artikel 32 och bilaga VIII. Ett organ för bedömning av överensstämmelse ska därefter antingen utfärda ett EU-typintyg eller avslå ansökan om ansökan avser EU-typkontroll (baserat på modul B) eller i de fall ansökan gäller överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H) fatta beslut om att antingen godkänna det aktuella kvalitetssystemet hos tillverkaren eller avslå ansökan om eventuella brister först inte åtgärdas. En till-

verkare av en produkt med digitala element måste således, beroende på den berörda produkten, hos det anmälda organet ansöka om EU-typkontroll (intyg) eller ett beslut om godkänt kvalitetssystem.

Frågan som inställer sig är om utfärdande av EU-typkontroll (intyg) baserat på modul B och beslut om godkänt kvalitetssystem baserat på modul H ska ses som en förvaltningsuppgift som innefattar myndighetsutövning. I båda fallen är det fråga om en obligatorisk författningsenlig bedömning av överensstämmelse som följer av lag och som utgör en förutsättning för att en enskild tillverkare lagligen ska kunna tillhandhålla den berörda produkten med digitala element på den inre marknaden.

I regeringsformen finns grundläggande krav som gäller för den statliga förvaltningen. De som fullgör offentliga förvaltningsuppgifter ska i sin verksamhet beakta allas likhet inför lagen samt iakttä saklighet och opartiskhet.³² Det är ett grundläggande krav på att uppgifterna ska utföras med stöd i lag eller annan författning och ett krav på objektivitet. Med myndighetsutövning avses beslut och andra åtgärder som en myndighet vidtar gentemot en enskild med stöd av en befogenhet som myndigheten har getts genom ett konkret beslut av regeringen eller riksdagen eller genom en offentlig-rättslig författning. Det kan innebära att en myndighet beslutar om att en medborgare ska få en viss förmån eller rättighet. Ett exempel på det är ett beslut om bidrag eller en rätt att bedriva en viss verksamhet. Myndighetsutövning kan också innebära att den enskilde åläggs en viss skyldighet eller ett straff eller administrativ sanktion. Karaktäristiskt för myndighetsutövning är att den enskilde befinner sig i en beroendeställning i förhållande till det allmänna och att detta inte har sin grund i ett frivilligt åtagande. Det innebär att myndigheten i dessa fall – till skillnad från exempelvis ett avtalsförhållande – ensidigt ska besluta i saken.³³

Normalt sett brukar förvaltningsuppgifter fullgöras av myndigheter. En förvaltningsuppgift kan också överlämnas till en annan juridisk eller enskild person. Om den förvaltningsuppgift som överlämnas till en annan juridisk eller enskild person innefattar myndighetsutövning, måste dock överlämnandet ske med stöd av lag.³⁴ Att överlämnandet måste ske med stöd av lag innebär att ett medgivande

³² 1 kap. 9 § regeringsformen.

³³ Prop. 2016/17:180 s. 47 ff. samt där angivna referenser.

³⁴ 12 kap. 4 § regeringsformen.

till överlämnandet måste regleras i lag.³⁵ Själva överlämnandet av förvaltningsuppgiften kan sedan regleras i en förordning eller i en myndighetsföreskrift. Det förutsätter att det finns ett bemyndigande som har stöd i lag.

Den fråga som nu uppkommer är om den verksamhet som de anmälda organen bedriver och som gäller bedömning av överensstämmelse för en produkt med digitala element är att anse som förvaltningsuppgifter som innebär myndighetsutövning.

Genom EU:s cyberresiliensförordning anges de krav som ligger till grund för det anmälda organets prövning av om den berörda produkten uppfyller kraven på cybersäkerhet eller om tillverkaren har ett tillräckligt kvalitetssystem för att få tillhandahålla produkten på den inre marknaden. Det är alltså cyberresiliensförordningen som anger vilka krav som tillverkaren ska uppfylla och det är det anmälda organet som ensidigt prövar om kraven är uppfyllda i det enskilda fallet. Om ett positivt beslut inte meddelas får sökanden inte tillhandahålla produkten på den inre marknaden. Ett anmält organ får också återkalla ett tidigare positivt beslut när kraven inte längre uppfylls, vilket sker med stöd av bestämmelserna i förordningen.

Tillverkare får därför genom en godkänd EU-typkontroll (intyg) eller beslut om godkänt kvalitetssystem av ett anmält organ särskilda förmåner som kan åberopas mot det allmänna, bland annat medför dessa beslut att tillverkaren lagligen får tillhandahålla berörda produkter med digitala element på den inre marknaden. Det bör samtidigt framhållas att det är de anmälda organens rätt att bestämma om tillverkare ska få de särskilda förmånerna som anses utgöra myndighetsutövning. Tillverkaren är således beroende av den bedömning som det anmälda organet gör vid sin kontroll och som mynnar ut i ett ställningstagande i ett beslut om EU-kontroll-intyg eller godkänt kvalitetssystem.

Det nu angivna talar för att anmälda organ genom bestämmelserna i EU:s cyberresiliensförordning har tilldelats förvaltningsuppgifter som innefattar myndighetsutövning. Bestämmelserna i nu angivet hänseende i förordningen, som är en EU-förordning som är direkt tillämplig, är att jämföras med lag. Därför behövs ingen kompletterande nationell reglering i detta fall.

³⁵ Se Holmberg m.fl. Grundlagarna (7 mars 2019, version 3A, JUNO) kommentaren till 12 kap. 4 § under rubriken Överlåtelse av förvaltningsuppgifter till andra än myndigheter.

6.13.2 Handläggning av ärenden

I artikel 41 i EU:s rättighetsstadga (rättighetsstadgan) slås fast att var och en har rätt till god förvaltning. Denna rättighet omfattar bland annat rätten till kommunikation, aktinsyn och motivering av beslut. Rätten till god förvaltning gäller enligt rättighetsstadgan bara i förhållande till unionens institutioner, organ och byråer. Som regeringen anför i propositionen *En modern och rättssäker förvaltning – ny förvaltningslag* (prop. 2016/17:180) (s. 44.) framstår det som naturligt att utgå från att de allmänna unionsrättsliga principer som gäller i ärenden som handläggs av unionens institutioner och organ också gäller för medlemsstaternas myndigheter, när de handlägger ärenden på unionsrättens område.

Handläggningsregler

De privata organen för bedömning av överensstämmelse utgör inte myndigheter i förvaltningslagens (2017:900) mening. Den lagen är därför inte tillämplig på organens handläggning av ärenden. De privata organen för bedömning av överensstämmelse ska emellertid i utövandet av den verksamheten beakta allas likhet inför lagen samt iaktta saklighet och opartiskhet.³⁶

Av EU:s cyberresiliensförordning följer att anmälda organ för bedömning av överensstämmelse ska uppfylla flera krav, bland annat krav på opartiskhet och tillhandahållande av beskrivningar av de förfaranden vid bedömningar som tillämpas i syfte att säkerställa insyn samt i övrigt uppfylla de krav som anges i relevanta standarder enligt förordning (EG) nr 765/2008. De anslutande rättsakterna till EU:s cyberresiliensförordning kan också komma att innefatta ytterligare regler som bland annat kan ha inverkan på handläggningen av ärenden enligt förordningen och anslutande rättsakter.

Frågan inställer sig då om det behövs nationella kompletterande bestämmelser för handläggning av ett ärende hos ett organ för bedömning av överensstämmelse som efter ansökan utför en bedömning och eventuella efterföljande åtgärder, till exempel kontroll av villkor som ligger till grund för tillverkarens behörighet att utfärda ett intyg enligt cyberresiliensförordningen.

³⁶ Jfr 1 kap. 9 § regeringsformen.

I frågan om vilka regler som bör gälla för bland annat handläggning av en ansökan om EU-typintyg eller bedömning av kvalitetsystem hos ett privat organ för bedömning av överensstämmelse, samt behovet av en möjlighet till omprövning av ett sådant beslut, gör utredningen följande överväganden.

När de privata organen utför bedömning av överensstämmelse enligt EU:s cyberresiliensförordning och anslutande föreskrifter, fattar de beslut som rör enskildas rättigheter och skyldigheter. Till exempel innefattar organens beviljande av eller avslag (beslut) på ansökan om angivna intyg eller kvalitetsbedömning myndighetsutövning.

Utgångspunkten i detta fall är att det är fråga om privaträttsliga subjekt, huvudsakligen i form av juridiska personer, till exempel ett aktiebolag. I likhet med vad som konstaterats i föregående avsnitt bör i första hand unionsrättsliga författningar som reglerar frågor om organens ärendehandläggning tillämpas, dvs. de regler som anges i det europeiska ramverket som tillämpas med stöd av EU:s cyberresiliensförordning och som är tillämpliga på organen. Eftersom de privata organen för bedömning av överensstämmelse inte utgör myndigheter i förvaltningslagens mening, även om de anförtrotts offentliga förvaltningsuppgifter som innefattar myndighetsutövning, är den lagen dock inte tillämplig på organens handläggning av ärenden. Däremot är lagen (1986:1142) om överklagande av beslut av enskilda organ med offentliga förvaltningsuppgifter tillämplig. I denna lag, som gäller subsidiärt, regleras främst hur beslut överklagas, överklagandetiden, rättidsprövning och avvisning av för sent inkomna överklaganden. Därutöver finns förfaranden för ärendehantering som framgår av tillämplig standard för ackrediteringen av anmälda organ och övriga standarder som ska tillämpas.

När offentliga förvaltningsuppgifter som innefattar myndighetsutövning överlämnas åt privaträttsliga organ brukar det i allmänhet anges i en särskild författning att vissa av förvaltningslagens (2017:900) bestämmelser ska tillämpas vid handläggningen av ärenden. De allmänna förvaltningsrättsliga principer som gäller för myndigheternas handläggning är bara i begränsad utsträckning direkt tillämpliga i de privaträttsliga organens verksamhet. Några exempel är dock principerna om legalitet, objektivet och saklighet som har sin grund i regeringsformen (1 kap. 1 och 9 §§ regeringsformen). Många av de specialförfattningar som avser privaträttsliga

organs ärendehandläggning innehåller regleringar som avviker från vad som gäller enligt förvaltningslagen (2017:900). Avvikande reglering finns till exempel när det gäller handläggningstiden och verkställighet av beslut.³⁷

Det kan i och för sig framstå som naturligt och konsekvent att samma krav på rättssäkerhet vid handläggningen av förvaltningsärenden upprätthålls oberoende av om uppgiften utförs av en myndighet eller överlämnats för att fullgöras av ett privaträttsligt organ. Tidigare utredningar har emellertid bedömt att det inte finns tillräckliga belägg för en ordning helt grundad på förvaltningslagen (2017:900) med samma förfaranderegler för privaträttsliga organ,³⁸ eftersom förvaltningslagens bestämmelser är utformade på ett sätt som inte alltid lämpar sig att tillämpas av privaträttsliga organ. Om det för handläggningen av en viss förvaltningsuppgift finns ett särskilt framträdande behov av att säkerställa att lagens förfaranderegler följs, bör detta kunna ske genom särskilda föreskrifter som meddelas för den verksamheten.

I propositionen *Följdändringar till ny förvaltningslag* (prop. 2017/18:235) bedömde regeringen att hänvisningar till andra bestämmelser i förvaltningslagen (2017:900) än bestämmelserna om utredningsansvaret i 23 § och om dokumentation av beslut i 31 § inte borde göras i uppräkningsavseringar som avser privaträttsliga organs ärendehandläggning. När det gäller bestämmelsen om utredningsansvaret konstaterade regeringen att det fick förutsättas att privaträttsliga organ redan vid sin ärendehandläggning utredde ärenden som rörde enskilda i den utsträckning som krävdes. Därför ansågs det både lämpligt och rimligt att de privaträttsliga organen skulle vara skyldiga att följa förvaltningslagens (2017:900) bestämmelser om utredningsansvaret. Med hänsyn till krav på rättssäkerhet framstod det enligt regeringen också som angeläget att skyldigheten att dokumentera skriftliga beslut skulle gälla för de privaträttsliga organen på samma sätt som för myndigheterna.³⁹

³⁷ Se prop. 2017/18:235 s. 124 ff.

³⁸ Se bland annat prop. 2016/17:180 s. 27.

³⁹ I till exempel växtskyddslagen (1972:318) föreskrivs att enskilda kontrollorgan ska tillämpa förvaltningslagen (2017:900) och fera av förvaltningslagens bestämmelser (11 a §). Jfr även 7 kap. 10 § lagen om offentliga uppköpserbjudanden på aktiemarknaden där ett organ med representativa företrädare för näringslivet som utför förvaltningsuppgifter ska tillämpa ett tiotal bestämmelser i förvaltningslagen.

I lagrådsremissen *En anpassning av bestämmelser om kontroll i livsmedelskedjan till EU:s nya kontrollförfordning*⁴⁰ anges att vissa bestämmelser i förvaltningslagen (2017:900) bör tillämpas när ett organ med delegerade uppgifter, eller en fysisk person som har delegerats uppgifter, utför offentlig kontroll eller annan offentlig verksamhet. För att en överprövande instans ska kunna ta ställning till om ett överklagat beslut är korrekt och för att enskilda ska kunna ta till vara sin möjlighet att överklaga ett beslut bör vissa bestämmelser i förvaltningslagen (2017:900) tillämpas. Det gäller att ett beslut ska vara motiverat (32 §), att den enskilde ska underlägga om beslutet (33 §) och hur ett överklagande går till (34 §). Vidare anges att bestämmelserna om legalitet, objektivitet och proportionalitet (5 §), partsinsyn (10 §), jäv (16–18 §§), utredningsansvar (23 §), när man får lämna uppgifter muntligt (24 §), kommunikation (25 §), dokumentation av uppgifter (27 §), dokumentation av beslut (31 §), rättelse av skrivfel och liknande (36 §), samt vem som får överklaga ett beslut (42 §) bör tillämpas.

Utredningen har övervägt om det finns behov av att införa dessa bestämmelser i den nya lagen med kompletterande bestämmelser vid ärendehandläggning hos privata organ för bedömning av överensstämmelse.

Det kan noteras att privata organ för bedömning av överensstämmelse inte har någon formell allmän serviceskyldighet som följer av förvaltningslagen. Samtidigt bör utgångspunkten för dessa organs verksamhet vara att iaktta motsvarande serviceskyldighet i sin verksamhet, även om det inte finns någon formell skyldighet i detta avseende. Detta särskilt mot bakgrund av att det är fråga om nya författningsbestämmelser på ett i vissa avseenden mycket komplext sakområde och att det är frågan om en överlämnad förvaltningsuppgift som i vissa fall även innefattar myndighetsutövning.

Den lagrådsremiss som hänvisas till ovan avser livsmedelskontroll genom privaträttsliga kontrollorgan på uppdrag av bland annat Livsmedelsverket. Även om det finns likheter med detta och det nu aktuella området föreligger också skillnader, bland annat ska det anmälda organet för bedömning av överensstämmelse som verkar i en-

⁴⁰ Europaparlamentets och rådets förordning (EU) 2017/625 om offentlig kontroll och annan offentlig verksamhet för att säkerställa tillämpningen av livsmedels- och foderlagstiftningen och av bestämmelser om djurs hälsa och djurskydd, växtskydd och växtskyddsmedel.

lighet med EU:s cyberresiliensförordning följa regler om handläggning enligt vad som anges i tillämpliga standarder.

I sammanhanget bör noteras att anmälda organ står under tillsyn av Swedac. Ett organ som är ackrediterat ska kunna visa att det uppfyller de krav som gäller för ackrediteringen. Kraven för ackreditering av organ som ansöker om att anmälas som organ för bedömning av överensstämmelse enligt EU:s cyberresiliensförordning framgår av förordningen, nationell lagstiftning och tillämpliga standarder.

Vidare ska noteras att tillämpliga standarder innehåller krav på organens verksamhet. Kraven syftar till att säkerställa att organen är objektiva och opartiska. Det finns också krav på att det ska finnas ett system för hantering av klagomål och överklaganden. I standarderna finns även krav på dokumentation och regler om sekretess som innebär att konfidentiell information inte får röjas om det inte följer av lag.

Den verksamhet som anmälda organ bedriver ska uppfylla de krav som ställs i respektive standard. Bedömningen är att detta kan säkerställas genom den tillsyn som Swedac bedriver. De krav som ställs i standarderna bör därför anses på ett tillräckligt sätt tillgodose de krav som från rättssäkerhetssynpunkt kan ställas på de anmälda organens handläggning.

Med hänsyn till att det redan finns en ordning för ärendehandläggning genom EU:s cyberresiliensförordning regelsystem och standarder som anmälda organ för bedömning av överensstämmelse ska tillämpa bedömer utredningen att det för närvarande inte föreligger skäl att, utöver en omprövningsskyldighet av beslut (se nedan), föreslå en ordning med formaliserade regler för handläggningen hos de privata organen. Till detta kommer att det, utöver möjlighet att begära omprövning av organets beslut, även finns möjlighet att vända sig till den anmälande myndigheten för tillsynsåtgärder respektive till marknadskontrollmyndigheten och framföra klagomål på fattade beslut (se nedan).

Mot den bakgrunden behöver därför inte införas några ytterligare bestämmelser om organens handläggning av ärenden enligt EU:s cyberresiliensförordning. Samtidigt bör framhållas att frågan om ytterligare reglering av ärendehandläggningen hos de privata organen bör övervägas när ytterligare erfarenheter erhållits av cyberresiliensförordningens tillämpning.

6.13.3 Ändring av beslut av ett privatorgan för bedömning av överensstämmelse

Utredningens förslag: Ett privat organ för bedömning av överensstämmelse ska ändra ett beslut som det har meddelat, om

1. organet anser att beslutet är uppenbart felaktigt i något väsentligt hänseende på grund av att det har tillkommit nya omständigheter eller av någon annan anledning, och
2. beslutet kan ändras snabbt och enkelt och utan att det blir till nackdel för någon enskild.

I artikel 48 i EU:s cyberresiliensförordning anges att medlemsstaterna ska säkerställa att det finns ett förfarande för överklagande av de anmälda organens beslut. Någon uttrycklig bestämmelse som ger rätt att först begära omprövning av ett sådant beslut finns emellertid inte i förordningen. Frågan uppkommer då om det finns behov av en sådan ordning och hur den i så fall ska vara utformad.

Till en början kan noteras att ett organ för bedömning som blivit ackrediterat och anmält av Swedac ska, enligt myndighetens föreskrifter för ackreditering⁴¹ och anmälan⁴² inrätta rutiner för omprövning av ett beslut. Föreskriften är riktad mot det ackrediterade anmälda organet och medför i sig inte någon tydlig författningssenlig rättighet att få beslutet omprövat. Det får därför anses saknas en författningsreglerad rättighet för den sökande att få ett tidigare beslut omprövat.

Frågan om behov av att författningsreglera rätten till omprövning av ett kontrollorgans beslut har tidigare behandlats av bland annat i betänkandet *EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering* (SOU 2020:58).

I denna fråga anförde utredningen bland annat följande (s. 247):

Det kan i detta sammanhang noteras att det i t.ex. fordonslagen (2002:574) finns en regel om att ackrediterade besiktningsorgan ska vidta omprövning i vissa fall. Besiktningsorganen är även skyldiga att rapportera betydelsefulla iakttagelser till föreskrivande myndigheter. Utöver detta föreskriver lagen inget om besiktningsorganens ärende-

⁴¹ Styrelsen för ackreditering och teknisk kontrolls föreskrifter och allmänna råd om ackreditering (STAFS 2020:1).

⁴² Styrelsen för ackreditering och teknisk kontrolls föreskrifter om organ som utför bedömning av överensstämmelse och som ska bli anmält och utsett (STAFS 2022:7).

handläggning. Lagrådet yttrade i prop. 2001/02:130 (s. 189) att det särskilt kunde övervägas huruvida den ordning för omprövning efter klagomål som AB Svensk Bilprovning iakttog borde regleras i författning. Bolaget använde nämligen som kvalitetssystem standarden ISO 17020 (tidigare EN45004) som angav möjligheten till omprövning av resultatet av t.ex. en kontrollbesiktning. Regeringen hänvisade till detta kvalitetssystem och framhöll att behovet av andra regler om ärendehandläggning än sådana som angav vad som skulle kontrolleras var relativt litet. I den efterföljande propositionen 2009/10:32 befarade regeringen emellertid att det inte var möjligt att under den då gällande ordningen ha uppsikt över att besiktningsorganen verkligen tillämpade godtagbara omprövningsmöjligheter, bl.a. då systemet skulle fungera för många olika aktörer och ISO-standardens reglering av omprövningsmöjligheten var ganska vag och övergripande till sin karaktär (s. 73). Man ansåg därför att det fanns ett starkt behov av att författningsreglerna om omprövningsskyldighet, utformad med ledning av förvaltningslagen.

Mot den bakgrunden, och då ärenden avseende cybersäkerhetscertifiering är av mycket teknisk karaktär, får behovet, som ovan framgår, av formella regler om ärendehandläggningen i dessa fall minska (jfr prop. 2001/02:130 s. 93). Det finns dock skäl att i författning reglera de ackrediterade bedömningsorganens skyldighet att ompröva ett tidigare beslut i ett certifieringsärende. En enskild bör därför ges möjlighet att i första hand få organen för bedömning av överensstämmelse att ompröva beslutet. Den regel om omprövningsskyldighet som behövs kan lämpligen utformas med ledning av den generella regeln om omprövningsskyldighet som finns i förvaltningslagen. Enligt 38 § i den lagen ska en myndighet ändra ett beslut som den har meddelat som första instans om den anser att beslutet är uppenbart felaktigt i något väsentligt hänseende på grund av att det har tillkommit nya omständigheter eller av någon annan anledning, och beslutet kan ändras snabbt och enkelt och utan att det blir till nackdel för någon enskild part.

I den efterföljande propositionen *Kompletterande bestämmelser till EU:s cybersäkerhetsakt* (prop. 2020/21:186) anförde regeringen att man delade utredningens bedömning och uttalade bland annat följande (s. 50):

I artikel 41 i Europeiska unionens stadga om de grundläggande rättigheterna av den 7 december 2000, anpassad den 12 december 2007 i Strasbourg, förkortad rättighetsstadgan, slås vidare fast att var och en har rätt till god förvaltning. Denna rättighet omfattar bl.a. rätten till kommunikation, aktinsyn och motivering av beslut. Rätten till god förvaltning gäller enligt rättighetsstadgan bara i förhållande till unionens institutioner, organ och byråer. Som regeringen anför i propositionen *En modern och rättssäker förvaltning – ny förvaltningslag* framstår det som naturligt att utgå från att de allmänna unionsrättsliga principer som gäller i ärenden som handläggs av unionens institutioner och organ också gäller för medlemsstaternas myndigheter, när de handlägger ärenden på unionsrättens område (prop. 2016/17:180 s. 44).

De privata organen för bedömning av överensstämmelse utgör inte myndigheter i förvaltningslagens mening. Förvaltningslagen är därför inte tillämplig på organens handläggning av ärenden.

De privata organen för bedömning av överensstämmelse ska i utövandet av den verksamheten beakta allas likhet inför lagen samt iakttta saklighet och opartiskhet (jfr 1 kap. 9 § regeringsformen). Härutöver bör, som utredningen föreslår, organen för bedömning av överensstämmelse ha en skyldighet att i vissa fall ompröva ett tidigare beslut i ett ärende om certifiering. Det bör i den nya lagen införas en särskild bestämmelse om detta. En lämplig förebild för bestämmelsen kan vara 38 § förvaltningslagen om när en myndighet ska ändra ett beslut.

Regeringen föreslår därför att ett privat organ för bedömning av överensstämmelse ska ändra ett beslut det har meddelat, om organet anser att beslutet är uppenbart felaktigt i något väsentligt hänseende på grund av att det har tillkommit nya omständigheter eller av någon annan anledning, om det kan ske snabbt och enkelt och utan att det blir till nackdel för någon enskild.

Det bör därför i den nya lagen införas en särskild bestämmelse om detta. En lämplig förebild för bestämmelsen kan vara 38 § förvaltningslagen om när en myndighet ska ändra ett beslut. Ett privat organ för bedömning av överensstämmelse ska ändra ett beslut det har meddelat, om organet anser att beslutet är uppenbart felaktigt i något väsentligt hänseende på grund av att det har tillkommit nya omständigheter eller av någon annan anledning, om det kan ske snabbt och enkelt och utan att det blir till nackdel för någon enskild.

De beslut som fattas av ett organ för bedömning av överensstämmelse enligt EU:s cyberresiliensförordning rör bedömning av överensstämmelse av – i vissa fall - komplicerade tekniska krav på cybersäkerhet och anslutande krav till stöd för att uppnå sådan säkerhet. Besluten är till sin karaktär av sådan art och omfattning att det måste anses föreligga ett inte obetydligt utrymme för att en felbedömning kan uppstå vid bedömningen eller att en ny omständighet tillkommer som inte var känd tidigare. Ett problem är att den reglering

som ligger till grund för att anmäla ett organ inte formellt säkerställer en rätt för sökanden att få ett beslut omprövat av det anmälda organet. Det finns därför skäl att organen för bedömning av överensstämmelse ska ha en skyldighet att i vissa fall ompröva ett tidigare beslut i ett ärende enligt EU:s cyberresiliensförordning. Det bör därför i den nya lagen införas en särskild bestämmelse om detta. En lämplig förebild för bestämmelsen kan – på skäl som anförs i den angivna propositionen – vara 38 § förvaltningslagen (2017:900) om när en myndighet ska ändra ett beslut. Utredningen föreslår därför att ett privat organ för bedömning av överensstämmelse ska ändra ett beslut det har meddelat, om organet anser att beslutet är uppenbart felaktigt i något väsentligt hänseende på grund av att det har tillkommit nya omständigheter eller av någon annan anledning, om det kan ske snabbt och enkelt och utan att det blir till nackdel för någon enskild.

Det bör därför i den nya lagen införas en särskild bestämmelse efter förebild av bestämmelsen i 38 § förvaltningslagen (2017:900).

6.14 Överklagande av beslut av anmälda organ och av förvaltningsmyndighet

Utredningens förslag: Ett beslut av en förvaltningsmyndighet eller ett anmält organ enligt EU:s cyberresiliensförordning, denna lag och anslutande föreskrifter får överklagas till allmän förvaltningsdomstol.

En myndighet får överklaga en förvaltningsmyndighets eller ett anmält organs beslut.

Förvaltningsmyndigheten eller det anmälda organet ska vid överklagande vara motpart i domstolen.

Prövningstillstånd ska krävas vid överklagande till kammarrätten.

I detta avsnitt behandlas överklagande av beslut av ett anmält organ för bedömning av överensstämmelse (avsnitt 6.14.1) och att organet ska vara motpart vid överklagande (avsnitt 6.14.2). I avsnitt 6.14.3 behandlas överklagande av beslut av en förvaltningsmyndighet. I avsnitt 6.14.4 behandlas frågan om att överklaga förvaltningsmyndighets beslut enligt den nya lagen. I avsnitt 6.14.5 behandlas beslu-

tande myndighets eller anmält organs motpartsställning i domstol. I avsnitt 6.14.6. behandlas frågan om prövningstillstånd vid överklagande till kammarrätten.

6.14.1 Överklagande av beslut av privat organ för bedömning av överensstämmelse

Enligt artikel 48 i EU:s cyberresiliensförordning ska medlemsstaterna säkerställa att det finns ett förfarande för överklagande av de anmälda organens beslut. Sådana beslut kan meddelas av antingen av ett offentligt eller privat organ för bedömning av överensstämmelse.

De beslut av organ för bedömning som främst torde komma i fråga gäller beslut efter ansökan om att utfärda ett EU-typkontrollintyg och beslut efter ansökan om godkännande av kvalitetssystem. Även beslut om att återkalla intyget eller godkännandet kan bli aktuellt. Även andra beslut i anslutning till dessa beslut torde komma i fråga.

Ett beslut som fattas av ett anmält organ för bedömning av överensstämmelse och där organet är en del av en förvaltningsmyndighet får normalt överklagas enligt förvaltningslagens bestämmelser som gäller för handläggning och överklagande av beslut av en förvaltningsmyndighet. Det finns därför inte behov av någon kompletterande reglering i dessa fall.

Frågan uppkommer dock om och hur de beslut som fattas av ett privat anmält organ för bedömning av överensstämmelse kan överklagas av den det berör och, i sådana fall, hur instansordningen bör utformas för att möta kraven i artikel 6.1 i europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR) och kraven i lagen (1986:1142) om överklagande av beslut av enskilda organ med offentliga förvaltningsuppgifter.

I 1 § första stycket lagen (1986:1142) om överklagande av beslut av enskilda organ med offentliga förvaltningsuppgifter anges att lagen gäller sådana beslut av enskilda organ som enligt särskilda bestämmelser får överklagas till regeringen, till en förvaltningsdomstol eller till en förvaltningsmyndighet. Närmare bestämmelser om hur beslut överklagas och hur överklagandet ska hanteras av överinstansen finns i 2–5 §§. I lagen – som gäller subsidiärt och tillämpas

på överklagade beslut av bolag och andra enskilda organ, som enligt särskilda bestämmelser får överklagas till bland annat förvaltningsmyndighet – regleras även tiden för överklagande, rättidsprövning och avvisning av för sent inkomna överklaganden. Av 2 § samma lag följer även att ett överklagande ska ges in till det organ som ska pröva överklagandet.

Förutsättningar för att beslut får överklagas till domstol

Den första frågan som utredningen behöver ta ställning till gäller hur kravet i artikel 48 i EU:s cyberresiliensförordning ska tolkas, dvs. den närmare innebörden av att medlemsstaterna ska säkerställa att det finns ett förfarande för överklagande av de anmälda organens beslut.

I dag saknas det formella regler i lag eller förordning om överklagande av de anmälda organens beslut. Möjligheten att överklaga ett beslut regleras i de standarder som gäller för ackreditering. Frågan uppkommer om det finns behov av att författningsreglera möjligheten att överklaga de anmälda organens beslut.

När det gäller handläggning och prövning av överklaganden finns det krav som ett ackrediterat anmält organ ska uppfylla enligt de standarder som är tillämpliga för ackreditering av organen. Sammanfattningsvis framgår av tillämpliga standarder att

- organet ska ha en dokumenterad process för hur överklaganden tas emot, utreds, bedöms och beslutas,
- organet har skyldighet att samla in all information som krävs för att bedöma ett överklagande,
- den eller de som beslutar om ett överklagande får inte tidigare ha deltagit i det kontrollarbete som överklagandet gäller, och
- organet ska ge besked om beslutet.

Det kan dock noteras att standarderna inte formellt säkerställer att det i det enskilda fallet ges en möjlighet att överklaga ett beslut. Den enskilde har inte någon på rättslig grund rätt att överklaga ett beslut med hänvisning till standarden. Vidare kan noteras att regleringen i standarden innebär att överklagandet av organets beslut prövas inom organet. Överprövningen sker alltså inte av någon instans som

är helt fristående från organet. Standardernas bestämmelser om prövning är således närmast att betrakta som ett krav på omprövning av tidigare fattat beslut.

Från rättsliga utgångspunkter bör det beaktas att ett beslut om att utfärda ett EU-kontrollintyg eller ett beslut om godkännande av ett kvalitetssystem, eller om det ska få behållas, begränsas eller förnyas, har verkningar för den som drabbas av beslutet. Ett ställningstagande som innebär ett beslut att tillverkarens produkt eller kvalitetssystem inte uppfyller kraven i EU:s cyberresiliensförordning får därför anses ha direkt betydelse för en tillverkare. Beslutet kan även få betydelse för den som har behov av att använda produkten, bland annat om det ställs författningsenliga krav på att produkten ska ha genomgått bedömning av överensstämmelse för att få användas i en viss verksamhet.

När det gäller myndighetsutövning brukar överklaganden i frågor av det här slaget regleras i lag eller förordning. Om frågorna prövas av förvaltningsmyndigheter tillämpas förvaltningslagens regler om överklagande. I lagen föreskrivs att ett beslut får överklagas till allmän förvaltningsdomstol om det kan antas påverka någons situation på ett inte obetydligt sätt. Beslutet får överklagas av den beslutet angår, om det har gått honom eller henne emot.⁴³ Bestämmelserna har grundläggande betydelse för den enskildes rättsskydd.⁴⁴

Som ovan nämnts är förvaltningslagen inte tillämplig på enskilda organ som handlägger förvaltningsärenden.⁴⁵ Är det fråga om förvaltningsuppgifter som har överlämnats till enskilda organ säkerställs rättsskyddet för den som påverkas av ett beslut normalt i respektive författning där överlämnandet sker.⁴⁶

Vidare ska i denna fråga beaktas artikel 6.1 i EKMR. Enligt denna artikel ska var och en, vid prövningen av civila rättigheter och skyldigheter eller av en anklagelse för brott, vara berättigad till en rättvis och offentlig förhandling inom skälig tid och inför en oavhängig och opartisk domstol, som upprättats enligt lag. Artikeln innebär att prövningen ska göras av någon som är fristående i förhållande till parterna i det ärende som överklagandet gäller. De ställnings-

⁴³ 40–42 §§ förvaltningslagen (2017:900).

⁴⁴ Jfr prop. 2016/17:180 s. 251 f.

⁴⁵ 1 § förvaltningslagen (2017:900).

⁴⁶ I fråga om beslut av kontrollorgan finns det exempelvis bestämmelser om överklagande av körförbud i fordonslagen. Överklagandet ska göras till Transportstyrelsen.

taganden som det anmälda organet gör och de beslut som det meddelar gäller rätten för en tillverkare att tillhandhålla en produkt med digitala element på den inre marknaden innebär i praktiken tillstånd att kunna bedriva viss ekonomisk verksamhet,⁴⁷ dvs. det är fråga om en prövning av civila rättigheter.⁴⁸ Det anmälda organets beslut i dessa frågor har därför rättsverkningar för enskilda.

Som framgår av artikel 6.1 i EKMR ska prövningen göra av domstol. Europadomstolen har förklarat att termen ”domstol” (”tribunal”) inte ska tolkas så att den enbart avser domstolar av traditionellt slag. Det avgörande är vilken funktion som den ifrågasvarande institutionen i realiteten har och inte hur den benämns eller klassificeras i nationell rätt.

Den första frågan som aktualiseras i detta sammanhang är om de angivna besluten är av sådant slag att den som berörs har en rätt till domstolsprövning enligt artikel 6.1 i EKMR.

För att besvara den frågan måste först bedömas om besluten, i enlighet med Europadomstolens praxis rör en reell och seriös tvist samt om beslutet rör en rättighet eller skyldighet enligt nationell rätt och om denna i så fall kan karaktäriseras som civil.⁴⁹

Bedömningen av om en tvist som rör ett beslut av ett organ för bedömning är reell och seriös ska göras mot bakgrund av de regler som enligt nationell rätt gäller för den rättighet eller skyldighet som tvisten avser. Det finns en presumtion för att uppkomna tvister är reella och seriösa.⁵⁰ Detta innebär att en domstol bara i klara fall får dra slutsatsen att en tvist inte är reell och seriös och att artikel 6.1 i EKMR därför inte är tillämplig.

De beslut som främst aktualiseras är som ovan framgår beslut om EU-kontrolltypintyg och beslut om kvalitetssystem eller avslag på en ansökan eller återkallelse av ett sådana beslut. Tvister mellan parterna som rör dessa beslut måste anses vara av reell och seriös natur. Tvisten måste också anses avse en rättighet eller skyldighet som följer av nationell rätt. Avgörande vid denna bedömning är dock inte enbart innehållet i de föreskrifter som är tillämpliga utan det ska också vägas in om tillämpningen av dem innebär att den

⁴⁷ Se Danelius, m.fl. Mänskliga rättigheter i europeisk praxis (2023, version 6, JUNO), s. 195.

⁴⁸ Prövningen av frågan om civila rättigheter brukar göras i två steg. Först bedöms om det gäller en rättighet i nationell rätt. Sedan prövas om det handlar om en civil rättighet se Högsta förvaltningsdomstolens avgörande HFD 2016 ref. 49.

⁴⁹ Se HFD 2019 ref. 10 p. 14 och HFD 2019 ref. 43.

⁵⁰ Se HFD 2019 ref. 10 p. 15 och där angivna rättsfall.

som uppfyller vissa kriterier i praktiken har en rätt till ett visst beslut.⁵¹ Om det handlar om rent skönsmässiga överväganden avser det normalt inte en rättighet, men när en myndighet har frihet att efter en lämplighetsbedömning avgöra om vissa krav är uppfyllda och därefter meddelar ett beslut att utfärda ett intyg eller godkännande innefattar prövningen en tillämpning av rättsliga regler eller principer.⁵²

I EU:s cyberresiliensförordning finns en uppräkningslista av de krav och processer som ska uppnås för produkten och som ett organ för bedömning bedömer enligt förordningens bestämmelser, bland annat ska produkter med digitala element uppfylla angivna väsentliga cybersäkerhetskrav. Organen har även skyldighet att tillämpa förfaranden och standarder som anges i eller följer av förordningen. Det är således inte fråga om beslut som meddelas efter rent skönsmässiga överväganden. För en tillverkare som på rimliga grunder kan hävda att denne uppfyller kriterierna för ett godkännande av ett kvalitetssystem eller att en produkt uppfyller kraven enligt EU:s cyberresiliensförordning får det anses vara fråga om en rättighet enligt nationell rätt. Denna rättighet är även civil till sin karaktär.⁵³ De uppgifter som ett organ för bedömning utför kan således utmynnas i beslut som får verkningar för en enskild och därmed påverka dennes situation på ett inte obetydligt sätt. Sådana beslut är normalt överklagningsbara även enligt allmänna förvaltningsrättsliga principer.⁵⁴

Utredningen bedömer att det förvaltningsrättsliga kravet på rättsskydd för enskilda och kravet på domstolsprövning i artikel 6.1 EKMR innebär att det finns behov att införa bestämmelser om rätt att överklaga beslut av ett anmält organ. Som ovan framgår gäller en motsvarande rätt till överklagande av ett anmält organs beslut även enligt 20 § lagen (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt. Det bör därför införas regler om överklagande av de anmälda organens beslut som i sak motsvarar de bestämmelser som gäller för överklagande av beslut enligt förvaltningslagen. En bestämmelse med denna innebörd ska därför finnas i den kompletterande lagen. Rätten till överklagandet bör dock begränsas till att omfatta frågor som regleras i EU:s cyber-

⁵¹ Se HFD 2016 ref. 49.

⁵² Se till exempel HFD 2016 ref. 49.

⁵³ Högsta förvaltningsdomstolen har tidigare uttalat att så bör anses vara fallet om det inte finns klart stöd för en annan bedömning (se till exempel HFD 2019 ref. 10 p. 19).

⁵⁴ Jfr 41 § förvaltningslagen och prop. 2016/17:180, s. 248 och 251 f.

resiliensförordning och anslutande föreskrifter. Ett överklagande med stöd av denna bestämmelse bör därför inte gälla för rent civilrättsliga tvister mellan parterna, exempelvis om betalning av avgifter.

Frågan om överklagandemyndighet

I sammanhanget uppkommer även frågan vilken instans som i första hand bör pröva överklaganden av anmälda organs beslut, dvs. om beslut av organ för bedömning ska kunna överklagas först till en överklagandemyndighet eller direkt till domstol. Av betydelse är här om arten och omfattningen av överklagbara beslut föranleder särskilda överväganden när det gäller vilken instansordning för överprövning som bör finnas för att vara rättssäker, ändamålsenlig och kostnadseffektiv.

I detta sammanhang gör sig fler aspekter gällande, bland annat om det bör finnas en överklagandemyndighet för alla eller vissa typer av beslut som fattas av ett anmält organ. Vidare bör beaktas att många av de beslut som kommer att fattas med stöd av EU:s cyberresiliensförordning även kan innefatta frågor som regleras i annan unionsrättslig eller nationell anslutande författning. Det kan till exempel avse beslut som gäller bedömning av överensstämmelse med väsentliga krav på cybersäkerhet och skyldigheter som gäller för sårbarhetshantering enligt EU:s cyberresiliensförordning och som samtidigt även berör giltigheten av ett certifikat för produkten enligt EU:s cybersäkerhetsakt. I den förstnämnda prövningen sker bedömning av överensstämmelse med de angivna cybersäkerhetskraven och skyldigheten att rapportera sårbarheter i produkten enligt EU:s cyberresiliensförordning och den ordning som ska gälla för marknadskontroll, dvs. det är i första hand den utpekade marknadskontrollmyndigheten som utövar tillsyn över att dessa skyldigheter fullgörs. Om produkten även är certifierad enligt en europeisk certifieringsordning kan även en fråga om certifikatets giltighet komma att uppstå, vilka kan aktualisera frågor som prövas enligt den nationella instansordning som för närvarande gäller för sådana mål enligt EU:s cybersäkerhetsakt och den kompletterande lagen. Om föremålet för domstolens prövning även rör en produkt som utgör en del av en digital plånbok enligt förordning (EU) 2024/1183 (eIDAS-förordningen) eller förordning (EU) 2024/1689 (AI-förord-

ningen) och som ingår i ett högrisk-AI-system som omfattas av AI-förordningens regelverk uppkommer en komplex frågeställning om hur den instansordningen som bör finnas för överprövning av dessa olika frågor bör vara utformad.

En ordning med en överklagandemyndighet finns i och för på andra rättsområden. I betänkandet *En ny förvaltningslag* (SOU 2010:29)⁵⁵ anges bland annat följande (s.698 f):

Enligt 4 § fordonslagen (2002:574) överklagas beslut i enskilda fall hos förvaltningsdomstol. Har beslutet fattats av organ utanför myndighetssfären gäller överklagandelagens regler. I 5 kap. 5 § har intagits en uttrycklig bestämmelse av samma innebörd som överklagandelagen, dvs. att ett överklagande ska ges in till den instans som ska pröva det. Enligt bestämmelsen får ett antal närmare angivna beslut utan begränsning till viss tid överklagas hos Transportstyrelsen, dit överklagandet också ska ges in.

Regeringen ansåg (prop. 2001/02:130 s. 99) att det fanns vissa typer av beslut, där det var motiverat att behålla Vägverket (numera Transportstyrelsen) som överprövningsinstans. Det gällde ärenden som främst avsåg rent tekniska frågor, t.ex. då det var fråga om beslut av en polisman, en bilinspektör eller ett besiktningsorgan om körförbud. Ett överklagande av ett sådant beslut borde främst av praktiska skäl ges in direkt till överklagandemyndigheten, dvs. Vägverket (Transportstyrelsen). Överinstansens prövning kunde därmed ske i nära anslutning till överklagandet och hela proceduren torde kunna ske tämligen omgående och på ett för fordonsägaren effektivt sätt. Regeringen pekade (s. 92 f.) också på att de ärenden som behandlas av besiktningsorganen huvudsakligen är av teknisk karaktär. Handläggningen består sålunda till stor del av en fysisk kontroll av fordonet, varför behovet av andra förfaranderegler än sådana som anger vad som ska kontrolleras torde vara relativt litet.

Genom lagändringar, som avses träda i kraft den 1 juli 2010 (prop.2009/10:32), kommer besiktningsverksamhet att kunna utföras av ett ökat antal enskilda subjekt. Samtidigt införs bl.a. bestämmelser om omprövning i 4 kap. 3 § fordonslagen. Detta innebär dock inte någon förändring avseende till vem ett överklagande ska ges in till.

Det kan noteras att frågan om behovet av en överklagandemyndighet för beslut av organ för bedömning inom cybersäkerhetsaktens tillämpningsområde var föremål för överväganden i betänkandet *EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering* (SOU 2020:58). I betänkandet anföras bland annat (s. 258):

⁵⁵ I betänkande finns en redogörelse för förekomsten av överklagandemyndigheter på andra rättsområden, s. 697 ff.

Utredningen har övervägt behovet av en ordning med en s.k. överklagandemyndighet som första instans. Också i det fallet gör sig behovet av kompetens och specialisering gällande. Den nationella myndigheten för cybersäkerhetscertifiering hade därmed kunnat komma i fråga som överklagandemyndighet. Utredningen anser att de föreslagna åtgärderna innebär tämligen generösa möjligheter till både omprövning och överklagande. Vidare ska en klagande, i tillämpliga fall, kunna vända sig till den nationella cybersäkerhetscertifieringsmyndigheten i fråga om tillsynsåtgärder. Sammantaget med målet att undvika onödig tidsutdräkt finner utredningen inte anledning att inrätta en instansordning med även en överklagandemyndighet.

I propositionen (2020/21:186) med *Kompletterande bestämmelser till EU:s cybersäkerhetsakt* anslöt sig regeringen till utredningens bedömning och anförde (s. 52 f):

Enligt artikel 6.1 i Europakonventionen, som gäller som lag, gäller att var och en vid prövningen av hans eller hennes civila rättigheter ska vara berättigad till en rättvis och offentlig förhandling inom skälig tid och inför en opartisk domstol som har upprättats enligt lag.

Beslut om bl.a. cybersäkerhetscertifiering och sanktionsavgifter enligt EU:s cybersäkerhetsakt och den föreslagna lagen innefattar prövningar som faller inom tillämpningsområdet för artikel 6.1. En överprövning av sådana beslut måste därför vara förenlig med konventionens krav i fråga om domstolsprövning. Regeringen föreslår därför, i linje med *Lunds universitets* synpunkter, att det i lagen införs bestämmelser om överklagande som innebär att beslut enligt EU:s cybersäkerhetsakt och den nya lagen av den nationella myndigheten för cybersäkerhetscertifiering eller av organ för bedömning av överensstämmelse ska få överklagas till allmän förvaltningsdomstol.

I likhet med vad som allmänt gäller i fråga om överklagande av förvaltningsbeslut bör det krävas prövningstillstånd vid överklagande till kammarrätten. Detta bör anges i lagtexten.

Domstolsverket uppmärksammar att det kan förekomma uppgifter som är säkerhetsklassificerade enligt säkerhetsskyddslagen (2018:585) i ett överklagat ärende. Regeringen anser dock inte att de praktiska och ekonomiska skäl som myndigheten pekar på ger anledning att i detta lagstiftningsärende överväga särskilda forumregler för mål i domstol enligt det aktuella regelverket.

Utredningens lagförslag reglerar inte frågan om vilken ställning ett privat organ har vid ett överklagande till domstol. Som *Förvaltningsrätten i Stockholm* uppmärksammar finns det dock rättspraxis som ger stöd för att ett enskilt rättssubjekt i vissa fall kan ges motpartsställning även utanför tillämpningsområdet för 7 a § förvaltningsprocesslagen (1971:291). Regeringen konstaterar att det inte finns beredningsunderlag för att överväga en eventuell sådan reglering.

Utredningen kan konstatera att när det gäller frågan en instansordning med en överklagandemyndighet gör sig även i detta fall frågan om behov av kompetens och specialisering sig gällande. Den föreslagna marknadskontrollmyndigheten skulle i och för sig kunna komma i fråga som överklagandemyndighet. Som framgår av artikel 6.1 EKMR ska prövningen göra av domstol. Europadomstolen har förklarat att termen ”domstol” (”tribunal”) inte ska tolkas så att den enbart avser domstolar av traditionellt slag. Det avgörande är vilken funktion som den ifrågavarande institutionen i realiteten har och inte hur den benämns eller klassificeras i nationell rätt. Den utpekade marknadskontrollmyndigheten skulle då kunna fylla en funktion som överklagandeinstans i ärenden som gäller EU-typkontrollintyg och beslut om godkännande av kvalitetssystem. För detta talar att den myndigheten i sin egenskap av marknadskontrollmyndighet på området får antas ha tillräcklig kompetens att pröva frågor av det här slaget. En klagande ska utöver att lämna klagomål även kunna vända sig till marknadskontrollmyndigheten i fråga om andra tillsynsåtgärder. Marknadskontrollmyndigheten ska vid behov samverka med det nationella ackrediteringsorganet Swedac i frågor som gäller tillsyn över organ för bedömning. För att säkerställa oberoendet vid prövning av dessa fall skulle krävas att myndighetens verksamhet organiseras på ett sätt som medför att frågan om myndighetens opartiskhet inte uppkommer.

Vidare framstår det som ovan anges som lämpligt att samma ordning som gäller för överklagande av beslut enligt lagen (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt även ska gälla för överklagande av beslut enligt EU:s cyberresiliensförordning.

Utredningen har därför inte funnit övertygande skäl för en instansordning med en överklagandemyndighet. Sammantaget med målet att åstadkomma en ändamålsenlig, effektiv och en rättssäker instansordning samt undvika onödig tidsutdräkt finner utredningen inte anledning att föreslå att en instansordning med en överklagandemyndighet ska inrättas.

Ett beslut av ett organ för bedömning av överensstämmelse ska därför överklagas till allmän förvaltningsdomstol. Prövningstillstånd ska krävas vid överklagande till kammarrätten.

6.14.2 Det anmälda organet ska vara motpart

Utredningen föreslår att ett anmält organs beslut ska vara överklagbart (se ovan). Om en myndighet fungerar som anmält organ följer enligt 7 a § förvaltningslagen (2017:900) att myndigheten i egenskap av förvaltningsmyndighet intar motpartsställning om det är en enskild som överklagar. Anmälda organ är dock ofta privaträttsliga organ. Av det skälet behöver ställningen som motpart vid ett överklagande för ett anmält organ som är ett privaträttsligt organ övervägas.

Det finns visst stöd i rättspraxis för att privaträttsliga organ kan ges motpartsställning i förvaltningsdomstol, se HFD 2019 ref. 43. Det är dock inte en självklarhet att ett enskilt privaträttsligt organ intar sådan ställning i förvaltningsrätt, utan det tycks krävas ett tillräcklig kvalificerat intresse av att få delta i processen.⁵⁶

I sammanhanget kan även nämnas att i förarbetena till lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt konstaterade regeringen att utredningens lagförslag inte reglerade frågan om vilken ställning ett privat organ har vid ett överklagande till domstol samt att det inte fanns beredningsunderlag för att överväga en reglering om att privata organ skulle inta motpartsställning i domstol. Av det skälet föreslog lagstiftaren inte någon reglering av privata organs ställning vid överklagande till domstol.⁵⁷ Utredningen gör bedömningen att en motsvarande oklarhet nu inte bör finnas i kompletteringslagen.

I syfte att klargöra det privata organets intresse av att vara motpart i förvaltningsdomstolsprocessen bör det privata organet i lag pekas ut som motpart i processen. Det finns därför övervägande skäl som talar för att det bör införas en bestämmelse som tydliggör att ett anmält organ är motpart i förvaltningsdomstol så att partsställningen tydliggörs, oavsett om beslutande organ är ett privat organ eller en förvaltningsmyndighet.

⁵⁶ Jfr von Essen, Förvaltningsprocesslagen (5 mars 2025, JUNO) kommentaren till 7 a § under rubriken Motpartsställning utanför paragrafens tillämpningsområde.

⁵⁷ Prop. 2020/21:186 Kompletterande bestämmelser till EU:s cybersäkerhetsakt, s. 52 f.

6.14.3 Överklagande av förvaltningsmyndighets beslut

Vid handläggning av ärenden hos förvaltningsmyndigheterna är förvaltningslagen (2017:900) tillämplig (1 §).

Enligt 40 § förvaltningslagen (2017:900) överklagas beslut till allmän förvaltningsdomstol.

Enligt 41 § får ett beslut överklagas om det kan antas påverka någons situation på ett inte obetydligt sätt. Den första förutsättningen för att ett beslut ska vara överklagbart är att det rör sig om ett beslut i ett förvaltningsärende, dvs. ett förvaltningsbeslut. Den andra förutsättningen är att beslutet kan antas påverka någons situation på ett visst sätt. Det är beslutets faktiska verkningar som avgör om det är överklagbart och prövningen av om ett visst beslut kan antas påverka någons situation utgår från en objektiv bedömning som tar sikte på beslutets faktiska verkningar, främst i förhållande till dennes personliga eller ekonomiska situation (se prop. 2016/17:180 s. 332).

Enligt 42 § förvaltningslagen (2017:900) får ett beslut överklagas av den som beslutet angår, om det har gått honom eller henne emot. Rätten att överklaga förutsätter att beslutet antingen påverkar klagandens rättsliga ställning eller rör ett intresse som han eller hon har och som erkänts av rättsordningen. Exempelvis kan det vara fråga om att den beslutande myndigheten ska ta hänsyn till intresset vid sin materiella prövning av ärendet. I vissa fall har även den som har ett beaktansvärt intresse i saken fått överklaga beslutet. Avgörande för rätten att överklaga är med andra ord den effekt som beslutet får för den som vill överklaga.

Som framgår av avsnitt 6.13.4 ställer artikel 6 i EKMR krav på att en enskild ska ha rätt till en rättvis domstolsprövning vid prövning av hans eller hennes civila rättigheter och skyldigheter. Myndigheter utgör inte några självständiga juridiska personer utan agerar som företrädare för staten. De kan därför i princip inte föra talan mot varandra. Statliga myndigheter anses inte utan författningsstöd kunna överklaga beslut av en annan myndighet, om inte myndigheten i fråga företräder ett rent privaträttsligt intresse.

Av FL framgår formerna för överklagande av en förvaltningsmyndighets beslut. En förvaltningsmyndighets beslut ska enligt 14 § andra stycket lagen (1971:289) om allmänna förvaltningsdom-

stolar överklagas till den förvaltningsrätt inom vars domkrets ärendet först prövats.⁵⁸

6.14.4 Rätt att överklaga myndighets beslut enligt den nya lagen

EU:s cyberresiliensförordning reglerar flera olika sakområden där en förvaltningsmyndighet, dvs. en anmälände myndighet eller en marknadskontrollmyndighet, kommer att besluta i frågor som kan antas påverka en enskilds eller en myndighets situation när de agerar som ekonomisk aktör, som förvaltare av programvara med fri och öppen källkod eller som organ för bedömning av överensstämmelse. Det gäller exempelvis beslut om åtgärder för marknadskontroll enligt artikel 14.4 i EU:s marknadskontrollförordning, om förelägganden att EU:s marknadskontrollförordning ska följas och beslut om sanktioner. Sådana beslut ska enligt utredningens förslag som huvudregel fattas av angivna förvaltningsmyndigheter, dvs. anmälände myndighet och marknadskontrollmyndigheten.

Rätten till överklagande bör därför gälla för såväl ekonomiska aktörer och förvaltare av programvara som för organ för bedömning av överensstämmelse och det oavsett om de är enskilda eller offentliga organ.

Utredningen har föreslagit att sanktionsavgift enligt förordningen ska få beslutas mot myndigheter (se avsnitt 10.3.2). Myndigheter bör mot den bakgrunden få överklaga förvaltningsmyndighetens beslut.

Kompletteringslagen bör därför innehålla en bestämmelse om överklagande av förvaltningsmyndighets beslut som ger myndigheter en uttrycklig rätt att överklaga förvaltningsmyndigheters beslut. Skälet för detta är att statliga myndigheter inte utgör självständiga juridiska personer utan agerar som företrädare för staten och därför i princip inte kan föra talan mot varandra. Statliga myndigheter anses inte utan författningsstöd kunna överklaga beslut av en annan myndighet, om inte myndigheten i fråga företräder ett rent privaträttsligt intresse.⁵⁹

⁵⁸ I förvaltningsdomstol gäller förvaltningsprocesslagen (1971:291).

⁵⁹ Lagrådsremissen Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag, s. 170.

När en myndighet, dvs. staten eller en kommun eller region, handlar som en enskild i form av en ekonomisk aktör torde det inte föreligga skäl att särbehandla myndigheten som då även bör ha rätt att överklaga en annan förvaltningsmyndighets beslut som riktas mot myndigheten. Men när en myndighet agerar i sin offentlig-rättsliga roll anses den inte ha klagorätt om det inte finns särskilda föreskrifter om det.⁶⁰

Begreppet förvaltningsmyndighets beslut innefattar i sammanhanget såväl beslut som fattas av en marknadskontrollmyndighet som beslut som fattas av anmälade myndighet. I syfte att undvika oklarheter om att en myndighet i rollen som ekonomisk aktör eller organ för bedömning av överensstämmelse ska ha en rätt att överklaga en förvaltningsmyndighets beslut, bör regleringen om överklagande utgöra ett författningsstöd även för dem. Detta gäller oavsett om en myndighet agerar som enskild eller i sin offentlig-rättsliga roll när myndigheten agerar i egenskap av ekonomisk aktör eller anmält organ enligt EU:s cyberresiliensförordning.

Utredningen har övervägt om det i bestämmelsen uttryckligen behöver anges att en myndighet får överklaga en förvaltningsmyndighets beslut för att bestämmelsen ska utgöra en sådan tydlig föreskrift om rätten för en statlig, kommunal eller regional myndighet att överklaga ett beslut.⁶¹

Utredningen bedömer att övervägande skäl talar för att det av tydlighetsskäl uttryckligen bör framgå av överklagandebestämmelsen att en myndighet får överklaga en förvaltningsmyndighets beslut och föreslår därför en sådan bestämmelse.

En förvaltningsmyndighets beslut enligt EU:s cyberresiliensförordning, den kompletterande lagen och föreskrifter som meddelas i anslutning till den bör kunna överklagas till den förvaltningsrätt inom vars domkrets ärendet först prövats. Denna ordning överensstämmer med huvudregeln i 14 § andra stycket lagen (1971:289) om allmänna förvaltningsdomstolar och med regleringen i den kompletterande lagen med bestämmelser till EU:s cybersäkerhetsakt och den nya cybersäkerhetslagen.

⁶⁰ Kommuners och regioners rätt att överklaga förvaltningsbeslut regleras bland annat genom speciallag och i andra fall avgörs överklaganderätten med ledning av regeln i 7 a § förvaltningsprocesslagen eller sedvanerätt.

⁶¹ Sådana föreskrifter finns i vissa andra regelverk, till exempel för Trafikverket och länsstyrelsen i 76 § väglagen (1971:948) samt för Transportstyrelsen, Strålsäkerhetsmyndigheten, Försvarsmakten och MSB i 13 kap. 14 § plan- och bygglagen (2010:900).

Rätten till överklagande bör således gälla för både offentliga och enskilda.

När det gäller beslut som fattas av anmälda organ som inte är myndigheter har utredningen övervägt och lämnat förslag på att det ska införas en överklagandeprocess som innebär en överprövning av förvaltningsdomstol (se avsnitt 6.14.1).

Eftersom bestämmelserna om anmälda organ i EU:s cyberresiliensförordning börjar tillämpas 11 juni 2026 finns i dag inga anmälda organ för bedömning av överensstämmelse i myndighetsform. Dock bör i sammanhanget beaktas att den möjligheten kan uppstå i framtiden och då gäller förvaltningslagens bestämmelser för överklagande av sådana beslut om inte annat är föreskrivet. Beslut som ett sådant organ i form av en myndighet fattar utgör ett förvaltningsbeslut enligt förvaltningslagen och ett sådant beslut får överklagas om beslutet kan antas påverka någons situation på ett inte obetydligt sätt.

6.14.5 Förvaltningsmyndighet ska vara motpart

EU:s cyberresiliensförordning reglerar ekonomiska aktörers rättigheter och skyldigheter när det gäller produkter med digitala element. Som regleringen är utformad kan såväl en enskild som ett offentligt organ vara en ekonomisk aktör i förordningens mening och därför omfattas av dess bestämmelser. Marknadskontroll ska därför utövas gentemot såväl enskilda som offentliga organ. Anmälade myndigheter ska bedriva tillsyn mot anmälda organ.

Av 7 a § förvaltningsprocesslagen följer vem som är motpart vid överklagande av en enskild.⁶² Det är emellertid inte givet att en förvaltningsmyndighet intar motpartsställning när en statlig myndighet överklagar en förvaltningsmyndighets beslut. Detta av det skälet att statliga myndigheter i princip inte får föra talan i domstol mot varandra. För att undvika otydligheter om motpartsställningen bör det framgå av överklagandebestämmelsen att förvaltningsmyndigheten ska vara motpart i domstolen. Motpartsförhållandet gäller därmed i förhållande till samtliga klaganden, dvs. såväl enskilda som myndigheter.

⁶² En statlig förvaltningsmyndighet ska ha ställning som motpart i förvaltningsrätt när en kommun överklagar dess beslut (HFD 2022 ref. 37).

6.14.6 Prövningstillstånd i kammarrätt

Beslut av förvaltningsmyndigheter kan enligt 40 § förvaltningslagen (2017:900) överklagas till allmän förvaltningsdomstol. Av andra stycket följer att det krävs prövningstillstånd vid överklagande till kammarrätten.

Enligt utredningen bör detsamma gälla även avseende beslut enligt EU:s cyberresiliensförordning, kompletteringslagen och föreskrift som har meddelats i anslutning till kompletteringslagen och beslut som fattas av anmälda organ, där förvaltningslagen inte är tillämplig. Det bör därför införas en bestämmelse i paragrafen om överklagande som anger att det krävs prövningstillstånd i kammarrätten.

7 Standardisering

7.1 Inledning

Förordning (EU) 2024/2847¹ (EU:s cyberresiliensförordning) bygger på lagstiftningsmetoden den nya lagstiftningsramen (New Legislative Framework, NLF). Rättsakterna enligt den nya lagstiftningsramen innehåller endast de grundläggande krav som en produkt ska uppfylla. De närmare tekniska detaljerna återfinns i stället i harmoniserade standarder som utarbetas av europeiska standardiseringsorgan på uppdrag av kommissionen, så kallad standardiseringsbegäran enligt artikel 10.1 i förordning (EU) 1025/2012² (EU:s standardiseringsförordning). Harmoniserade standarder spelar därmed en avgörande roll i denna lagstiftningsmetod genom att fungera som verktyg för att uppfylla lagkraven på ett tydligt och effektivt sätt. Harmoniserade standarder som är publicerade i Europeiska unionens officiella tidning ger presumtion om överensstämmelse med lagstiftningen vilket innebär att när en produkt följer en harmoniserad standard anses den automatiskt uppfylla lagstadgade krav.

Processerna för att ta fram standarder kan komma att innebära ett omfattande åtagande både i fråga om resurser och personal för bland annat deltagande i standardiseringsorganisationernas arbetskommittéer. Utredningen ska därför bedöma vilka konsekvenser standardiseringsarbetet som följer av förslagen kan antas medföra för berörda myndigheter, företag och andra nationella organisationer.

¹ Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen).

² Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG.

I detta kapitel redogörs närmare för det standardiseringsarbete som utförs till stöd för EU:s cyberresiliensförordning, intressenter-
nas roll i detta arbete och de utmaningar som arbetet medför för
dessa intressenter.

7.2 Standardisering i Sverige

7.2.1 De tre nationella standardiseringsorganen

Det operativa standardiseringsarbetet utförs i Sverige av de tre formellt utsedda standardiseringsorganen Svenska Institutet för Standarder (SIS), SEK Svensk Elstandard (SEK) och Svenska Informations- och Telekommunikationsstandardiseringen (ITS). De tre organen är ideella föreningar med medlemmar som kommer från näringsliv, statlig förvaltning och organisationer.

SIS ansvarar för all svensk standardisering utom inom el- och telekommunikationsområdet. SEK ansvarar för svensk standardisering inom elområdet och inom vissa grundläggande angränsande teknikområden. ITS är det nationella standardiseringsorganet för informations- och telekommunikationsområdet. För att representera konsument- och arbetstagare i standardiseringen har Sveriges konsument- och arbetstagarrådet (SKA-rådet) bildats.³

SIS, SEK och ITS är utsedda av regeringen som nationella standardiseringsorgan och är anmälda till kommissionen enligt artikel 27 i EU:s standardiseringsförordning. Europeiska kommittén för standardisering (Comité Européen de Normalisation, CEN), Europeiska kommittén för elektroteknisk standardisering (Comité Européen de Normalisation Électrotechnique, Cenelec) och Europeiska institutet för telekommunikationsstandarder (European Telecommunications Standards Institute, ETSI) är de av kommissionen erkända europeiska standardiseringsorganen enligt artikel 2.8 i EU:s standardiseringsförordning.

Internationella standardiseringsorganisationen (International Organization for Standardization, ISO), Internationella elektrotekniska kommissionen (International Electrotechnical Commis-

³ SKA-rådet, som bildades 1990 som SSR Konsumentråd, har bland annat till uppgift att säkerställa användarnas inflytande i nationell och internationell standardiseringen och att öka medvetenheten om användarfrågornas betydelse. I SKA-rådet finns representanter för Funktionsrätt Sverige, Sveriges Konsumenter, Naturskyddsföreningen, LO, SACO och TCO. Sedan 2024 är SKA-rådet en del av SIS.

sion, IEC) och Internationella teleunionen (International Telecommunication Union, ITU) är de tre internationella standardiseringsorganen.

Den svenska organisationen följer den formella europeiska strukturen som i sin tur följer den formella internationella strukturen för hur standardisering är organiserad. Arbetsfördelningen kan enklast beskrivas utifrån de områden som omfattas av respektive organisation. SEK/Cenelec/IEC ansvarar för det elektrotekniska området, ITS/ETSI/ITU för telekommunikationsområdet och SIS/CEN/ISO för alla övriga områden.

Organens arbetssätt och förutsättningar skiljer sig till viss del åt. Standardisering inom SIS och SEK sker på nationell nivå. Deltagande i europeisk och internationell standardisering sker genom nationell delegation. Standardiseringen på informations- och telekommunikationsområdet utmärks av att medverkan i arbetet sker direkt av deltagarna i ETSI och den internationella motsvarande organisationen (ITU-T) utan nationell representation. ITS är ett forum för informations- och erfarenhetsutbyte och ansvarar för beslut och omröstningar som enligt förordning (EU) 2022/2480⁴ ska fattas av de nationella standardiseringsorganen.

7.2.2 Standardiseringsorganens finansiering

SIS och SEK finansierar sin verksamhet genom en kombination av olika intäktskällor. Dessa inkluderar medlemsavgifter, försäljning av standarder och utbildningar, samt anslag från staten. ITS finansierar sin verksamhet genom medlemsavgifter samt anslag från staten.

Det statliga stödet till SIS, SEK och ITS samt SKA-rådet fastställs årligen i ett regeringsbeslut som innehåller riktlinjer för stödet. För 2025 har regeringen tilldelat SIS 33 000 000 kronor, SEK 4 136 000 kronor och ITS 2 500 000 kronor. SKA-rådet har tilldelats 5 500 000 kronor. För framtagande av harmoniserade standarder ska SIS använda 6 000 000 kronor, SEK 1 200 000 kronor och ITS 1 200 000 kronor. Regeringen har även särskilt beslutat att SIS ska använda 3 300 000 kronor för digitalisering och cybersäkerhet. SEK ska använda 200 000 kronor för digitalisering och

⁴ Europaparlamentets och rådets förordning (EU) 2022/2480 av den 14 december 2022 om ändring av förordning (EU) nr 1025/2012 vad gäller europeiska standardiseringsorganisationers beslut om europeiska standarder och europeiska standardiseringsprodukter.

cybersäkerhet. Tilldelade medel för digitalisering och cybersäkerhet ska användas för att bland annat främja säker och hållbar digitalisering, näringslivets och samhällets digitala strukturuomvandling samt öka kunskap om cybersäkerhet i standardiseringsarbetet. Det statliga bidraget låg mellan 2017 och 2024 på 31 336 00 kronor men har för 2025 höjts med 13 800 000 kronor till 45 136 000 kronor för att adekvat resurssätta svensk standardisering och för att effektivt bevaka och främja svenska intressen inom standardiseringen på europeisk och internationell nivå.⁵

Det kan även förekomma projektfinansiering.⁶

7.3 Kommissionens standardiseringsbegäran

Kommissionen har lämnat en standardiseringsbegäran⁷ till CEN, Cenelec och ETSI för att ta fram sammanlagt 41 harmoniserade standarder⁸ som stöd för EU:s cyberresiliensförordning. CEN och Cenelec har fått i uppdrag att ta fram 15 horisontella standarder och tre vertikala standarder för kritiska produkter med digitala element. I framtagandet av de tre standarderna för kritiska produkter får endast representanter från organisationer som är etablerade inom EU eller individer som möter unionsintressen delta. De övriga 23 vertikala produktstandarderna ska CEN, Cenelec och ETSI gemensamt ta fram.

CEN, Cenelec och ETSI ska ta fram ett gemensamt arbetsprogram och regelbundet avrapportera till kommissionen. De första två horisontella standarderna ska levereras i augusti 2026, de

⁵ Regeringsbeslut daterat 2024-12-19, UD2024/17860, Riktlinjer för budgetåret 2025 avseende Svenska institutet för standarder (SIS), Sveriges konsument- och arbetstagarråd (SKA-rådet), Svensk Elstandard (SEK), Svenska informations- och telekommunikationsstandardiseringen (ITS).

⁶ Exempelvis från European Innovation Council and SMEs Executive Agency (EISMEA).

⁷ Commission Implementing Decision of 3.2.2025 on a standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), C(2025) 618 final.

⁸ Det rör sig om 15 horisontella och 26 vertikala standarder. Horisontella standarder adresserar gemensamma cybersäkerhetskrav som gäller för olika produktkategorier och fastställer en grundläggande säkerhetsnivå. Vertikala standarder är specifika för olika produktkategorier med detaljerade cybersäkerhetskrav anpassade till de unika egenskaperna hos dessa produktkategorier.

26 vertikala produktstandarderna ska levereras i oktober 2026 och de övriga 13 horisontella standarderna ska levereras i oktober 2027.

De harmoniserade standarderna ska återspegla den allmänt erkända tekniska utvecklingen (state of the art) i syfte att minimera de cybersäkerhetsrisker som uppstår vid planering, design, utveckling, produktion, leverans och underhåll av produkter med digitala element, i syfte att förebygga säkerhetsincidenter och minimera effekterna av sådana incidenter. De harmoniserade standarder som utvecklas ska bygga vidare på det arbete som pågår för att stödja kommissionens delegerade förordning (EU) 2022/30.⁹ Där det är möjligt bör CEN, Cenelec och ETSI uppdatera existerande standarder för att anpassa dem efter kraven i EU:s cyberresiliensförordning. Standarderna ska även vara förenliga med andra relevanta europeiska och harmoniserade standarder inom olika sektorer. De horisontella harmoniserade standarderna ska behandla olika aspekter och mekanismer för produktcybersäkerhet och ska stödja utvecklingen av detaljerade vertikala harmoniserade standarder för specifika produkter eller produkttyper och stödja tillverkare med att definiera och genomföra de säkerhetskrav som gäller för deras respektive produkter, särskilt för produkter som inte omfattas av befintliga eller planerade vertikala standarder. Den horisontella harmoniserade standarden för sårbarhetshantering ska tillhandahålla specifikationer för processer för hantering av sårbarheter som täcker alla relevanta produktkategorier som ska implementeras av tillverkare av produkter med digitala element. De vertikala harmoniserade standarder som ska tas fram ska tillhandahålla specifikationer för cybersäkerhetskraven för viktiga och kritiska produkter med digitala element.

7.4 Intressenternas roll och fördelar med att delta i standardiseringsarbete

Ett av målen enligt Regeringens strategi för standardisering är att stärka Sveriges inflytande i de internationella och europeiska standardiseringsorganen. Myndigheter, företag, institutioner för forsk-

⁹ Kommissionens delegerade förordning (EU) 2022/30 av den 29 oktober 2021 om komplettering av Europaparlamentets och rådets direktiv 2014/53/EU vad gäller tillämpningen av de väsentliga krav som avses i artikel 3.3 d, e och f i det direktivet.

ning och utbildning samt användarorganisationer spelar alla en viktig roll i detta arbete.¹⁰

Enligt den Nationella strategin för cybersäkerhet 2025–2029 ska Sverige slå vakt om fortsatt inflytande inom internationell standardisering och bidra till välanpassade internationella standarder som främjar säkra leveranskedjor. Berörda statliga myndigheter, i samarbete med näringslivet, ska verka bland annat för att nya standarder för cybersäkerhet utvecklas transparent samt att svenska behov och prioriteringar får genomslag.¹¹

Standardiseringen är en intressentstyrd verksamhet som bygger på intressenternas aktiva bidrag med expertkunskap och arbetstid. Särskilt viktigt är att de intressenter som i praktiken ska uppfylla standardens krav, och de som kommer att påverkas av hur standarden används, ges stort inflytande. För att säkerställa att standarder uppfyller mindre företags behov måste även dessa vara vederbörligen företrädna när standarder utvecklas. Genom att påverka utformningen av standarder kan företag stärka sin egen konkurrenskraft, trovärdighet och varumärke. Deltagande i standardisering ger även möjlighet att stärka sitt branschnätverk genom att nätverka och skapa kontakter inom industrin. Intressenterna får även insyn i förändringar, marknadstrender och utveckling i branschen som kan användas inom ramen för verksamhetsplaneringen. Sammantaget bidrar deltagande i standardiseringsarbetet till en positiv samhällsutveckling.

Det är även nödvändigt att myndigheter ges mandat till, resurser för och själva prioriterar ett aktivt deltagande i standardiseringsarbete. Det gäller i synnerhet när standarder som används som referens i myndighetsutövning tas fram. Marknadskontrollmyndigheternas engagemang i standardiseringsarbetet är viktigt för att säkerställa en adekvat kravnivå för produkter med digitala element. Harmoniserade standarder används även i marknadskontroll varför det är av vikt för marknadskontrollmyndigheten att ha goda kunskaper om standarder och standardisering. Dessutom har EU-domstolen kommit med flera avgöranden där den har granskat harmoniserade standarders legala status och som fastslår att harmoniserade standarder

¹⁰ Regeringens strategi för standardisering, <https://www.regeringen.se/contentassets/8728299ccd5940fcb7b927d1c81d4fa7/regeringens-strategi-for-standardisering/>, s. 3.

¹¹ Regeringens skrivelse 2024/25:121, Nationell strategi för cybersäkerhet 2025–2029, s. 18.

är att se som en del av EU-lagstiftningen.¹² Marknadskontrollmyndigheternas medarbetare behöver ha god kontakt med teknikutvecklingen, öka sin kompetens och kan fånga upp tidiga trender. Vidare behöver marknadskontrollmyndigheternas medarbetare med sin kompetens påverka så att relevanta cybersäkerhetskrav ställs. Arbetet i standardiseringskommittéerna gör också att frågeställningar blir allsidigt belysta och kraven blir tekniskt möjliga att uppfylla. I myndighetens roll ingår också att se till konsumenterna och allmänhetens intressen.

Intresseorganisationer såsom konsument-, arbetstagar- och miljöorganisationer samt andra ideella organisationer har en roll i standardiseringen för att föra in ett tydligt användarperspektiv i standardiseringen.

När forskning och utveckling av nya produkter och innovationer inleds bör hänsyn tas till befintliga standarder redan från början för att underlätta marknadstillträdet. Delaktighet och engagemang i internationellt standardiseringsarbete har därför en avgörande betydelse för kommersialisering och nyttiggörande av nya produkter och tjänster.¹³

7.5 Standardiseringsarbete som stöd för EU:s cyberresiliensförordning

7.5.1 CEN och Cenelec

Standardiseringsarbetet för framtagandet av de femton horisontella harmoniserade standarderna sker i CEN och Cenelecs gemensamma tekniska kommitté CEN/CLC/JTC 13 Cybersecurity and Data Protection, WG 9 Special Working Group on Cyber Resilience Act.

De vertikala harmoniserade standarder för kritiska produkter med digitala element tas fram i CEN och Cenelecs gemensamma tekniska kommitté CEN/CLC/JTC 13 Cybersecurity and Data Protection, WG 6 Product Security, Cenelecs tekniska kommitté CLC/TC 47X Semiconductors and Trusted Chip Implementation, WG 3 SmartCards and Secure Element Platforms och CEN:s tekniska kommitté CEN/TC 224 Personal identification and related

¹² Se bland annat EU-domstolens dom i mål C-613/14 James Elliott och EU-domstolens dom i mål C-588/21 P Public.Resource.Org och Right to Know mot kommissionen m.fl.

¹³ Regeringens strategi för standardisering, s. 23 f.

personal device with secure elements, systems, operations and privacy in multi sectoral environment, WG 17 Protection Profiles in the context of SSCD.

7.5.2 CEN, Cenelec och ETSI

Standardiseringsarbetet för framtagandet av de vertikala harmoniserade standarderna, med undantag för vertikala standarder för kritiska produkter med digitala element, sker i CEN, Cenelec och ETSI. CEN, Cenelec och ETSI har ett samarbetsavtal¹⁴ som bland annat reglerar fem olika samarbetsformer¹⁵. Standardiseringsarbetet för EU:s cyberresliensförordning sker i mode 2 och mode 4. Mode 2 innebär att ett standardiseringsorgan tar ledningen och de andra standardiseringsorganen kan lämna skriftliga bidrag under arbetets gång. Denna arbetsform inkluderar även fullständig informationsdelning via nominerade delegater från de andra organisationerna. Mode 4 innebär att ett standardiseringsorgan tar ledningen och nominerade delegater från de andra organisationerna deltar på arbetsmöten och bidrar med teknisk expertis.

Arbetsledningen för de vertikala standarderna ligger hos:

CENs tekniska kommitté

- CEN/TC 224 Personal identification and related personal devices with secure elements, systems, operations and privacy in multi sectoral environment, WG 17 Protection Profiles in the context of SSCD för en harmoniserad standard.

Cenelecs tekniska kommittéer

- CLC/TC 47X Semiconductors and Trusted Chip Implementation, WG 1 Microprocessors and Microcontrollers with security related functionalities, WG 2 Tamper resistant Microprocessors and Microcontrollers, WG 3 SmartCards and Secure Element

¹⁴ Basic Co-operation Agreement between CEN (the European Committee for Standardisation), CENELEC (the European Committee for Electrotechnical Standardisation) and ETSI (the European Telecommunication Standards Institute).

¹⁵ The 5 modes of co-operation: Mode 1 – Informative relation, Mode 2 – Contributive relation, Mode 3 – Sub-contracting relation, Mode 4 – Collaborative relation, Mode 5 – Integrated relation.

Platforms och WG CRA Cyber Resilience Act för tre harmoniserade standarder.

- CLC/TC 65X Industrial-process measurement, control and automation, WG 3 Cyber Security för sex harmoniserade standarder.

ETSI:s tekniska kommitté

- TC CYBER-EUSR Cybersecurity för 18 harmoniserade standarder

Från ETSI:s sida deltar även TC ESI Electronic Signatures and Trusted Infrastructure och TC SET Secure Element Technologies i arbetet.

För deltagande i CEN och Cenelecs tekniska kommittéer krävs deltagande i de nationella spegelkommittéerna om sådana finns.

Deltagande i standardiseringen i ETSI skiljer sig från deltagande i CEN och Cenelec. ETSI tillämpar inte nationell delegation utan har direktmedlemskap. Alla företag, organisationer och myndigheter som är medlemmar i ETSI kan direkt delta i standardiseringsarbetet på europainivå. Det finns inte några begränsningar för hur många representanter från en och samma medlemsorganisation som kan delta i olika tekniska kommittéer och arbetsgrupper inom ETSI.

7.5.3 Svenskt deltagande i standardiseringsarbetet

Deltagande i CEN och Cenelecs gemensamma tekniska kommitté

Deltagande i standardiseringsarbetet inom CEN/CLC/JTC 13 WG 9 Special Working Group on Cyber Resilience Act samt inom CEN/CLC/JTC 13 WG 6 Product security sker via den tekniska kommittén SIS/TK 318 Informationssäkerhet, cybersäkerhet och integritetsskydd och mer specifikt genom dess arbetsgrupp AG 61 Produktsäkerhet som är den svenska spegelkommittén. Inom AG 61 finns deltagare från tillverkande och produktutvecklande företag, myndigheter, forskningsinstitut, tjänsteföretag och informations- och cybersäkerhetskonsulter, både stora bolag, små- och medelstora företag och mikroföretag.

Standardiseringsarbetet pågår i tre projektgrupper (Project Teams, PT). Sverige har i skrivande stund cirka tio aktiva deltagare i projektgrupperna.

Det finns önskemål om både utökad och bredare representation av organisationer och intressentkategorier inom standardiseringsarbetet.

Deltagarna i SIS/TK 318 anser att den befintliga representationen är tillräckligt bred i dag, men skulle gärna se fler deltagare från små- och medelstora företag. Det finns även behov av fler deltagare som aktivt kan bidra i internationella och nationella arbetsgrupper. De intressentkategorier som har en låg representation i SIS/TK 318 i dag är ideella organisationer och konsumentorganisationer. Detta beror delvis på att arbetet stundtals har en mycket teknisk karaktär. Denna intressentkategoris perspektiv är dock viktigt att beakta i standardiseringsarbetet. Eftersom cybersäkerhetsområdet och cyberresiliens berör alla branscher och verksamhetsområden är det viktigt att användarperspektivet kommer fram även i standarderna, och att det ska vara enkelt att förstå och använda dem.

Deltagarna i SIS/TK 318 anser själva att kompetensen hos de som deltar aktivt är tillräcklig. Däremot finns det många som följer och bevakar arbetet i syfte att lära sig. Det finns önskemål från deltagarna i SIS/TK 318 om att samla ytterligare experter såväl som ytterligare kompetens för att säkerställa tillräckligt stor bas av aktiva deltagare för att kunna bidra aktivt i standardiseringsutvecklingens alla områden.

Deltagande i CEN:s kommittéer

För att delta i arbetet med de vertikala standarderna som leds av CEN:s kommitté CEN/TC 224 WG 17 krävs deltagande i SIS/TK 448 Personlig identifiering. SIS deltagare deltar inte eller i mycket begränsad omfattning i arbetet med dessa standarder.

Deltagande i Cenelecs tekniska kommittéer

För deltagande i arbetet med de vertikala standarderna som leds av Cenelecs kommittéer CLC/TC 47X och CLC/TC 65X krävs deltagande i SEK. Deltagandet i CLC/TC 65X sker via den tekniska

kommittén SEK/TK 65 Industriell processtyrning. För CLC/TC 47X har SEK sedan 2012 inte haft någon spegelkommitté på grund av avsaknad av intresserade deltagare. Eventuella frågor som rör CLC/TC 47X hanteras av SEK:s Elektrotekniska råd.

Deltagande i ETSI:s tekniska kommitté

Deltagande i ETSI är inte knuten till deltagande eller medlemskap i ITS. Enligt ETSI:s webbsida och deltagarlistor för TC CYBER-EUSR finns endast ett fåtal svenska deltagare.

ITS ansvarar däremot för alla beslut om godkännande och avslag av begäran om standardisering, beslut om godkännande av nya arbetsuppgifter som behövs för att tillmötesgå kommissionens standardiseringsbegäran och beslut om antagande, översyn och återkallande av europeiska standarder eller andra europeiska standardiseringsprodukter i relation till det standardiseringsarbete som utförs av ETSI.

7.5.4 Utmaningar för standardiseringsarbetet

Ett relativt nytt standardiseringsområde

Cybersäkerhet och cyberresiliens är ett förhållandevis nytt område, när det gäller regulativa produktkrav och därmed för utvecklingen av harmoniserade standarder. Det finns därför inte lika stor kunskap och erfarenhet av standardisering inom detta område, varken i Sverige eller på europeisk nivå som det finns inom exempelvis maskinsäkerhetsområdet. Noterbart är dock att cybersäkerhetsfrågor spiller över till andra mer traditionella standardiseringsområden samt att cybersäkerhet och cyberresiliens är mycket relevanta aspekter för verksamheter inom alla branscher och samhällssektorer. Det innebär att det finns ett extra stort behov av att klargöra, förstå och få samsyn kring samband och beroenden mellan olika verksamheter och områden, vilket talar för att utvecklad samordning mellan standardiseringsområden är önskvärt om inte helt nödvändigt för att en lyckad framtagning så väl som implementering av standarder kan ske. Givet att det regulatoriska landskapet inom cyberresiliens har ökat dramatiskt de senaste åren, bland annat med kommissionens

delegerade förordning (EU) 2022/30¹⁶ och EU:s cyberresiliensförordning samt andra regleringar utanför den inre marknaden är det viktigt att prioritera arbetet med att ta fram standarder till detta område. Det är viktigt att de olika europeiska standardiseringsorganen samarbetar inom detta område. Vidare behöver Sverige och svenska intressenter ha förutsättningar att ta plats i det europeiska standardiseringsarbetet. Arbetet ställer krav på tid och resurser, både hos de svenska standardiseringsorganen och svenska experter. SIS har framfört att ett utökat finansiellt stöd för att möjliggöra nödvändig mobilisering och engagemang av de svenska experterna vore värdefullt.

Tidsramar för standardiseringsarbetet

Korta och pressade tidplaner i kommissionens standardiseringsbegäran för att ta fram harmoniserade standarder försvårar möjligheten att mobilisera svenska experter och få en önskvärd och nödvändig bredd av deltagande organisationer och perspektiv, vilket riskerar att försämra kvaliteten i standardiseringsarbetet, samt att få in breda kommentarer och remissvar på standardförslagen. Detta gäller inte bara för det arbete som sker i nationella spegelkommittéer utan även för arbetet i ETSI.

Pressade tidsramar kan innebära en risk att organisationer med stora resurser och/eller egna agendor får möjlighet att styra arbetet utifrån egna intressen. Detta skulle kunna medföra att standarderna inte får önskvärd kvalitet.

Det är därför viktigt att säkerställa att tiden för mobilisering av deltagare samt att skapa konsensus får prioritet och/eller förlängs, i förhållande till administrativa processer som exempelvis konsultationer och översättningar.

Många organisationer deltar i standardiseringsarbetet i första hand för att få tidig information eller bevaka området, eftersom de inser att det är av stor vikt för deras verksamhet och för att ha möjlighet att hinna ställa om verksamhet. Det riskerar att medföra att det finns

¹⁶ Kommissionens delegerade förordning (EU) 2022/30 av den 29 oktober 2021 om komplettering av Europaparlamentets och rådets direktiv 2014/53/EU vad gäller tillämpningen av de väsentliga krav som avses i artikel 3.3 d, e och f i det direktivet.

många deltagare, men få som faktiskt deltar för att bidra och påverka till standardiseringsarbetet.

Det har av intressenter framförts till utredningen att det behöver läggas mer resurser på stöd och information till berörda verksamheter och företag samt att öka stödet och uppmuntran att bidra i standardiseringsarbetet för de experter som innehar önskvärd och relevant kompetens. Utredningen delar denna bedömning. Stöd och information för att uppmuntra deltagande i standardiseringsarbetet är något som till exempel SIS arbetar aktivt med i form av stöd och kompetensinsatser. Även ITS har ett forum för informationsutbyte specifikt på cybersäkerhetsområdet.

Prioritering

Arbetet med att ta fram standarder har låg prioritet hos flera organisationer, både vad gäller strategiskt perspektiv och fördelning av resurser. Detta är inte unikt för cybersäkerhetsområdet utan gäller generellt för alla standardiseringsområden. Det finns en risk att personer eller funktioner utan nödvändig kompetens inom sakområdet och/eller standardisering deltar i standardiseringsarbetet vilket i sin tur orsakar att standarderna riskerar att få lägre kvalitet. För att motverka detta är det, såsom det anges i den nationella cybersäkerhetsstrategin, nödvändigt att standardisering prioriteras, att standardiseringen ses som ett strategiskt påverkansverktyg och skapa möjligheter till stöd för att delta i standardiseringsarbete.

SIS har bland annat framfört att den stora mängden standarder, en pressad tidplan och behov av brett deltagande gör att deltagare i standardiseringsarbetet kan behöva mer stöd från SIS projektledning än tidigare. För att möjliggöra det behöver formerna för hur arbetet bedrivs ses över och projektledningens tid dedikeras till de insatser som gör mest nytta.

Resursplanering och resursavsättning

En generell svårighet på de flesta standardiseringsområden är att få gehör för interna resurser att avsätta tid för att delta i standardiseringsarbete. Detta gäller såväl företag, myndigheter och andra organisationer. Om experter ska kunna delta aktivt krävs stor arbets-

insats under en kort tidsperiod, vilket kan orsaka en hög arbetsbelastning för deltagande experter.

Myndigheter behöver göra sin resursplanering långsiktigt och i god tid. Det gör det svårt för att mobilisera och säkerställa att rätt kompetenser finns tillgängliga i tillräckligt stor omfattning för intensiva standardiseringsarbeten med kort varsel.

Att medverka i framtagandet av standarder sker utan ersättning, vilket kan göra medverkan svår att prioritera för mindre företag.

Bristande vana och kompetens inom standardisering hos vissa deltagare gör att ambitionsnivå och påverkansmöjlighet varierar. Diskussionerna får fel fokus och de slutliga standarderna träffar inte rätt utifrån ursprungligt syfte eller behov. En förutsättning för att uppnå de överenskommelser som behövs inom standardiseringen är att olika experter kan samarbeta med varandra. Det kan underlättas genom deltagande i möten, helst fysiskt, vilket också kräver resurser i form av tid och resor.

Information och kommunikation

Det finns även stora utmaningar för de ekonomiska aktörer eller organisationer som ska använda eller uppfylla kraven i standarderna. Det råder brist på information till dem som behöver uppfylla regelverken innan standarden är helt färdig. Det är svårt för de ekonomiska aktörerna att hinna med att uppfylla reglerna när de väl har trätt i kraft. Det är även viktigt att upphandlande organisationer får kunskap om standarderna för att kunna kravställa på ett korrekt och framtidssäkrat sätt.

Genom öppet standardiseringsarbete samt genom att ge fler möjlighet att delta kan organisationer och företag på ett tidigt stadium få inblick i arbetet och kommande standarder.

7.6 Överväganden

Utredningens bedömning: Det finns inte några åtgärder som i närtid kan vidtas för att kunna påverka standardiseringsarbetet för EU:s cyberresiliensförordning. De intressenter som är tillgängliga bedöms redan delta i arbetet.

För att skyndsamt kunna medverka vid ny lagstiftning som förutsätter harmoniserade standarder bör de svenska standardiseringsorganen och övriga intressenter arbeta mer långsiktigt. Utredningen bedömer att behovet av åtgärder för ett strategiskt och mer långsiktigt arbete med rekrytering av experter på framtida standardiseringsområden omhändertas i regeringens nationella strategier på området.

Det finns även behov av att utvärdera vilka effekter det ökade statsbidraget till de svenska standardiseringsorganen har medfört.

Utredningen anser att svenska intressenter från alla delar av samhället behöver vara aktiva i standardiseringsarbetet kopplat till cybersäkerhet och cyberresiliens. De nationella standardiseringsorganen behöver kunna delta på ett effektivt sätt för att svenska intressen ska kunna födas in i arbetet.

Deltagande i standardisering är resurskrävande och resursfrågan är avgörande för intressenternas engagemang.

Fler myndigheter bör delta i tekniska kommittéer på europeisk och internationell nivå. Myndigheterna behöver arbeta långsiktigt och strategiskt med standardisering och bör ta fram konkreta interna strategier om hur de kan arbeta med dessa frågor.

Uteblivet nationellt deltagande i relevanta spegelkommittéer kan innebära negativa konsekvenser för nationella aktörer som påverkas av EU:s cyberresiliensförordning. Genom att delta i arbetet, antingen aktivt eller genom en mer bevakande roll, kan behoven för kommande regulativa produktkrav effektivare förstås. Därmed kan dessa krav även förmedlas löpande till den egna organisationen vilket bygger kompetens, rutiner och arbetssätt i enlighet med kommande krav.

Arbetet med att ta fram harmoniserade standarder för EU:s cyberresiliensförordning pågår nu och befinner sig i ett intensivt och på många sätt komplext skede. De första standarderna ska levereras i

augusti 2026, medan de sista ska vara färdiga i oktober 2027. Detta arbete är i hög grad resurs- och tidskrävande och sker parallellt i ett stort antal tekniska kommittéer och arbetsgrupper, vilka har sina egna processer, prioriteringar och interna samordningsutmaningar att hantera.

Standardiseringsverksamhet behöver på ett långsiktigt och hållbart sätt byggas upp med sakkunskap från de intressenter som har möjlighet att bidra. Detta är särskilt viktigt för att säkerställa att rätt kompetens finns tillgänglig i rätt tid så att de relevanta standardiseringskommittéerna och arbetsgrupperna kan bemannas med kort varsel när ny lagstiftning introduceras och nya standardiseringsbegäran tas fram. För att lyckas med detta krävs en kontinuerlig och aktiv omvärldsbevakning, både från intressenternas sida och från standardiseringsorganens sida, så att man i god tid kan identifiera trender, behov och potentiella förändringar i omvärlden. Det handlar ytterst om att kunna agera snabbt, flexibelt och effektivt när situationen så kräver. I detta arbete bör Regeringens strategi för standardisering och på cybersäkerhetsområdet även Nationell strategi för cybersäkerhet 2025–2029 beaktas.

Utredningen bedömer att ett sådant långsiktigt och strategiskt arbete som beskrivs i mål 4 i den Nationella strategin för cybersäkerhet kommer verka positivt för att lyckas med rekrytering av experter på framtidsrelevanta standardiseringsområden. Området bör också särskilt beaktas vid uppdatering och uppföljning av den Nationella strategin för cybersäkerhet.

Utredningen kan däremot inte identifiera förslag eller åtgärder som på kort sikt skulle kunna bidra till en sådan standardiseringsinfrastruktur som skulle kunna vara till nytta för framtagandet av harmoniserade standarder för EU:s cyberresiliensförordning. Det som främst saknas i dagsläget är experter som aktivt deltar i arbetet.

Utredningen bedömer att ytterligare statsbidrag till de svenska standardiseringsorganen inte kommer att ge effekt för standardiseringsarbetet inom ramen för EU:s cyberresiliensförordning. Statsbidraget till svensk standardisering ökades för 2025 med 13 800 000 kronor. En del av bidraget är öronmärkt för verksamhet inom området digitalisering och cybersäkerhet. Utredningen anser att i ett första skede bör de svenska standardiseringsorganen i sin återrapportering utvärdera vilka effekter det ökade statsbidraget har gett.

8 Sårbarhets- och incidentrapportering

8.1 Inledning

I detta kapitel behandlas sårbarhets- och incidentrapportering enligt artikel 14 och 15 i förordning (EU) 2024/2847¹ (EU:s cyberresiliensförordning).

Den CSIRT-enhet som har utsetts till samordnare i respektive medlemsstat är enligt EU: cyberresiliensförordning mottagare av dessa sårbarhets- och incidentrapporter. CSIRT-enheten som har utsetts till samordnare är enligt artikel 3.51 i EU:s cyberresiliensförordning den CSIRT-enhet som har utsetts till samordnare enligt artikel 12.1 i direktiv (EU) 2022/2555² (NIS 2-direktivet).

Enligt artikel 10 i NIS 2-direktivet ska varje medlemsstat utse eller inrätta en eller flera CSIRT-enheter. Enligt artikel 12.1 i direktivet ska varje medlemsstat utse en av sina CSIRT-enheter till samordnare för den samordnade delgivningen av information om sårbarheter.

Artikel 12.1 i NIS 2-direktivet har ännu inte genomförts i svensk rätt. I propositionen 2025/26:28 *Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag* av den 9 oktober 2025 lämnar dock regeringen förslag om hur NIS 2-direktivet ska genomföras i svensk rätt.

¹ Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen).

² Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

Den motsvarande bestämmelsen till artikel 12.1 i NIS 2-direktivet finns i direktivets föregångare och har genomförts i svensk rätt genom förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. Enligt 12 § i den förordningen är Myndigheten för samhällsskydd och beredskap (MSB) CSIRT-enhet i Sverige.

I Sverige finns således endast en CSIRT-enhet och det är den som avses när EU:s cyberresiliensförordning innehåller bestämmelser om den CSIRT-enhet som utsetts till samordnare.

Frågan om ikraftträdande- och övergångsbestämmelser behandlas i kapitel 14.

8.2 Tillverkarens skyldigheter

8.2.1 Vem ska rapportera vad?

Tillverkare har enligt artikel 14.1 och 14.3 i EU:s cyberresiliensförordning en skyldighet att rapportera alla aktivt utnyttjade sårbarheter i och allvarliga incidenter som påverkar säkerheten för produkten med digitala element som tillverkaren får kännedom om. I artikel 3 i EU:s cyberresiliensförordning definieras vad en aktivt utnyttjad sårbarhet är. I artikel 14.5 i EU:s cyberresiliensförordning anges förutsättningarna för att en incident ska anses vara allvarlig.

Skyldigheten i artikel 14 gäller samtliga produkter som finns på marknaden, även sådana som har släppts ut på marknaden före den 11 december 2027 när EU:s cyberresiliensförordning träder i kraft, se vidare avsnitt 14.4.

Tillverkarens rapporteringsskyldighet kan enligt artikel 18 i EU:s cyberresiliensförordning delegeras till tillverkarens representant. Vidare kan enligt artikel 21 i EU:s cyberresiliensförordning skyldigheten gälla för importörer och distributörer. Enligt artikel 22 i EU:s cyberresiliensförordning kan skyldigheten gälla för fysiska eller juridiska personer, annan än tillverkaren, importören eller distributören, som utför en väsentlig ändring av en produkt med digitala element och som tillhandahåller den produkten på marknaden. I artikel 24.3 i EU:s cyberresiliensförordning finns bestämmelser när tillverkarens skyldigheter ska tillämpas på förvaltare av programvara med fri och öppen källkod.

Utöver tillverkarens obligatoriska rapporteringsskyldighet enligt artikel 14 i EU:s cyberresiliensförordning finns det i artikel 15 i förordningen en möjlighet till frivillig rapportering.

Artikel 15 i EU:s cyberresiliensförordning föreskriver att tillverkare och andra fysiska eller juridiska personer, på frivillig basis, får rapportera eventuella sårbarheter i en produkt med digitala element och cyberhot som kan påverka riskprofilen för en produkt med digitala element samt incidenter som påverkar säkerheten för produkten med digitala element och tillbud som hade kunnat leda till en sådan incident.

8.2.2 Till vem ska rapporterna lämnas och hur ska det göras?

Rapportering till CSIRT-enheten

Enligt artikel 14.1 och 14.3 i EU:s cyberresiliensförordning ska de obligatoriska sårbarhets- och incidentrapporterna lämnas till CSIRT-enheten och samtidigt till Europeiska unionens cybersäkerhetsbyrå (Enisa). Enligt artikel 14.7 ska rapporterna lämnas in hos den CSIRT-enhet i den medlemsstat där tillverkarna har sitt huvudsakliga verksamhetsställe i unionen. Enligt artikel 15.1 och 15.2 i EU:s cyberresiliensförordning får frivilliga rapporter lämnas till CSIRT-enheten eller Enisa.

Sårbarhets- och incidentrapporterna ska lämnas via en gemensam rapporteringsplattform som ska inrättas enligt artikel 16 i EU:s cyberresiliensförordning. Artikel 16.1 i EU:s cyberresiliensförordning föreskriver att för att förenkla tillverkarnas rapporteringsskyldigheter ska Enisa inrätta en gemensam rapporteringsplattform för de rapporter som avses i artiklarna 14.1, 14.3, 15.1 och 15.2. Den dagliga driften av den gemensamma rapporteringsplattformen ska skötas och upprätthållas av Enisa. Strukturen för den gemensamma rapporteringsplattformen ska göra det möjligt för medlemsstaterna och Enisa att införa sina egna slutpunkter för elektronisk anmälan. Den CSIRT-enhet som mottar en rapport ska enligt artikel 16.2 i EU:s cyberresiliensförordning utan dröjsmål sprida rapporten via den gemensamma rapporteringsplattformen till de CSIRT-enheter som utsetts till samordnare på det territorium där tillverkaren har angett att produkten med digitala element har tillhandahållits. Enligt artikel 14.9 i EU:s cyberresiliensförordning ska kommissionen

senast den 11 december 2025 anta delegerade akter som specificerar villkoren för att skjuta upp spridningen av rapporter.

I artikel 16.4 och 16.5 i EU:s cyberresiliensförordning finns bestämmelser om Enisas skyldighet att vidta åtgärder för att hantera säkerhetsriskerna i den gemensamma plattformen och den information som lämnas in eller sprids via plattformen, samt gentemot de slutpunkter som respektive medlemsstat inrättar på nationell nivå. Artikel 17 i EU:s cyberresiliensförordning innehåller bestämmelser om hur Enisa får och ska använda informationen från inkomna incidentrapporter.

CSIRT-enheten ska enligt artikel 17.6 i EU:s cyberresiliensförordning tillhandahålla hjälptjänster³ i samband med rapporterings-skyldigheterna enligt artikel 14 till tillverkare, särskilt tillverkare som kan betecknas som mikroföretag eller små eller medelstora företag, se vidare avsnitt 8.3 och även kapitel 12.

Underrättelse till användare

Artikel 14.8 i EU:s cyberresiliensförordning anger att en tillverkare, efter att ha fått kännedom om en aktivt utnyttjad sårbarhet eller en allvarlig incident, ska underrätta de drabbade användarna av produkten med digitala element, och när så är lämpligt alla användare, om den sårbarheten eller incidenten och, vid behov, om riskreducering och eventuella korrigerande åtgärder som användarna kan vidta för att begränsa konsekvenserna av denna sårbarhet eller incident, om lämpligt i ett strukturerat, maskinläsbart format som är enkelt att automatiskt behandla. Om tillverkaren underlåter att underrätta användarna i tid får CSIRT-enheten som utsetts till samordnare lämna sådan information till användarna när detta anses vara proportionellt och nödvändigt för att förebygga eller mildra konsekvenserna av sårbarheten eller incidenten.

³ För vägledning kring begreppet "hjälp-tjänster", jämför den engelska språkversionen av cyberresiliensförordningen som använder begreppet "helpdesk support".

8.2.3 Vilka uppgifter ska rapporteras och inom vilken tid ska rapporterna lämnas?

I artikel 14.2 i EU:s cyberresiliensförordning anges när i tiden en rapport av *en aktivt utnyttjad sårbarhet* i en produkt med digitala element ska lämnas och vilka uppgifter som ska rapporteras. Tillverkaren ska utan onödigt dröjsmål och under alla omständigheter senast 24 timmar efter kännedom lämna in en tidig varning och, i tillämpliga fall, ange de medlemsstater på vars territorium tillverkaren känner till att produkten med digitala element har tillhandahållits. Inom 72 timmar från kännedom ska tillverkaren lämna ytterligare information, om denna information inte redan har lämnats. Det rör sig om allmän information, om sådan finns tillgänglig, om den berörda produkten med digitala element, den allmänna karaktären av utnyttjandet och sårbarheten i fråga samt eventuella korrigeringar eller riskreducerande åtgärder som vidtagits och korrigerande eller riskreducerande åtgärder som användarna kan vidta, och som också, i tillämpliga fall, ska ange hur känslig tillverkaren anser att den anmälda informationen är. Senast 14 dagar efter det att en korrigerande eller riskreducerande åtgärd blivit tillgänglig ska tillverkaren lämna in en slutrapport, om informationen inte redan har lämnats. Den ska åtminstone innehålla en beskrivning av sårbarheten och dess allvarlighetsgrad och konsekvenser, i förekommande fall information om en fientlig aktör som har utnyttjat eller som utnyttjar sårbarheten samt detaljer om säkerhetsuppdateringen eller andra korrigerande åtgärder som har gjorts tillgängliga för att avhjälpa sårbarheten.

I artikel 14.4 i EU:s cyberresiliensförordning anges när en rapport av *en allvarlig incident* som påverkar säkerheten för produkten med digitala element ska göras och vilka uppgifter som ska rapporteras. Tillverkaren ska utan onödigt dröjsmål och under alla omständigheter senast 24 timmar efter kännedom lämna in en tidig varning och åtminstone ange om tillverkaren misstänker att incidenten orsakats av olagliga eller fientliga handlingar, och i tillämpliga fall även ange de medlemsstater på vars territorium tillverkaren känner till att produkten med digitala element har tillhandahållits. Inom 72 timmar från kännedom ska tillverkaren lämna ytterligare information i en incidentrapport, om denna information inte redan har lämnats. Det rör sig om allmän information, om sådan finns tillgänglig, om

arten av incident, en första bedömning av incidenten samt eventuella korrigerande eller riskreducerande åtgärder som vidtagits och korrigerande eller riskreducerande åtgärder som användarna kan vidta, och som också, i tillämpliga fall, ska ange hur känslig tillverkaren anser att den anmälda informationen är. Inom en månad efter att incidentrapporten lämnats ska tillverkaren lämna in en slutrapport, om informationen inte redan har lämnats. Den ska åtminstone innehålla en detaljerad beskrivning av incidenten inbegripet dess allvarlighetsgrad och konsekvenser, den typ av hot eller grundorsak som sannolikt har utlöst incidenten samt tillämpade och pågående riskreducerande åtgärder.

Enligt artikel 14.6 i EU:s cyberresiliensförordning får CSIRT-enheten som utsetts till samordnare vid behov begära att tillverkarna lämnar en delrapport om relevanta statusuppdateringar om den aktivt utnyttjade sårbarheten eller allvarliga incidenten som påverkar säkerheten för produkten med digitala element.

De skyldigheter som fastställs i EU:s cyberresiliensförordning får enligt artikel 2.8 i förordningen inte medföra tillhandahållande av information vars utlämnande skulle strida mot väsentliga intressen i fråga om medlemsstaternas nationella säkerhet, allmänna säkerhet eller försvar, se vidare kapitel 5.

8.3 CSIRT-enhetens uppgifter

CSIRT-enheten är som ovan angetts mottagare av sårbarhets- och incidentrapporter enligt EU:s cyberresiliensförordning.

I NIS 2-direktivet ställs uttryckliga krav som CSIRT-enheter ska uppfylla och direktivet anger också ett antal uppgifter för CSIRT-enheter. I EU:s cyberresiliensförordning anges vilka ytterligare uppgifter har enligt den förordningen.

CSIRT-enheten har följande skyldigheter enligt EU:s cyberresiliensförordning.

- Efter att ha mottagit en rapport om en aktivt utnyttjad sårbarhet eller om en allvarlig incident ska CSIRT-enheten, enligt artikel 16.2 i EU:s cyberresiliensförordning, utan dröjsmål, sprida rapporten via den gemensamma rapporteringsplattformen till de CSIRT-enheter som utsetts till samordnare på det territorium där tillverkaren har angett att produkten med digitala element

har tillhandahållits. Det finns dock, under förutsättningar som anges i artikeln, möjlighet att i vissa fall skjuta upp spridningen av en rapport. Kommissionen ska enligt artikel 14.9 senast den 11 december 2025 anta delegerade akter som specificerar villkoren för att skjuta upp spridningen av rapporter. Skyldigheten för CSIRT-enheten att sprida rapporterna gäller enligt artikel 15.3 även rapporter som inkommit på frivillig basis. CSIRT-enheten får dock prioritera behandlingen av obligatoriska rapporter före behandlingen av frivilliga rapporter.

- Efter att ha mottagit en rapport om en aktivt utnyttjad sårbarhet eller om en allvarlig incident ska CSIRT-enheten enligt artikel 16.3 i EU:s cyberresiliensförordning förse marknadskontrollmyndigheterna med den information som behövs för att marknadskontrollmyndigheterna ska kunna fullgöra sina skyldigheter enligt cyberresiliensförordningen. Skyldigheten för CSIRT-enheten att förse myndigheterna med rapporter gäller enligt artikel 15.3 även rapporter som inkommit på frivillig basis. CSIRT-enheten får dock prioritera behandlingen av obligatoriska rapporter före behandlingen av frivilliga rapporter.
- Om en annan fysisk eller juridisk person än tillverkaren anmäler en aktivt utnyttjad sårbarhet eller en allvarlig incident som påverkar säkerheten för en produkt med digitala element ska CSIRT-enheten enligt artikel 15.4 i EU:s cyberresiliensförordning utan onödigt dröjsmål, informera tillverkaren.
- När det gäller frivilliga rapporter ska CSIRT-enheten enligt artikel 15.5 i EU:s cyberresiliensförordning säkerställa konfidentialitet och lämpligt skydd för den information som tillhandahålls av den anmälande fysiska eller juridiska personen.
- CSIRT-enheten ska enligt artikel 17.6 i EU:s cyberresiliensförordning tillhandahålla hjälptjänster i samband med rapporterings-skyldigheterna enligt artikel 14 till tillverkare, särskilt tillverkare som kan betecknas som mikroföretag eller små eller medelstora företag.

Utöver dessa skyldigheter har CSIRT-enheten även följande befogenheter.

- Vid behov får CSIRT-enheten, enligt förutsättningarna som anges i artikel 14.6 i EU:s cyberresiliensförordning, begära att tillverkarna lämnar en delrapport om relevanta statusuppdateringar om en rapporterad sårbarhet eller incident.
- Om tillverkare underlåter att underrätta användarna av produkter med digitala element i tid får CSIRT-enheten enligt artikel 14.8 i EU:s cyberresiliensförordning lämna sådan information till användarna när detta anses vara proportionellt och nödvändigt för att förebygga eller mildra konsekvenserna av sårbarheten eller incidenten.
- Om en CSIRT-enhet som utsetts till samordnare har uppmärksamats på en aktivt utnyttjad sårbarhet, som en del av ett förfarande för samordnad delgivning av information om sårbarheter som avses i artikel 12.1 i NIS 2-direktivet, får CSIRT-enheten enligt artikel 16.6 i EU:s cyberresiliensförordning skjuta upp spridningen av den berörda anmälan via den gemensamma rapporteringsplattformen på grundval av motiverade cybersäkerhetsrelaterade skäl under en period som inte är längre än vad som är absolut nödvändigt och till dess att de berörda parterna inom samordnad delgivning av information om sårbarheter har gett sitt samtycke till utlämnande. Detta krav ska inte hindra tillverkarna från att frivilligt anmäla en sådan sårbarhet i enlighet med förfarandet i denna artikel.
- Om det är nödvändigt att informera allmänheten för att förebygga eller begränsa en allvarlig incident som påverkar säkerheten för produkten med digitala element eller för att hantera en pågående incident, eller om ett avslöjande av incidenten på annat sätt ligger i allmänhetens intresse, får CSIRT-enheten enligt artikel 17.2 i EU:s cyberresiliensförordning, efter samråd med den berörda tillverkaren och, när så är lämpligt, i samarbete med Enisa, informera allmänheten om incidenten eller kräva att tillverkaren gör detta.

Vidare finns följande bestämmelser i EU:s cyberresiliensförordning som berör CSIRT-enheten.

- Artikel 52.4 i EU:s cyberresiliensförordning föreskriver att när det gäller tillsynen över genomförandet av rapporteringsskyldigheterna enligt artikel 14 i förordningen ska de utsedda marknads-kontrollmyndigheterna samarbeta och regelbundet utbyta information med CSIRT-enheten och Enisa.
- Artikel 52.5 i EU:s cyberresiliensförordning föreskriver att marknads-kontrollmyndigheterna får be CSIRT-enheten eller Enisa att ge tekniska råd i frågor som rör genomförandet och efterlevnaden av EU:s cyberresiliensförordning. Vid genomförandet av en utredning enligt artikel 54 får marknads-kontrollmyndigheterna be CSIRT-enheten som utsetts till samordnare eller Enisa att tillhandahålla en analys till stöd för utvärderingar av överens-stämmelse för produkter med digitala element.
- Artikel 52.10 i EU:s cyberresiliensförordning föreskriver att marknads-kontrollmyndigheterna får ge ekonomiska aktörer vägledning och råd om genomförandet av förordningen, med stöd av kommissionen och CSIRT-enheten och Enisa när så är lämpligt.
- Artikel 52.14 i EU:s cyberresiliensförordning föreskriver att för produkter med digitala element som omfattas av denna förordning och som klassificeras som AI-system med hög risk enligt artikel 6 i förordning (EU) 2024/1689⁴ (AI-förordningen) ska de marknads-kontrollmyndigheter som utsetts enligt den förordningen vara de myndigheter som ansvarar för den marknads-kontroll som föreskrivs i den här förordningen. De marknads-kontrollmyndigheter som utsetts enligt AI-förordningen ska vid behov samarbeta med den marknads-kontrollmyndighet som utsetts i enlighet med EU:s cyberresiliensförordning och, när det gäller tillsyn över genomförandet av rapporteringsskyldigheten enligt artikel 14 i EU:s cyberresiliensförordning, med CSIRT-enheten och Enisa.

⁴ Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

- Artikel 54.1 föreskriver att om marknadskontrollmyndigheten har tillräckliga skäl att anse att en produkt med digitala element, inbegripet dess sårbarhetshantering, utgör en betydande cybersäkerhetsrisk, ska den, utan onödigt dröjsmål och om lämpligt i samarbete med den berörda CSIRT-enheten, göra en utvärdering av den berörda produkten med digitala element med avseende på dess uppfyllande av alla krav som fastställs i denna förordning.

CSIRT-enheten i Sverige har redan i dag omfattande uppgifter att stötta samhället i arbetet med att hantera och förebygga it-incidenter. Bland annat arbetar den svenska CSIRT-enheten med att öka it-säkerhetsmedvetandet genom att förmedla kunskap och fakta samt utfärda varningar och råd om sårbarheter i it-system. CSIRT-enheten tar även emot incidentrapporter och tillgängliggör informationen i incidentrapporter för tillsynsmyndigheter samt hanterar it-incidenter genom att sprida information och att samordna åtgärder för att avhjälpa eller lindra effekter av det inträffade. Vid en incident kan CSIRT-enheten ge rådgivning om hur incidenten ska hanteras, göra eventuella kopplingar till pågående eller tidigare händelser samt göra en teknisk analys av angripna system. När flera intressenter behöver samverka kan CSIRT-enheten koordinera det arbetet. För att minska risken för spridning publicerar CSIRT-enheten råd om sårbarheter och rekommenderade åtgärder. CSIRT-enheten är Sveriges kontaktpunkt gentemot andra länders motsvarande verksamhet. CSIRT-enheten samarbetar med nationella och internationella funktioner. CSIRT-enhetens tjänster riktar sig till offentlig sektor, privata företag och organisationer.

Dessa uppgifter är likartade dem som följer av EU:s cyberresiliensförordning. EU:s cyberresiliensförordning får dock till följd att betydligt fler aktörer omfattas av rapporteringsskyldigheterna och att rapporteringsskyldigheten, till skillnad från NIS-regleringen, inte rör sårbarheter och incidenter i nätverks- och informationssystem utan i produkter med digitala element. Dessutom får EU:s cyberresiliensförordning till följd att CSIRT-enheten behöver samverka med en ny kategori av tillsynsmyndighet i form av marknadskontrollmyndigheterna.

8.4 Kompletterande EU-lagstiftning

Utredningens bedömning: Det finns inget behov av att införa kompletterande reglering till bestämmelserna om sårbarhets- och incidentrapportering i EU:s cyberresiliensförordning.

Kommissionen får enligt artikel 14.10 i EU:s cyberresiliensförordning genom genomförandeakter ytterligare specificera formatet och förfarandena för de rapporter som avses i artikel 14 samt i artiklarna 15 och 16 i EU:s cyberresiliensförordning.

Mot den bakgrunden bedömer utredningen att det vid tidpunkten för att EU:s cyberresiliensförordning ska börja tillämpas kommer att finnas tillräcklig och ändamålsenlig reglering kring sårbarhets- och incidentrapporteringen. Det saknas således skäl att införa eventuella kompletterande bestämmelser om rapporteringsskyldigheten eller att införa befogenheter för CSIRT-enheten att till exempel begära in uppgifter eller meddela föreskrifter.

8.5 CSIRT-enhet i Sverige

Utredningens bedömning: I [föreslagna] 27 § förordningen (2025:000) om cybersäkerhet⁵ finns bestämmelser om vilken myndighet som är CSIRT-enhet.

Enligt 12 § förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster är MSB CSIRT-enhet i Sverige.

I delbetänkandet *Nya regler om cybersäkerhet* (SOU 2024:18) föreslår utredningen att MSB, när NIS 2-direktivet genomförs i svensk rätt, fortsatt ska vara CSIRT-enhet i Sverige och föreslår att detta ska regleras i 27 § i en ny förordning om cybersäkerhet.

I slutbetänkandet *Samlade förmågor för ökad cybersäkerhet* (SOU 2025:79) föreslår dock den utredningen att Försvarets radioanstalt (FRA) ska vara CSIRT-enhet. Enligt förslagen i SOU 2025:79 ska 27 § i förslaget till förordning om cybersäkerhet i dess lydelse enligt SOU 2024:18 ändras så att det framgår att FRA ska utföra uppdraget från och med den 1 juli 2026.

⁵ Se delbetänkandet *Nya regler om cybersäkerhet* (SOU 2024:18).

Utredningens bedömning är att det i förordningen med kompletterande bestämmelser till EU:s cyberresiliensförordning ska införas en upplysningsbestämmelse som anger att det i föreslagna 27 § förordningen (2025:000) om cybersäkerhet⁶ finns bestämmelser om vilken myndighet som är CSIRT-enhet. Utredningen bedömer att upplysningsbestämmelsen bör träda i kraft den 11 september 2026, se vidare avsnitt 14.4.

⁶ Se delbetänkandet *Nya regler om cybersäkerhet* (SOU 2024:18).

9 Marknadskontroll

9.1 Inledning

Förordning (EU) 2024/2847¹ (EU:s cyberresiliensförordning) ställer krav på produkter med digitala element. Det rör sig om väsentliga cybersäkerhetskrav för produkter med digitala element och krav på sårbarhetshantering samt administrativa krav som produkter med digitala element ska uppfylla. Det ställs även krav på de ekonomiska aktörerna som tillhandahåller produkter med digitala element på marknaden.

EU:s cyberresiliensförordning ställer vidare krav på att medlemsstaterna ska utse en eller flera myndigheter för att säkerställa ett effektivt genomförande av denna förordning.

I detta kapitel behandlas förutsättningar för marknadskontroll, förslag på fördelning av marknadskontrollansvar för marknadskontroll enligt EU:s cyberresiliensförordning i Sverige samt förslag till kompletterande lagstiftning i relation till marknadskontroll.

9.2 Syftet med marknadskontroll

En av hörnstenarna inom EU är principen om den fria rörligheten för varor på den inre marknaden. Principen innebär att varor ska kunna cirkulera fritt mellan EU:s medlemsländer och EES-länderna Norge, Island och Liechtenstein utan att hindras av tullar, avgifter, diskriminering eller nationella krav.

För att uppnå fri rörlighet för varor har EU bland annat beslutat ett stort antal gemensamma regler med produktkrav som gäller i

¹ Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen).

alla medlemsstater. Sådana enhetliga regler finns för bland annat radioutrustning, leksaker och personlig skyddsutrustning. Reglerna är tänkta att underlätta för till exempel tillverkare som bara behöver förhålla sig till dessa gemensamma produktstandarder för att kunna sälja sin produkt på hela den inre marknaden. Detta kan i sin tur gynna konsumenter som får tillgång till ett större utbud av produkter, vilket även ökar konkurrensen.

Det är som huvudregel tillverkarens ansvar att en produkt uppfyller gällande krav och det krävs inte någon förhandskontroll av produkten från en myndighet innan den får släppas ut på marknaden. För att säkerställa att produkter på marknaden överensstämmer med gällande krav används marknadskontroll.

Marknadskontroll syftar inte bara till att upptäcka och undvika farliga produkter och produkter som inte uppfyller vissa funktionskrav, utan även till att säkerställa en väl fungerande inre marknad. Genom att tillverkare vars produkter inte uppfyller gällande krav kan hindras från att sälja sina produkter, motverkas osund konkurrens samtidigt som slutanvändare skyddas från osäkra produkter. För att säkerställa att produkter uppfyller en hög skyddsnivå och för att förhindra en snedvriden konkurrens är det nödvändigt att marknadskontroll sker likvärdigt inom hela EU.

9.3 Reglering av marknadskontroll inom EU

Marknadskontroll regleras på EU-nivå i olika regelverk, både sektorsövergripande och i sektorslagstiftning på produktnivå.

En sektorsövergripande reglering av marknadskontroll finns i EU:s marknadskontrollförordning² som tillämpas på produkter som omfattas av den harmoniserade unionslagstiftning som förtecknas i bilaga I till denna förordning. I denna bilaga, som ändrades genom artikel 66 i EU:s cyberresiliensförordning, förtecknas EU:s cyberresiliensförordning och andra lagstiftningar som reglerar specifika produktkrav.

Enligt EU:s marknadskontrollförordning ska marknadskontrollmyndigheterna bedriva en effektiv marknadskontroll av produkter som görs tillgängligt på och utanför internet, säkerställa att ekono-

² Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011.

miska aktörer vidtar korrigerande åtgärder samt besluta om lämpliga åtgärder om inte den ekonomiska aktören vidtar korrigerande åtgärder. Beslut om vilka kontroller som ska utföras ska baseras på en riskbaserad metod som tar hänsyn till bland annat graden av potentiell fara, ekonomiska aktörers verksamhet samt uppgifter som tagits emot från konsumenter och andra aktörer.

EU:s marknadskontrollförordning reglerar uppgifter för ekonomiska aktörer, uppgifter om stöd till och samarbete med ekonomiska aktörer, marknadskontrollmyndigheternas skyldigheter samt samordning mellan marknadskontrollmyndigheter och det nationella centrala samordningskontoret, gränsöverskridande assistans mellan marknadskontrollmyndigheter samt samverkan med tullmyndigheterna när det gäller kontroll av produkter som förs in på unionsmarknaden. Det finns krav på att marknadskontrollmyndigheter dokumenterar enskilda marknadskontrollärenden i ett gemensamt informations- och kommunikationssystem. EU:s marknadskontrollförordning reglerar vidare specifika åtgärder för marknadskontroll och innehåller ett antal minimibefogenheter som medlemsstaterna ska tilldela sina marknadskontrollmyndigheter.

EU:s cyberresiliensförordning är en av de sektorslagstiftningar som förtecknas i bilaga I till EU:s marknadskontrollförordning och som innehåller ytterligare bestämmelser om marknadskontroll för produkter med digitala element, däribland bestämmelser om samarbete med andra myndigheter, gemensamma marknadskontrollaktiviteter och samordnade tillsynsåtgärder. Det finns även bestämmelser om förfaranden på unionsnivå i fråga om skyddsåtgärder och förfaranden på unionsnivå för produkter med digitala element som utgör en betydande cybersäkerhetsrisk.

För konsumentprodukter och risker eller riskkategorier som inte omfattas av någon sektorslagstiftning innehåller den allmänna produktsäkerhetsförordningen³ kompletterande regler om säkerhet och marknadskontroll.

³ Europaparlamentets och rådets förordning (EU) 2023/988 av den 10 maj 2023 om allmän produktsäkerhet, ändring av Europaparlamentets och rådets förordning (EU) nr 1025/2012 och Europaparlamentets och rådets direktiv (EU) 2020/1828 och om upphävande av Europaparlamentets och rådets direktiv 2001/95/EG och rådets direktiv 87/357/EEG.

9.4 Organiseringen av marknadskontroll i Sverige

Sverige har ett decentraliserat system för marknadskontroll och ansvaret för kontrollen är uppdelat mellan flera statliga myndigheter som har olika ansvarsområden enligt sektorsspecifika författningar. Därtill utövar Sveriges 290 kommuner kontroll av produktkrav på ett begränsat antal områden.

Uppdelningen av marknadskontrollansvaret utgår oftast från olika egenskaper eller risker hos produkterna snarare än själva produktslaget, till exempel att en produkt är avsedd att användas på arbetsplatser respektive för privat bruk eller att den är brandfarlig. Det medför att det kan finnas flera ansvariga myndigheter för samma produktslag men för olika egenskaper hos produkten. Ett exempel på ett delat ansvar är leksaker, för vilka Konsumentverket har huvudansvaret för marknadskontrollen medan Kemikalieinspektionen utövar marknadskontroll när det gäller leksakers brännbarhet och kemiska egenskaper samt Elsäkerhetsverket när det gäller leksakers elektriska egenskaper.

Förordning (2014:1039) om marknadskontroll av varor och annan närliggande tillsyn kompletterar EU:s marknadskontrollförordning. Denna förordning innehåller bland annat skyldigheter för marknadskontrollmyndigheter såsom att årligen utarbeta och genomföra program för marknadskontroll och följa upp tidigare års program. Genom förordningen inrättas även ett marknadskontrollråd vid Styrelsen för ackreditering och teknisk kontroll (Swedac) och Swedac är dessutom utsett till centralt samordningskontor för marknadskontroll enligt artikel 10.3 i EU:s marknadskontrollförordning. Marknadskontrollrådet, som består av 17 myndigheter, fungerar framför allt som ett forum för informations- och erfarenhetsutbyte mellan myndigheter och har bland annat till uppgift att fungera som ett samordningsorgan i frågor om marknadskontroll.

Sverige har enligt artikel 13.3 i EU:s marknadskontrollförordning upprättat en nationell strategi för marknadskontroll. Den nationella strategins syfte är att främja ett konsekvent, övergripande och samlat tillvägagångssätt för marknadskontroll och för tillämpningen av harmoniserad unionslagstiftning i Sverige.

9.5 Utgångspunkter för fördelningen av marknadskontrollansvaret på en eller flera myndigheter

9.5.1 EU:s cyberresiliensförordning

Tänkbara myndigheter

Av artikel 52.2 i EU:s cyberresiliensförordning framgår att varje medlemsstat ska utse en eller flera marknadskontrollmyndigheter för att säkerställa ett effektivt genomförande av denna förordning. Medlemsstaterna får utse en befintlig eller en ny myndighet till att fungera som marknadskontrollmyndighet inom ramen för denna förordning. Enligt skäl 107 kan befintliga myndigheter exempelvis vara behöriga myndigheter utsedda eller inrättade enligt artikel 8 i direktiv 2022/2555⁴ (NIS 2-direktivet), nationella myndigheter för cybersäkerhetscertifiering utsedda enligt artikel 58 i EU:s cybersäkerhetsakt⁵ eller marknadskontrollmyndigheter utsedda enligt radioutrustningsdirektivet⁶. I Sverige är sådana befintliga myndigheter Statens energimyndighet (Energimyndigheten), Transportstyrelsen, Finansinspektionen, Inspektionen för vård och omsorg (IVO), Läkemedelsverket, Livsmedelsverket, Post- och telestyrelsen (PTS) samt Länsstyrelserna i Norrbottens, Skåne, Stockholm och Västra Götalands län när det gäller NIS 2-direktivet⁷, Försvarets materielverk (FMV) när det gäller EU:s cybersäkerhetsakt och PTS när det gäller radioutrustningsdirektivet.

Artikel 52.14 i EU:s cyberresiliensförordning reglerar att för produkter med digitala element som klassificeras som AI-system

⁴ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2 direktivet).

⁵ Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

⁶ Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG.

⁷ Enligt förslaget till förordningen om cybersäkerhet, se SOU 2024:18, *Nya regler om cybersäkerhet*, Delbetänkande av Utredningen om genomförande av NIS2- och CER-direktiven. Se även prop. 2025/26:28, *Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag*, s. 123–124.

med hög risk enligt artikel 6 i AI-förordningen⁸ ska de marknadskontrollmyndigheter som utsetts enligt AI-förordningen vara de myndigheter som ansvarar för den marknadskontroll som föreskrivs i EU:s cyberresiliensförordning. Enligt artikel 74.3 i AI-förordningen ska för AI-system med hög risk som är relaterade till produkter som omfattas av unionens harmoniseringslagstiftning som förtecknas i avsnitt A i bilaga I⁹ marknadskontrollmyndigheten vid tillämpning av denna förordning vara den myndighet ansvarig för marknadskontroll som utsetts enligt de rättsakterna. Det rör sig om uppskattningsvis åtta myndigheter som ansvarar för lagstiftningen som förtecknas i bilagan.¹⁰ Medlemsstater kan genom undantag från denna regel utse en annan behörig myndighet att fungera som marknadskontrollmyndighet under förutsättning att de säkerställer samordning med de berörda sektorsspecifika marknadskontrollmyndigheter som är ansvariga för kontroll av efterlevnaden av unionens harmoniseringslagstiftning som förtecknas i bilaga I. Enligt artikel 74.6 och artikel 74.8 i AI-förordningen ska för AI-system med hög risk som används av finansinstitut samt för AI-system med hög risk som används för vissa ändamål och som förtecknas i bilaga III till AI-förordningen utpekats ytterligare ett antal marknadskontrollmyndigheter. Betänkandet *Anpassningar till AI-förordningen* (SOU 2025:101) föreslår Arbetsmiljöverket, Boverket, Elsäkerhetsverket, Finansinspektionen, Integritetsskyddsmyndigheten (IMY), Kemikalieinspektionen, Konsumentverket, Läke-medelsverket, MSB, PTS och Transportstyrelsen som marknadskontrollmyndigheter enligt AI-förordningen.¹¹

⁸ Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828.

⁹ Denna bilaga innehåller en förteckning över tolv harmoniseringslagstiftningsakter som bygger på den nya lagstiftningsramen (New Legislative Framework, NLF) och åtta övriga harmoniseringslagstiftningsakter.

¹⁰ Arbetsmiljöverket, Konsumentverket, Transportstyrelsen, Boverket, Elsäkerhetsverket, PTS, MSB, Läke-medelsverket.

¹¹ SOU 2025:101, *Anpassningar till AI-förordningen*, s. 225–305.

Kompetens och resurser

Enligt artikel 52.8 i EU:s cyberresiliensförordning ska medlemsstaterna säkerställa att de utsedda marknadskontrollmyndigheterna har tillräckliga ekonomiska och tekniska resurser och kompetenser som dessa marknadskontrollmyndigheter behöver för att utföra sina marknadskontrolluppgifter enligt denna förordning.

Samarbete och samordning

I EU:s cyberresiliensförordning regleras även samarbete mellan olika myndigheter. Detta gäller de myndigheter som tar emot incident- och sårbarhetsrapporter (CSIRT-enhet), Enisa, de nationella myndigheter för cybersäkerhetscertifiering, de myndigheter som utövar tillsyn över unionens dataskyddsrätt samt de myndigheter som är ansvariga för andra krav som rör en produkt med digitala element (artiklarna 52.4–52.7 i EU:s cyberresiliensförordning). FMV är utpekad som nationell myndighet för cybersäkerhetscertifiering. IMY är den myndighet som utövar tillsyn över unionens dataskyddsrätt. MSB är utpekad som CSIRT-enhet.¹² Myndigheter med ansvar för andra krav för produkter med digitala element är potentiellt de 15 marknadskontrollmyndigheterna som ingår i marknadskontrollrådet.

9.5.2 Marknadskontrollmyndighetens uppgifter

Den marknadskontrollmyndighet eller de marknadskontrollmyndigheter som pekas ut för EU:s cyberresiliensförordning ska kontrollera att produkter med digitala element uppfyller de väsentliga cybersäkerhetskraven, krav på märkning och information, dokumentationskrav samt krav på sårbarhets- och incidentrapportering som regleras i kapitel II och III i EU:s cyberresiliensförordning. Det bör noteras att EU:s cyberresiliensförordning reglerar produkternas hela livscykel under vilken tillverkaren är skyldig att tillhandahålla säkerhetsuppdateringar. Kontroll kan bli aktuell inte bara när produkten med digitala element tillhandahålls på marknaden utan

¹² Enligt förslaget i betänkandet *Samlade förmågor för ökad cybersäkerhet* (SOU 2025:79) ska arbetsuppgifter inom informations- och cybersäkerhet (inklusive CSIRT-verksamhet) överföras från MSB till FRA.

även om tillverkaren uppfyller skyldigheten att tillhandahålla säkerhetsuppdateringar.

Marknadskontroll omfattar även förebyggande verksamhet som informationsgivning till ekonomiska aktörer, utbildnings- och kommunikationsinsatser, omvärldsbevakning, deltagande i internationellt arbete med mera.

Marknadskontroll kan vara proaktiv eller reaktiv. Med proaktiv marknadskontroll avses marknadskontrollåtgärder som marknadskontrollmyndigheten har planerat på förhand och som genomförs i enlighet med marknadskontrollmyndighetens marknadskontrollplan. Med reaktiv marknadskontroll avses marknadskontroll som inleds efter att en anmälan som gjorts, till exempel av andra myndigheter, konsumenter eller ekonomiska aktörer. Enligt artikel 11.3 i EU:s marknadskontrollförordning ska marknadskontrollmyndigheterna i den proaktiva marknadskontrollen följa en riskbaserad metod när beslut fattas om vilka kontroller som ska utföras på vilka typer av produkter och i vilken omfattning.

En initial kontroll, både vid proaktiv och reaktiv marknadskontroll, består av visuella kontroller av till exempel märknings- och informationskrav (såsom CE-märkning, identifieringsmärkning, märkning med de ekonomiska aktörernas kontaktuppgifter, att en EU-försäkran om överensstämmelse följer med produkten, om användarinstruktioner finns och uppfyller kraven i bilaga II till EU:s cyberresiliensförordning). Denna kontroll kan enkelt utföras för alla produkter och lämpar sig bland annat för automatiserade kontroller med hjälp av IT-verktyg eftersom endast en begränsad bedömning ingår.

Vid stickprovskontroll eller reaktiv kontroll krävs mer kvalificerade insatser för att kontrollera om produkten uppfyller de relevanta väsentliga cybersäkerhetskraven. Här kan marknadskontrollmyndigheten behöva kontrollera hela eller delar av den tekniska dokumentationen. Exempelvis kan myndigheten granska innehållet i EU-försäkran om överensstämmelse, tillverkarens riskbedömning, eventuella provningsrapporter eller andra delar av den tekniska dokumentationen. Kontroller är tänkbara på olika nivåer, till exempel att det finns beskrivningar av funktioner och risker, att funktioner som ska finnas finns eller att de funktioner som ska finnas är tillräckliga för produkten.

Om det finns behov att kontrollera om produkten uppfyller de relevanta väsentliga cybersäkerhetskraven kan produkten även behöva provas på testlabb.

Eftersom det finns andra regelverk vid sidan om EU:s cyberresiliensförordning som är relevanta för produkter med digitala element regleras i artikel 52 i EU:s cyberresiliensförordning samarbete mellan olika myndigheter. Den eller de marknadskontrollmyndigheter som ansvarar för EU:s cyberresiliensförordning kommer att behöva samarbeta med dessa myndigheter i sin marknadskontroll.

Om marknadskontrollmyndigheten konstaterar att en produkt inte uppfyller kraven ska den kräva att den ekonomiska aktören vidtar nödvändiga åtgärder inom en viss tidsfrist. Det kan handla om olika typer av korrigerande åtgärder, försäljningsförbud eller tillbakadragande eller återkallande av produkten. Om den ekonomiska aktören inte vidtar åtgärderna ska marknadskontrollmyndigheten säkerställa att produkten till exempel dras tillbaka och informera bland annat kommissionen.

Utöver kontroll av produkter med digitala element ska marknadskontrollmyndigheten även kontrollera att skyldigheterna för sårbarhets- och incidentrapporteringsskyldigheterna enligt artikel 14 i EU:s cyberresiliensförordning har uppfyllts. Marknadskontrollmyndigheten behöver samarbeta med CSIRT-enheten i en sådan kontroll.

Marknadskontrollmyndigheten eller marknadskontrollmyndigheterna får även informations- och rapporteringskrav (artiklarna 52.10 och 52.11 i EU:s cyberresiliensförordning), krav på samarbete med berörda parter (artikel 52.12 i EU:s cyberresiliensförordning) och krav på information och samarbete med marknadskontrollmyndigheterna i andra medlemsstater när det gäller produkter med digitala element som på olika sätt inte uppfyller kraven och som tillhandahålls på olika delar av unionsmarknaden (artiklarna 54–57 i EU:s cyberresiliensförordning). Marknadskontrollmyndigheterna ska vidare utföra gemensamma aktiviteter och samordnade tillsynsåtgärder (artiklarna 59 och 60 i EU:s cyberresiliensförordning).

Den marknadskontrollmyndighet eller de marknadskontrollmyndigheter som pekas ut ska även delta i den Adco-grupp som ska bildas enligt artikel 52.15 i EU:s cyberresiliensförordning bland annat för att säkerställa en likartad tolkning och tillämpning av förordningen.

När det gäller övriga uppgifter regleras i förordning (EU) nr 1025/2012¹³ (EU:s standardiseringsförordning) att medlemsstaterna ska, där så är lämpligt, främja deltagande av myndigheter, däribland marknadskontrollmyndigheter, i nationell standardiseringsverksamhet som syftar till att utarbeta eller revidera standarder på begäran av kommissionen. Detta gäller specifikt inom de områden som omfattas av unionens harmoniseringslagstiftning avseende produkter där det är viktigt att myndigheterna deltar i standardiseringen under alla skeden av utvecklingen av de relevanta standarderna. Eftersom överensstämmelse med harmoniserade standarder ger presumtion om att produkter med digitala element överensstämmer med de väsentliga cybersäkerhetskraven i EU:s cyberresiliensförordning är det lämpligt att marknadskontrollmyndigheten deltar i standardiseringsarbete.

9.5.3 Kompetensbehov

Den marknadskontrollmyndighet eller de marknadskontrollmyndigheter som utses behöver ha eller bygga upp både kompetens för cybersäkerhet och kompetens för marknadskontroll.

Marknadskontrollkompetens finns på de 15 marknadsmyndigheter som ingår i marknadskontrollrådet som förtecknas i bilagan till förordning (2014:1039) om marknadskontroll av varor och annan närliggande tillsyn.

Cybersäkerhetskompetens finns endast på ett fåtal myndigheter och den är med stor sannolikhet svår att rekrytera. Även om marknadskontrollmyndigheten bestämmer sig för att upphandla vissa kontrolltjänster från externa leverantörer, till exempel dokumentkontroll eller provning, krävs det åtminstone en grundläggande cybersäkerhetskompetens på myndigheten. Denna grundläggande kompetens behövs för att kunna upphandla kontrolltjänsterna och utvärdera och hantera resultat och rapporter från de externa leverantörerna.

¹³ Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG.

Harmoniserade standarder är ett sätt att visa överensstämmelse med kraven i EU:s cyberresiliensförordning. Även för marknadskontrollmyndigheterna är harmoniserade standarder ett viktigt verktyg. Marknadskontrollmyndigheter behöver därför ha grundläggande cybersäkerhetskompetens för att kunna delta i standardiseringsarbete på cybersäkerhetsområdet.

Frågan är i vilken mån det kan krävas övrig kompetens. I samband med övriga kompetensbehov kan noteras att artikel 8.1 i EU:s cyberresiliensförordning identifierar krav för europeisk cybersäkerhetscertifiering för de tillfällen att kritiska produkter med digitala element används av väsentliga entiteter som omfattas av NIS 2-direktivet. I detta sammanhang behöver cybersäkerhetsrisker bedömas utifrån produkternas avsedda ändamål och det kritiska beroendet av dem av väsentliga entiteter som avses i artikel 3.1 i NIS 2-direktivet.

Även viktiga produkter med digitala element och övriga produkter med digitala element används inom olika sektorer, miljöer eller omgivningar. Produkter med digitala element kan exempelvis användas i maskiner, radioutrustning, elektronisk utrustning eller leksaker. Här skulle det kunna krävas särskild kompetens för att kunna bedöma om en funktion, som utgör ett väsentligt cyberresilienskrav, som behöver finnas i en produkt med digitala element är tillräcklig för den produkt eller i den miljö där produkten används.

9.5.4 Överväganden

Utredningens bedömning: En myndighet bör utses som marknadskontrollmyndighet.

Utredningen har beaktat följande faktorer i sina överväganden om en eller flera marknadskontrollmyndigheter ska utses. Utredningen har inhämtat upplysningar från Elsäkerhetsverket, FMV, Konsumentverket, MSB, PTS, Energimyndigheten och Swedac om en lämplig och ändamålsenlig fördelning av marknadskontrollansvaret.

Kompetensbehov

Utredningen bedömer att cybersäkerhetskompetens är avgörande för frågan om en eller flera myndigheter ska utses som marknadskontrollmyndighet. Cybersäkerhetskompetens kommer att krävas bland annat hos de ekonomiska aktörerna, hos organ för bedömning av överensstämmelse och hos marknadskontrollmyndigheterna. Denna kompetens kommer att vara svår att rekrytera. Skulle marknadskontrollansvaret spridas ut på ett flertal myndigheter behöver samtliga dessa myndigheter bygga upp åtminstone grundläggande cybersäkerhetskompetens. Dessa myndigheter kommer i så fall konkurrera om kompetensen med varandra och de andra aktörerna som har behov av sådan kompetens. Behovet av cybersäkerhetskompetens talar därför för att endast utse en myndighet som marknadskontrollmyndighet.

Utredningen bedömer vidare att behovet av sektorkompetens för att bedöma om en funktion, som utgör ett väsentligt cybersäkerhetskrav, är tillräcklig för den miljö eller omgivning där produkten används inte väger tyngre än cybersäkerhetskompetens. I de fall där sektorkompetens är avgörande för att bedöma om produkten med digitala element uppfyller de väsentliga cybersäkerhetskraven behövs bör marknadskontrollmyndigheten samarbeta med den marknadskontrollmyndighet som ansvarar för sektorslagstiftningen. Samarbete skulle kunna organiseras enligt nedan.

Samarbete, samordning och andra omständigheter

Även utifrån behovet av samarbete mellan olika myndigheter bedömer utredningen att det är lämpligt att endast en myndighet ska utses som marknadskontrollmyndighet. Det kan krävas samarbete med ett tjugotal myndigheter. Ett sådant samarbete skulle exempelvis kunna organiseras i kluster där de myndigheter som ansvarar för vissa produkttyper eller produkter som omfattas av en viss riskkategori (till exempel kritiska produkter) ingår.

En likartad tillämpning och tolkning av EU:s cyberresiliensförordning, både på nationell och på EU-nivå, kommer också att gagnas av om ansvaret endast ligger på en myndighet. Ju fler myndigheter och individer som involveras i arbetet desto större blir behovet av ensning av processer, rutiner eller tolkningar. Ansvaret för en samordnad tolk-

ning och tillämpning av EU:s cyberresiliensförordning på EU-nivå har bland annat Adco-gruppen. Ett effektivt arbetssätt i Adco-gruppen, som består av experter från medlemsstaterna, kommer att kunna uppnås på ett enklare sätt med ett mindre antal deltagare.

Det finns även andra omständigheter som talar för att endast en myndighet bör utpekas. Utredningen bedömer att det inte finns någon naturlig fördelning som säkerställer tydliga och avgränsade ansvarsområden för olika myndigheter i relation till de produkter med digitala element som omfattas av EU:s cyberresiliensförordning. Produkter med digitala element är exempelvis routrar avsedda att anslutas till internet, smarta hemprodukter med säkerhetsfunktioner eller internetanslutna leksaker. Produkter med digitala element är även komponenter såsom lösenordshanterare eller brandväggar som släpps ut på marknaden separat för att integreras i olika produkttyper. Fördelas ansvar på flera myndigheter finns det risk för en otydlighet i ansvaret eftersom det kan finnas produkter med digitala element som omfattas av flera produktregelverk (till exempel robotgräsklippare, smart hushållsutrustning, radiostyrda leksaker). Det finns även produkter med digitala element som inte omfattas av någon produktlagstiftning (till exempel vissa kategorier av mjukvara som inte omfattas av allmänna produktsäkerhetsförordningen) som skulle behöva hanteras.

Bedömning

Utifrån ovan diskuterade kriterier bedömer utredningen att endast en marknadskontrollmyndighet ska utses som marknadskontrollmyndighet för EU:s cyberresiliensförordning. Den marknadskontroll som ska utövas enligt EU:s cyberresiliensförordning ställer höga krav på kompetens på cybersäkerhetsområdet. Det är därför lämpligt att en specialiserad myndighet ansvarar för marknadskontroll.

9.6 Val av marknadskontrollmyndighet

9.6.1 Generella utgångspunkter

Marknadskontrollmyndigheten kommer att få omfattande uppgifter. För dessa uppgifter krävs tillräckliga ekonomiska och tekniska resurser, verktyg och personalresurser med nödvändig cybersäkerhetskompetens. Det är viktigt att marknadskontrollmyndigheten kan utföra sina uppgifter på ett effektivt sätt. I detta sammanhang är det en fördel om myndigheten sedan tidigare har erfarenhet av marknadskontroll och tillsyn, arbete på EU-nivå, erfarenhet av harmonisering och standardisering särskilt avseende cybersäkerhet. Teknisk kompetens och sakkunskap på cybersäkerhetsområdet eller förutsättningar att skaffa och bygga ut sådan kompetens är också viktiga faktorer att ta i beaktande vid val av marknadskontrollmyndighet.

Det finns ett antal myndigheter som i dag har verksamhet inom cybersäkerhetsområdet och/eller marknadskontroll. Dessa myndigheter är Statens energimyndighet (Energimyndigheten), Försvarets materielverk (FMV), Försvarets radioanstalt (FRA), Konsumentverket, Myndigheten för samhällsskydd och beredskap (MSB), Post- och telestyrelsen (PTS) och Styrelsen för ackreditering och teknisk kontroll (Swedac). Nedan beskrivs myndigheternas verksamhet med fokus på cybersäkerhet och marknadskontroll respektive tillsyn.

9.6.2 Statens energimyndighet

Energimyndigheten är förvaltningsmyndighet för frågor om tillförsel och användning av energi i samhället. Myndigheten leder samhällets omställning till ett hållbart energisystem, där ekologisk hållbarhet, konkurrenskraft och försörjningstrygghet går hand i hand. Målet är stabil och kostnadseffektiv energi med låg påverkan på hälsa, miljö och klimat.

Energimyndigheten bidrar med fakta, kunskap och analyser om tillförsel och användning av energi i samhället och ansvarar för Sveriges officiella energistatistik. Myndigheten ger stöd till forskning och utveckling av framtidens energilösningar och ny teknik, främjar affärsutveckling som gör det möjligt att kommersialisera och sprida innovationer och deltar i internationella klimatsamarbe-

ten och hanterar stödsystem som elcertifikatsystemet och handeln med utsläppsrätter.

Energimyndigheten har också en central roll som beredskapsmyndighet och ett sektorsansvar inom energiområdet med syfte att stärka samhällets förmåga att hantera energiförsörjningen vid kris och höjd beredskap.

Beskrivning av myndighetens verksamhet på cybersäkerhetsområdet

Energimyndigheten är tillsynsmyndighet inom energisektorn enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster med tillhörande förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. Tillsynsansvaret innebär att myndigheten kontrollerar efterlevnaden av NIS-regleringen hos leverantörer av samhällsviktiga tjänster inom energisektorn. Det gäller sektorerna el, olja/drivmedel och gas. Energimyndigheten är föreslagen att fortsatt vara tillsynsmyndighet över energisektorn för kommande NIS 2-regleringen. Det innebär bland annat att fler sektorer kommer omfattas av cybersäkerhetskraven, däribland fjärrvärme och vätgas.

Energimyndigheten är även tillsynsmyndigheten enligt 8 kap. 1 § säkerhetsskyddsförordning (2021:955) för områdena fjärrvärme-, naturgas-, olje- och drivmedelsförsörjning.

Energimyndigheten är utpekad behörig myndighet över kommissionens delegerade förordning om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden.¹⁴ Det innebär bland annat ansvar över att identifiera vilka aktörer som ska omfattas, att genomföra en nationell riskbedömning över cybersäkerhetsaspekter i gränsöverskridande elflöden och att framöver ta fram en process för tillsyn.

Energimyndigheten bedriver internt regelbunden omvärldsbevakning om bland annat cybersäkerhet inom energisektorn.

Det finns ett pågående arbete med att bygga upp cybersäkerhetskompetens inom området uppkopplade produkter.

¹⁴ Kommissionens delegerade förordning (EU) 2024/1366 av den 11 mars 2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2019/943 genom inrättandet av en nätföreskrift om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden.

Beskrivning av myndighetens marknadskontrollverksamhet

Energimyndigheten är enligt 3 a § förordningen (2016:187) om ekodesign ansvarig marknadskontrollmyndighet för produkter som omfattas av ekodesigndirektivet¹⁵, enligt 22 § punkten 2 b förordningen (2025:784) med instruktion för Statens energimyndighet marknadskontrollmyndighet för produkter som omfattas av energimärkningsförordningen¹⁶ och enligt 22 § punkten 2 d marknadskontrollmyndighet för produkter som omfattas av förordningen om märkning av däck¹⁷.

Med stöd av lagstiftningen och de beslutade produktförordningarna utövar Energimyndigheten marknadskontroll genom att kontrollera produkter som finns på den svenska marknaden. Kontroller görs genom provning av produkter, dokumentkontroller samt kontroller av information i webbutiker och fysiska butiker. Kraven som omfattas reglerar bland annat energiprestanda, utsläpp i luft och vattenanvändning, ljudnivå samt viktiga funktioner för olika produkter. Därutöver omfattas olika typer av material- och resurseffektivitetskrav. Vissa krav finns gällande hur mjukvaror och uppdateringar får påverka produktens prestanda och på programvarors tillgänglighet. Krav på ekodesign och energimärkning utvecklas löpande genom revidering och tillägg av fler produktgrupper. Preliminära förslag (ej beslutade) finns om ökade krav på monitorering och rapportering av data från produkter i drift.

Energimyndigheten deltar i EU-arbete, bland annat i Adco-grupperna inom sektorerna ekodesign, energimärkning samt energimärkning av däck. Energimyndigheten ingår i marknadskontrollrådet.

Energimyndighetens marknadskontroll är anslagsfinansierad.

9.6.3 Försvarets materielverk

FMV har regeringens uppgift att upphandla och leverera materiel och tjänster till Försvarsmakten. FMV stödjer Sveriges förmåga att bidra till Natos avskräckning och dess kollektiva försvar och bidrar

¹⁵ Europaparlamentets och rådets direktiv 2009/125/EG av den 21 oktober 2009 om upprättande av en ram för att fastställa krav på ekodesign för energirelaterade produkter.

¹⁶ Europaparlamentets och rådets förordning (EU) 2017/1369 av den 4 juli 2017 om fastställande av en ram för energimärkning och om upphävande av direktiv 2010/30/EU.

¹⁷ Europaparlamentets och rådets förordning (EU) 2020/740 av den 25 maj 2020 om märkning av däck med avseende på drivmedelseffektivitet och andra parametrar, om ändring av förordning (EU) 2017/1369 samt om upphävande av förordning (EG) nr 1222/2009.

till att försvara Sverige genom att i samarbete med Försvarsmakten utforma, upphandla och tillhandahålla materiel som möter Försvarsmaktens operativa behov. FMV utför även liknande tjänster till andra kunder inom myndighetens ansvarsområde. FMV har även fått ett regeringsuppdrag att stödja Ukraina i anskaffning och materielförsörjning.

Innan materielen lämnas över testas den vid FMV:s egna provplatser. Fordon, vapen och ledningssystem kontrolleras så att de har tekniska egenskaper och möjligheter som kravställningen säger samt att den ska gå att användas på ett sätt som gör att uppdrag kan utföras på ett effektivt sätt.

FMV är även enligt 3 § förordning (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt utsett att vara nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt.

Beskrivning av myndighetens verksamhet på cybersäkerhetsområdet

Uppgifter kopplade till cybersäkerhetscertifiering

Inom FMV finns avdelningen cybersäkerhet och certifiering som är den del av myndigheten som utför uppdraget som nationell myndighet för cybersäkerhetscertifiering samt bedriver samverkan och tillsyn enligt EU:s cybersäkerhetsakt. Avdelningen består av enheterna Sveriges certifieringsorgan för IT-säkerhet (CSEC) och Inspektionen för cybersäkerhetscertifiering (ICC).

I sin roll som nationell myndighet för cybersäkerhetscertifiering har FMV bland annat ansvar för att granska, pröva och utfärda be- myndiganden och förhandsgodkännanden i enlighet med EU:s cybersäkerhetsakt samt relevanta certifieringsordningar. Myndigheten ska också bedriva tillsyn enligt den akten. Den nationella tillsynsverksamheten är i ett uppstartsskede och förväntas utvecklas under de närmaste åren.

Verksamheten omfattar samordning och deltagande i EU-grupper för utveckling och underhåll av certifieringsordningar. FMV är delegat i Europeiska gruppen för cybersäkerhetscertifiering (ECCG) som upprättats enligt EU:s cybersäkerhetsakt. FMV deltar även i den kommitté som hanterar kommittéförfarandet för genomför-

andeakter enligt EU:s cybersäkerhetsakt. Utöver detta har myndigheten ett samverkans- och informationsuppdrag för att säkerställa kunskap och stöd på den svenska marknaden. FMV bedriver därmed ett aktivt informationsarbete och etablerar samverkan med intressenter och aktörer i Sverige och övriga EU/EES. Här ingår även det arbete som utförs av FMV som samverkansmyndighet med Nationellt cybersäkerhetscenter (NCSC).

EU:s etablering av ramverket för cybersäkerhetscertifiering i IKT-produkter, -tjänster och -processer samt utlokaliserade säkerhetstjänster enligt EU:s cybersäkerhetsakt kommer att fortsätta etableras under kommande år. Utöver den första certifieringsordningen för IKT-produkter (European Common Criteria-based cybersecurity certification scheme, EUCC) inom vilken certifikat kan börja utfärdas under 2025 är ytterligare certifieringsordningar under utveckling till exempel rörande certifiering av molntjänster och så kallade utlokaliserade säkerhetstjänster.

Som ett resultat av ikraftträdandet av EU:s första certifieringsordning för IKT-produkter (EUCC) kommer merparten av den typ av certifieringsverksamhet som Sveriges Certifieringsorgan för IT-säkerhet (CSEC) utför under 2026 kunna utföras av privata certifieringsaktörer på marknaden med FMV som tillsynsmyndighet. Det finns redan nu etablerade aktörer på den svenska marknaden som är ackrediterade för att kunna certifiera enligt EUCC.

FMV deltar i Common Criteria Recognition Arrangement (CCRA) i rollen som signatär. CCRA är ett arrangemang för samverkan och ömsesidigt erkännande av certifikat enligt metodiken Common Criteria mellan 33 länder och deras berörda myndigheter. Ett övergripande mål med samarbetet är att granskning av it-säkerhet i produkter och system ska ske med hög tillförlitlighet och konsistens genom att standarden Common Criteria används för kravställning. Arbetet omfattar både certifieringsverksamhet (som kommer påverkas av EU-reglernas tillämpning) och deltagande i tekniska arbetsgrupper och ömsesidig granskning mellan de deltagande organisationerna.

FMV är även ansvarig nationell myndighet för certifiering av it-produkter inom ramen för Natos regelverk för säkerhet i kommunikations- och informationssystem och ska verka vid anmälan av certifierade it-produkter till Natos produktlista enligt Natos regelverk samt bistå svenska leverantörer vid sådan anmälan. Formerna

för genomförande av uppdraget och dess koppling till genomförande av andra delar av Natoregelverkets systematik och myndighetsroller på området utvecklas vidare.

Samverkansmyndighet i Nationella cybersäkerhetscentret (NCSC)

FMV är enligt 4–5 och 7 §§ förordning (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt samverkansmyndighet till det Nationella cybersäkerhetscentret (NCSC) inom FRA.

FMV deltar i det strategiska samverkansrådet till NCSC.

Övriga uppgifter kopplade till cybersäkerhet

En inte oväsentlig del av FMV:s uppgifter inom cybersäkerhet är av vikt för målen i den nationella strategin för cybersäkerhet 2025–2029¹⁸ och ingår som aktiviteter i strategins tillhörande handlingsplan. Några av dessa uppgifter, varav vissa regeringsuppdrag, handlar om att bistå FRA och MSB och utförs inom ramen för samverkan inom NCSC.

Tillsyn enligt EU:s cybersäkerhetsakt

FMV har i sin roll som nationell myndighet för cybersäkerhetscertifiering tillsynsansvar över aktörer och certifikat för certifierade IKT-produkter, -tjänster och -processer, se artikel 58.7 och 58.8 i EU:s cybersäkerhetsakt.

I dessa tillsynsuppgifter ingår bland annat att:

- övervaka och kontrollera efterlevnaden av bestämmelserna i europeiska ordningar för cybersäkerhetscertifiering,
- kontrollera att tillverkare eller leverantörer av IKT-produkter, IKT-tjänster eller IKT-processer samt utlokaliserade säkerhetstjänster som är etablerade i Sverige fullgör och verkställer sina skyldigheter,

¹⁸ Nationell strategi för cybersäkerhet 2025–2029, Skr. 2024/25:121.

- aktivt bistå och stödja de nationella ackrediteringsorganen med övervakning och kontroll av verksamhet som bedrivs av organen för bedömning av överensstämmelse,
- behandla klagomål från fysiska eller juridiska personer avseende europeiska cybersäkerhetscertifikat på nivå hög.

Utöver tillsynsuppgifterna som följer av rollen som nationell myndighet för cybersäkerhetscertifiering ska FMV även i den rollen fatta ett antal olika myndighetsbeslut kopplat till organ för bedömning av överensstämmelse. Det rör bland annat beslut om bemyndigande för ett organ att utfärda certifikat om det påkallas av en certifieringsordning (särskilda och ytterligare krav) och förhandsgodkännande för enskilda certifikat som ska utfärdas av ett privat certifieringsorgan på assurancesnivå hög. FMV har även rollen som anmälade myndighet för de organ som blivit ackrediterade och i tillämpliga fall bemyndigande enligt en europeisk certifieringsordning.

Annan tillsyn med koppling till cybersäkerhetsområdet

FMV är tillsynsmyndighet enligt 8 kap. 1 § säkerhetsskyddsförordningen (2021:955) för området försvarsmateriel.

Beskrivning av myndighetens marknadskontrollverksamhet

FMV har inte några sådana uppgifter.

9.6.4 Försvarets radioanstalt

FRA är en civil myndighet under Försvarsdepartementet. FRA är en del av svensk underrättelsetjänst med uppgift att bedriva signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet och till lagen anslutande förordning.

FRA bedriver signalspaning i syfte att kartlägga bland annat yttre militära hot, hot mot svensk personal under internationella insatser, internationell terrorism, främmande underrättelseverksamhet mot svenska intressen och övriga internationella företeelser som har betydelse för svensk utrikes-, säkerhets- och försvarspolitik. All

signalspaning är riktad mot utländska förhållanden och sker på uppdrag av regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen inom Polismyndigheten. Uppdragsgivarna är fortlöpande i behov av underrättelserapportering och signalspaningsverksamheten bidrar kontinuerligt till att skydda Sverige och svenska intressen. All inhämtning genom signalspaning kräver tillstånd från Försvarsunderrättelsedomstolen.

FRA bedriver även cybersäkerhetsverksamhet. FRA ska ha hög teknisk kompetens inom informationssäkerhetsområdet och får efter begäran stödja sådana statliga myndigheter och enskilda verksamhetsutövare som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende.

Beskrivning av myndighetens verksamhet på cybersäkerhetsområdet

FRA har till huvuduppgift att bedriva signalspaning och stödja andra myndigheter i frågor som rör signalspaning och kryptologi. Enligt 4 § förordning (2007:937) med instruktion för Försvarets radioanstalt ska myndigheten därtill ha en hög teknisk kompetens på informationssäkerhetsområdet. Myndigheten får efter begäran stödja sådana statliga myndigheter och enskilda verksamhetsutövare som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. Myndigheten ska särskilt kunna stödja insatser vid nationella kriser med it-inslag, medverka till identifiering av iblandade aktörer vid it-relaterade hot mot samhällsviktiga system, genomföra it-säkerhetsanalyser och ge annat tekniskt stöd. Myndigheten ska även samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet.

Inom FRA finns enligt 4 a § förordning (2007:937) med instruktion för Försvarets radioanstalt ett nationellt cybersäkerhetscenter (NCSC). Centret har till uppgift att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter.

Beskrivning av myndighetens marknadskontrollverksamhet

FRA har inte några sådana uppgifter.

9.6.5 Konsumentverket

Konsumentverket är förvaltningsmyndighet för konsumentfrågor och har bland annat ansvar för att utöva tillsyn, inklusive marknadskontroll, enligt de konsumentskyddande regler som ligger inom myndighetens ansvarsområde. Utöver arbetet med produktsäkerhet ska Konsumentverket bevaka och analysera marknaderna ur ett konsumentperspektiv samt vid behov vidta eller föreslå åtgärder. Vidare ska myndigheten genom information och vägledning ge konsumenter goda förutsättningar att ta till vara sina intressen, vilket Konsumentverket gör bland annat genom information till företag, information och vägledning till konsumenter, samt stöd till skola och samhällsaktörer.

Beskrivning av myndighetens verksamhet på cybersäkerhetsområdet

Konsumentverket har ingen verksamhet som är direkt kopplat till cybersäkerhetsområdet.

Beskrivning av myndighetens marknadskontrollverksamhet

Myndigheten är utpekad marknadskontrollmyndighet avseende leksaker, personlig skyddsutrustning, tjänster och övriga konsumentprodukter som inte omfattas av speciallagstiftning.

Konsumentverket har enligt 17 § förordningen (2011:703) om leksakers säkerhet det huvudsakliga marknadskontrollansvaret för leksakers säkerhet men delar ansvaret med Elsäkerhetsverket (avseende elektriska egenskaper) och Kemikalieinspektionen (avseende brännbara och kemiska egenskaper). Enligt 16 § förordningen (2011:703) om leksakers säkerhet ska de tre marknadskontrollmyndigheterna samordna sina åtgärder om kontrollen avser samma leksak eller om åtgärderna riktar sig mot samma ekonomiska aktör. Konsumentverket är enligt 2 § förordningen (2018:127) med kompletterande

bestämmelser till EU:s förordning om personlig skyddsutrustning marknadskontrollmyndighet för personlig skyddsutrustning avsedd för privat bruk. Arbetsmiljöverket har motsvarande ansvar avseende utrustning för yrkeslivet enligt 3 § förordningen (2018:127) med kompletterade bestämmelser till EU:s förordning om personlig skyddsutrustning. Konsumentverket deltar i standardiseringsarbetet på dessa områden.

Konsumentverket är även marknadskontrollmyndighet för konsumentprodukter som faller inom området för allmän produktsäkerhet (tillsammans med Elsäkerhetsverket, Kemikalieinspektionen, Läkemedelsverket, Arbetsmiljöverket, Boverket och MSB). Ytterligare ett antal statliga myndigheter har ett tillsynsansvar enligt produktsäkerhetslagen (2004:451) och produktsäkerhetsförordningen (2004:469) i fråga om vissa konsumentvaror, tjänster eller risker.

Vissa cybersäkerhetsaspekter regleras i allmänna produktsäkerhetsförordningen. Enligt artikel 6.1 g i allmänna produktsäkerhetsförordningen ska cybersäkerhetsrisker beaktas vid bedömning av huruvida en produkt är en säker produkt, såvitt dessa cybersäkerhetsrisker påverkar konsumenters säkerhet och inte hanteras genom sektorsspecifik lagstiftning. Hittills har Konsumentverket i princip inte kommit i kontakt med frågor kopplade till cybersäkerhet inom detta område.

Konsumentverkets marknadskontroller görs genom riktade stickprovskontroller. Varor och tjänster med misstänkt dålig säkerhet eller annan bristande överensstämmelse väljs ut för provning eller dokumentkontroll. Kontrollen kan också ske genom att Konsumentverket gör planerade besök hos utvalda ekonomiska aktörer. Verket kan också göra marknadskontroll om det hänt en olycka eller om en anmälan inkommit. Syftet med marknadskontrollerna är att säkerställa konsumenternas säkerhet och hälsa samt att bidra till mer rättvis konkurrens mellan företag.

Konsumentverket deltar i EU-arbete, bland annat i Adco-grupperna inom sektorerna leksaker och personlig skyddsutrustning. Konsumentverket ingår i marknadskontrollrådet.

Konsumentverkets marknadskontroll är anslagsfinansierad. Dessutom ska de ekonomiska aktörerna ersätta Konsumentverket för kostnader för provtagning och undersökning av prov om det visat sig att de provade leksakerna eller produkterna som omfattas av produktsäkerhetslagen är farliga (se 19 § förordning (2011:703) om

leksaker säkerhet, 11 § produktsäkerhetsförordningen (2004:469)) eller om den provade personliga skyddsutrustningen inte överensstämmer med kraven (se 7 § lagen (2018:125)) med kompletterande bestämmelser till EU:s förordning om personlig skyddsutrustning).

9.6.6 Myndigheten för samhällsskydd och beredskap

MSB har ansvar för frågor om skydd mot olyckor, krisberedskap och civilt försvar, i den utsträckning inte någon annan myndighet har ansvaret. Ansvaret avser åtgärder före, under och efter en olycka, kris, krig eller krigsfara.

I myndighetens uppdrag ingår ansvar för informations- och cybersäkerhet, samhällsviktiga kommunikationer och säker informationsdelning, ledningsplatser, rymdsäkerhet, samordning av krisberedskap och civilt försvar, skydd mot olyckor och farliga ämnen, insatsverksamhet etcetera.

Beskrivning av myndighetens verksamhet på cybersäkerhetsområdet

MSB:s uppdrag kring information- och cybersäkerhet är omfattande och omfattar ansvar kring förbyggande såväl som operativ och strategisk cybersäkerhet. Området är under ständig utveckling vilket sannolikt kommer påverka myndighetens uppdrag på kort och lång sikt. Bland annat har myndigheten givits ett antal regeringsuppdrag på området.

Stärka forskning och innovation för informations- och cybersäkerhet, inklusive att utgöra nationellt samordningscenter NCC-SE

Myndigheten är enligt 11 c § i förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap nationellt samordningscenter (NCC-SE) enligt artikel 6 i förordning (EU) 2021/887 (CCCN-förordningen).¹⁹

¹⁹ Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum.

Inom ramen för MSB:s forskningsutlysningar inom samhällsskydd och beredskap så görs även utlysningar av forskningsmedel som kopplar till informations- och cybersäkerhet. Inriktningen för MSB:s kommande utlysningar beskrivs i en flerårig strategi.

Därutöver deltar MSB i olika samarbeten för att främja forskning, kunskapsutveckling och innovation för informations- och cybersäkerhet. Som del i detta är MSB medlem i Centrum för cyberförsvar och informationssäkerhet (CDIS) och Cybercampus.

Analysera och bedöma omvärldsutvecklingen avseende informations- och cybersäkerhet

MSB ökar kunskapen i samhället om informations- och cybersäkerhet genom att analysera och bedöma omvärldsutvecklingen nationellt och internationellt, samt genom att sprida resultatet till identifierade målgrupper. I uppgiften ingår att bedriva strategisk analys i syfte att skapa underlag för MSB:s arbete med att inrikta arbetet på området, samt ta fram rapporter och övriga produkter som stöd för samhällets aktörer. I leveranserna ingår även olika former av formell rapportering till regeringen, exempelvis en årlig analys av it-incidentrapporteringen.

I uppdraget ingår att utveckla och tillhandahålla verktyg till organisationer som stödjer uppföljning och förbättring av det systematiska arbetet med informations- och cybersäkerhet. I uppgiften ingår även att regelbundet rapportera en samlad bedömning av nivån på det systematiska arbetet med informations- och cybersäkerhet i samhället, genom Cybersäkerhetskollen.

Utgöra gemensam nationell kontaktpunkt enligt NIS-direktivet och vara Sveriges representant i NIS samarbetsgrupp

MSB är enligt 22–23 § förordningen (2018:1175) om informations-säkerhet för samhällsviktiga och digitala tjänster utsedd till gemensam nationell kontaktpunkt samt företrädar Sverige i NIS samarbetsgrupp. Syftet med samarbetsgruppen är att underlätta strategiskt samarbete och informationsutbyte mellan medlemsstaterna samt stärka förtroende och tillit. Gruppen har ett stort antal uppgifter som beskrivs närmare i NIS-direktivet. I gruppens uppgifter ingår

bland annat att tillhandahålla vägledning och utbyta praxis i fråga om NIS-direktivets genomförande.

Inom ramen för uppdraget ingår deltagande i flertal subgrupperingar.

MSB ska leda ett samarbetsforum där tillsynsmyndigheterna och Socialstyrelsen ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

Utgöra svensk teknisk kontaktpunkt för OSSE på cyberområdet

MSB har ett regeringsuppdrag som lyder att myndigheten ska stödja Utrikesdepartementet med en teknisk kontaktperson inom OSSE Confidence Building Measure (CBM) 8 Cyber och informationsteknologi och (i begränsad utsträckning) CBM 14 för privat-offentlig samverkan. I rollen som teknisk kontaktpunkt ingår det att vid behov stödja den politiska kontaktpunkten på Utrikesdepartementet samt samverka gentemot den svenska representationen i Wien.

Normering inom området informations- och cybersäkerhet

MSB föreskriver om säkerhet i nätverk och informationssystem för leverantörer som omfattas av NIS-regleringen. I uppgiften ingår att förvalta och utveckla ett föreskriftspaket som omfattar informations-säkerhet, it-säkerhet och incidentrapportering för leverantörer av samhällsviktiga tjänster.

MSB föreskriver om säkerhetskrav för informationshanteringssystem, inklusive it-incidentrapportering, för statliga myndigheter. I uppgiften ingår att förvalta och utveckla ett föreskriftspaket som omfattar informationssäkerhet, it-säkerhet och incidentrapportering för statliga myndigheter.

Relaterat till området ska MSB förvalta, utveckla och tillhandahålla en databas för termer inom informations- och cybersäkerhet som kan utvecklas över tid samt är allmänt tillgänglig och kostnadsfri. Databasen ska löpande fyllas på med aktuella termer. MSB deltar också i och stödjer i standardiseringsarbetet på informations- och cybersäkerhetsområdet.

*Lämna råd och stöd om förebyggande arbete
med informations- och cybersäkerhet*

MSB ökar medvetenheten om behovet av informations- och cybersäkerhet hos allmänheten och framför allt små och medelstora företag. Uppgiften genomförts tillsammans med ett stort antal aktörer i samhället och handlar om att kommunicera en-till-många på bred front i samhället, i detta ingår olika former av råd och stöd. Regelbundna leveranser är nationella informationskampanjer ("Tänk säkert") samt ett samarbete med Stöldskyddsföreningen (SSF).

MSB lämnar råd och stöd i fråga om förebyggande arbete på informations- och cybersäkerhet till andra statliga myndigheter, kommuner och regioner samt företag och organisationer.

MSB lämnar stöd till samhällsviktig verksamhet i fråga om förebyggande arbete när det gäller cybersäkerhet i cyberfysiska system. Syftet är att öka säkerheten i cyberfysiska system samt bidra till höjd förmåga inom totalförsvaret att förebygga störningar och incidenter. MSB:s arbete med cyberfysiska system sker inom två huvudgrupper: industriella information- och styrsystem (ICS) respektive Internet of Things (IoT).

MSB lämnar råd och stöd i fråga om organisationers arbete med säkerhetsåtgärder och it-säkerhet mer generellt.

Som en del i att lösa uppgiften utvecklar och tillhandahåller MSB forum och nätverk för informationsutbyte och samverkan inom informations- och cybersäkerhetsområdet.

*Se till att utbildningar kommer tillstånd
inom området informations- och cybersäkerhet*

MSB tillhandahåller utbildning inom informations- och cybersäkerhet i en begränsad omfattning. I detta ingår att genomföra eller tillhandahålla ett fåtal specifika utbildningar i egen regi. Vidare kan även MSB i specifika fall beställa utbildningar av externa parter.

Huvudprincipen är dock att utbildningsväsendet och marknaden tillhandahåller utbildningar på informations- och cybersäkerhetsområdet. I uppgiften ingår också att MSB medverkar i specifika utbildningar och även bevakar och stödjer utbildningsområdet.

*Se till att övningar kommer tillstånd
inom området informations- och cybersäkerhet*

MSB planerar, genomför och utvärderar olika former av cybersäkerhetsövningar. Arbetet sker tillsammans med ett stort antal externa parter, och prioritet ges till nationella övningar och etablerade övningsserier. I uppgiften ingår både olika former av tekniska övningar och bredare samverkansövningar (cyberkris). Målsättningen är att de breda övningarna ska ske genom samarbetet i Nationellt cybersäkerhetscenter (NCSC).

MSB deltar i nationella och internationella cybersäkerhetsövningar enligt löpande inriktning. Prioritet ges till övningar som genomförs som en del av ett formellt samarbete, exempelvis inom EU, Nato och Norden. Deltagande i övningar kopplas till en formell roll, exempelvis nationell CSIRT-enhet eller nationell kontaktpunkt.

MSB stödjer, tillsammans med Försvarsmakten, arbetet vid Totalförsvarets forskningsinstitut (FOI) att utveckla och tillhandahålla en nationell cyber range. Arbetet syftar till att Sverige ska kunna erbjuda en modern nationell cyber range för praktisk utbildning, träning och övning i informations- och cybersäkerhet. Fokus är totalförsvarets behov och hänsyn tas till de kommersiella aktörer som bygger upp anläggningar för utbildning och övning kopplat till cybersäkerhet. MSB:s uppgift omfattar att lämna ekonomiskt bidrag till arbetet, krävställa och inrikta verksamheten samt samverka kring nyttjandet av anläggningen.

*Vara CERT-SE och utgöra nationell CSIRT-enhet
– förebygga och hantera it-incidenter och cyberangrepp*

CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stötta samhället i arbetet med att hantera och förebygga it-incidenter. Verksamheten är en del av MSB. CERT-SE:s tjänster riktar sig till offentlig sektor, privata företag och organisationer.

CERT-SE är Sveriges CSIRT-enhet enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen). Utpekade CSIRT-enheter ska uppfylla krav enligt denna lagstiftning när det gäller teknisk kapacitet och utbildad personal, säker och motståndskraftig kommunikations- och informations-

infrastruktur och säkra lokaler. Uppgiften omfattar att förvalta och utveckla förutsättningsskapande verksamhet i syfte att kunna leva upp till NIS-direktivets grundkrav på en nationell CSIRT-enhet.

Som nationell CSIRT-enhet representerar MSB Sverige i det europeiska nätverket för nationella CSIRT-enheter (CSIRT-network).

Samordning av och stöd till cyberkrishantering

MSB ska som nationell cyberskrishanteringsmyndighet ansvara för hanteringen av storskaliga cybersäkerhetsincidenter och kriser i enlighet med kommande nationella plan för hantering av storskaliga cybersäkerhetsincidenter och kriser. MSB representerar Sverige i EU CyCLONe.

MSB har fått i uppdrag att vara nationell kontaktpunkt för EU:s snabbinsatsförmåga mot hybridhot.

Samverkansmyndighet i Nationella cybersäkerhetscentret (NCSC)

MSB är enligt 4–5 och 7 §§ förordning (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt samverkansmyndighet till det Nationella cybersäkerhetscentret (NCSC) inom FRA.

MSB deltar i det strategiska samverkansrådet till NCSC.

Förslag att överföra centrala delar av MSB:s verksamhet på informations- och cybersäkerhetsområde till FRA

I betänkandet *Samlande förmågor för ökad cybersäkerhet* (SOU 2025:79) konstateras att FRA och MSB har överlappande ansvarsområden på informations- och cybersäkerhetsområdet och det föreslås att centrala delar av MSB:s verksamhet på detta område ska föras över till FRA. Förslagen innebär bland annat att följande uppgifter, som regleras i förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap, ska flyttas över till FRA.

- Ansvaret för att stödja och samordna arbetet med samhällets informations- och cybersäkerhet samt analysera och bedöma omvärldsutvecklingen som nu återfinns i 11 a § första stycket.

- Rapporteringsskyldigheten till regeringen på informations- och cybersäkerhetsområdet som regleras i 11 a § andra och tredje stycket.
- Uppdraget att ha en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter som i dag regleras i 11 b §.
- MSB:s uppdrag enligt 11 c § att utgöra nationellt samordningscenter (NCC-SE) enligt artikel 6 i CCCN-förordningen.
- Uppgiften i 18 j § att utgöra teknisk kontaktpunkt för Organisationen för säkerhet och samarbete i Europa.

Även ansvaret för informations- och cybersäkerhetsarbetet i det nationella beredningssystemet, specifikt ansvaret för incidentrapporteringsfunktionen, som regleras i förordning (2022:524) om statliga myndigheters beredskap ska överföras till FRA.

Utredningen föreslår även att de uppgifter som i betänkandet *Nya regler om cybersäkerhet* (SOU 2024:18) föreslås att ges till MSB i stället ska ges till FRA. Det rör sig om rollen som CSIRT-enhet, gemensam kontaktpunkt och cyberkrismyndighet samt att stå värd för ett samarbetsforum för de myndigheter som tilldelas tillsynsuppgifter för NIS 2-direktivet.

Beskrivning av myndighetens marknadskontrollverksamhet

MSB är enligt 23 § förordningen (2010:1075) om brandfarliga och explosiva varor marknadskontrollmyndighet för de produkter som omfattas av ett antal direktiv.²⁰ Myndigheten är enligt 7 § tredje stycket i förordning (2006:311) om transport av farligt gods marknadskontrollmyndighet för produkter som omfattas av direktivet om transportabla tryckbärande anordningar²¹ och enligt 2 § förordning (2018:1179) med kompletterande bestämmelser till EU:s förord-

²⁰ Rådets direktiv 75/324/EEG av den 20 maj 1975 om tillnärmning av medlemsstaternas lagar och andra författningar beträffande aerosolbehållare när det gäller aerosolbehållare med brandfarligt innehåll, Europaparlamentets och rådets direktiv 2013/29/EU av den 12 juni 2013 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av pyrotekniska artiklar, och Europaparlamentets och rådets direktiv 2014/28/EU av den 26 februari 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden och övervakning av explosiva varor för civilt bruk.

²¹ Europaparlamentets och rådets direktiv 2010/35/EU av den 16 juni 2010 om transportabla tryckbärande anordningar.

ning om gasanordningar marknadskontrollmyndighet för produkter som omfattas av förordningen om aerosolbehållare²² (till exempel sprayburkar med färg, deodorant), transportabla tryckbärande anordningar (till exempel gasflaskor), gasanordningar (till exempel gasolgrillar, gasspisar), pyrotekniska artiklar (till exempel fyrverkerier, airbags) och explosiva varor för civilt bruk.

MSB har ansvaret för att lämpliga kontroller av dessa produkters egenskaper utförs i tillräcklig omfattning och ansvaret omfattar produkter som görs tillgängliga i Sverige, både på och utanför internet.

MSB deltar i EU-arbete, bland annat i Adco-grupperna inom sektorerna transportabla tryckbärande anordningar, pyroteknik, explosiva varor för civilt bruk samt anordningar för förbränning av gasformiga bränslen. MSB ingår i marknadskontrollrådet.

MSB:s marknadskontroll är anslagsfinansierad.

Marknadskontrolluppgiften enligt ovan hanteras av en annan avdelning än den som ansvarar för cybersäkerhet.

Myndigheten bedriver i dag ingen marknadskontroll eller tillsyn med koppling till cybersäkerhet.

9.6.7 Post- och telestyrelsen

PTS är förvaltningsmyndighet med ett samlat ansvar inom postområdet och området för elektronisk kommunikation. PTS har till uppgift att verka för att målen inom politiken för informationssamhället uppnås. Inom området elektronisk kommunikation ingår telekommunikationer, it och radio. Myndigheten arbetar också med att främja tillgången till grundläggande betaltjänster. Utöver detta är PTS också sektorsansvarig beredskapsmyndighet, vilket innebär ansvar för beredskapssektorn elektroniska kommunikationer och post. Arbetet inom de olika ansvarsområdena sker framför allt genom reglering och tillsyn samt främjande insatser genom bland annat samverkan.

PTS är marknadskontrollmyndighet enligt radioutrustningslagen (2016:392) och lagen (2023:254) om vissa produkters och tjänsters tillgänglighet.

²² Europaparlamentets och rådets förordning (EU) 2016/426 av den 9 mars 2016 om anordningar för förbränning av gasformiga bränslen. Produkter som omfattas är aerosolbehållare.

Myndigheten har de senaste åren tillförts en rad nya uppgifter. PTS har bland annat fått i uppdrag att vara samordnande myndighet för tillämpningen av EU:s förordning om digitala tjänster (DSA)²³ och EU:s dataförvaltningsförordning (DGA)²⁴.

PTS och Myndigheten för digital förvaltning (Digg) fick den 5 december 2024 i uppdrag att lämna ett gemensamt förslag på hur Diggs uppgifter skulle kunna överföras till och inordnas i PTS. Regeringens besked i budgetpropositionen för 2026, som kom den 22 september 2025, är att PTS och Digg ska gå samman till en gemensam myndighet. Syftet är att kraftsamla och stärka digitaliseringsarbetet i Sverige. Sammangåendet ska göras genom att Diggs uppgifter flyttas över till PTS. Diggs nuvarande uppdrag är att göra den offentliga förvaltningen mer effektiv och ändamålsenlig. Myndigheten samordnar och stödjer den förvaltningsgemensamma digitaliseringen och ansvarar för den förvaltningsgemensamma digitala infrastrukturen. Det officiella uppdraget förväntas komma först efter att riksdagen beslutar om budgeten för 2026 i december. Organisationsförändringen ska träda i kraft senast den 1 januari 2027.

Beskrivning av myndighetens verksamhet på cybersäkerhetsområdet

PTS arbetar med frågor rörande cybersäkerhet och samverkar med andra myndigheter inom cybersäkerhet. Cybersäkerhetsfrågorna har sin grund i flera olika regelverk som redovisas nedan. PTS arbetar också med standardisering inom cybersäkerhet och nya cybersäkerhetsfrågor som till exempel inom ramen för EU:s cyberresiliensförordning, NIS 2-direktivet²⁵, EU:s cybersäkerhetsakt, CER-direktivet²⁶ och AI-förordningen.

²³ Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster).

²⁴ Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten).

²⁵ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS2-direktivet).

²⁶ Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

Myndigheten har även ansvar inom betrodda tjänster utifrån bestämmelser i eIDAS-förordningen²⁷, till exempel införandet av den europeiska digitala identitetsplånboken.

NIS-lagen

PTS är tillsynsmyndighet för sektorn digital infrastruktur och digitala tjänster enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen).

eIDAS-förordningen

Inom ramen för eIDAS-förordningen är PTS tillsynsmyndighet över tillhandahållare av betrodda tjänster och de betrodda tjänster som tillhandahålls och över offentlig förvaltnings anslutning till den svenska eIDAS-noden.

Syftet med eIDAS-förordningen är att skapa en säker och enhetlig grund för elektronisk identifiering och betrodda tjänster inom hela EU.

PTS tar även emot och handlägger incidentrapporter från tillhandahållare av betrodda tjänster.

Säkerhetsskyddslagen (2018:585)

PTS är tillsynsmyndighet enligt säkerhetsskyddslagen (2018:585) för enskilda verksamhetsutövare som bedriver säkerhetskänslig verksamhet inom områdena elektronisk kommunikation och posttjänster.

Lagen (2022:482) om elektronisk kommunikation

PTS bedriver tillsyn över tillhandahållare av allmänna kommunikationsnät samt allmänt tillgängliga elektroniska kommunikationstjänster enligt lagen (2022:482) om elektronisk kommunikation (LEK). PTS har som uppdrag att utöva tillsyn över säkerheten i

²⁷ Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet.

allmänna elektroniska kommunikationsnät och kommunikationstjänster samt skyddet av behandlade uppgifter.

PTS handlägger också rapporterade incidenter från marknadens aktörer.

Samverkansmyndighet i Nationella cybersäkerhetscentret (NCSC)

PTS är enligt 4–5 och 7 §§ förordning (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt samverkansmyndighet till det Nationella cybersäkerhetscentret (NCSC) inom FRA.

PTS deltar i det strategiska samverkansrådet till NCSC.

NIS 2- och CER-direktiven

NIS 2-direktivet kommer att implementeras genom cybersäkerhetslagen. PTS föreslås bli tillsynsmyndighet för sektorerna digital infrastruktur, förvaltning av IKT-tjänster, rymden, post- och budtjänster och digitala leverantörer.

PTS föreslås även få tillsynsansvar för sektorerna digital infrastruktur och rymden enligt den kommande lagen om motståndskraft som genomför CER-direktivet.

PTS externa aktiviteter inom cybersäkerhet

PTS har genomfört ett antal aktiviteter inom cybersäkerhet de senaste åren exempelvis:

- Sedan 2019 representerat Sverige i NIS 5G Cybersecurity WS och varit vice ordförande i framtagandet av bland annat ”5G Toolbox”,
- Sedan 2020 infört villkor i spektrumvillkor som innehåller bland annat cybersäkerhetskontroller,
- Mellan 2021–2024 representerat Sverige i framtagande av en 5G-cerifieringsordning som del av EU:s cybersäkerhetsakt,
- Genomfört två regeringsuppdrag angående cybersäkerhetsriskanalyser i 5G-näten i Sverige,

- Deltagit i olika cybersäkerhetsstandardiseringsaktiviteter (exempelvis ETSI OpenRAN, SIS/TK 318, ITS WG cybersecurity),
- Deltar med delegat i OECD:s Working Party on Digital Security,
- Deltagit med suppleant i Enisa:s styrelse,
- Deltagit med svensk National Liaison Officer vid Enisa.

PTS aktiviteter inom ramen för EU:s cyberresiliensförordning

PTS deltog i rådsförhandlingarna av EU:s cyberresiliensförordning under Sveriges ordförandeskap i Europeiska unionens råd 2023. PTS deltar tillsammans med representanter från FMV och Swedac i kommissionens expertgrupp. PTS deltar även i kommissionens cyberresilienskommitté som inrättats enligt artikel 62.1 i EU:s cyberresiliensförordning. Av 7 § punkten 3 förordning (2007:951) med instruktion för Post- och telestyrelsen framgår att PTS ska delta i nationellt och internationellt standardiseringsarbete. PTS uppfyller denna skyldighet även på cybersäkerhetsområdet genom att delta i arbetet med framtagandet av harmoniserade standarder för EU:s cyberresiliensförordning främst genom deltagande i SIS/TK 318. PTS bevakar även standardiseringsarbetet inom ETSI på en övergripande nivå.

Beskrivning av myndighetens marknadskontrollverksamhet

Marknadskontroll med kopplingar till cybersäkerhet

PTS är enligt 9 § förordningen (2016:394) om radioutrustning marknadskontrollmyndighet för produkter som omfattas av radioutrustningsdirektivet, med undantag för produkternas egenskaper när det gäller elsäkerhet.

Radioutrustningsdirektivet innehåller utöver krav på hälsa och säkerhet, krav på elektromagnetisk kompatibilitet och radiokrav även krav på cybersäkerhet för vissa kategorier av radioutrustning. Dessa krav har införts genom kommissionens delegerade förordning om

cybersäkerhetskrav.²⁸ Kraven tillämpas från och med 1 augusti 2025. Syftet med regleringen är att skapa en säkrare och mer robust miljö för internetuppkopplad radioutrustning, radioutrustning som är konstruerad eller avsedd uteslutande för barnomsorg samt radioutrustning som omfattas av leksaksdirektivet och radioutrustning, som är konstruerad eller avsedd att bäras på olika delar av människokroppen eller spännas fast på olika klädesplagg som bärs av människor, som behandlar personuppgifter, trafikuppgifter eller lokaliseringssuppgifter. Regleringen ska öka motståndskraften i nätverk genom att tillverkare måste införa säkerhetsmekanismer i sina produkter som ska minska risker för att uppkopplad utrustning används för att störa andra tjänster i ett nätverk. Kopplat till detta ska också den personliga integriteten vid användning av uppkopplad utrustning stärkas genom att mekanismer för att skydda personliga data införs. Slutligen ska även åtgärder som minskar risker för att utsättas för monetärt bedrägeri vid elektroniska betalningar implementeras.

PTS marknadskontroll består av kontroll av radioutrustning på den svenska marknaden samt informations- och utbildningsinsatser kring regelverket. Den planerade (proaktiva) marknadskontrollen är riskbaserad och följer PTS program för marknadskontroll. Marknadskontrollverksamheten inkluderar även samarbete med Tullverket för att kontrollera radioutrustning innan den övergår till fri omsättning.

PTS marknadskontrollinspektörer kontrollerar om utrustningen uppfyller de administrativa kraven. För kontroll av de väsentliga kraven för elektromagnetisk kompatibilitet och radio har PTS upphandlat ett ackrediterat testlabb som utför provningar. Testlabbet har bekräftat att de även har möjlighet att kontrollera cybersäkerhetskrav med utgångspunkt i de tre harmoniserade standarderna som är publicerade i Europeiska unionens officiella tidning (EUT).

PTS deltar på EU-nivå i kommissionens expertgrupp och kommitté som inrättats genom radioutrustningsdirektivet, i Adco-gruppen samt när det gäller standardisering i ETSI. På nationell nivå deltar PTS i Marknadskontrollrådet och dess undergrupper samt när det gäller standardisering i ITS och SEK:s tekniska kommittéer. När

²⁸ Kommissionens delegerade förordning (EU) 2022/30 av den 29 oktober 2021 om komplettering av Europaparlamentets och rådets direktiv 2014/53/EU vad gäller tillämpningen av de väsentliga krav som avses i artikel 3.3 d, e och f i det direktivet.

det gäller standardisering på cybersäkerhetsområdet deltar PTS även i SIS tekniska kommittéer.

PTS marknadskontroll enligt radioutrustningslagen är avgiftsfinansierad. Enligt 15 § radioutrustningslagen (2016:392) ska den som är anmäld enligt 2 kap. 1 § lagen (2022:482) om elektronisk kommunikation eller som har tillstånd enligt 3 kap. 1 § samma lag betala en avgift. Förordning (2016:602) om finansiering av Post- och telestyrelsens verksamhet reglerar närmare de avgifter som ska tas ut. Enligt 9 kap. 2 § Post- och telestyrelsens föreskrifter (2023:2) om radioutrustning ska den ekonomiska aktören vars radioutrustning har kontrollerats ersätta myndigheten för kostnader som uppkommit vid provning i de fall utrustningen vid kontrollen visar sig inte uppfylla kraven.

Övrig marknadskontroll

PTS är även marknadskontrollmyndighet enligt lagen (2023:254) om vissa produkters och tjänsters tillgänglighet. Lagstiftningen, som trädde i kraft 28 juni 2025, syftar till att främja likvärdig tillgänglighet för personer med funktionsnedsättning och etablerar konkreta krav som måste uppfyllas för att säkerställa att digitala produkter och tjänster kan användas på samma villkor för alla, oavsett funktionsförmåga.

Betänkandet *Anpassningar till AI-förordningen* (SOU 2025:101) har föreslagit ett system för marknadskontroll för AI-förordningen som består av flera marknadskontrollmyndigheter och där PTS ska vara marknadskontrollmyndighet med huvudsakligt ansvar för AI-förordningen. Utredningen har även föreslagit att PTS i denna egenskap ska vara samordnande marknadskontrollmyndighet.²⁹

9.6.8 Styrelsen för ackreditering och teknisk kontroll

Swedac är en statlig myndighet med uppdrag att verka för en effektiv och välfungerande kvalitetsinfrastruktur. Myndigheten ansvarar bland annat för ackreditering, reglerad mätteknik, samordning av marknadskontroll och för att utse och anmäla organ för bedömning av överensstämmelse enligt harmoniserad EU-lagstiftning.

²⁹ SOU 2025:101, *Anpassningar till AI-förordningen*, s. 203–305.

Som nationellt ackrediteringsorgan enligt förordning (EG) nr 765/2008³⁰ bedömer Swedac organ som utför bedömningar av överensstämmelse till exempel genom provning, certifiering eller kontroll. Inom området reglerad mätteknik ansvarar myndigheten för regelutveckling samt för tillsyn och marknadskontroll av mätinstrument och ädelmetallarbeten.

Swedac är även centralt samordningskontor enligt EU:s marknadskontrollförordning och leder Marknadskontrollrådet. Myndigheten har därmed en samordnande roll inom svensk marknadskontroll, inklusive uppgifter kopplade till strategi, rapportering och EU-samverkan.

Swedac är därtill anmälade myndighet för organ som ska utföra uppgifter enligt unionslagstiftning om bedömning av överensstämmelse, utom inom områden där annan myndighet har det specifika ansvaret.

Beskrivning av myndighetens verksamhet på cybersäkerhetsområdet

Ackreditering enligt EU:s cybersäkerhetsakt

Inom cybersäkerhetsområdet utgör ackreditering en grundläggande del i det europeiska systemet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt. Ackrediteringen syftar till att bedöma att certifieringsorgan och provningslaboratorier har den tekniska kompetens, opartiskhet och kvalitet som krävs för att utföra sina uppgifter på ett enhetligt och tillförlitligt sätt. Som nationellt ackrediteringsorgan har Swedac i uppgift att bedöma och ackreditera dessa organ och utföra löpande tillsyn av organen i syfte att säkerställa att de upprätthåller sin kompetens på området.

Certifiering enligt EUCC

Den första certifieringsordning som tagits fram enligt EU:s cybersäkerhetsakt är den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC). EUCC syftar till

³⁰ Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93.

att stärka cybersäkerheten inom informations- och kommunikationsteknik genom gemensamma krav och metoder för certifiering av produkter, tjänster och processer. Ordningen bygger på två typer av organ: certifieringsorgan och provningslaboratorier. Certifiering kan ske på två olika assurancesnivåer – ”betydande” och ”hög” – där den högre nivån kräver att det certifierande organet, utöver ackreditering, även har bemyndigande från den nationella myndigheten för cybersäkerhetscertifiering.

Swedac ansvarar för att ackreditera de organ som ansöker om att få verka inom EUCC-systemet i Sverige. Ackreditering sker enligt relevanta internationella standarder, exempelvis ISO/IEC 17065 och ISO/IEC 17025, beroende på organets verksamhet.

Samverkan med FMV

Swedac samverkar med FMV som är den myndighet som är utsedd till nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt. FMV ansvarar bland annat för bemyndigande av organ, anmälan av organ för bedömning av överensstämmelse till kommissionen och Sveriges representation i Europeiska gruppen för cybersäkerhetscertifiering (ECCG).

Övrig ackrediteringsverksamhet med anknytning till cybersäkerhet

Swedac ackrediterar även certifieringsorgan och provningslaboratorier för Common Criteria - ett ramverk för säkerhet i it-produkter – vilket också EUCC bygger på. Swedac ackrediterar också provningslaboratorier inom frivilliga ackrediteringsområden som gränsar till cybersäkerhet, exempelvis inom it- och kommunikationsprovning samt certifieringsorgan inom informationssäkerhet enligt ISO/IEC 27001.

Beskrivning av myndighetens marknadskontrollverksamhet

Swedac är enligt 6 § förordningen (2021:1252) med instruktion för Styrelsen för ackreditering och teknisk kontroll centralt samordningskontor i Sverige som har inrättats enligt artikel 10.3 i EU:s

marknadskontrollförordning. Swedac ska i denna egenskap ta fram förslag till en samordnad ståndpunkt och lämna förslaget till Regeringskansliet, åtminstone vart fjärde år ta fram och lämna ett förslag till en nationell strategi för marknadskontroll till regeringen och årligen följa upp den nationella strategin för marknadskontroll. Det centrala samordningskontoret ska också bistå i samarbetet mellan marknadskontrollmyndigheterna i olika medlemsstater om gränsöverskridande ömsesidig assistans. Ytterligare uppgifter för det centrala samordningskontoret är att delta i unionsnätverket för produktöverensstämmelse (EUPCN) och föra in information om bland annat de nationella marknadskontrollmyndigheterna i informations- och kommunikationssystemet ICSMS.

Enligt 1 § punkten 4 förordningen (2021:1252) med instruktion för Styrelsen för ackreditering och teknisk kontroll ska myndigheten särskilt ansvara för samordning av marknadskontroll och tillsammans med andra myndigheter verka för en effektiv och behovsanpassad marknadskontroll nationellt och inom EU, bland annat genom Marknadskontrollrådet och genom tillämpning av EU:s marknadskontrollförordning samt vara centralt samordningskontor.

Swedac har enligt 1 § punkterna 1 och 2 förordningen (2021:1252) med instruktion för Styrelsen för ackreditering och teknisk kontroll ansvar för marknadskontroll inom områdena reglerad mätteknik och handel med ädelmetallarbeten. Reglerad mätteknik syftar till att kvalitetssäkra mätvärden och omfattar olika typer av mätinstrument såsom elmätare, vågar, vatten- och värmemätare samt bensinpumpar. Inom handel med ädelmetallarbeten utför Swedac marknadskontroll för att säkerställa att ädelmetallarbeten uppfyller krav på bland annat stämplarna och angiven finhalt.

Swedac deltar i EU-arbete, bland annat i Adco-grupperna för reglerad mätteknik. Swedac ingår i marknadskontrollrådet. Myndighetens marknadskontroll inom reglerad mätteknik och handel med ädelmetallarbeten är avgiftsfinansierad.

Swedac har inte något uppdrag kring marknadskontroll med direkta kopplingar till cybersäkerhet.

9.6.9 Post- och telestyrelsen bör ges marknadskontrollansvar för EU:s cyberresiliensförordning

Utredningens förslag: Den myndighet eller de myndigheter som regeringen bestämmer är marknadskontrollmyndighet.

Utredningens bedömning: Post- och telestyrelsen är marknadskontrollmyndighet.

Baserat på de krav som EU:s cyberresiliensförordning ställer på marknadskontrollmyndigheten som utredningen har redovisat i avsnitt 9.5 bedömer utredningen att det krävs både cybersäkerhetskompetens och erfarenhet av marknadskontroll. Utifrån dessa utgångspunkter finns det ett antal myndigheter som är relevanta att överväga som marknadskontrollmyndighet. Som redovisat i avsnitt 9.6.2–9.6.8 finns det några myndigheter som har kompetens på cybersäkerhetsområdet, såsom FMV, MSB och PTS. Några av dessa myndigheter har samtidigt erfarenhet av marknadskontroll, såsom MSB och PTS. Därför skulle FMV, MSB och PTS kunna vara relevanta att utses som marknadskontrollmyndigheter för EU:s cyberresiliensförordning.

Enligt utredningens bedömning är PTS mest lämpad att ha rollen som marknadskontrollmyndighet enligt EU:s cyberresiliensförordning.

PTS har redan i dag bred erfarenhet på cybersäkerhetsområdet inom ramen för NIS-lagstiftningen, eIDAS-lagstiftningen samt LEK och då i relation till säkerheten i allmänna kommunikationsnät och kommunikationstjänster. Genom sitt uppdrag att utöva tillsyn över säkerheten i allmänna elektroniska kommunikationsnät och kommunikationstjänster, eIDAS- och NIS-lagstiftningen har PTS erfarenhet av att bedöma incidentrapporter vilket kan vara en bra erfarenhet i arbetet med tillsyn över genomförandet av tillverkarnas rapporteringsskyldigheter. Genom detta arbete har PTS även teknisk expertis vad gäller nätverkssäkerhet, IoT-säkerhet och sårbarhetsanalys som kan byggas ut för att fördjupa kompetensen inom cybersäkerhet.

Genom sitt deltagande i rådsförhandlingarna av EU:s cyberresiliensförordning under Sveriges ordförandeskap i Europeiska unionens råd 2023 har myndigheten kunskap om lagstiftningen.

PTS deltar vidare redan i dag i den kommitté och den expertgrupp som har inrättats enligt EU:s cyberresiliensförordning.

Det faktum att PTS redan är marknadskontrollmyndighet för flera tekniska produktkategorier och har tillsynsansvar inom informations- och kommunikationssäkerhet gör att myndigheten har erfarenhet och en etablerad arbetsstruktur för tillsyn och marknadskontroll som kan byggas ut till att omfatta cybersäkerhetskrav för produkter med digitala element. PTS har även en lång erfarenhet av marknadskontroll och tillsyn. Från och med augusti 2025 omfattar PTS marknadskontroll inom radioutrustningsområdet även kontroll av cybersäkerhetskrav för internetuppkopplad radioutrustning enligt kommissionens delegerade förordning om cybersäkerhetskrav. Inom sin etablerade marknadskontrollstruktur har PTS erfarenhet av att tillämpa komplexa EU-regelverk, tillgång till och erfarenhet av att använda laboratorier och tekniska resurser för att verifiera att produkter uppfyller lagstadgade krav, erfarenhet av tullsamverkan och användning av informationshanteringssystem såsom ICSMS. I denna struktur arbetar inspektörer och jurister som är vana vid att arbeta i gränsytan mellan teknik och juridik.

Vidare har PTS en lång erfarenhet av samarbete med andra marknadskontrollmyndigheter, både nationellt inom ramen för Marknadskontrollrådet och internationellt genom deltagandet i Adco-grupper och andra samarbetsstrukturer på EU-nivå såsom kommittéer och expertgrupper. Dessutom har myndigheten etablerade kanaler för att informera företag och konsumenter om regler, brister och aktuella trender. Denna samlade erfarenhet innebär att PTS inte behöver bygga upp marknadskontrollverksamheten från grunden utan kan bygga på ett befintligt system.

Genom den roll som marknadskontrollmyndighet med huvudsakligt ansvar för AI-förordningen och samordnande marknadskontrollmyndighet som PTS föreslås få enligt betänkandet *Anpassningar till AI-förordningen* (SOU 2025:101) skulle PTS också ha goda förutsättningar att samordna övriga marknadskontrollmyndigheters marknadskontroll av cybersäkerhetskraven enligt artikel 52.14 i EU:s cyberresiliensförordning.

PTS medverkar redan i dag i de nationella och internationella standardiseringsorgan där cybersäkerhetsstandarder utvecklas. Ett förstärkt deltagande i standardiseringsarbetet som stöd för EU:s cyberresiliensförordning inom ITS och ETSI kommer inte heller innebära

några ytterligare kostnader för medlemskap eftersom dessa standardiseringsorganisationer debiterar för deltagandet i arbetet per organisation och inte per individ.

PTS har till utredningen förmedlat att myndigheten är beredd att vara marknadskontrollmyndighet för EU:s cyberresiliensförordning.

Utredningen har även övervägt om MSB eller FMV skulle kunna vara lämpliga marknadskontrollmyndigheter för EU:s cyberresiliensförordning. Båda myndigheterna har uppdrag vad gäller cybersäkerhet samt tillsyn respektive marknadskontroll som redovisningen i avsnitt 9.6.3 och 9.6.6 visar.

MSB:s huvudsakliga uppgift är att ansvara för frågor om skydd mot olyckor, krisberedskap och civilt försvar. För närvarande pågår ett arbete med att se över MSB:s verksamhet inom cybersäkerhetsområdet. Redan 2024 har regeringen beslutat att flytta ansvaret för det nationella cybersäkerhetscentret (NCSC) till FRA, se 4 a § förordningen (2007:937) med instruktion för Försvarets radioanstalt. Enligt förslagen i betänkandet *Samlande förmågor för utökad cybersäkerhet* (SOU 2025:79) ska andra centrala delar av MSB:s verksamhet på informations- och cybersäkerhetsområdet föras över till FRA. Det rör sig bland annat om MSB:s ansvar för att stödja och samordna arbetet med samhällets informations- och cybersäkerhet samt myndighetens uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter. Den utredningen föreslår även att FRA, i stället för MSB, ska utses till CSIRT-enhet, gemensam kontaktpunkt och cyberkrismyndighet samt få ansvar för tillsynsamordning enligt NIS 2-direktivet. Mot bakgrund av dessa förslag är det troligt att MSB:s i framtiden inte kommer att ha någon större roll som aktör på cybersäkerhetsområde. Utredningen anser därför att det inte är lämpligt att utse MSB som marknadskontrollmyndighet för EU:s cyberresiliensförordning.

Vid sidan om sin huvudverksamhet att upphandla och leverera materiel och tjänster till Försvarsmakten har FMV genom rollen som nationell myndighet för cybersäkerhetscertifiering och tillsynsmyndighet enligt cybersäkerhetsakten en roll i Sveriges cybersäkerhetsinfrastruktur.

FMV har dock framfört att myndigheten inte ser sig i rollen som marknadskontrollmyndighet för EU:s cyberresiliensförordning eftersom detta skulle innebära otydlighet kring i vilken roll myn-

digheten agerar, som tillsynsmyndighet enligt EU:s cybersäkerhetsakt eller marknadskontrollmyndighet enligt EU:s cyberresiliensförordning, i förhållande till marknadsaktörer, tillsynsobjekt och objektansvariga. Utredningens bedömning är därför att inte utse FMV som marknadskontrollmyndighet.

9.7 Förbättra kompetensen i en cyberresilient digital miljö

Utredningens förslag: Regeringen bör ge Post- och telestyrelsen i uppdrag att ta fram förslag som främjar åtgärder och strategier för att utveckla cybersäkerhetskompetens och skapa organisatoriska och tekniska verktyg för att säkerställa tillräcklig tillgång till kvalificerad arbetskraft för att stödja verksamheten vid marknadskontrollmyndigheterna och organen för bedömning av överensstämmelse.

Enligt artikel 10.a i EU:s cyberresiliensförordning ska medlemsstaterna vid tillämpningen av denna förordning och för att tillgodose yrkesutövarnas behov, till stöd för genomförandet av denna förordning, främja åtgärder och strategier som syftar till att utveckla cybersäkerhetskompetensen och skapa organisatoriska och tekniska verktyg för att säkerställa tillräcklig tillgång till kvalificerad arbetskraft för att stödja verksamheten vid marknadskontrollmyndigheterna och organen för bedömning av överensstämmelse. Detta ska ske när så är lämpligt med stöd av kommissionen, Europeiska kompetenscentrumet för cybersäkerhet och Enisa.

Cybersäkerhetskompetens är avgörande både för marknadskontrollmyndigheter och för organ för bedömning av överensstämmelse.

För en marknadskontrollmyndighet som ska kontrollera produkter med digitala element är kompetensen viktig av flera skäl. Myndigheten måste kunna identifiera risker, dvs. förstå sårbarheter, hot och tekniska brister i produkter för att bedöma om de uppfyller de grundläggande cybersäkerhetskraven. För att bedöma efterlevnad måste myndigheten kunna granska tillverkarens dokumentation, testresultat och eventuella certifieringar. Eftersom digitala produkter utvecklas snabbt är det viktigt att myndigheterna håller jämna steg med teknikutvecklingen.

Förslagen bör bidra till att skapa förutsättningar för kontinuerlig kompetensutveckling och kunskapsförsörjning samt förutsättningar för att rekrytera och behålla kvalificerad personal, men också för att etablera rutiner och arbetsmetoder som ger en enhetlig och rättssäker tillämpning av regelverket. Förslagen bör även beakta de samarbetsaspekter som följer av artikel 52.14 i EU:s cyberresiliensförordning. Framför allt för att säkerställa en rättssäker tillämpning av regelverket i de fall där flera myndigheter ansvarar för marknadskontroll av de cybersäkerhetskrav som följer av EU:s cyberresiliensförordning.

Vikten av cybersäkerhetskompetens hos organ för bedömning av överensstämmelse behandlas i avsnitt 6.9. Utifrån denna bedömning och av vad som framkommer i rapporten från Governo AB³¹ bedömer utredningen att det även bör tas fram förslag som främjar åtgärder och strategier som kan bidra till att utveckla och säkra tillgång till personal med kompetens på cybersäkerhetsområdet vid organen för bedömning av överensstämmelse.

Utredningen bedömer att Post- och telestyrelsen (PTS) bör ges uppdrag att ta fram förslag som främjar åtgärder och strategier för att utveckla cybersäkerhetskompetens och skapa organisatoriska och tekniska verktyg för att säkerställa tillräcklig tillgång till kvalificerad arbetskraft för att stödja verksamheten vid marknadskontrollmyndigheterna och organen för bedömning av överensstämmelse.

9.8 Förslag till kompletterande lagstiftning

9.8.1 Upplysningar om marknadskontroll och marknadskontrollmyndigheter

Utredningens förslag: Bestämmelser om marknadskontroll finns i Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011.

Av artikel 52.14 i EU:s cyberresiliensförordning framgår att för produkter med digitala element som omfattas av EU:s cyberresiliensförordning och som klassificeras som AI-system med

³¹ Governo AB:s rapport finns som bilaga 3 i betänkandet.

hög risk enligt artikel 6 i Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) ska de marknadskontrollmyndigheter som utsetts enligt förordning (EU) 2024/1689 vara de myndigheter som ansvarar för den marknadskontroll som föreskrivs i EU:s cyberresiliensförordning.

Utredningens bedömning: I [föreslagna] förordningen (2025:000) med kompletterande bestämmelser till EU:s förordning om artificiell intelligens finns bestämmelser om vilka myndigheter som är marknadskontrollmyndigheter enligt Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

Enligt artikel 52.1 i EU:s cyberresiliensförordning ska förordning (EU) 2019/1020 tillämpas på produkter med digitala element som omfattas av denna förordning. En upplysning om detta bör införas i lagen med kompletterande bestämmelser till EU:s cyberresiliensförordning.

Av artikel 52.14 i EU:s cyberresiliensförordning framgår att för produkter med digitala element som omfattas av EU:s cyberresiliensförordning och som klassificeras som AI-system med hög risk enligt artikel 6 i AI-förordningen ska de marknadskontrollmyndigheter som utsetts enligt AI-förordningen vara de myndigheter som ansvarar för den marknadskontroll som föreskrivs i EU:s cyberresiliensförordning. En upplysningsparagraf om detta bör införas i lagen med kompletterande bestämmelser till EU:s cyberresiliensförordning.

Med anledning av regleringen av marknadskontrollansvar för cyberresilienskrav för produkter med digitala element som klassificeras som AI-system med hög risk i artikel 52.14 i EU:s cyberresi-

liensförordning bör det även införas en upplysningsparagraf om i vilken svensk författning dessa marknadskontrollmyndigheter utses. Denna upplysningsparagraf bör införas i förordningen med kompletterande bestämmelser till EU:s cyberresiliensförordning.

9.8.2 Marknadskontrollmyndighetens befogenheter

Utredningens förslag: Vid marknadskontroll enligt förordning (EU) 2019/1020 har en marknadskontrollmyndighet befogenhet att enligt

1. artikel 14.4 a–14.4 c kräva att ekonomiska aktörer eller förvaltare av programvara med fri och öppen källkod ska tillhandahålla handlingar, specifikationer, data eller uppgifter,
2. artikel 14.4 d utföra oanmälda inspektioner på plats och fysiska kontroller av produkter,
3. artikel 14.4 e få tillträde till lokaler, mark eller transportmedel,
4. artikel 14.4 f inleda undersökningar på eget initiativ,
5. artikel 14.4 g kräva att ekonomiska aktörer eller förvaltare av programvara med fri och öppen källkod ska vidta lämpliga åtgärder för att få en bristande överensstämmelse att upphöra eller att eliminera en risk,
6. artikel 14.4 h själv vidta åtgärder,
7. artikel 14.4 j införskaffa, inspektera och demontera varuprover, och
8. artikel 14.4 k kräva att innehåll på ett onlinegränssnitt ska avlägsnas, att en varning ska visas eller att åtkomsten ska begränsas.

Befogenheten enligt första stycket 8 gäller inte i fråga om databaser som omfattas av tryckfrihetsförordningens eller yttrandefrihetsgrundlagens skydd.

När ändrade förhållanden ger anledning till det, ska en marknadskontrollmyndighet besluta att åtgärder enligt första stycket 8 inte längre behöver gälla.

En marknadskontrollmyndighet får införskaffa ett varuprov under dold identitet enligt artikel 14.4 j i förordning (EU) 2019/1020 endast om det är nödvändigt för att syftet med kontrollen ska uppnås. Myndigheten ska underrätta den ekonomiska aktören eller förvaltaren av programvara med fri och öppen källkod om att införskaffandet har skett under dold identitet, så snart det går utan att syftet med åtgärden går förlorat.

Enligt EU:s marknadskontrollförordning ska medlemsstaterna tilldela marknadskontrollmyndigheterna befogenheter att

1. kräva att ekonomiska aktörer ska tillhandahålla handlingar, specifikationer, data eller uppgifter (artikel 14.4 a–14.4 c),
2. utföra oanmälda inspektioner på plats och fysiska kontroller av produkter (artikel 14.4 d),
3. få tillträde till lokaler, mark eller transportmedel (artikel 14.4 e),
4. inleda undersökningar på eget initiativ (artikel 14.4 f),
5. kräva att ekonomiska aktörer ska vidta lämpliga åtgärder för att få en bristande överensstämmelse att upphöra eller att eliminera en risk (artikel 14.4 g),
6. själv vidta åtgärder (artikel 14.4 h),
7. införskaffa, inspektera och demontera varuprover (artikel 14.4 j), och
8. kräva att innehåll på ett onlinegränssnitt ska avlägsnas, att en varning ska visas eller att åtkomsten ska begränsas (artikel 14.4 k).

Befogenheterna avseende onlinegränssnitt är begränsade i fråga om databaser som omfattas av tryckfrihetsförordningens eller yttrandefrihetsgrundlagens skydd. När ändrade förhållanden ger anledning till det ska marknadskontrollmyndigheten också besluta att åtgärderna inte längre behöver vidtas. Befogenheterna inkluderar även att under vissa omständigheter få inhandla varuprover under dold identitet.

Det finns ingen sektorsövergripande lag som ger marknadskontrollmyndigheterna dessa befogenheter. Befogenheterna förs i stället in i varje separat sektorslagstiftning som införlivar eller kom-

pletterar harmoniserade EU-rättsakter. De myndigheter som blir ansvariga för marknadskontroll enligt EU:s cyberresiliensförordning behöver därför tilldelas de befogenheter som krävs enligt EU:s marknadskontrollförordning.

När EU:s marknadskontrollförordning antogs infördes kompletterande bestämmelser till denna förordning i svensk sektorslagstiftning som genomför eller kompletterar de rättsakter som förtecknas i bilaga I till EU:s marknadskontrollförordning. De överväganden som gjordes i samband med detta är relevanta även nu.³²

Eftersom EU:s cyberresiliensförordning i artikel 24 reglerar skyldigheter för förvaltare av programvara med fri och öppen källkod behöver marknadskontrollmyndigheten tilldelas dessa befogenheter även i relation till förvaltare av programvara med fri och öppen källkod.

9.8.3 Beslut om förelägganden

Utredningens förslag: En marknadskontrollmyndighet får besluta de förelägganden som behövs i ett enskilt fall för att EU:s cyberresiliensförordning, denna lag, anslutande föreskrifter och förordning (EU) 2019/1020 ska följas.

Ett beslut om föreläggande enligt första stycket eller 6 § får förenas med vite.

En marknadskontrollmyndighet får när den fattar beslut enligt 6 eller 8 § bestämma att beslutet ska gälla omedelbart.

För att marknadskontrollmyndigheten ska kunna utföra sina arbetsuppgifter på ett effektivt sätt bör de i enskilda fall kunna meddela de förelägganden som behövs för att EU:s cyberresiliensförordning ska följas. För att åtgärder som vidtas inom ramen för marknadskontrollen ska kunna tillämpas i praktiken och få genomslag bör myndighetens förelägganden få förenas med vite.

Om marknadskontrollmyndigheten har konstaterat att det finns förutsättningar för ett föreläggande finns det ibland behov av att beslutet genast blir gällande. I dessa situationer kan det vara angeläget att beslutet inte fördröjs genom att det överklagas.

³² Prop. 2021/22:238, *Anpassningar till EU:s marknadskontrollförordning – del 2*, s. 132–160.

Frågan om när ett beslut får verkställas regleras i 35 § förvaltningslagen (2017:900). Ett beslut får enligt 35 § andra stycket förvaltningslagen alltid verkställas omedelbart, om beslutet gäller anställning av någon, om det gäller endast tillfälligt eller kretsen av dem som har rätt att överklaga är så vid eller obestämd att det inte går att avgöra när överklagandetiden går ut. En myndighet får enligt 35 § tredje stycket även verkställa ett beslut omedelbart om ett väsentligt allmänt eller enskilt intresse kräver det.

I samband med att kompletterande bestämmelser till EU:s marknadskontrollförordning antogs bedömde regeringen att det fanns ett behov av att en marknadskontrollmyndighet ska kunna bestämma att ett föreläggande om att förordningen ska följas ska gälla omedelbart, särskilt om produkten kan medföra risk för skada.³³ Regeringen anförde även att motsvarande bestämmelser redan finns inom en rad sektorslagstiftningar och att det är ändamålsenligt att marknadskontrollmyndigheterna har enhetliga befogenheter i detta avseende. En sådan möjlighet till omedelbar verkställighet kan inte garanteras genom en tillämpning av förvaltningslagens allmänna bestämmelser. Regeringen bedömde därför att regleringen bör finnas i sektorslagarna och utnyttjas i de fall när det är särskilt angeläget att verkställa beslutet. Samma skäl gör sig även gällande för marknadskontroll av produkter med digitala element och en bestämmelse om omedelbar verkställighet bör därför införas.

9.8.4 Hjälپ från Polismyndigheten

Utredningens förslag: Polismyndigheten ska på begäran av marknadskontrollmyndigheten lämna den hjälp som behövs när myndigheten vidtar åtgärder enligt 6 §.

Hjälپ enligt första stycket får begäras endast om

1. det på grund av särskilda omständigheter kan befaras att åtgärden inte kan utföras utan att en polismans särskilda befogenheter enligt 10 § polislagen (1984:387) behöver tillgripas, eller
2. det annars finns synnerliga skäl.

³³ Prop. 2021/22:238, *Anpassningar till EU:s marknadskontrollförordning – del 2*, s. 170–171.

Vid utövandet av befogenheterna enligt artikel 14.4 i EU:s marknadskontrollförordning kan marknadskontrollmyndigheterna i vissa situationer behöva hjälp av Polismyndigheten. Det kan till exempel handla om att en ekonomisk aktör motsätter sig att en marknadskontrollmyndighet får tillträde till aktörens lokaler för att kontrollera att produkterna uppfyller gällande krav. I samband med detta kan myndigheterna behöva hjälp och få skydd för sin personal. Som ett komplement till dessa befogenheter bör marknadskontrollmyndigheterna kunna få hjälp av Polismyndigheten när de vidtar åtgärder. Möjligheten till hjälp bör begränsas till de situationer då det finns ett verkligt behov av myndighetens särskilda befogenheter att använda våld. Det får anses vara fallet om det på grund av särskilda omständigheter kan befaras att åtgärden inte kan utföras utan att en polismans särskilda befogenheter behöver tillgripas eller om det finns synnerliga skäl, se 10 § polislagen (1984:387).

9.8.5 Bestämmelser om vissa avgifter för marknadskontroll

Utredningens förslag: Av lagen (2014:140) med bemyndigande att meddela vissa föreskrifter om marknadskontroll av varor och annan närliggande tillsyn framgår att föreskrifter för avgifter för kontroll enligt förordning (EU) 2019/1020 får meddelas.

Utredningens bedömning: En marknadskontrollmyndighet får meddela föreskrifter om avgifter för marknadskontroll enligt Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011.

Det finns inga bestämmelser om hur marknadskontrollen ska finansieras i EU:s cyberresiliensförordning. Av artikel 15 i EU:s marknadskontrollförordning följer att medlemsstaterna får ge sina marknadskontrollmyndigheter rätt att från den relevanta ekonomiska aktören återkräva alla kostnader för sin verksamhet avseende fall av bristande överensstämmelse. Bestämmelsen möjliggör för medlemsstaterna att ta ut avgifter för det fall en aktör inte följer regelverket men hindrar inte att någon annan ordning tillämpas. Det står såle-

des medlemsstaten fritt att såväl låta kontrollen vara statligt finansierad som att även i andra situationer än vid bristande överensstämmelse återkräva kostnader.

För att anpassa svensk rätt till artikel 15 i EU:s marknadskontrollförordning har det införts ett generellt bemyndigande i lagen (2014:140) med bemyndigande att meddela vissa föreskrifter om marknadskontroll av varor och annan närliggande tillsyn som ger regeringen eller den myndighet som regeringen bestämmer möjlighet att meddela föreskrifter om avgifter för marknadskontroll enligt EU:s marknadskontrollförordning.³⁴ Bemyndigandet gäller även för marknadskontroll av produkter med digitala element. Det bör dock av tydlighetsskäl införas en upplysningsbestämmelse i den nya lagen att det av lagen (2014:140) med bemyndigande att meddela vissa föreskrifter om marknadskontroll av varor och annan närliggande tillsyn framgår att föreskrifter om avgifter för kontroll enligt EU:s marknadskontrollförordning får meddelas.

I förordningen med kompletterande bestämmelser till EU:s cyberresiliensförordning ska införas ett bemyndigande att ta ut avgifter för PTS samt de myndigheter som enligt artikel 52.14 i EU:s cyberresiliensförordning är ansvariga marknadskontrollmyndigheter för kontroll av cybersäkerhetskraven av produkter med digitala element som klassas som AI-system med hög risk enligt AI-förordningen.

9.8.6 Överklagande

Frågan om överklagande av en förvaltningsmyndighets, bland annat en marknadskontrollmyndighets, beslut behandlas i avsnitt 6.14.

³⁴ En närmare redogörelse för rätten att ta ut avgifter finns i prop. 2021/22:238, *Anpassningar till EU:s marknadskontrollförordning – del 2*, s. 179–183.

10 Sanktioner

10.1 Inledning

I artikel 64 i förordning (EU) 2024/2847¹ (EU:s cyberresiliensförordning) anges att medlemsstaterna ska fastställa regler om sanktioner för överträdelser av bestämmelserna i förordningen och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande.

I detta kapitel behandlas frågan om behov av kompletterande nationella bestämmelser i anslutning till artikel 64 i förordningen.

I avsnitt 10.2 behandlas bland annat frågan om krav på strikt ansvar eller uppsåt och vårdslöshet vid överträdelse av förordningen. I avsnitt 10.3 behandlas vissa allmänna bestämmelser avseende sanktioner och vilka myndigheter som ska besluta om sanktionsavgift. I avsnitt 10.4 behandlas frågor om förfaranderegler och preskription.

10.2 Bestämmelser om sanktionsavgifter

Utredningens bedömning: Bestämmelser om sanktionsavgifter finns i artikel 64 i EU:s cyberresiliensförordning som är en unionsrättslig författning som är direkt tillämplig i medlemsstaterna.

Det finns dock behov av kompletterande nationell författningsreglering om sanktionsavgifter för myndigheter, betalning, verkställighet och preskription.

¹ Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen).

Enligt 8 kap. 2 § första stycket 2 regeringsformen ska föreskrifter meddelas genom lag om de avser förhållandet mellan enskilda och det allmänna. Detta gäller under förutsättning att föreskrifterna gäller skyldigheter för enskilda eller i övrigt avser ingrepp i enskildas personliga eller ekonomiska förhållanden. Mot denna bakgrund ska bestämmelser om sanktionsavgift finnas i lag.

I artikel 64.2 i EU:s cyberresiliensförordning föreskrivs att bristande efterlevnad av de väsentliga cybersäkerhetskrav som anges i bilaga I och de skyldigheter som fastställs i artiklarna 13 och 14 ska medföra administrativa sanktionsavgifter på upp till 15 000 000 EUR eller, om överträdelsen begås av ett företag, upp till två och en halv (2,5) procent av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

I artikel 64.3 föreskrivs att bristande efterlevnad av de skyldigheter som anges i artiklarna 18–23, 28, 30.1–30.4, 31.1–31.4, 32.1, 32.2 och 32.3, 33.5,² 39, 41, 47, 49 och 53 ska bli föremål för administrativa sanktionsavgifter på upp till 10 000 000 EUR eller, om överträdelsen begås av ett företag, upp till två (2) procent av dess totala globala årsomsättning för det föregående räkenskapsåret, beroende på vilket som är högst.

I artikel 64.4 föreskrivs att tillhandahållande av oriktig, ofullständig eller vilseledande information till anmälda organ och marknadskontrollmyndigheter som svar på en begäran ska medföra administrativa sanktionsavgifter på upp till 5 000 000 EUR eller, om överträdelsen begås av ett företag, upp till en (1) procent av dess totala globala årsomsättning för det föregående räkenskapsåret, beroende på vilket som är högst.

Bestämmelser om sanktionsavgifter finns i artikel 64.2–4 i EU:s cyberresiliensförordning som är en unionsrättslig förordning som är direkt tillämplig i medlemsstaterna och därför har formen av lag.

Det finns dock behov av kompletterande nationell författningsreglering när det gäller att en sanktionsavgift inte ska beslutas i ringa eller ursäktligt fall eller då förmildrande omständigheter annars föreligger samt att en sanktionsavgift kan påföras en myndighet vid överträdelser av nu angivna bestämmelser.

² Fel i översättningen.

10.2.1 Det ska vara obligatoriskt att ta ut sanktionsavgift

Av artikel 64.2–4 i EU:s cyberresiliensförordning följer att en objektivt konstaterad bristande efterlevnad av angivna bestämmelser ska medföra en sanktionsavgift.

I detta sammanhang inställer sig frågan om det vara obligatoriskt att ta ut sanktionsavgift vid en objektivt sett konstaterad överträdelse. En motsvarande frågeställning behandlades i propositionen *Kompletterande bestämmelser till EU:s cybersäkerhetsakt* (prop. 2020/21:186, s. 36) varvid följande anges:

Det ska vara obligatoriskt att ta ut sanktionsavgift

En fråga är om det bör vara obligatoriskt att ta ut sanktionsavgift när en viss bestämmelse har överträtts. Sanktionsavgifter bör, som anförs ovan, tas ut endast till följd av lätt konstaterbara överträdelser för vilka utredningsinslaget är begränsat. Ansvar är således vanligtvis strikt i dessa fall, men andra varianter förekommer. Som regeringen anför i propositionen *Informationssäkerhet för samhällsviktiga och digitala tjänster* bör tillsynsmyndighetens möjligheter till mer skönsmässiga bedömningar som utgångspunkt vara begränsade med hänsyn till behovet av likabehandling, objektivitet och proportionalitet (prop. 2017/18:205 s. 69 och 70). Regelverket om cybersäkerhetscertifiering kan dock vara komplext, och innebära en resurskrävande hantering för tillsynsmyndigheten. Regeringen anser i likhet med utredningen att övervägande skäl talar för att det på det nu aktuella området bör vara obligatoriskt att besluta om sanktionsavgift när förutsättningarna för detta är uppfyllda. Detta minskar utrymmet för skönsmässiga bedömningar av den nationella myndigheten för cybersäkerhetscertifiering och framstår även som mest ändamålsenligt vid mer allvarliga överträdelser av regelverket.

Regleringen i artikel 64.2–4 innebär enligt sin ordalydelse att en sanktionsavgift ska påföras vid bristande efterlevnad av angivna skyldigheter. Det sagda leder till slutsatsen att sanktionsavgift ska beslutas vid en objektivt sett konstaterad överträdelse. Det ska därför vara obligatoriskt att ta ut sanktionsavgift i de fall förutsättningarna för detta är uppfyllda. Bestämmelserna om sanktionsavgift bör formuleras på så sätt att sanktionsavgift ska tas ut om förutsättningarna för det är uppfyllda.

10.2.2 Frågan om strikt ansvar eller uppsåt och vårdslöshet

Utredningens bedömning: Regleringen i artikel 64.2–4 i EU:s cyberresiliensförordning innebär enligt sin ordalydelse att en obligatorisk sanktionsavgift ska påföras vid bristande efterlevnad av angivna skyldigheter.

Det finns inte någon reglering i EU:s cyberresiliensförordning som föreskriver att det ska föreligga uppsåt eller vårdslöshet från en ekonomisk aktör vid en överträdelse av regelverket för att en sanktionsavgift ska kunna påföras. Förordningen ger inte heller medlemsstaterna befogenhet att i detta avseende komplettera förordningens bestämmelser med nationell reglering. Det får därför anses föreligga strikt ansvar för en ekonomisk aktör vid en objektivt konstaterad överträdelse enligt artikel 64.2–4, samtidigt som vad som anges i artikel 64.5 ska beaktas vid bestämmande av sanktionsavgiftens storlek.

Som ovan anges följer av artikel 64.2–4 i EU:s cyberresiliensförordning att en *objektivt* konstaterad bristande efterlevnad av angivna bestämmelser *ska* medföra att en sanktionsavgift till högst det föreskrivna beloppet beslutas, eller och om överträdelsen begås av ett företag, bestämmas till högst det föreskrivna beloppet av dess årliga omsättning. I EU:s cyberresiliensförordning finns dock inga bestämmelser som närmare uttrycker eller reglerar att *strikt ansvar* ska anses gälla för den ekonomiska aktören vid en konstaterad överträdelse av de skyldigheter som anges i artikel 64.2–4 eller om det krävs att uppsåt eller vårdslöshet hos aktören föreligger för att denne ska kunna påföras en sanktionsavgift.

Utredningen bedömer att även om ordalydelsen i bestämmelserna om sanktionsavgift kan medge slutsatsen att en sådan avgift alltid ska påföras när en överträdelse av angivna skyldigheter föreligger bör frågan om strikt ansvar eller krav på uppsåt eller vårdslöshet övervägas i detta sammanhang.

Påförande av sanktioner för överträdelser av det europeiska ramverket för cybersäkerhetscertifiering regleras i artikel 58.8 f och artikel 65 EU:s cybersäkerhetsakt³. Av den första artikeln följer att en nationell myndighet för cybersäkerhetscertifiering ska ha befogen-

³ Förordning (EU) 2019/881.

het att utdöma sanktioner i enlighet med nationell rätt, enligt artikel 65, och kräva att överträdelser av skyldigheterna i förordningen omedelbart upphör. I artikel 65 anges att medlemsstaterna bland annat ska fastställa regler om sanktioner vid överträdelser av europeiska ordningar för cybersäkerhetscertifiering och vidta alla nödvändiga åtgärder för att se till att de tillämpas. Vidare anges att sanktionerna ska vara effektiva, proportionella och avskräckande.

Frågan om det ska föreligga strikt ansvar eller om det bör krävas uppsåt eller vårdslöshet för en sanktionsavgift vid överträdelse av bestämmelser enligt det europeiska ramverket för cybersäkerhetscertifiering behandlades i betänkandet *EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering* (SOU 2020:58). I betänkandet (s. 217) anges bland annat:

Huvudregeln vid användande av sanktionsavgift är att avgiftsskyldigheten ska bygga på strikt ansvar. Det behöver då inte bevisas att handlandet varit avsiktligt eller oaktsamt, vilket medför att system med sanktionsavgifter anses vara effektiva (se t.ex. prop. 2017/18:232 s. 324). För att inte den fördelen ska gå förlorad bör berörd aktör ha ett strikt ansvar för sådana överträdelser som kan föranleda att sanktionsavgift tas ut. Det är också svårt att se att överträdelser i normalfallet kan bero på annat än uppsåt eller oaktsamhet (jfr regeringens riktlinjer för att använda sanktionsavgift, prop. 1981/82:142 s. 24 och 25). Utredningen anser att det inte finns skäl att avvika från denna grundprincip när det gäller överträdelser av det europeiska ramverket för cybersäkerhetscertifiering. Den ordning som föreslås bygger således på strikt ansvar, utan krav på uppsåt eller oaktsamhet. Det är tillräckligt för att kunna ta ut en sanktionsavgift att en överträdelse har ägt rum.

I den efterföljande propositionen *Kompletterande bestämmelser till EU:s cybersäkerhetsakt* (prop. 2020/21:186, s. 36 och 37) anges bland annat följande:

System med sanktionsavgifter bygger typiskt sett på principen om strikt ansvar. Strikt ansvar innebär att varken uppsåt eller oaktsamhet är ett krav för att ta ut sanktionsavgift. Det räcker att en bestämmelse har överträtts. Regeringen håller med utredningen om att det inte finns skäl att avvika från grundprincipen för sanktionsavgifter att ansvaret ska vara strikt. Det är framför allt den omständigheten att det inte behöver bevisas att ett visst handlande har varit avsiktligt eller avgöras hur oaktsamt handlandet varit som gör en sådan ordning effektiv. Det är också svårt att se att överträdelser i normalfallet kan bero på annat än uppsåt eller oaktsamhet.

Regeringen anser alltså, i likhet med utredningen, men till skillnad från *Sveriges advokatsamfund*, att en ordning ska införas som innebär att

överträdelser av det europeiska ramverket för cybersäkerhetscertifiering bygger på strikt ansvar.

Av intresse i detta fall är även vad utredningen om genomförande av NIS2- och CER-direktiven uttalade rörande motsvarande frågeställning i sitt delbetänkande *Nya regler om cybersäkerhet* (SOU 2024:18). Utredningen anförde bland annat:

Den nuvarande regleringen i NIS-lagen (29 §) innebär att det är tillsynsmyndigheten som fattar beslut om sanktionsavgift och att tillsynsmyndigheten ska fatta sådant beslut till följd av att en verksamhetsutövare inte följt lagens eller anslutande författningsbestämmelser. Ordningen bygger på ett system med strikt ansvar, dvs. att sanktionsavgift ska tas ut oavsett om överträdelsen skett av oaktsamhet eller uppsåt. Utredningen noterar i detta sammanhang att sådant strikt ansvar nyligen underkänts av EU-domstolen i fråga om GDPR-överträdelser.⁴ Utredningen bedömer dock att medlemsstaternas handlingsutrymme är större i fråga om direktiv än förordningar, med följderna att ett system med strikt ansvar i fråga om sanktionsavgifter kan föreslås avseende NIS2-direktivets genomförande i svensk rätt. Vidare anser utredningen att det, precis som i fråga om överträdelser av nuvarande NIS-lagen, finns en stark presumption för att överträdelser av NIS2-direktivet sker av oaktsamhet eller uppsåtligt. Det föreslagna systemet bör därför bygga på strikt ansvar. En sådan systematik kräver dock ventiler för att kunna fånga upp överträdelser som skett utan vållande. Utredningen föreslår därför att tillsynsmyndigheten i varje enskilt fall ska avgöra om sanktionsavgift ska tas ut.

I regeringens proposition (2025/26:28) *Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag* föreslås tillsynsmyndigheten få besluta att ta ut en sanktionsavgift av en verksamhetsutövare om verksamhetsutövaren åsidosatt sina skyldigheter att utse företrädare, göra en anmälan, vidta säkerhetsåtgärder, låta de personer som ingår i ledningen genomgå utbildning, rapportera betydande incidenter eller informera vid betydande incidenter och betydande cyberhot. I propositionen framhålls (s. 168) att påföljdssystemet bör bygga på ett strikt ansvar. Detta innebär att avgiften ska kunna tas ut oberoende av om överträdelsen har varit uppsåtlig eller berott på oaktsamhet eller inte. Strikt ansvar innebär emellertid inte att sanktionsavgift ska tas ut vid varje överträdelse. Det bör ankomma på tillsynsmyndigheten att bedöma om en överträdelse ska leda till en sanktionsavgift i det enskilda fallet.

⁴ Se EU-domstolens domar av den 5 december 2023 i mål nr C-683/21 (ECLI:EU:C:2023:949) och C-807/21 (ECLI:EU:C:2023:950).

I betänkandet *Marknadskontrollmyndigheter – befogenheter och sanktionsmöjligheter* (SOU 2017:69) uttalade 2016 års marknads-kontrollutredning (s. 194 f) bland annat följande:

När det gäller möjligheten att påföra en ekonomisk aktör sanktionsavgifter vid överträdelse av produktregler skiljer sig denna möjlighet något åt myndigheterna emellan samt även mellan olika produktslag som kontrolleras av samma myndighet. Enligt produktsäkerhetslagen finns en sådan möjlighet i fråga om konsumentprodukter om näringsidkaren uppsåtligen eller av oaktsamhet har brutit mot vissa av lagens bestämmelser. Regler om sanktionsavgifter finns också i viss sektorslagstiftning, t.ex. i lagen om leksakers säkerhet, plan- och bygglagen, radioutrustningslagen och miljöbalken (miljösanktionsavgift). Bestämmelserna om sanktionsavgifter skiljer sig också något åt sinsemellan; i några regelverk krävs att den ekonomiska aktören uppsåtligen eller av oaktsamhet gjort sig skyldig till överträdelse av vissa bestämmelser medan det i andra rättsakter anges att sanktionsavgifter i normalfallet ska påföras aktören oavsett om det kan konstateras oaktsamhet eller uppsåt hos denne, dvs. avgiftsskyldigheten baseras då på s.k. strikt ansvar. I de sistnämnda fallen kan den enskilda myndigheten själv besluta om att om avgiftsskyldighet, medan det i fråga om de regelverk som kräver en bedömning om oaktsamhet eller uppsåt förelegat krävs att myndigheten hos förvaltningsdomstol ansöker om utdömande av avgiften.

Utredningen anförde (s. 255 f) vidare:

Frågan om sanktionsavgifters användningsområde och utformning behandlades av regeringen under förarbetena till bestämmelsen om förverkande i 36 kap. 4 § brottsbalken. Regeringen uttalade att sanktionsavgifter bör användas inom områden där regelöverträdelser är särskilt frekventa eller där det finns speciella svårigheter med att beräkna storleken av den vinst eller besparing som uppnås i det enskilda fallet. Avgifter bör enligt regeringen vidare endast förekomma inom speciella och klart avgränsade rättsområden där det relativt lätt kan fastställas om en överträdelse skett eller inte. Vidare bör sanktionsavgifter kunna beräknas utifrån parametrar som gör det möjligt att i förväg förutse och fastställa avgiftens storlek. Om avgiftsskyldigheten ska bygga på ett strikt ansvar bör det finnas starkt stöd för en presumtion om att överträdelser inte kan förekomma annat än som en följd av uppsåt eller oaktsamhet.⁵ De riktlinjer som uppställdes i propositionen har regeringen även i senare lagstiftningsärenden hänvisat till.⁶

I den mån det saknas möjligheter att komma till rätta med överträdelser på frivillig väg används vanligen förelägganden och förbud, ofta i

⁵ Prop. 1981/82:142, om ändring i brottsbalken (ekonomiska sanktioner vid brott i näringsverksamhet), s. 21 ff.

⁶ Se t.ex. skr. 2009/10:79 s. 45 f. och proposition 2007/08:107, *Administrativa sanktioner på yrkesfiskets område*, s. 14.

förening med vite. Det är dock viktigt att myndigheterna har möjlighet att ingripa mot redan begångna regelöverträdelser. En effektiv marknadskontroll kan inte säkerställas enbart genom en möjlighet att meddela förelägganden eller förbud, eftersom sådana åtgärder endast gäller framåt i tiden. En möjlighet att ingripa med kraft vid redan begångna överträdelser är således avgörande för att säkerställa en effektiv marknadskontroll. Sanktionsavgifter kan påföras såväl fysiska som juridiska personer, och kan komma att uppgå till betydligt högre belopp än ett bötesstraff. I allvarliga fall kan mycket höga sanktionsavgifter påföras. Detta kan antas ha en preventiv och avskräckande verkan. Mot denna bakgrund kan det konstateras att det finns ett behov för marknadskontrollmyndigheterna att kunna använda sig av sanktionsavgifter.

Utredningen kan notera att det inte finns någon reglering i EU:s cyberresiliensförordning som föreskriver att det ska föreligga uppsåt eller vårdslöshet från en ekonomisk aktör vid en överträdelse av regelverket för att frågan om en sanktionsavgift ska aktualiseras. Förordningen ger inte heller medlemsstaterna befogenhet eller utrymme att i detta avseende komplettera förordningens bestämmelser med nationell reglering. Det får därför anses föreligga strikt ansvar för en ekonomisk aktör vid en objektivt konstaterad överträdelse enligt artikel 64.2–4, samtidigt som vad som anges i artikel 64.5 ska beaktas vid bestämmande av sanktionsavgiftens storlek. Som anges nedan ska en sanktionsavgift dock inte tas ut för ringa fall eller ursäktlig eller om det annars med hänsyn till omständigheterna vore oskäligt att besluta om sanktion.

10.3 Gemensamma bestämmelser för sanktionsavgift

I detta avsnitt behandlas de bestämmelser i artikel 64 i EU:s cyberresiliensförordning som är gemensamma när det gäller bedömning av en överträdelse och beslut om sanktion med stöd av artikel 64.2–4.

10.3.1 Omständigheter som ska beaktas vid bedömning av sanktionsavgift

Utredningens bedömning: Av artikel 64.5 i EU:s cyberresiliensförordning framgår vilka omständigheter som ska beaktas vid fastställande av sanktionsavgift. Bestämmelsen kräver ingen kompletterande författning i denna del, utom såvitt att en sanktionsavgift behöver inte tas ut när överträdelsen bedöms som ringa eller ursäktlig, eller om det annars med hänsyn till omständigheterna vore oskäligt att besluta om en sanktion.

Utredningens förslag: Den anmälade myndigheten och en marknadskontrollmyndighet får avstå från att ta ut en sanktionsavgift när överträdelsen bedöms som ringa eller ursäktlig, eller om det annars med hänsyn till omständigheterna vore oskäligt att besluta om en sanktion.

Av artikel 64.5 i EU:s cyberresiliensförordning framgår att vid beslut om storleken på den administrativa sanktionsavgiften i varje enskilt fall ska alla relevanta omständigheter i den specifika situationen beaktas och vederbörlig hänsyn ska tas till

- a) överträdelsens art, allvarlighetsgrad och varaktighet samt dess konsekvenser,
- b) huruvida administrativa sanktionsavgifter redan har påförts av samma eller andra marknadskontrollmyndigheter på samma ekonomiska aktör för en liknande överträdelse,
- c) storleken på, särskilt när det gäller mikroföretag, små och medelstora företag, inbegripet uppstartsföretag, och marknadsandelen för den ekonomiska aktör som begått överträdelsen.

I skäl 120 och 121 till cyberresiliensförordningen anges när det gäller bedömningen av en överträdelse och påförande av en sanktionsavgift bland annat följande:

(120) För att säkerställa en effektiv efterlevnadskontroll av de skyldigheter som fastställs i denna förordning bör varje marknadskontrollmyndighet ha befogenhet att påföra eller begära påförande av administrativa sanktionsavgifter.

Det bör därför fastställas maxnivåer för administrativa sanktionsavgifter som kommer att föreskrivas i nationell rätt med avseende på bristande uppfyllande av de skyldigheter som fastställs i denna förordning.

När det administrativa sanktionsbeloppet fastställs i varje enskilt fall bör alla relevanta omständigheter i den specifika situationen beaktas och som ett minimum de som uttryckligen fastställs i denna förordning, inbegripet huruvida tillverkaren är ett mikroföretag eller ett småföretag eller medelstort företag, inbegripet ett uppstartsföretag, och huruvida samma eller andra marknadskontrollmyndigheter redan har påfört samma ekonomiska aktör administrativa sanktionsavgifter för en liknande överträdelse.

Sådana omständigheter skulle kunna vara antingen försvårande, i situationer där samma ekonomiska aktörs överträdelse fortsätter på territoriet för andra medlemsstater än den där den administrativa sanktionsavgiften redan har påförts, eller förmildrande, genom att säkerställa att eventuella administrativa sanktionsavgifter som övervägs av en annan marknadskontrollmyndighet för samma ekonomiska aktör eller samma typ av överträdelse redan bör beakta sanktioner som påförts i andra medlemsstater och storleken på dessa, tillsammans med andra relevanta särskilda omständigheter. I samtliga fall bör den kumulativa administrativa sanktionsavgift som marknadskontrollmyndigheter i flera medlemsstater kan påföra samma ekonomiska aktör för samma typ av överträdelse fastställas med iakttagande av proportionalitetsprincipen. Med tanke på att administrativa sanktionsavgifter inte tillämpas på mikroföretag eller små företag för en underlåtenhet att iaktta tidsfristen på 24 timmar avseende en tidig varning om aktivt utnyttjade sårbarheter eller allvarliga incidenter som påverkar säkerheten för produkten med digitala element, och inte heller på förvaltare av programvara med fri och öppen källkod för någon överträdelse av denna förordning, och med förbehåll för principen om att sanktioner bör vara effektiva, proportionella och avskräckande, bör medlemsstaterna inte lägga dessa enheter andra typer av sanktioner av ekonomisk karaktär.

(121) Om administrativa sanktionsavgifter påförs en person som inte är ett företag, bör den behöriga myndigheten ta hänsyn till den allmänna inkomstnivån i medlemsstaten och personens ekonomiska situation, när den överväger lämplig sanktionsavgift. Det bör vara upp till medlemsstaterna att fastställa om och i vilken utsträckning myndigheter ska omfattas av administrativa sanktionsavgifter.

Av artikel 64.5 följer att när sanktionsavgift beslutas ska överträdelsens art, allvarlighetsgrad och varaktighet samt dess konsekvenser beaktas. Bestämmelsen kräver ingen kompletterande reglering, utom såvitt att en sanktionsavgift inte behöver tas ut när överträdelsen bedöms som ringa eller ursäktlig, eller om det annars med hänsyn till omständigheterna vore oskäligt att besluta om en sank-

tion. Vad som är ringa fall måste bedömas utifrån situationen i det enskilda fallet. Typiskt sett kan det vara fråga om ett åsidosättande som har haft mindre allvarliga konsekvenser, till exempel att produkten har tillhandahållits på marknaden endast i begränsad omfattning. Det kan också handla om mindre allvarliga överträdelser av de formella krav som följer av cyberresiliensförordningen, till exempel att tillverkaren eller importören har underlåtit att på produkten ange någon av de uppgifter som föreskrivs. Vidare kan det även vara fråga om fall där en sanktionsavgift har påförts med stöd av en annan författning för samma överträdelse.

10.3.2 Sanktionsavgifter kan påföras offentliga myndigheter och offentliga organ

Utredningens bedömning: Om en myndighet eller offentligt organ i sin verksamhet uppfyller kraven som ställs på en ekonomisk aktör som faller under tillämpningsområdet för EU:s cyberresiliensförordning och myndigheten eller organet gör sig skyldig till en överträdelse av regelverket ska en administrativ sanktionsavgift kunna påföras myndigheten eller organet enligt artikel 64.2–4 i EU:s cyberresiliensförordning och anslutande rättsakter.

Utredningens förslag: Sanktionsavgiften för en myndighet ska bestämmas till högst 10 000 000 kronor vid överträdelser som avses i artikel 64.2 i EU:s cyberresiliensförordning och anslutande föreskrifter, i den ursprungliga lydelsen, till högst 5 000 000 kronor vid överträdelser som avses i artikel 64.3 och till 2 500 000 kronor vid överträdelser som avses i artikel 64.4.

I artikel 64.7 i EU:s cyberresiliensförordning anges att varje medlemsstat ska fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter och offentliga organ som är inrättade i medlemsstaten.

I den svenska rättsordningen finns lagbestämmelser som föreskriver att en myndighet eller annat offentligt organ kan påföras sanktionsavgift för överträdelse av en regel i en författning, till exempel en upphandlinsskadeavgift.

Frågan huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter och offentliga organ vid överträdelse av olika författningar behandlas i prop. 2017/18:105 *Ny dataskyddslag* (s. 140–142) varvid följande anges:

Enligt artikel 83.7 är det upp till varje medlemsstat att fastställa regler om och i vilken utsträckning sanktionsavgifter ska kunna påföras offentliga myndigheter och organ i den medlemsstaten. Utredningen föreslår att svenska myndigheter ska kunna påföras sanktionsavgifter vid överträdelser av dataskyddsregleringen, dock med lägre högsta belopp än de som enligt dataskyddsförordningen gäller för privata aktörer.

Enligt regeringsformens terminologi, som bör användas även vid tolkningen av dataskyddsförordningen (se avsnitt 8.1), är alla offentliga organ utom riksdagen och kommun- och landstingsfullmäktige myndigheter.

Privaträttsliga organ är varken myndigheter eller offentliga organ, även om de utövar offentlig makt. Med anledning av Falköpings kommuns och Jönköpings läns landstings synpunkt kan det således konstateras att kommunala bolag bör anses som privata organ vid tillämpningen av dataskyddsförordningen och att de därmed inte omfattas av utredningens förslag. Däremot omfattas de av de direkt tillämpliga bestämmelserna om sanktionsavgifter i dataskyddsförordningen.

Flera av de remissinstanser som är kritiska till utredningens förslag om att sanktionsavgifter ska kunna tas ut av myndigheter ifrågasätter sanktionsavgifternas effektivitet, främst i förhållande till statliga myndigheter. Till exempel menar Göteborgs universitet att betalningen av en hög avgift minskar utrymmet för myndigheten att fullgöra sitt egentliga uppdrag och att sanktionsavgifter därför kan leda till att ytterligare medel måste tillföras, vilket skapar en rundgång i statskassan. Vidare framför bl.a. Polismyndigheten och Försäkringskassan att det i den offentliga sektorn – i motsats till den privata sektorn – redan finns en straffrättslig sanktion i form av tjänstefelsansvar, vilket vid sidan av möjligheten att vidta disciplinära åtgärder utgör ett skydd mot att enskilda tjänstemän i offentlig verksamhet gör sig skyldiga till grövre överträdelser. Dessutom påpekar de att myndigheten kan bli skadeståndsskyldig gentemot de registrerade.

Dessa invändningar skulle kunna framföras mot alla former av sanktionsavgifter mot myndigheter. Som framgår av utredningens redogörelse har det dock på flera andra områden ansetts utgöra en effektiv och nödvändig sanktion att kunna rikta viten och sanktionsavgifter mot statliga och kommunala myndigheter. Som exempel kan nämnas vite enligt diskrimineringslagen och upphandlingsskadeavgift enligt lagen (2016:1145) om offentlig upphandling. I detta sammanhang förtjänar det också att nämnas att EU-kommissionen har föreslagit att sanktionsavgifter ska kunna tas ut av EU-institutionerna och andra unionsorgan vid överträdelser av den förordning som reglerar bl.a. institutionernas egen behandling av personuppgifter, parallellt med disciplinära påföljder för den ansvarige tjänstemannen (COM (2017) 8 final).

Vidare måste den enskildes intresse av skydd för sin personliga integritet anses väga lika tungt då uppgifter behandlas i det allmänna verksamheten som då behandlingen sker i den privata sektorn. För att utföra sina uppgifter måste såväl statliga som kommunala myndigheter behandla mycket stora mängder personuppgifter, ofta av känslig karaktär. Denna behandling måste givetvis ske i enlighet med dataskyddsregleringen. Vid tillsynsmyndigheternas granskning under senare år har det dock framkommit fall där myndigheter begått förhållandevis allvarliga överträdelser av dataskyddsregleringen. Det kan alltså inte tas för givet att myndigheter alltid följer regleringen om dataskydd.

Tjänstefelsansvar eller disciplinansvar på individnivå är enligt regeringens mening inte tillräckligt effektiva sanktioner mot systematiska överträdelser. För att komma till rätta med sådana överträdelser krävs ofta investeringar i förbättrad teknik eller tydliga riktlinjer från myndighetens högsta ledning. Vetskapen om att brister i personuppgiftsbehandlingen skulle kunna leda till att höga sanktionsavgifter påförs, kommer enligt regeringens bedömning att leda till att myndighetsledningen, i normalfallet, tillser att åtgärder vidtas för att regleringen ska följas. Beslut om att faktiskt påföra en myndighet sanktionsavgifter torde därmed mycket sällan behöva komma i fråga. Sanktionsavgifter skulle således fylla en viktig preventiv funktion, även när det gäller myndigheter, och innebära en verklig förstärkning av integritetsskyddet för enskilda. Denna effekt kan inte enbart uppnås genom skadeståndsinstitutet, eftersom detta är beroende av att den registrerade driver en skadeståndstalan.

Sammanfattningsvis menar regeringen, liksom utredningen, att övervägande skäl talar för att sanktionsavgifter ska kunna tas ut av statliga och kommunala myndigheter vid överträdelser av bestämmelserna i dataskyddsförordningen.

Bestämmelsen i artikel 83.7 om medlemsstaternas möjligheter att bestämma i vilken utsträckning myndigheter ska kunna påförs avgifter innebär att medlemsstaterna har utrymme att bestämma ett tak för de belopp som kan påförs myndigheter. Visserligen kan det, i enlighet med vad Företagarna och Stiftelsen för internetinfrastruktur anför, framstå som rimligt att samma typ av överträdelse leder till samma typ av sanktion, oavsett om överträdelsen begåtts av en myndighet eller ett privat subjekt. Regeringen anser dock, i likhet med utredningen, att det maximala belopp som ska kunna påförs myndigheter bör ligga i paritet med andra sanktionsavgifter i svensk rätt och därmed vara väsentligt lägre än det högsta belopp som skulle kunna tas ut av ett företag enligt dataskyddsförordningen. Inom den privata sektorn kan en överträdelse av dataskyddsregleringen, förutom att kränka enskildas personliga integritet, medföra otillbörliga konkurrensfördelar som snedvrider den inre marknaden. Någon sådan ekonomisk vinning, på bekostnad av andra aktörer på marknaden, kan myndigheter inte dra. Här kan också noteras att i kommissionens förslag till den förordning som reglerar institutionernas och unionsorganens egen behandling av personupp-

gifter sätts beloppsgränsen för sanktionsavgifterna betydligt lägre än enligt dataskyddsförordningen. En institution ska enligt förslaget kunna påföras sanktionsavgifter om maximalt 500 000 euro per år.

Sanktionsavgifter ska enligt dataskyddsförordningen tas ut enligt två olika nivåer – en lägre nivå vid överträdelser som betraktas som mindre allvarliga och en högre nivå vid allvarligare överträdelser och underlåtenhet att följa förelägganden eller beslut av tillsynsmyndigheten eller att på annat sätt bistå den. Även för myndigheter finns det skäl att ha två olika avgiftsnivåer. Utredningen föreslår att ett maxbelopp om 10 000 000 kronor ska kunna påföras för mindre allvarliga överträdelser. För allvarliga överträdelser föreslår utredningen att maxbeloppet ska vara 20 000 000 kronor. Vissa remissinstanser, t.ex. *Centrala studiestödsnämnden*, anser att beloppen är orimliga och främmande för svensk förvaltningstradition. *Trafikverket* påpekar att 20 000 000 kronor är dubbelt så mycket som den högsta sanktionsavgift som kan påföras en svensk myndighet enligt gällande rätt.

Det kan konstateras att 10 000 000 kronor är vad som i dag maximalt kan påföras en myndighet i upphandlingsskadeavgift. Regeringen anser att högre belopp än så inte heller bör kunna påföras en myndighet vid överträdelser av dataskyddsförordningen. Enligt regeringens bedömning skulle en avgift om 10 000 000 kronor utgöra en effektiv, proportionell och avskräckande sanktion också mot allvarliga överträdelser av förordningen, även för de allra största myndigheterna.

Det finns, utifrån förordningens modell, skäl att bestämma beloppen för mindre allvarliga överträdelser till hälften, dvs. 5 000 000 kronor. Vidbestämmandet av vad som utgör en mindre allvarlig respektive en allvarlig överträdelse bör förordningens artikel 83.4 respektive 83.5 gälla.

I förordningens artikel 83.1–3 anges vilka omständigheter som ska beaktas vid beslut om att ta ut sanktionsavgifter och vid bestämmande av beloppets storlek. Dessa bestämmelser bör tillämpas även då sanktionsavgifter tas ut av myndigheter. Detta innebär att en avgift kan påföras med allt ifrån 0 kronor upp till maxbeloppet, beroende på vad som i det enskilda fallet är lämpligt med hänsyn till de olika omständigheter som anges i artikel 83.1–2.

Statens skolverk, *Sveriges Kommuner och Landsting* och flera kommuner påpekar i detta sammanhang att en hög sanktionsavgift kan komma att slå orimligt hårt mot mindre myndigheter. Enligt artikel 83.2 a ska dock vederbörlig hänsyn tas till bl.a. den aktuella personuppgiftsbehandlings omfattning och antalet berörda registrerade. Eftersom små myndigheter ofta behandlar färre personuppgifter innebär detta i praktiken att myndighetens storlek kan få betydelse när avgiften bestäms. Vidare ska tillsynsmyndigheten, enligt artikel 83.1, säkerställa att påförande av administrativa sanktionsavgifter i varje enskilt fall är effektivt, proportionellt och avskräckande. Även denna bestämmelse innebär att tillsynsmyndigheten måste, i enlighet med den proportionalitetsprincip som gäller vid all myndighetsutövning, anpassa avgiftens storlek till den aktuella myndighetens budgetram.

Sammanfattningsvis föreslår regeringen att tillsynsmyndigheten ska få ta ut sanktionsavgifter även av statliga och kommunala myndigheter vid överträdelser av bestämmelserna i dataskyddsförordningen. För mindre allvarliga överträdelser bör avgiften uppgå till högst 5 000 000 kronor och för allvarigare överträdelser till högst 10 000 000 kronor. Vid bestämmandet av avgiftens storlek i det enskilda fallet bör dataskyddsförordningens bestämmelser tillämpas. Med hänsyn till behovet av förutsebarhet i fråga om vilka sanktioner som kan bli följden av överträdelser, bör hänvisningen till dataskyddsförordningen i denna bestämmelse vara statisk, dvs. avse förordningen i den ursprungliga lydelsen.

I artikel 64.2 i EU:s cyberresiliensförordning anges att den som inte efterlever de väsentliga cybersäkerhetskrav som anges i bilaga 1 och de skyldigheter som fastställs i artiklarna 13 och 14 kan påföras sanktionsavgift vid bristande efterlevnad av. Bestämmelsen riktar sig i första hand mot tillverkare av produkter med digitala element. I artikel 64.3 anges att bristande efterlevnad av de övriga skyldigheter som anges i bestämmelsen kan medföra sanktionsavgift. Denna bestämmelse omfattar fler ekonomiska aktörer än bara tillverkaren. I artikel 64.4 anges att tillhandahållande av oriktig, ofullständig eller vilseledande information i vissa fall kan föranleda att den som lämnar informationen kan påföras en sanktionsavgift.

I artikel 64.7 anges att varje medlemsstat ska fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter och offentliga organ som är inrättade i medlemsstaten. Formuleringen i artikeln ger utrymme för medlemsstaten att i ett första steg bedöma om det föreligger behov av en sådan nationell reglering, och om ett behov kan anses föreligga, i nästa steg ange i vilken utsträckning som en sanktionsavgift bör påföras.

Frågan om behovet av en nationell reglering bör ta sin utgångspunkt i syftet med bestämmelserna i EU:s cyberresiliensförordning och vilka ekonomiska aktörer som omfattas av regleringen.

Enligt artikel 3 i förordningen avses med ekonomisk aktör tillverkaren, tillverkarens representant, importören, distributören eller en annan fysisk eller juridisk person som omfattas av skyldigheter i enlighet med denna förordning. Med andra ord inbegriper begreppet samtliga typer av aktörer i leveranskedjan som har ansvar enligt förordningen, det vill säga tillverkare, tillverkarens representant, importör och distributör.

Motsvarande gäller verksamhet som anmält organ för bedömning av överensstämmelse, dvs. om det finns ett sådant organ för bedömning i en myndighetsorganisation och som faller under förordningens tillämpningsområde.

Till en början kan noteras att regleringen i artikel 64.2 i första hand riktar sig till tillverkare av produkter med digitala element som tillhandhåller produkten på den inre marknaden. För att det ska bli aktuellt att överväga en reglering enligt artikel 64.7 bör det finnas myndigheter eller andra offentliga organ som bedriver sådan verksamhet som omfattas av den reglering som riktar sig mot tillverkaren. Som framhålls i ovan angivna prop. 2017/18:105 är – enligt regeringsformens terminologi – alla offentliga organ utom riksdagen och kommun- och landstingsfullmäktige myndigheter. Privaträttsliga organ är varken myndigheter eller offentliga organ, även om de utövar offentlig makt. Kommunala bolag kan anses som privata organ vid tillämpningen av dataskyddsförordningen. Det är således i första hand myndigheter som kan bli aktuella för en reglering.

Utredningen bedömer det dock som mindre sannolikt att en svensk myndighet kan komma att i kommersiellt syfte tillverka och saluföra produkter med digitala element på den inre marknaden och därmed även omfattas av förordningen bestämmelser som träffar en tillverkare av sådana produkter. Motsvarande gäller för rollen som importör eller distributör. Det kan dock inte uteslutas att en myndighet i framtiden skulle kunna komma att i något fall bli att betrakta som en ekonomisk aktör och därför komma att omfattas av bestämmelserna i förordningen. Det finns därför skäl att överväga att en sanktionsavgift även bör kunna tas ut av en myndighet vid överträdelse av bestämmelserna i EU:s cyberresiliensförordning.

Vad gäller i vilken uträkning som sanktionsavgiften bör påföras och till vilket belopp gör utredningen följande överväganden. Vad som anges i prop. 2017/18:105 bör utgöra utgångspunkt för regleringen och sanktionsavgift.

När det gäller frågan om ett beloppstak bör införas för myndigheter beaktar utredningen följande. Som utgångspunkt anser utredningen att samma typ av överträdelse av EU:s cyberresiliensförordning bör som princip leda till samma typ av sanktion oavsett om överträdelsen begås av en ekonomisk aktör eller en myndighet. Samtidigt bör sanktionsavgifter som påförs en myndighet för överträdelser av förordningen vara jämförbara med andra sanktionsavgifter i

svensk rätt. Enligt 6 kap. 2 § andra stycket lagen med kompletterande bestämmelser till EU:s dataskydds-förordning kan sanktionsavgiften vid en myndighets överträdelse av EU:s dataskyddsförordnings uppgå till 5 000 000 kronor eller 10 000 000 kronor. En sanktionsavgift enligt säkerhetsskyddslagen får bestämmas till högst 10 000 000 kronor för en statlig myndighet, en kommun eller en region. För upphandlingsskadeavgift enligt lagen om offentlig upphandling är det högsta belopp som kan beslutas 20 000 000 kronor eller tio procent av upphandlingens värde.

Sammanfattningsvis anser utredningen att om en myndighet i sin verksamhet uppfyller kraven som ställs för att betraktas som en ekonomisk aktör som faller under förordningens tillämpningsområde och myndigheten i den egenskapen gör sig skyldig till en överträdelse av regelverket bör en administrativ sanktionsavgift påföras myndigheten. Det finns därför behov av kompletterande nationell reglering i detta avseende.

Mot bakgrund av det ovan angivna anser utredningen att sanktionsavgiften bör för bristande efterlevnad enligt artikel 64.2 uppgå till högst 10 000 000 kronor och enligt artikel 64.3 till högst 5 000 000 kronor samt enligt artikel 64.4 till högst 2 500 000 kronor.

Marknadskontrollmyndigheten ska med tillämpning av artikel 64.3 beakta samtliga omständigheter och bör även ta hänsyn till myndighetens förutsättningar i det enskilda fallet.

10.3.3 Anmälande myndighet och marknadskontrollmyndigheten ska besluta om sanktionsavgift

Utredningens förslag: 1. En marknadskontrollmyndighet ska besluta att ta ut sanktionsavgift vid överträdelse av artikel 13 och 14 samt väsentliga cybersäkerhetskrav i bilaga I i EU:s cyberresiliensförordning och anslutande föreskrifter.

Avgiftens storlek ska bestämmas med tillämpning av artikel 64.5 i EU:s cyberresiliensförordning.

Sanktionsavgiften ska bestämmas till högst 15 000 000 euro eller, om överträdelsen begås av ett företag, till 2,5 procent av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

Sanktionsavgiften för en myndighet ska bestämmas till högst 10 000 000 kronor.

2. En marknadskontrollmyndighet ska besluta att ta ut en sanktionsavgift vid överträdelse av artikel 18–23, 28, 30.1–30.4, 31.1–31.4, 32.1–32.3, 33.5 och 53 i EU:s cyberresiliensförordning och anslutande föreskrifter.

Avgiftens storlek ska bestämmas med tillämpning av artikel 64.5 i EU:s cyberresiliensförordning.

Sanktionsavgiften ska bestämmas till högst 10 000 000 euro eller, om överträdelsen begås av ett företag, upp till 2 procent av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

Sanktionsavgiften för en myndighet ska bestämmas till högst 5 000 000 kronor.

3. Den anmälade myndigheten ska besluta att ta ut en sanktionsavgift vid överträdelse av artikel 39, 41, 47 och 49 i EU:s cyberresiliensförordning och anslutande föreskrifter.

Avgiftens storlek ska bestämmas med tillämpning av artikel 64.5 i EU:s cyberresiliensförordning.

Sanktionsavgiften ska bestämmas till högst 10 000 000 euro eller, om överträdelsen begås av ett företag, upp till 2 procent av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

Sanktionsavgiften för en myndighet ska bestämmas till högst 5 000 000 kronor.

4. En marknadskontrollmyndighet ska besluta att ta ut en sanktionsavgift vid överträdelse av artikel 64.4 i EU:s cyberresiliensförordning och anslutande föreskrifter.

Avgiftens storlek ska bestämmas med tillämpning av artikel 64.5 i förordningen.

Sanktionsavgiften ska bestämmas till högst 5 000 000 euro eller, om överträdelsen begås av ett företag, upp till 1 procent av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

Sanktionsavgiften för en myndighet ska bestämmas till högst 2 500 000 kronor.

Enligt artikel 64.8 i EU:s cyberresiliensförordning ska reglerna om administrativa sanktionsavgifter tillämpas på ett sådant sätt att sanktionsavgifterna beslutas av en myndighet eller utdöms av behöriga nationella domstolar.

I svensk rätt är det som regel en myndighet eller domstol som på ansökan av en myndighet beslutar om sanktionsavgift.

Frågan om en myndighet eller en domstol efter ansökan av en myndighet bör fatta beslut om sanktionsavgift har behandlats i tidigare lagstiftningsärenden. 2016 års *Marknadskontrollutredning* uttalade (s. 258 f.) i betänkandet *Marknadskontrollmyndigheter – befogenheter och sanktionsmöjligheter* (SOU 2017:69) bland annat följande:

De regelverk som i dag ger vissa marknadskontrollmyndigheter möjlighet att använda sig av sanktionsavgifter i sin verksamhet skiljer sig något åt i sin utformning. Enligt produktsäkerhetslagen, som flera sektorslagstiftningar hänvisar till i fråga om sanktionsavgifter, krävs det uppsåt eller oaktsamhet hos den ekonomiska aktören för att sanktionsavgifter ska kunna påföras vid regelöverträdelse. Enligt regelverk som är utformade på detta sätt är det förvaltningsdomstolarna som beslutar om sanktionsavgifter efter ansökan av berörd kontrollmyndighet.

Det förekommer även att marknadskontrollmyndigheters regelverk om sanktionsavgifter bygger på s.k. strikt ansvar, vilket innebär att betalningsskyldighet åläggs när en regelöverträdelse objektivt kan konstateras. I de fall avgiftsskyldighet baseras på strikt ansvar kan myndigheten påföra avgiften utan att behöva vända sig till domstol. Ett beslut om påförande av avgift kan dock överklagas till förvaltningsdomstol.

Om en avgiftsskyldighet ska bygga på strikt ansvar bör det, som behandlats ovan, enligt regeringen förutsättas att det finns en stark presumption att regelöverträdelser inte kan aktualiseras annat än som en följd av uppsåt eller oaktsamhet. Det strikta ansvaret anses normalt godtagbart när de som kan tänkas bli avgiftsskyldiga kan förväntas ha god kännedom om gällande regelverk och dessutom ha en särskild anledning att se till att dessa regler följs.⁷

I marknadskontrollverksamhet är det ekonomiska aktörer som är föremål för kontrollen och som skulle kunna bli avgiftsskyldiga vid konstaterade regelöverträdelser. Det är alltså tillverkare, importörer och distributörer som skulle kunna påföras avgift. Dessa aktörer har särskild anledning att väl känna till och följa det regelverk som omgärdar den produkt som de tillverkar eller hanterar i sin verksamhet. Om en produkt inte överensstämmer med gällande krav bör det därför i normalfallet kunna presumeras att regelöverträdelsen har skett uppsåtligt eller av oaktsamhet. I vart fall bör det ofta kunna betraktas som oaktsamt att en ekonomisk aktör inte sätter sig in i de regler som gäller på det område där han eller hon verkar. Med hänsyn till regeringens

⁷ Proposition (2007/08:43) *Rapporteringskyldighet av ej verkställda beslut enligt lagen (1993:387) om stöd och service till vissa funktionshindrade, m.m.*, s. 19.

ovan redovisade ståndpunkt bör således avgiftsskyldighet som baseras på strikt ansvar vara ändamålsenligt för marknadskontrollverksamhet.

Vidare bidrar en avgiftsskyldighet som bygger på ett objektiva ansvar till en förenkling och effektivisering av sanktionssystemet. Myndigheten ska då endast kontrollera att en överträdelse har förekommit och fastställa avgiften enligt en fastställd beräkningsgrund i stället för att ansöka om påförande av avgift hos domstol, ett förfarande som kan medföra tidsutdräkt och således minska den önskade effektiviteten.

Utredningen kan notera att generellt sett anses en myndighet lämplig att besluta om sanktionsavgift när bestämmelserna är relativt enkla att tillämpa, beslutsfattandet är förhållandevis schabloniserat och sanktionsbestämmelserna bygger på strikt ansvar. En fördel med att tillsynsmyndigheten fattar beslut är att handläggningen kan bli snabbare om inte flera myndigheter behöver delta i hanteringen. En domstol anses normalt sett bättre lämpad att besluta om sanktionsavgift om det är aktuellt att pröva subjektiva rekvisit eller andra svårbedömda rekvisit.

Utredningen kan även notera att åtgärder för marknadskontroll utgörs till en del av att myndigheterna övervakar marknaden, direkt genom inspektion eller indirekt med hjälp av olika informationskällor. Den andra delen består av de åtgärder som vidtas för att aktören ska avhjälpa upptäckta brister, vilket kan ske genom frivillig rättelse från den berörda aktörens sida eller genom att myndigheten vidtar tvångsåtgärder. Vid upptäckt av en produkt som inte uppfyller gällande krav har myndigheter som bedriver marknadskontroll olika befogenheter och möjligheter att rikta sanktioner mot den ekonomiska aktören som är ansvarig för tillverkning, import eller annan distribution av produkten. Det kan till exempel vara fråga om beslut om försäljningsförbud eller om återkallelse av produkten. Även sanktionsavgift kan aktualiseras för vissa regelöverträdelser.

Skillnader i olika regelverk vad avser befogenheter och sanktionsmöjligheter kan leda till att ekonomiska aktörer riskerar att behandlas olika om deras produkter inte uppfyller gällande krav trots att det kan vara fråga om relativt likartade regelöverträdelser. Skillnaderna i regelverken kan också vara svåröverskådliga, både för kontrollmyndigheterna och för den enskilde aktören. I vissa regelverk som genomför harmoniserad lagstiftning saknas även ett uttryckligt utpekande av marknadskontrollmyndighet, vilket kan medföra att marknadskontrollansvaret inte är tydligt för myndigheten och att det är oklart vilka befogenheter och sanktionsmöjligheter myn-

digheten kan använda sig av. De aspekter som gör sig gällande i detta sammanhang är att de överträdelser som i första hand är aktuella avser den ekonomiska aktörens bristande efterlevnad av att säkerställa att de väsentliga cybersäkerhetskraven för den aktuella produkten uppfylls och därtill knutna efterföljande skyldigheter avseende CE-märkning, sårbarhets- och incidentrapportering samt upprättande och bevarande av teknisk dokumentation. Det är således främst frågor som avser tekniska krav, rapportering och dokumentation inom området för marknadskontroll. Marknadskontrollmyndigheten får antas att vara väl förtrogen med det regelverk som sanktioneras och ha förutsättningar att upptäcka regelöverträdelser. Det är marknadskontrollmyndigheten som måste anses ha bäst förutsättningar att bedöma om en ekonomisk aktör har underlåtit att följa regelverket. Som ovan anges får den nationella myndigheten för cybersäkerhetscertifiering besluta om en sanktionsavgift vid konstaterad överträdelse av det europeiska regelverket för cybersäkerhetscertifiering (EU:s cybersäkerhetsakt). De överträdelser som därvid kan komma att bli aktuella är i många fall till sin karaktär av motsvarande art som kan bli aktuella vid en överträdelse av EU:s cyberresiliensförordning, vilket talar för att befogenheten att besluta om sanktioner bör utformas på motsvarande sätt.

Utredningen har valt att i den kompletterande lagen använda begreppet överträdelse i stället för begreppet bristande efterlevnad när det gäller förutsättning för att påföra sanktionsavgift. Begreppet är mer vanligt förekommande i svensk rätt än vad begreppet bristande efterlevnad är.⁸ Någon saklig skillnad föreligger dock inte.

Utredningen anser att det bör vara marknadskontrollmyndigheten som bestämmer om sanktionsavgift vid överträdelse av artikel 13 och 14 samt väsentliga cybersäkerhetskrav i bilaga I, artikel 18–23, 28, 30.1–30.4, 31.1–31.4, 32.1–32.3, 33.5, 53 och 64.4 i EU:s cyberresiliensförordning och anslutande föreskrifter. Av artikel 64.6 framgår att marknadskontrollmyndigheter som påför administrativa sanktionsavgifter ska meddela marknadskontrollmyndigheterna i andra medlemsstater detta via det informations- och kommunikationssystem som avses i artikel 34 i förordning (EU) 2019/1020.

⁸ Se exempelvis 4 kap. lagen (2024:1278) med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn, 3 kap. lagen (2019:1215) med kompletterande bestämmelser till EU:s förordning om värdepapperisering och regeringens proposition (2025/26:28) *Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag*.

Utredningen anser vidare att den anmälände myndigheten ska besluta att ta ut en sanktionsavgift vid överträdelse av artikel 39, 41, 47 och 49 i EU:s cyberresiliensförordning och anslutande föreskrifter.

Sanktionsavgifternas storlek ska bestämmas med tillämpning av artikel 64.5 i förordningen.

10.3.4 Vite och sanktionsavgift för samma överträdelse

Utredningens förslag: En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande vid vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

I artikel 64.9 i EU:s cyberresiliensförordning anges att administrativa sanktionsavgifter får, beroende på omständigheterna i det enskilda fallet, påföras utöver eventuella andra korrigerande eller begränsande åtgärder som marknadskontrollmyndigheterna tillämpar på samma överträdelse.

Den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och några av dess tilläggsprotokoll, däribland det sjunde tilläggsprotokollet, gäller som svensk lag enligt lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna. I 2 kap. 19 § regeringsformen finns ett förbud mot att meddela lag eller föreskrift som står i strid med Sveriges åtaganden enligt Europakonventionen. I artikel 4.1 i sjunde tilläggsprotokollet till Europakonventionen finns ett förbud mot dubbel lagföring eller dubbla straff.

Marknadskontrollmyndigheten ska enligt förslaget få meddela de förelägganden som behövs för att EU:s cyberresiliensförordning och EU:s marknadskontrollförordning ska följas (se kap. 9). Sådana förelägganden ska kunna förenas med vite. Ett vite har karaktär av straff och aktualiserar tillämpningen av förbudet mot dubbel lagföring och dubbla straff i sjunde tilläggsprotokollet till Europakonventionen. Högsta domstolen har i sin praxis fastslagit att det inte enbart är ett slutligt avgörande som utgör ett hinder mot andra förfaranden, utan att även en pågående prövning utgör ett sådant hinder enligt svenska grundläggande processuella principer (se bland annat Högsta domstolens avgörande NJA 2013 s. 502). I regelverk där det är möj-

ligt att utfärda ett vitesföreläggande och ta ut en sanktionsavgift för samma överträdelse är det därför brukligt att införa bestämmelser som syftar till att hindra dubbelbestraffning. Dessa brukar utformas på så sätt att sanktionsavgift inte får beslutas om överträdelsen även omfattas av ett vitesföreläggande och överträdelsen ligger till grund för en ansökan om utdömande av vite. Det bör därför i den nya kompletterande lagen föreskrivas att den som har överträtt ett vitesföreläggande eller vitesförbud inte kan åläggas en sanktionsavgift enligt lagen för en överträdelse som omfattas av ett föreläggande eller förbud.

Det bedöms som osannolikt att den omvända situationen skulle uppstå, det vill säga att en beslutad sanktionsavgift skulle utgöra hinder mot ett föreläggande eller utdömande av vite. Ett vitesföreläggande syftar till att få enskilda att vidta en åtgärd eller underlåta att göra något, det vill säga att påverka ett framtida handlande. En sanktionsavgift däremot syftar till att utdöma en sanktion för ett tidigare agerande. Ett vitesföreläggande som beslutas efter en sanktionsavgift kan därför inte omfatta samma händelse. Det är inte heller sannolikt att marknadskontrollmyndigheten skulle använda sig av ett vitesföreläggande eller ansöka om utdömande av vite för en överträdelse för vilken en sanktionsavgift har beslutats. Risker för dubbelbestraffning i den beskrivna situationen är mot denna bakgrund osannolika och motiverar därför inte en bestämmelse om förbud mot dubbelprövning⁹ (jfr propositionen *Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation* (prop. 2021/22:136 s. 363 och 364).

10.3.5 Undantag

Utredningen bedömning: I artikel 64.10 i EU:s cyberresiliensförordning anges att genom undantag från artikel 64.2–9 ska de administrativa sanktionsavgifter som avses i dessa punkter inte tillämpas på angivna fall.

Bestämmelsen är direkt tillämplig och kräver ingen kompletterande författningsreglering.

⁹ Fråga om ett meddelat förbud och en sanktionsavgift avser samma gärning, se Högsta förvaltningsdomstolen HDF 2024: ref. 61.

I artikel 64.10 EU:s cyberresiliensförordning anges att genom undantag från artikel 64.2–9¹⁰ ska de administrativa sanktionsavgifter som avses i dessa punkter inte tillämpas på följande:

1. Tillverkare som klassificeras som mikroföretag eller små företag när det gäller underlåtenhet att iaktta den tidsfrist som avses i artikel 14.2 a eller 14.4 a.
2. Alla överträdelser av denna förordning som begås av förvaltare av programvara med fri och öppen källkod.

Bestämmelsen är direkt tillämplig i angivna fall och behöver ingen kompletterande författningsreglering. När det gäller mikroföretag och små och medelstora företag ska bestämmelserna i bilagan till kommissionens rekommendation 2003/361/EG tillämpas i sin helhet vid fastställandet av vilken kategori ett företag omfattas av. Vid beräkningen av personalstyrkan och de finansiella taken för att fastställa företagskategorierna ska bestämmelserna i artikel 6 i bilagan till kommissionens rekommendation 2003/361/EG om fastställande av uppgifter för ett företag med hänsyn till särskilda typer av företag, såsom partnerföretag eller anknutna företag, också tillämpas.

10.4 Förfaranderegler och preskription

Utredningens förslag: Sanktionsavgiften ska betalas till den anmälade myndigheten och marknadskontrollmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften fick laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas i tid, ska den anmälade myndigheten och marknadskontrollmyndigheten lämna den obetalda avgiften för indrivning.

Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

¹⁰ 2025/90555 Rättelse till Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen) (Europeiska unionens officiella tidning L, 2024/2847, 20 november 2024). I rättelsen anges följande: sidan 65, artikel 64.10, inledningsfrasen: I stället för: "Genom undantag från punkterna 3–9 ska de administrativa sanktionsavgifter som avses i dessa punkter inte tillämpas på följande:" ska det stå: "Genom undantag från punkterna 2–9 ska de administrativa sanktionsavgifter som avses i dessa punkter inte tillämpas på följande:".

En sanktionsavgift tillfaller staten.

Innan den anmälade myndigheten och marknadskontrollmyndigheten beslutar om sanktionsavgift ska den som avgiften ska tas ut av få tillfälle att yttra sig. Om så inte har skett inom två år från det att överträdelsen skedde får någon sanktionsavgift inte beslutas.

Ett beslut om sanktionsavgift ska delges.

En beslutad sanktionsavgift ska falla bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

I detta avsnitt behandlas frågor som rör förfaranderegler vid uttag av sanktionsavgift och preskription av en sådan avgift.

Eftersom det är anmälade myndighet och marknadskontrollmyndigheten som ska besluta om sanktionsavgift kommer förvaltningslagen (2017:900) att gälla för förfarandet. Det är dock vanligt att bestämmelser om sanktionsavgifter åtföljs av särskilda förfarandebestämmelser om bland annat preskription och verkställighet.

En sanktionsavgift ska betalas till den anmälade myndigheten och marknadskontrollmyndigheten inom 30 dagar från det att beslutet om avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. Om avgiften inte betalas i tid bör myndigheten vara skyldig att lämna den obetalda avgiften för indrivning enligt lagen (1993:891) om indrivning av statliga fordringar m.m. Av 3 kap. 1 § utsökningslagen följer att en förvaltningsmyndighets beslut som innefattar betalningsskyldighet och som är överklagbart är en verkställbar exekutionstitel. Enligt 3 kap. 20 § utsökningsbalken får ett sådant beslut verkställas när det fått laga kraft.

Sanktionsavgifter tillfaller normalt sett staten. Det finns inte skäl att låta någon annan ordning gälla i fråga om sanktionsavgifter som tas ut med stöd av cyberresiliensförordningens bestämmelser.

Ett beslut om sanktionsavgift är en ingripande åtgärd. Behovet av att ingripa mot en överträdelse minskar över tid. Det bör därför finnas en bortre tidsgräns för den behöriga myndighetens handläggning och möjligheten att besluta om sanktionsavgift. Om det efter överträdelsen har gått mer än två år utan att den som avgiften ska tas ut av har fått tillfälle att yttra sig, bör en sanktionsavgift inte få beslutas.

Ett beslut om avgift ska delges den betalningsskyldige enligt delgivningslagen (2010:1932).

I likhet med det som i allmänhet gäller för sanktionsavgifter ska avgiften även preskriberas till den del verkställighet inte har skett inom fem år.

11 Sekretess

11.1 Inledning

I detta kapitel behandlas frågan om sekretess och informationsdelning. Utredningen analyserar relevant sekretessreglering utifrån de olika intressen som ska skyddas enligt förordning (EU) 2024/2847¹ (EU:s cyberresiliensförordning) samt lämnar de överväganden och förslag som utredningen bedömer behövs för att uppfylla förordningens krav. I kapitlet behandlas även frågan om behandling av personuppgifter.

11.2 Bakgrund

EU:s cyberresiliensförordning innehåller bestämmelser som innebär att det allmänna ges tillgång till information som kan vara känslig.

Tillverkare, eller i förekommande fall andra ekonomiska aktörer, samt förvaltare av programvara med fri och öppen källkod kommer enligt EU:s cyberresiliensförordning att vara skyldiga att till CSIRT-enheten rapportera aktivt utnyttjande sårbarheter och allvarliga incidenter. Förordningen innehåller även bestämmelser om frivillig sårbarhets- och incidentrapportering. Rapporterna kan innehålla känsliga uppgifter om bland annat sårbarheter i produkter, uppgifter om hot mot eller andra risker för produkter med digitala element, beskrivningar av incidenter, deras orsak och konsekvenser samt uppgifter om riskreducerande åtgärder. Även information om en rapports förekomst kan vara en känslig uppgift till exempel om det rör sårbar-

¹ Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen).

heter för vilka en säkerhetsuppdatering eller andra säkerhetsåtgärder ännu inte är tillgänglig.

Ekonomiska aktörer och förvaltare av programvara med fri och öppen källkod kommer även att vara skyldiga att till marknadskontrollmyndigheterna tillhandahålla information som är nödvändig för marknadskontroll. Vidare behöver den som deltar i en av marknadskontrollmyndigheten inrättad regulatorisk sandlåda för cyberresiliens tillhandahålla information som behövs för den verksamhet som bedrivs i sandlådan. Information som tillhandahålls inom ramen för marknadskontroll kan innehålla känsliga uppgifter om bland annat en ekonomisk aktörs verksamhet, säkerhets- och bevakningsåtgärder, leveranskedjor och distributionsnäts utformning samt information och dokumentation om specifika produkter och bedömningar av cybersäkerhetsrisker. Information som tillhandahålls inom ramen för regulatoriska sandlådor kan innehålla känsliga uppgifter om bland annat utveckling och utformning av innovativa produkter med digitala element.

Ekonomiska aktörer kommer även behöva tillhandahålla information till organ för bedömning av överensstämmelse, i den utsträckning ett sådant organ anlitas. Informationen kan innehålla känsliga uppgifter om bland annat riskbedömningar, uppgifter om utformningen, tillverkningen och funktionen av den aktuella produkten samt uppgifter om hur processerna för sårbarhetshantering genomförs.

Vidare kommer organ för bedömning av överensstämmelse att vara skyldiga att inom ramen för anmälan och ackreditering lämna uppgifter om sin verksamhet till den myndighet som är anmälände myndighet enligt EU:s cyberresiliensförordning. Organ som blivit anmälda har dessutom en informationsskyldighet gentemot den anmälände myndigheten.

Känsliga uppgifter som olika aktörer mottar och samlar in med stöd av EU:s cyberresiliensförordning behöver enligt förordningen skyddas. Samtidigt förutsätter EU:s cyberresiliensförordning att de aktörer som har befogenhet att kräva in viss information eller som av annan anledning är mottagare av informationen enligt förordningen många gånger ska samverka och dela informationen med andra aktörer såväl nationellt som internationellt. Utredningen behöver därför överväga om det i svensk rätt finns en tillräcklig sekretessreglering för känsliga uppgifter och om svenskt rätt tillgodoser förordningens

krav på utlämnande av information. Det gäller både nationellt och inom EU.

11.3 Bestämmelser om konfidentialitet i EU:s cyberresiliensförordning

EU:s cyberresiliensförordning innehåller bestämmelser om konfidentialitet och tystnadsplikt. Dessutom innehåller förordningen bestämmelser om undanhållande av viss information under vissa förutsättningar.

Artikel 63 i EU:s cyberresiliensförordning innehåller en generell bestämmelse om konfidentialitet. Enligt bestämmelsen ska alla parter som deltar i tillämpningen av förordningen respektera konfidentialiteten för den information och de data som de erhåller när de utför sina uppgifter och sin verksamhet på ett sådant sätt att de skyddar följande:

- a) Immateriella rättigheter och en fysisk eller juridisk persons konfidentiella affärsinformation eller företagshemligheter, inbegripet källkod, utom i de fall som avses i artikel 5 i direktiv (EU) 2016/943².
- b) Ett ändamålsenligt genomförande av denna förordning, särskilt med avseende på inspektioner, utredningar eller revisioner.
- c) Intressen som rör allmän och nationell säkerhet.
- d) Integriteten i straffrättsliga eller administrativa förfaranden.

Utan att det påverkar tillämpningen av punkterna ovan får information som utbyts på konfidentiell basis mellan marknadskontrollmyndigheterna och mellan marknadskontrollmyndigheter och kommissionen inte lämnas ut utan föregående samtycke från den marknadskontrollmyndighet som ursprungligen lämnat informationen. Artikeln föreskriver vidare att vad som tidigare angetts i artikeln inte påverkar kommissionens, medlemsstaternas och de anmälda organens rättigheter och skyldigheter när det gäller att utbyta information och utfärda varningar och inte heller de berörda personernas skyldighet

² Europaparlamentets och rådets direktiv (EU) 2016/943 av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs.

att lämna information enligt medlemsstaternas straffrätt. Slutligen föreskriver artikeln att kommissionen och medlemsstaterna vid behov får utbyta känslig information med berörda myndigheter i tredje-länder med vilka de har slutit bilaterala eller multilaterala avtal om konfidentialitet som garanterar en tillräcklig skyddsnivå.

Artikel 14.2 och 14.4 i EU:s cyberresiliensförordning reglerar vilka uppgifter som ska rapporteras i händelse av en aktivt utnyttjad sårbarhet eller en allvarlig incident. Av bestämmelserna framgår att tillverkaren i rapporten, i tillämpliga fall, ska ange hur känslig tillverkaren anser att den rapporterade informationen är.

Skäl 71 anger att när tillverkarna anmäler en aktivt utnyttjad sårbarhet eller en allvarlig incident som påverkar säkerheten för produkten med digitala element bör de ange hur känslig de anser att den anmälda informationen är. Den CSIRT-enhet som först tar emot anmälan bör ta hänsyn till denna information när den bedömer huruvida anmälan ger upphov till exceptionella omständigheter som motiverar att spridningen av anmälan till de andra relevanta CSIRT-enheter på grundval av motiverade cybersäkerhetsrelaterade skäl skjuts upp. Den bör också ta hänsyn till denna information när den bedömer huruvida anmälan om en aktivt utnyttjad sårbarhet ger upphov till ovanligt exceptionella omständigheter som motiverar att den fullständiga anmälan inte samtidigt görs tillgänglig för Enisa. Slutligen bör CSIRT-enheter kunna beakta denna information när de fastställer lämpliga åtgärder för att begränsa de risker som härrör från sådana sårbarheter och incidenter.

Enligt artikel 15.5 i EU:s cyberresiliensförordning, gällande frivilliga sårbarhets- och incidentrapporter, ska CSIRT-enheten säkerställa konfidentialitet och lämpligt skydd för den information som tillhandahålls av den anmälade fysiska eller juridiska personen.

Gällande obligatoriska sårbarhets- och incidentrapporter föreskriver artikel 16.2 i EU:s cyberresiliensförordning att CSIRT-enheten under exceptionella omständigheter och under en tidsperiod som är absolut nödvändig får skjuta upp spridningen av sårbarhets- och incidentrapporter till de CSIRT-enheter på det territorium där tillverkaren har angett att produkten med digitala element har tillhandahållits. Under *särskilt* exceptionella omständigheter får CSIRT-enheten undanhålla en fullständig rapport för både EU:s cybersäkerhetsbyrå (Enisa) och de andra CSIRT-enheterna. Vidare föreskriver artikel 16.6 att om en CSIRT-enhet har uppmärksamats på en ak-

tivt utnyttjad sårbarhet, som en del av ett förfarande för samordnad delgivning av information om sårbarheter som avses i artikel 12.1 i direktiv (EU) 2022/2555³ (NIS 2-direktivet), får den CSIRT-enhet som först tog emot anmälan skjuta upp spridningen av den berörda rapporten via den gemensamma rapporteringsplattformen på grundval av motiverade cybersäkerhetsrelaterade skäl under en period som inte är längre än vad som är absolut nödvändigt och till dess att de berörda parterna inom samordnad delgivning av information om sårbarheter har gett sitt samtycke till utlämnande.

Enligt artikel 37.5 i EU:s cyberresiliensförordning ska en anmälände myndighet skydda den konfidentiella information som den mottar.

Enligt artikel 39.10 i EU:s cyberresiliensförordning ska personalen vid ett organ för bedömning av överensstämmelse iakttä tystnadsplikt beträffande all information som de erhåller vid utförandet av sina uppgifter enligt bilaga VIII eller bestämmelser i nationell rätt som genomför den, utom gentemot marknadskontrollmyndigheterna i den medlemsstat där verksamheten bedrivs. Vidare ska äganderätten vara skyddad.

Enligt artikel 52.1 i EU:s cyberresiliensförordning ska förordning (EU) 2019/1020⁴ (EU:s marknadskontrollförordning) tillämpas på produkter med digitala element. Enligt artikel 17 i EU:s marknadskontrollförordning ska marknadskontrollmyndigheterna bland annat respektera principen om konfidentialitet samt om yrkes- och affärshemligheter och ska skydda personuppgifter i enlighet med unionsrätten och nationell rätt.

³ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

⁴ Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011.

11.4 Bestämmelser om informationsdelning i EU:s cyberresiliensförordning

Inom ramen för EU:s cyberresiliensförordning kommer CSIRT-enheten, marknadskontrollmyndigheterna, den anmälade myndigheten och anmälda organ att hantera olika slags uppgifter samt samverka såväl nationellt som internationellt.

11.4.1 CSIRT-enheten

Hantering av sårbarhets- och incidentrapporter

CSIRT-enheten är mottagare av sårbarhets- och incidentrapporter enligt artikel 14 och 15 i EU:s cyberresiliensförordning.

Rapporterna kan inkomma till CSIRT-enheten från fysiska eller juridiska personer i den egna medlemsstaten, Enisa eller CSIRT-enheter i andra medlemsstater.

I EU:s cyberresiliensförordning finns bestämmelser om CSIRT-enhetens uppgiftsskyldigheter gällande sårbarhets- och incidentrapporter enligt artikel 14 och 15 i förordningen.

Artikel 16.2 i EU:s cyberresiliensförordning föreskriver att den CSIRT-enhet som först tog emot en sårbarhets- eller incidentrapport enligt artikel 14 eller 15 ska sprida rapporten via den gemensamma rapporteringsplattformen till de CSIRT-enheter på det territorium där tillverkaren har angett att produkten med digitala element har tillhandahållits.

Artikel 16.3 i EU:s cyberresiliensförordning föreskriver att CSIRT-enheten efter att ha mottagit en rapport om en aktivt utnyttjad sårbarhet i en produkt med digitala element eller om en allvarlig incident som påverkar säkerheten för en produkt med digitala element ska förse marknadskontrollmyndigheterna i sina respektive medlemsstater med den rapporterade information som behövs för att marknadskontrollmyndigheterna ska kunna fullgöra sina skyldigheter enligt EU:s cyberresiliensförordning.

Vidare får CSIRT-enheten under vissa förutsättningar lämna information till användare och allmänheten.

Artikel 14.8 i EU:s cyberresiliensförordning föreskriver att efter att ha fått kännedom om en aktivt utnyttjad sårbarhet eller en allvarlig incident som påverkar säkerheten för produkten med digitala ele-

ment, ska tillverkaren underrätta de drabbade användarna av produkten med digitala element, och när så är lämpligt alla användare, om den sårbarheten eller incidenten och, vid behov, om riskreducering och eventuella korrigerande åtgärder som användarna kan vidta för att begränsa konsekvenserna av denna sårbarhet eller incident, om lämpligt i ett strukturerat, maskinläsbart format som är enkelt att automatiskt behandla. Om tillverkaren underlåter att underrätta användarna av produkten med digitala element i tid får de CSIRT-enheter som utsetts till samordnare som mottagit anmälan lämna sådan information till användarna när detta anses vara proportionellt och nödvändigt för att förebygga eller mildra konsekvenserna av sårbarheten eller incidenten.

Artikel 17.2 i EU:s cyberresiliensförordning föreskriver att CSIRT-enheten får efter samråd med den berörda tillverkaren och, när så är lämpligt, i samarbete med Enisa, informera allmänheten om incidenten eller kräva att tillverkaren gör detta om det är nödvändigt att informera allmänheten för att förebygga eller begränsa en allvarlig incident som påverkar säkerheten för produkten med digitala element eller för att hantera en pågående incident, eller om ett avslöjande av incidenten på annat sätt ligger i allmänhetens intresse.

Analyser och rådgivning

CSIRT-enheten kan genomföra analyser och lämna tekniska råd.

I EU:s cyberresiliensförordning finns bestämmelser om det samarbete som ska ske mellan CSIRT-enheten och marknadskontrollmyndigheterna.

Artikel 52.5 i EU:s cyberresiliensförordning föreskriver att marknadskontrollmyndigheterna får be CSIRT-enheten eller Enisa att ge tekniska råd i frågor som rör genomförandet och efterlevnaden av EU:s cyberresiliensförordning. Vid genomförandet av en utredning enligt artikel 54 får marknadskontrollmyndigheterna be CSIRT-enheten som utsetts till samordnare eller Enisa att tillhandahålla en analys till stöd för utvärderingar av överensstämmelse för produkter med digitala element.

Artikel 54.1 föreskriver att om marknadskontrollmyndigheten i en medlemsstat har tillräckliga skäl att anse att en produkt med digitala element, inbegripet dess sårbarhetshantering, utgör en betydande

cybersäkerhetsrisk, ska den, utan onödigt dröjsmål och om lämpligt i samarbete med den berörda CSIRT-enheten, göra en utvärdering av den berörda produkten med digitala element med avseende på dess uppfyllande av alla krav som fastställs i denna förordning.

11.4.2 Marknadskontrollmyndigheterna

Marknadskontroll med mera

Marknadskontrollmyndigheterna är mottagare av all den information som myndigheterna behöver för marknadskontroll. Marknadskontrollmyndigheterna är även mottagare av den information som behövs för bedömning av medlemsstaternas och unionens beroende av programvarukomponenter.

Marknadskontrollmyndigheterna har rätt att själva begära in information men är även av annan anledning mottagare av information. Informationen kan tillhandahållas av ekonomiska aktörer samt förvaltare av programvara med fri och öppen källkod, CSIRT-enheten, andra marknadskontroll- och tillsynsmyndigheter, Enisa, kommissionen samt andra medlemsstater.

I EU:s cyberresiliensförordning finns bestämmelser om marknadskontrollmyndigheternas uppgiftsskyldigheter som kan innebära att skyddsvärda uppgifter delas med andra.

Artikel 52.4 i EU:s cyberresiliensförordning föreskriver att marknadskontrollmyndigheterna, när så är lämpligt, ska samarbeta med de nationella myndigheter för cybersäkerhetscertifiering som utsetts enligt artikel 58 i förordning (EU) 2019/881⁵ och regelbundet utbyta information med dessa.

Samma artikel föreskriver vidare att när det gäller tillsynen över genomförandet av rapporteringsskyldigheterna enligt artikel 14 i EU:s cyberresiliensförordning ska de utsedda marknadskontrollmyndigheterna samarbeta och regelbundet utbyta information med CSIRT-enheten och Enisa.

Artikel 52.6 i EU:s cyberresiliensförordning föreskriver att marknadskontrollmyndigheterna, när så är relevant, ska samarbeta med andra marknadskontrollmyndigheter som utsetts på grundval av

⁵ Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

annan unionsharmoniseringslagstiftning än EU:s cyberresiliensförordning och regelbundet utbyta information med dessa.

Artikel 52.7 i EU:s cyberresiliensförordning föreskriver att marknadskontrollmyndigheterna vid behov ska samarbeta med de myndigheter som utövar tillsyn över unionens dataskyddsrätt. I detta samarbete ingår att underrätta dessa myndigheter om alla iakttagelser av betydelse för deras fullgörande av sina befogenheter, inbegripet utfärdande av vägledning och råd enligt artikel 52.10 om vägledningen och råden rör behandling av personuppgifter.

Artikel 52.14 i EU:s cyberresiliensförordning föreskriver att för produkter med digitala element som omfattas av EU:s cyberresiliensförordning och som klassificeras som AI-system med hög risk enligt artikel 6 i förordning (EU) 2024/1689⁶ (AI-förordningen) ska de marknadskontrollmyndigheter som utsetts enligt den förordningen vara de myndigheter som ansvarar för den marknadskontroll som föreskrivs i den här förordningen. De marknadskontrollmyndigheter som utsetts enligt AI-förordningen ska vid behov samarbeta med de marknadskontrollmyndigheter som utsetts i enlighet med EU:s cyberresiliensförordning och, när det gäller tillsyn över genomförandet av rapporteringsskyldigheten enligt artikel 14 i EU:s cyberresiliensförordning, med CSIRT-enheten och Enisa. De marknadskontrollmyndigheter som utsetts enligt AI-förordningen ska i synnerhet underrätta de marknadskontrollmyndigheter som utsetts enligt EU:s cyberresiliensförordning om alla iakttagelser av betydelse för fullgörandet av deras uppgifter förbundna med genomförandet av EU:s cyberresiliensförordning.

Artikel 54.1 i EU:s cyberresiliensförordning föreskriver att om marknadskontrollmyndigheten i en medlemsstat har tillräckliga skäl att anse att en produkt med digitala element, inbegripet dess sårbarhetshantering, utgör en betydande cybersäkerhetsrisk, ska den, utan onödigt dröjsmål och om lämpligt i samarbete med den berörda CSIRT-enheten, göra en utvärdering av den berörda produkten med digitala element med avseende på dess uppfyllande av alla krav som fastställs i EU:s cyberresiliensförordning.

⁶ Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

Marknadskontrollmyndigheten ska informera det berörda anmälda organet om detta.

Artikel 54.2 i EU:s cyberresiliensförordning föreskriver att om en marknadskontrollmyndighet har tillräckliga skäl att anse att en produkt med digitala element utgör en betydande cybersäkerhetsrisk mot bakgrund av icke-tekniska riskfaktorer ska den informera de behöriga myndigheter som utsetts eller inrättats enligt artikel 8 i NIS 2-direktivet och när så krävs samarbeta med dessa myndigheter.

Artikel 54.3 i EU:s cyberresiliensförordning föreskriver att om marknadskontrollmyndigheten anser att den bristande överensstämmelsen inte bara gäller det nationella territoriet, ska den informera kommissionen och de andra medlemsstaterna om utvärderingsresultaten och om de åtgärder som den har ålagt den ekonomiska aktören att vidta.

Artikel 54.5 i EU:s cyberresiliensförordning föreskriver att om den ekonomiska aktören inte vidtar lämpliga korrigerande åtgärder ska marknadskontrollmyndigheten vidta alla lämpliga provisoriska åtgärder för att förbjuda eller begränsa tillhandahållandet av produkten med digitala element på sin nationella marknad, dra tillbaka produkten från den marknaden eller återkalla den. Myndigheten ska utan dröjsmål anmäla dessa åtgärder till kommissionen och de andra medlemsstaterna.

Artikel 57.3 i EU:s cyberresiliensförordning föreskriver att medlemsstaten omedelbart ska underrätta kommissionen och de andra medlemsstaterna om de åtgärder som vidtagits enligt artikel 57.1.

Regulatoriska sandlådor

Artikel 33.2 föreskriver att medlemsstaterna får, när så är lämpligt, inrätta regulatoriska sandlådor för cyberresiliens. Eventuella regulatoriska sandlådor för cyberresiliens ska inrättas under marknadskontrollmyndigheternas direkta tillsyn, vägledning och stöd. För det fall regulatoriska sandlådor för cyberresiliens inrättas får marknadskontrollmyndigheterna del av den information som deltagare i sandlådan tillhandahåller.

11.4.3 Den anmälade myndigheten

Den anmälade myndigheten är mottagare av den information som behövs för anmälan och ackreditering av organ för bedömning av överensstämmelse. Myndigheten är utöver det mottagare av information som omfattas av de anmälda organens informationsskyldighet.

I EU:s cyberresiliensförordning finns bestämmelser om den anmälade myndighetens uppgiftsskyldigheter.

Artikel 35.1 i EU:s cyberresiliensförordning föreskriver att medlemsstaterna ska till kommissionen och övriga medlemsstater anmäla vilka organ som fått i uppdrag att utföra bedömningar av överensstämmelse i enlighet med förordningen. Artikel 43.1 föreskriver att de anmälade myndigheterna endast ska anmäla de organ för bedömning av överensstämmelse som har uppfyllt kraven i artikel 39. Ändringar i anmälan ska tillkännages kommissionen och övriga medlemsstater, se artikel 43.6 och 45.1.

Artikel 46 i EU:s cyberresiliensförordning föreskriver att kommissionen ska undersöka alla fall där den hyser tvivel, eller där den upplysts om sådana tvivel, om ett anmält organs kompetens eller ett anmält organs fortsatta uppfyllande av de krav och skyldigheter som det omfattas av. Den anmälade medlemsstaten ska på begäran ge kommissionen all information om grunderna för anmälan eller det berörda organets fortsatta kompetens.

11.4.4 Anmälda organ

Anmälda organ får, i tillämpliga fall, den information som behövs för bedömning av överensstämmelse. Informationen tillhandahålls av tillverkare.

I EU:s cyberresiliensförordning finns bestämmelser om de anmälda organens uppgiftsskyldigheter.

Artikel 49.1 föreskriver att de anmälda organen ska underrätta den anmälade myndigheten om följande:

- a) Avslag på ansökan om intyg, eller begränsning, tillfälligt tillbakadragande eller återkallelse av ett intyg.
- b) Omständigheter som inverkar på räckvidden och villkoren för anmälan.

- c) Begäran från marknadskontrollmyndigheterna om information om bedömningar av överensstämmelse.
- d) På begäran, bedömningar av överensstämmelse som gjorts inom ramen för anmälan och all annan verksamhet, inklusive gränsöverskridande verksamhet och underentreprenad.

Artikel 49.2 i EU:s cyberresiliensförordning föreskriver att de anmälda organen ska ge de andra organ som anmälts enligt förordningen, och som utför liknande bedömningar av överensstämmelse som täcker samma produkter med digitala element, relevant information om frågor som rör negativa och, på begäran, positiva resultat av bedömningar av överensstämmelse.

11.5 Offentlighet och sekretess

Offentlighetsprincipen innebär att allmänheten har rätt till insyn i och tillgång till information om statens och kommunernas verksamhet. Offentlighetsprincipen kommer till uttryck på olika sätt i Sveriges grundlagar, exempelvis genom rätten till yttrande- och meddelarfrihet för tjänstemän, genom domstolsoffentlighet och genom allmänna handlingars offentlighet.

Allmänna handlingar offentlighet regleras i 2 kap. tryckfrihetsförordningen (TF). För att främja ett fritt meningsutbyte, en fri och allsidig upplysning och ett fritt konstnärligt skapande är utgångspunkten enligt 1 § att var och en har rätt att ta del av allmänna handlingar. Rätten får begränsas om det krävs med hänsyn till vissa intressen som räknas upp i 2 §. Sådana godtagbara hänsyn är till exempel rikets säkerhet eller dess förhållande till en annan stat eller en mellanfolklig organisation, intresset av att förebygga eller beivra brott, det allmännas ekonomiska intresse samt skyddet för enskildas personliga eller ekonomiska förhållanden. En begränsning av rätten att ta del av allmänna handlingar ska anges noga i en bestämmelse i en särskild lag eller, om det anses lämpligare i ett visst fall, i en annan lag som den särskilda lagen hänvisar till. Detta gäller även i de fall begränsningen har sitt ursprung i en internationell överenskommelse. En sekretessbestämmelse i ett internationellt avtal eller en EU-rättsakt måste således motsvaras av en särskild tillämplig bestämmelse för att kraven i TF ska vara uppfyllda.

Begränsningar av rätten att ta del av allmänna handlingar regleras främst i offentlighets- och sekretesslagen (2009:400) (OSL). OSL innehåller bestämmelser om myndigheter och vissa andra organs hantering av allmänna handlingar, om tystnadsplikt i det allmännas verksamhet och om förbud att lämna ut allmänna handlingar.

Sekretess enligt OSL innebär enligt 3 kap. 1 § OSL ett förbud mot att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt. Sekretessen innebär alltså såväl handlingssekretess som tystnadsplikt. Till den del sekretessbestämmelserna innebär tystnadsplikt medför de en begränsning av yttrandefriheten enligt regeringsformen.

Förbudet mot att röja eller utnyttja en uppgift gäller enligt 2 kap. 1 § OSL för myndigheter och personer som fått kännedom om uppgiften genom att för det allmännas räkning delta i en myndighets verksamhet på grund av anställning, uppdrag, tjänsteplikt eller liknande grund. För att sekretess även ska gälla privat sektor krävs en särskild bestämmelse om tystnadsplikt.

Enligt 8 kap. 1 och 2 §§ OSL gäller sekretess både i förhållande till enskilda personer och andra myndigheter. Sekretess gäller även inom en myndighet om det där finns olika verksamhetsgrenar som är att betrakta som självständiga i förhållande till varandra. Enligt 8 kap. 3 § OSL gäller dessutom sekretess i förhållande till utländska myndigheter och mellanfolkliga organisationer.

I vissa fall måste dock myndigheter kunna utbyta uppgifter för att kunna utföra sina uppgifter. Vidare kan enskilda i vissa fall ha ett berättigat behov av att få ta del av uppgifter som annars omfattas av sekretess. Sekretessregleringen innehåller därför särskilda sekretessbrytande bestämmelser som innebär att uppgifterna får lämnas ut under vissa förutsättningar. Dessa har utformats efter en intresseavvägning mellan myndigheternas eller enskildas behov av att ta del av uppgifterna och de intressen de aktuella sekretessbestämmelserna avser att skydda. Sekretessbrytande bestämmelser och bestämmelser om undantag från sekretess finns främst i 10 kap. OSL.

Sekretess följer som huvudregel inte med en uppgift när den lämnas till en annan myndighet. För att sekretess ska gälla även hos den mottagande myndigheten krävs enligt 7 kap. 2 § OSL att sekretess följer av en primär sekretessbestämmelse som är tillämplig hos den mottagande myndigheten eller att det finns en bestämmelse om överföring av sekretess. Om inte någon av dessa förutsättningar är upp-

fyllda blir uppgiften offentlig hos den mottagande myndigheten. Motsvarande gäller om en myndighet har direktåtkomst till sekretessreglerade uppgifter hos en annan myndighet.

Vid konkurrens mellan flera tillämpliga sekretessbestämmelser i ett enskilt fall är huvudregeln enligt 7 kap. 3 § OSL att den eller de bestämmelser enligt vilka uppgiften är sekretessbelagd har företräde framför bestämmelser enligt vilka uppgiften ska lämnas ut.

En sekretessbestämmelse är normalt uppbyggd med tre rekvisit: sekretessens föremål, dess räckvidd och dess styrka. Sekretessens styrka bestäms med ett så kallat skaderekvisit. Ett skaderekvisit kan vara antingen rakt eller omvänt. Ett rakt skaderekvisit innebär en presumption för att uppgifterna är offentliga och att sekretess gäller endast om det kan antas att viss skada uppstår om uppgiften lämnas ut. Vid ett omvänt skaderekvisit är utgångspunkten den motsatta; uppgifterna omfattas av sekretess om det inte står klart att uppgiften kan lämnas ut utan att viss skada uppstår. En del bestämmelser innehåller ett kvalificerat rakt skaderekvisit, vilket innebär att det krävs särskilt mycket för att sekretess ska gälla. Sekretess kan även vara absolut, det vill säga uppgiften omfattas av sekretess utan att någon skadeprövning ska göras när uppgiften begärs ut. Om en bestämmelse saknar skaderekvisit innebär det att uppgifter omfattas av absolut sekretess.

11.6 Sekretess till skydd för sårbarhets- och incidentrapporter med mera

Utredningens förslag: Sekretess gäller för uppgift i en sårbarhets- eller incidentrapport enligt artikel 14 eller 15 i EU:s cyberresiliensförordning samt för uppgift om vilka åtgärder som har vidtagits till följd av cyberhotet, tillbudet, sårbarheten eller incidenten om det inte står klart att uppgiften kan röjas utan skada för tillverkaren av produkten med digitala element eller för förvaltaren av programvara med fri och öppen källkod i den mån denne deltar i utvecklingen av produkter med digitala element, för den som ingett rapporten, för användaren eller för den verksamhet där den aktuella produkten används eller för att de åtgärder som tillverkaren eller förvaltaren av programvara med fri och öppen källkod vidtagit motverkas. För uppgift i en allmän handling gäller sekretessen i högst fyrtio år.

Sekretess hindrar inte CSIRT-enheten att underrätta användarna av produkter med digitala element enligt vad som anges i artikel 14.8 i EU:s cyberresiliensförordning eller att informera allmänheten enligt vad som anges i artikel 17.2 i EU:s cyberresiliensförordning.

Rätten att meddela och offentliggöra uppgifter ska inte ha företräde framför den tystnadsplikt som följer av den nya sekretessbestämmelsen.

Utredningens bedömning: 3 § offentlighets- och sekretessförordningen (2009:641) bör gälla diarium över sårbarhets- och incidentrapporter enligt artikel 14 och artikel 15 i EU:s cyberresiliensförordning vid den myndighet som är CSIRT-enhet enligt föreslagna 27 § förordningen (2025:000) om cybersäkerhet⁷, en marknadskontrollmyndighet och en myndighet som rapporterar sådana sårbarheter eller incidenter.

11.6.1 Analys av gällande rätt

Sårbarhets- och incidentrapporter enligt artikel 14 och 15 i EU:s cyberresiliensförordning kan utöver uppgift om vem som givit in rapporten innehålla uppgifter om sårbarheter, säkerhets- och bevakningsåtgärder samt om hot och risker.

När det gäller sekretess till skydd för uppgifter hänförliga till sårbarhets- och incidentrapporter bedömer utredningen att den bestämmelse som är av intresse framför allt är 18 kap. 8 § OSL. Utöver 18 kap. 8 § OSL skulle dock vissa uppgifter hänförliga till sårbarhets- och incidentrapporter eventuellt även kunna omfattas av annan sekretessreglering. Det gäller till exempel försvarssekretess enligt 15 kap. 2 § OSL som skulle kunna aktualiseras för till exempel uppgifter om sårbarheter eller incidenter som sammantaget skulle kunna antas utgöra en sådan fara för Sveriges säkerhet om de röjs att försvarssekretess gäller. Bestämmelsen är emellertid endast tillämplig under vissa specifika förutsättningar vilket är anledningen till att den

⁷ I delbetänkandet *Nya regler om cybersäkerhet* (SOU 2024:18) föreslås Myndigheten för samhällsskydd och beredskap vara CSIRT-enhet och att det regleras i 27 § i en ny förordning om cybersäkerhet. I slutbetänkandet *Samlade förslag för ökad cybersäkerhet* (SOU 2025:79) föreslår dock den utredningen att Försvarets radioanstalt ska vara CSIRT-enhet och att förslagna 27 § ska ändras i enlighet med det.

inte berörs vidare och att endast 18 kap. 8 § OSL behandlas i utredningens vidare analys.

18 kap. 8 § OSL reglerar sekretess avseende säkerhets- eller bevakningsåtgärder. Specifikt punkten 3 i den bestämmelsen är av relevans här. Enligt 18 kap. 8 § 3 OSL gäller sekretess för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd som avser telekommunikation eller system för automatiserad behandling av information om det kan antas att syftet med åtgärden motverkas om uppgiften röjs.

Med telekommunikation avses överföring av meddelanden med tråd, radio eller liknande metod. Med system för automatiserad behandling av information avses system där datorer, telekommunikation eller annan teknisk utrustning samverkar för att insamla, ordna, bearbeta, söka eller distribuera information. Bestämmelsen avser till exempel att skydda funktioner för användning av lösenord, loggning och kryptering, installation av brandväggar och antivirusprogram samt administrativa rutiner för till exempel utdelning av lösenord eller bevakning av loggar och larm. Något som däremot faller utanför sekretessens räckvidd är beskrivningar av hur ett program fungerar i stora drag och vilka typer av uppgifter som bearbetas i ett program.⁸

Bestämmelsen föreskriver ett rakt skaderekvisit, det vill säga det råder en presumtion för offentlighet.

18 kap. 8 § 3 OSL har analyserats i slutbetänkandet *Motståndskraft i samhällsviktiga tjänster* (SOU 2024:64)⁹ gällande incidentrapporteringen enligt den av utredningen föreslagna cybersäkerhetslagen (2025:000). Utredningen har lämnat förslag på en ny sekretessbestämmelse kopplad till incidentrapporteringen. Av propositionen 2025/26:28 *Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag* framgår att regeringen i huvudsak delar utredningens bedömningar och förslag.¹⁰

Av motsvarande skäl som anges i prop. 2025/26:28 och SOU 2024:64 råder det även i detta sammanhang en osäkerhet om sårbarhets- och incidentrapporter alltid kan rymmas inom begreppet ”säkerhets- eller bevakningsåtgärd” samt om lydelsen i punkten 3 kan antas relevant i ett modernt språkbruk och dessutom heltäck-

⁸ Prop. 2003/04:93, *Några frågor om sekretess, m.m.*, s. 82.

⁹ Sid. 253 ff.

¹⁰ Sid. 194 ff.

ande för de uppgifter som behöver omfattas av reglering, samt om ett rakt skaderekvisit kan verka begränsande för viljan att rapportera sårbarheter och incidenter. Sedan 18 kap. 8 § OSL trädde i kraft har utvecklingen på it-området varit omfattande. Produkter har utvecklats på ett sådant sätt som inte var möjligt att förutse vid bestämmelsens tillkomst. Dessutom har nya metoder att både angripa och skydda produkter tillkommit liksom att cyberhoten har ökat och förändrats. Det kan inte uteslutas att det kan finnas uppgifter i sårbarhets- och incidentrapporter som, även om uppgifterna är mycket känsliga, inte skulle omfattas av sekretess enligt aktuell bestämmelse. Detta leder till att uppgifter som bör omfattas av sekretess i stället blir offentliga.

Det är av vikt att det finns en tydlig sekretessreglering avseende sårbarhets- och incidentrapporter enligt artikel 14 och 15 i EU:s cyberresiliensförordning. Ett system kring rapportering av sårbarheter och incidenter bygger på att de som ska rapportera har en hög tilltro till systemet och att känsliga uppgifter ges ett fullgott skydd. Om tilltron minskar kan aktörerna till exempel förhålla sig restriktiva till rapporteringen och utelämna uppgifter som de anser är känsliga. Detta riskerar att motverka ändamålet med rapporteringen vilket kan medföra brister i cybersäkerheten för produkter. Rapporterna kan innefatta uppgifter som vid en första anblick kan verka harmlösa, men som i ett större perspektiv kan få stora konsekvenser om uppgifterna röjs. Exempel på sådana uppgifter är uppgifter som kan framkomma i ett tidigt skede under ett it-angrepp där omfattningen av angreppet ännu inte blivit känt.

Intresset av att myndigheterna ska kunna motverka bland annat cyberattacker och i förlängningen också bidra till att förebygga och beivra brott samt intresset av att svenska myndigheter kan delta på ett effektivt sätt i det internationella samarbetet enligt EU:s cyberresiliensförordning, får enligt utredningen anses väga tyngre än det motstående intresset av insyn i myndigheternas verksamhet.

11.6.2 En ny sekretessbestämmelse för uppgift i sårbarhets- och incidentrapporter samt en ny sekretessbrytande bestämmelse

Enligt vad som ovan anförts bedömer utredningen att 18 kap. 8 § 3 OSL endast delvis tillgodoser behovet av skydd för uppgifter som kan komma att behandlas inom ramen för rapportering av sårbarheter och incidenter enligt artikel 14 och 15 i EU:s cyberresiliensförordning. Vissa uppgifter skulle sannolikt kunna hänföras till 18 kap. 8 § 3 OSL medan andra uppgifter inte nödvändigtvis har ett givet sekretesskydd. Osäkerheter avseende huruvida uppgifter om en rapports förekomst, uppgifter som beskriver en sårbarhet eller incident, uppgift om vidtagna korrigerande eller riskreducerande åtgärder eller uppgift om att sådana åtgärder inte vidtagits alls samt uppgift om vem som har rapporterat omfattas av en sekretessreglering eller inte gör att utredningen bedömer att det är motiverat att införa en ny sekretessbestämmelse.

Sekretessens föremål och räckvidd

Föremålet för sekretessen i den nya bestämmelsen är uppgifter i en sårbarhets- eller incidentrapport enligt artikel 14 eller 15 i EU:s cyberresiliensförordning samt för uppgift om åtgärd som vidtagits till följd av rapporterade cyberhot, tillbud, sårbarheter eller incidenter. Bestämmelsen gäller således inte bara obligatoriska sårbarhets- och incidentrapporter utan även frivilliga rapporter.

Sekretess gäller oaktat inom vilken offentlig verksamhet rapporten finns i.

Vidare gäller sekretess om det inte står klart att uppgiften kan röjas utan skada för tillverkaren av produkten med digitala element, för förvaltaren av programvara med fri och öppen källkod i den mån denne deltar i utvecklingen av produkter med digitala element, för den som ingett rapporten eller för den verksamhet där den aktuella produkten används eller utan att de åtgärder som har vidtagits motverkas. Genom denna formulering säkerställs att alla som inger rapporter omfattas av sekretessregleringen men även tillverkare samt förvaltare av programvara med fri och öppen källkod för det fall någon annan än dessa inger en rapport. Även verksamheter där den aktuella produkten används omfattas. Utöver uppgift om en rapport

förekomst och uppgifter i rapporten omfattas även uppgifter om åtgärder som vidtagits med anledning av cyberhot, tillbud, sårbarheter eller incidenter. Regleringen syftar till att motverka negativa effekter för olika aktörers pågående och framtida säkerhetsarbete, att förhindra avslöjandet av säkerhetsbrister eller konsekvenser av en sårbarhet eller incident för olika verksamheter. Det syftar även till att uppgifter om vem som är ingivare av en sårbarhets- eller incidentrapport sekretessregleras eftersom det i vissa fall kan vara en känslig uppgift. Till exempel kan det ge information till en antagonist om ett angrepp har lyckats eller har upptäckts och om ingivarens it-system är sårbart för attacker.

När det gäller den nya sekretessbestämmelsen som föreslås i prop. 2025/26:28, avseende incidentrapporteringen enligt den föreslagna cybersäkerhetslagen (2025:000), formuleras bestämmelsen så att sekretess gäller om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens *framtida verksamhet* skadas eller syftet med vidtagen åtgärd motverkas. Formuleringen syftar till att förtydliga att det framför allt är fråga om sådana begränsningar som krävs med hänsyn till intresset av att förebygga och beivra brott. Utredningen har övervägt en liknande formulering i den nu föreslagna sekretessregleringen men funnit det svårt att formulera bestämmelsen på detta sätt eftersom sekretessen inte bara avser att skydda tillverkarens verksamhet utan även den som till exempel frivilligt har ingett en sårbarhets- eller incidentrapport, till skillnad från förslaget i prop. 2025/26:28, och i detta fall är skyddsintresset den som i sig har ingett rapporten och inte dennes framtida verksamhet.

Bestämmelsen ska träda i kraft den 11 september 2026, se vidare avsnitt 14.4.

Undantag från sekretessen

Sekretess enligt den föreslagna bestämmelsen ska dock inte hindra CSIRT-enhetens informationsdelning till enskilda som krävs enligt artikel 14.8 och 17.2 i EU:s cyberresiliensförordning.

Enligt artikel 14.8 får CSIRT-enheten under vissa förutsättningar informera användare av produkter med digitala element som drabbats av en aktivt utnyttjad sårbarhet eller en allvarlig incident om tillver-

karen underlåter att göra detta. Enligt artikel 17.2 får CSIRT-enheten under vissa förutsättningar och efter samråd med den berörda tillverkaren informera allmänheten om en incident.

Enligt 8 kap. 1 § OSL får en uppgift som är sekretessbelagd enligt OSL inte röjas för enskilda eller för andra myndigheter, om inte annat anges i OSL eller i lag eller förordning som OSL hänvisar till.

För att möjliggöra den informationsdelning som föreskrivs i artikel 14.8 och 17.2 i EU:s cyberresiliensförordning krävs en sekretessbrytande bestämmelse.

När det gäller informationsdelning enligt artikel 14.8 och 17.2 i EU:s cyberresiliensförordning gör utredningen bedömningen att det saknas en heltäckande sekretessbrytande bestämmelse för att säkerställa att denna informationsdelning kan ske. Avseende artikel 17.2 skulle dock 12 kap. 2 § OSL i vissa fall kunna tillämpas. Bestämmelsen innebär att en enskild helt eller delvis kan häva sekretess som gäller till skydd för honom eller henne. Artikel 17.2 förutsätter att CSIRT-enheten först samråder med den berörda tillverkaren innan allmänheten informeras. Om tillverkaren i samband med det godkänner att sekretessbelagda uppgifter delas med allmänheten skulle den sekretessbrytande bestämmelsen i 12 kap. 2 § OSL kunna tillämpas. Det skulle dock vara möjligt att det uppstår en situation där CSIRT-enheten ser ett behov av att informera allmänheten enligt artikel 17.2 men där den enskilde inte vill häva sekretessen som gäller. För en sådan situation saknas således en sekretessbrytande bestämmelse.

Utredningen föreslår därför en ny sekretessbrytande bestämmelse som innebär att sekretessen till skydd för sårbarhets- och incidentrapporter med mera inte hindrar CSIRT-enheten att underrätta användarna av produkter med digitala element enligt vad som anges i artikel 14.8 i EU:s cyberresiliensförordning eller att informera allmänheten enligt vad som anges i artikel 17.2 i EU:s cyberresiliensförordning.

Frågan om informationsdelning mellan myndigheter, inklusive sekretessbrytande bestämmelser och överföring av sekretess, behandlas i avsnitt 11.14.

Sekretessens styrka (skaderekvisit)

Av motsvarande skäl som anförs i prop. 2025/26:28 och SOU 2024:64 anser utredningen att den nya sekretessbestämmelsen till skydd för sårbarhets- och incidentrapporter, till skillnad från vad som gäller enligt 18 kap. 8 § 3 OSL, bör utformas med ett omvänt skaderekvisit, dvs. en presumtion för sekretess. Ett omvänt skaderekvisit måste dock vägas mot behovet av allmänhetens intresse av tillgång till uppgifter om sårbarheter och incidenter.

Enligt artikel 14.8 i EU:s cyberresiliensförordning ska en tillverkare, efter att ha fått kännedom om en aktivt utnyttjad sårbarhet eller en allvarlig incident, underrätta de drabbade användarna av produkten med digitala element, och när så är lämpligt alla användare, om den sårbarheten eller incidenten och, vid behov, om riskreducering och eventuella korrigerande åtgärder som användarna kan vidta för att begränsa konsekvenserna av denna sårbarhet eller incident, om lämpligt i ett strukturerat, maskinläsbart format som är enkelt att automatiskt behandla. Om tillverkaren underlåter att underrätta användarna i tid får CSIRT-enheten lämna sådan information till användarna när detta anses vara proportionellt och nödvändigt för att förebygga eller mildra konsekvenserna av sårbarheten eller incidenten. Enligt artikel 17.2 i EU:s cyberresiliensförordning får CSIRT-enheten efter samråd med den berörda tillverkaren och, när så är lämpligt, i samarbete med Enisa, informera allmänheten om incidenten eller kräva att tillverkaren gör detta om det är nödvändigt att informera allmänheten för att förebygga eller begränsa en allvarlig incident som påverkar säkerheten för produkten med digitala element eller för att hantera en pågående incident, eller om ett avslöjande av incidenten på annat sätt ligger i allmänhetens intresse. Enligt artikel 17.3 i EU:s cyberresiliensförordning ska Enisa vartannat år, på grundval av inkomna rapporter, utarbeta en teknisk rapport om nya trender i fråga om cybersäkerhetsrisker i produkter med digitala element. Enisa ska även, enligt artikel 17.5 i EU:s cyberresiliensförordning, efter det att en säkerhetsuppdatering eller någon annan form av korrigerande eller riskreducerande åtgärd finns tillgänglig, i samförstånd med tillverkaren av den berörda produkten med digitala element, lägga till den allmänt kända sårbarhet som rapporterats enligt artikel 14.1 eller 15.1 i förordningen i den europeiska sårbarhetsdata-

basen¹¹. Vidare gäller sekretess enligt den föreslagna bestämmelsen endast så länge skaderekvisitet är uppfyllt. Uppgifter i sårbarhets- och incidentrapporter, eller uppgifter om åtgärder som har vidtagits, kan ofta lämnas ut relativt tidigt efter att en sårbarhet upptäckts eller en incident inträffat. Så snart åtgärder för att hantera sårbarheten eller incidenten har vidtagits bör uppgifter inte sällan kunna lämnas ut.

Underrättelser till användare, information till allmänheten, Enisas publikationer, den europeiska sårbarhetsdatabasen och det faktum att eventuell sekretess för uppgifter om sårbarheter och incidenter många gånger endast gäller en begränsad tid gör att allmänhetens intresse av tillgång till uppgifter om sårbarheter och incidenter tillgodoses. Utredningen anser genom detta att offentlighetsintresset är tillgodosett och att ett omvänt skaderekvisit kan gälla.

Sekretesstid

Trots vad som ovan angetts om att sekretess många gånger endast kommer att gälla en begränsad tid kan emellertid sekretessen för vissa uppgifter behöva kvarstå en längre tid. Utredningen har därför, av motsvarande skäl som anförs i prop. 2025/26:28 och SOU 2024:64, bedömt att sekretessen bör gälla upp till 40 år, vilket även är samma sekretesstid som gäller för incidentrapporter i domstolar med mera enligt 18 kap. 8 a § OSL.

Bestämmelsens placering

Som även anförs i prop. 2025/26:28 och SOU 2024:64 bör en ny sekretessreglering kopplad till incidentrapportering kunna placeras i avslutning till 18 kap. 8 § OSL då den kompletterar nämnda paragraf och i huvudsak har samma skyddsintresse. Förslaget gäller i första hand skydd för allmänna intressen men får ändå till effekt att uppgifter om enskilda indirekt skyddas så länge uppgifterna hänför sig till sårbarhets- och incidentrapporter enligt artikel 14 eller 15 i EU:s cyberresiliensförordning.

¹¹ Den europeiska sårbarhetsdatabasen som inrättas genom artikel 12.2 i Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148.

Rätten att meddela och offentliggöra uppgifter bör begränsas

Sekretess innebär enligt 3 kap. 1 § OSL ett förbud att röja en uppgift, vare sig det sker genom utlämnande av allmän handling, muntligt eller på annat sätt. Den rätt att meddela och offentliggöra uppgifter som följer av yttrandefrihetsgrundlagarna, den så kallade meddelarfriheten, har emellertid som huvudregel företräde framför tystnadsplikten. I likhet med vad som anförs i prop. 2025/26:28 och SOU 2024:64 finns det enligt utredningens bedömning tillräckliga skäl att införa ett undantag från rätten att meddela och offentliggöra uppgifter, trots att det vid prövningen om det ska göras ett undantag bör iaktas stor återhållsamhet. Det rör sig här bland annat om sekretess med ett omvänt skaderekvisit och där ett offentliggörande skulle kunna orsaka skada för tillverkare av en produkt med digitala element, den som har rapporterat en sårbarhet eller incident enligt artikel 14 eller 15 i EU:s cyberresiliensförordning samt för de verksamheter där produkten används. Som utredningen anført ovan tillgodoses intresset av insyn genom underrättelser till användare, information till allmänheten, Enisas publikationer, den europeiska sårbarhetsdatabasen och det faktum att eventuell sekretess för uppgifter många gånger endast gäller en begränsad tid. En inskränkning av meddelarfriheten är mot den bakgrunden motiverad. Rätten att meddela och offentliggöra uppgifter bör därför inte ha företräde framför den tystnadsplikt som följer av utredningens föreslagna bestämmelse i 18 kap. OSL. Detta gäller redan i dag för bestämmelsen i 18 kap. 8 §. Av bestämmelsen i 18 kap. 19 § OSL framgår i vilka fall den tystnadsplikt som följer av en bestämmelse om sekretess i 18 kap. OSL inskränker rätten att meddela och offentliggöra uppgifter. Den föreslagna bestämmelsen bör därför läggas till i uppräknningen i 18 kap. 19 § OSL.

Synpunkter från Försvarets radioanstalt och Myndigheten för samhällsskydd och beredskap

Försvarets radioanstalt (FRA) och Myndigheten för samhällsskydd och beredskap (MSB) har till utredningen framfört att de visserligen ser positivt på den föreslagna sekretessregleringen till skydd för sårbarhets- och incidentrapporter men att det måste säkerställas att regleringen inte hindrar att åtgärder kan vidtas för att skydda samhällets

funktionalitet. FRA och MSB framför att det är angeläget att hantera sekretessfrågor avseende incident- och sårbarhetsrapportering enligt olika regelverk på ett samlat sätt. Det finns ett behov av en samlad översyn av de förslag om sekretesskydd som lämnas i olika betänkan- den och som avser gälla i sådan verksamhet som kommer bedrivas av det nationella cybersäkerhetscentret (NCSC) vid FRA. I det ar- betet är det även viktigt att närmare utreda hur olika regleringars syften ska omhändertas så att målkonflikter inte uppstår. Det kan till exempel handla om regleringen i 3 § 2 förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt (NCSC-förordningen) där det anges att centret särskilt ska lämna råd och stöd till privata och offentliga aktörer i frågor om hot, sår- barheter och risker med koppling till cybersäkerhet samt kraven på att skyndsamt sprida information om sårbarheter eller cyberhot för att skydda användare och infrastruktur enligt artikel 11.3 i NIS 2- direktivet visavi kraven om informationsplikt och samråd med till- verkare för att undvika att sårbarheter utnyttjas innan de är åtgär- dade i artiklarna 14 och 17 i EU:s cyberresiliensförordning.

Utredningens bedömning är att den föreslagna bestämmelsen om sekretess för uppgift i en sårbarhets- eller incidentrapport behövs för att säkerställa en hög tilltro till systemet, för att känsliga uppgifter skyddas och för att brott ska kunna förebyggas och beivras. Befint- lig reglering i OSL och utredningens förslag på sekretessbrytande be- stämmelse möjliggör den informationsdelning till enskilda som före- skrivs i EU:s cyberresiliensförordning (artikel 14.8 och 17.2). I övrigt bedömer utredningen att de frågor som FRA och MSB lyfter inte är något som kan hanteras inom denna utrednings uppdrag men anser att en sådan översyn behöver övervägas i det fortsatta arbetet i den utsträckning det är möjligt och lämpligt.

Samlade förmågor för ökad cybersäkerhet (SOU 2025:79)

I betänkandet *Samlade förmågor för ökad cybersäkerhet* (SOU 2025:79) föreslås en överföring av arbetsuppgifter från MSB till FRA. Det gäller bland annat uppgiften att vara CSIRT-enhet.

SOU 2025:79 överlämnades den 1 juli 2025. I betänkandet lämnas förslag om ändringar av vissa förslag som lades fram i prop. 2025/26:28 och i SOU 2024:64. Bland annat gäller det förslaget om en ny sek-

retessbestämmelse för uppgifter i incidentrapporter. SOU 2025:79 föreslår i detta sammanhang i stället att en ny sekretessbestämmelse införs i 40 kap. 7 g § OSL som skyddar uppgifter om enskildas personliga och ekonomiska förhållanden som förekommer hos FRA. Bestämmelsen föreslås ha ett omvänt skaderekvisit.

Förslaget i SOU 2025:79 skulle kunna vara ett alternativ till utredningens förslag att införa en ny sekretessbestämmelse för uppgifter i sårbarhets- och incidentrapporter enligt artikel 14 och 15 i EU:s cyberresiliensförordning. Förslaget i SOU 2025:79 förutsätter emellertid en del kompletteringar.

Visserligen bedömer utredningen att det är tillräckligt att en ny sekretessreglering avgränsas till uppgifter i sårbarhets- och incidentrapporter enligt artikel 14 och 15 i EU:s cyberresiliensförordning men konstaterar att det är uppgifter som faller in under det mycket bredare tillämpningsområdet för förslaget i SOU 2025:79 (uppgifter om enskildas personliga och ekonomiska förhållanden). Förslaget i SOU 2025:79 gäller dock endast när uppgifterna förekommer hos FRA. Det är inte tillräckligt när det gäller uppgifterna i sårbarhets- och incidentrapporter enligt EU:s cyberresiliensförordning. Dessa uppgifter behöver kunna omfattas av en sekretessreglering, inte bara hos FRA, utan även när de finns hos marknadskontrollmyndigheterna och andra myndigheter som ska kunna ta del av uppgifterna enligt förordningen. För att förslaget i SOU 2025:79 ska fungera utifrån EU:s cyberresiliensförordning behöver förslaget således kompletteras med en sekretessreglering även hos marknadskontrollmyndigheterna (för det fall en tillverkare inger en sårbarhets- eller incidentrapport direkt till någon av marknadskontrollmyndigheterna) samt sekretessbrytande bestämmelser som tillgodoser förordningens krav på utlämnande av information och bestämmelser om överföring av sekretess.

11.6.3 En ny sekretessbestämmelse för diarier för sårbarhets- och incidentrapporter

En uppgift om förekomsten av en sårbarhets- och incidentrapport i sig kan vara en känslig uppgift som bör sekretessregleras. Dessutom innehåller, som tidigare redovisats, EU:s cyberresiliensförordning bestämmelser som innebär att CSIRT-enheter ska kunna undanhålla eller skjuta upp spridningen av sårbarhets- och incidentrapporter.

Diarier över ärenden och allmänna handlingar är normalt sett offentliga hos myndigheter. I 3 § OSF finns det undantag från den principen genom att vissa diarier hos vissa myndigheter i sin helhet får omfattas av sekretess.

Av motsvarande skäl som anförs i SOU 2024:64 bör diarier som innehåller uppgifter om sårbarhets- och incidentrapporter enligt artikel 14 och 15 i EU:s cyberresiliensförordning omfattas av sekretess och därmed skyddas dessa från de negativa effekter som offentlighet för uppgifterna kan medföra. En ny bestämmelse om sekretess bör därför införas i 3 § offentlighets- och sekretessförordningen (2009:641) som gäller diarium över sårbarhets- och incidentrapporter enligt artikel 14 och artikel 15 i EU:s cyberresiliensförordning. Bestämmelsen bör träda i kraft den 11 september 2026, se vidare avsnitt 14.4.

CSIRT-enheten är mottagare av rapporterna och ska förse marknadskontrollmyndigheterna med den rapporterade informationen som behövs för tillsyn. Utöver det kan en myndighet komma att vara den som inger en sårbarhets- och incidentrapporter enligt artikel 14 eller 15 i EU:s cyberresiliensförordning. Bestämmelsen bör således gälla diarier hos CSIRT-enheten, marknadskontrollmyndigheter och myndighet som rapporterar sårbarheter eller incidenter.

11.7 Sekretess till skydd för risk- och sårbarhetsanalyser med mera

Utredningens bedömning: Bestämmelsen i 18 kap. 13 § offentlighets- och sekretesslagen (2009:400) ger ett tillräckligt skydd för risk- och sårbarhetsanalyser med mera.

Enligt 18 kap. 13 § OSL gäller sekretess för uppgift som hänför sig till en myndighets verksamhet som består i risk- och sårbarhetsanalyser avseende fredstida krissituationer, planering och förberedelser inför sådana situationer eller hantering av sådana situationer, om det kan antas att det allmännas möjligheter att förbygga och hantera fredstida kriser motverkas om uppgiften röjs.

CSIRT-enheten kan komma att göra vissa analyser med mera till stöd för marknadskontroll, jämför till exempel artikel 52.5 i EU:s

cyberresiliensförordning. Frågan är om sekretessregleringen i 18 kap. 13 § OSL kan anses omfatta den typen av analyser.

18 kap. 13 § OSL har analyserats i SOU 2024:64. Den utredningen konstaterar att bestämmelsen i praxis har tillämpats för skilda slag av analyser.¹² Denna praxis följer även av motiven i propositionen av den aktuella bestämmelsen som anger att begreppet ”verksamhet som består i risk- och sårbarhetsanalyser avseende fredstida krissituationer eller planering och förberedelser för hantering av sådana situationer” även innefattar ett insamlande av sådana uppgifter som behövs i verksamheten när detta insamlande utförs av andra handläggare inom myndigheten än de som primärt arbetar med analys-, planerings- och förberedelsearbetet.¹³ Genom att sekretessregleringen i 18 kap. 13 § OSL berör ett flertal olika analyser torde bestämmelsen utgöra tillräckligt skydd för CSIRT-enhetens verksamhet i denna del. Det saknas skäl att införa nya bestämmelser om sekretess till skydd för risk- och sårbarhetsanalyser med mera.

11.8 Sekretess till skydd för enskild vid marknads kontroll och utredning

Utredningens bedömning: Bestämmelsen om sekretess för uppgifter om enskildas affärs- eller driftsförhållanden vid tillsyn med mera i 30 kap. 23 § offentlighets- och sekretesslagen (2009:400) görs tillämplig genom att en ny punkt om marknads kontroll och utredning enligt EU:s cyberresiliensförordning och anslutande föreskrifter införs i bilagan till offentlighets- och sekretessförordningen (2009:641). Bestämmelsen ska inte gälla beslut i ärenden. Sekretessen gäller inte heller om förhållande som rör människors hälsa och säkerhet, miljön eller redligheten i handeln eller ett liknande allmänintresse har sådan vikt att uppgiften bör lämnas ut.

Uppgifter som marknads kontrollmyndigheterna mottar och samlar in med stöd av EU:s cyberresiliensförordning kan innehålla känsliga uppgifter om enskilda. Även de risk- och sårbarhetsanalyser som CSIRT-enheten kan komma att göra, jämför till exempel artikel 52.5

¹² Exempelvis har delar av en pandemiplan ansetts omfattas av sekretess enligt 18 kap. 13 § OSL, se Kammarrätten i Göteborgs dom av den 21 juli 2021 i mål nr 1727-21.

¹³ Prop. 2004/05:5, *Vårt framtida försvar*, s. 263.

i EU:s cyberresiliensförordning, skulle kunna innehålla känsliga uppgifter om enskilda.

30 kap. OSL reglerar sekretess till skydd för enskild i verksamhet som avser tillsyn med mera i fråga om näringslivet. Kapitlet innehåller både sekretessbestämmelser som tar sikte på särskilda sektorer och generella bestämmelser.

Enligt 30 kap. 23 § OSL gäller sekretess, i den utsträckning regeringen meddelar föreskrifter om det, i en statlig myndighets verksamhet som består i bland annat utredning, tillståndsgivning, tillsyn eller stödverksamhet med avseende på produktion, handel, transportverksamhet eller näringslivet i övrigt för uppgift om en enskilds affärs- eller driftsförhållanden, uppfinningar eller forskningsresultat, om det kan antas att den enskilde lider skada om uppgiften röjs. Sekretess gäller även för uppgift om andra ekonomiska eller personliga förhållanden för den som har trätt i affärsförbindelse eller liknande förbindelse med den som är föremål för myndighetens verksamhet.

Begreppet tillsyn bör inte ges en alltför snäv tolkning utan får anses omfatta alla de fall där en myndighet har en övervakande eller styrande funktion i förhållande till näringslivet. Även rådgivning som sker som ett led i en myndighets tillsynsverksamhet anses falla in under begreppet tillsyn.¹⁴

Första punkten i bestämmelsen föreskriver ett rakt skaderekvisit, dvs. det råder en presumtion för offentlighet. Sekretessen i andra punkten är absolut.

Som framgår av bestämmelsen ger den inte i sig själv upphov till någon sekretess utan förutsätter att regeringen föreskriver om sekretess. Sådana föreskrifter har meddelats i 9 § offentlighets- och sekretessförordningen (2009:641) (OSF) och i bilagan till den förordningen.

Sekretess gäller enligt punkten 12 i bilagan utredning, tillståndsgivning och tillsyn enligt lagen (2011:791) om ackreditering och teknisk kontroll eller enligt motsvarande äldre föreskrifter. Bestämmelsen tillgodoser behovet av sekretessreglering avseende uppgifter om organ för bedömning av överensstämmelse inom ramen för anmälan och ackreditering av dessa hos den anmälade myndigheten enligt EU:s cyberresiliensförordning för de fall 30 kap. 24 § OSL inte gäller i stället, se avsnitt 11.11. Det saknas således skäl att införa nya bestämmelser till skydd för dessa organ.

¹⁴ Prop. 1979/80:2 Del A, *Förslag till sekretesslag m.m.*, s. 235.

I syfte att säkerställa att även den marknadskontroll som föreskrivs i EU:s cyberresiliensförordning och de risk- och sårbarhetsanalyser som CSIRT-enheten kan komma att genomföra omfattas av sekretessregleringen i 30 kap. 23 § OSL föreslår utredningen att det införs en ny punkt i bilagan till OSF som avser detta. I likhet med vad som gäller vid marknadskontroll enligt EU:s marknadskontrollförordning är allmänhetens intresse så starkt att beslut i ärenden bör undantas från sekretesskyddet. Det gäller även uppgifter om förhållanden som rör människors hälsa och säkerhet, miljön eller redligheten i handeln som bör lämnas ut om intresset av allmän kännedom har sådan vikt att uppgifterna bör lämnas ut. Bestämmelsen gäller om inte 30 kap. 24 § OSL i stället gäller, se avsnitt 11.11.

Frågan om sekretessreglering för ekonomiska aktörer i egenskap av klienter till anmälda organ behandlas i avsnitt 11.13 om tystnadsplikt.

11.9 Sekretess till skydd för enskild inom ramen för regulatoriska sandlådor för cyberresiliens

Utredningens förslag: Sekretess gäller i verksamhet avseende regulatorisk sandlåda för cyberresiliens enligt artikel 33 i EU:s cyberresiliensförordning för uppgift om en enskilds affärs- eller driftförhållanden, uppfinningar eller forskningsresultat om det kan antas att den enskilde lider avsevärd skada om uppgiften röjs. För uppgift i en allmän handling gäller sekretessen i högst tjugo år.

11.9.1 Analys av gällande rätt

Artikel 33.2 i EU:s cyberresiliensförordning föreskriver att medlemsstaterna får, när så är lämpligt, inrätta regulatoriska sandlådor för cyberresiliens. Frågan om regulatoriska sandlådor för cyberresiliens behandlas ytterligare i avsnitt 12.5.

Uppgifter som behandlas inom ramen för en regulatorisk sandlåda för cyberresiliens kan vara känsliga för enskilda, på samma sätt som uppgifter som behandlas inom ramen för bedömning av överensstämmelse samt marknadskontroll.

När det gäller sekretess till skydd för uppgifter i denna typ av verksamhet bedömer utredningen att den bestämmelse som är av intresse framför allt är 30 kap. 23 §.

30 kap. 23 § OSL gäller, i den utsträckning regeringen meddelar föreskrifter om det, i en statlig myndighets verksamhet som består i bland annat utredning, tillståndsgivning, tillsyn eller stödverksamhet med avseende på produktion, handel, transportverksamhet eller näringslivet i övrigt. Som anförts i avsnitt 11.8 bör begreppet tillsyn i 30 kap. 23 § OSL inte ges en alltför snäv tolkning. Artikel 33.2 i EU:s cyberresiliensförordning föreskriver att de regulatoriska sandlådorna ska inrättas under marknadskontrollmyndigheternas direkta tillsyn, vägledning och stöd. Frågan är om regulatoriska sandlådor för cyberresiliens därmed kan omfattas av tillämpningsområdet för 30 kap. 23 § OSL.

Artikel 33.2 i EU:s cyberresiliensförordning föreskriver att regulatoriska sandlådor för cyberresiliens ska tillhandahålla kontrollerade provmiljöer för innovativa produkter med digitala element för att underlätta utvecklingen, utformningen, valideringen och provningen av dem i syfte att uppfylla kraven i denna förordning under en begränsad tidsperiod innan de släpps ut på marknaden.

De regulatoriska sandlådorna för cyberresiliens har således ett innovationsfrämjande syfte till skillnad från 30 kap. 23 § OSL som snarare handlar om myndigheters övervakande eller styrande funktion i förhållande till näringslivet. Utredningen bedömer att verksamhet som består i en regulatorisk sandlåda för cyberresiliens således faller utanför regleringen i 30 kap. 23 § OSL. Till stöd för den bedömningen kan även nämnas begreppet ”tillsyn” i artikel 33.2 i EU:s cyberresiliensförordning där den engelska språkversionen använder begreppet ”supervision”.

Det saknas således enligt utredningen en sekretessreglering till skydd för uppgifter om enskilda affärs- och driftförhållanden, uppfinningar och forskningsresultat när uppgifterna finns i en statlig myndighets verksamhet avseende regulatorisk sandlåda för cyberresiliens. Det är dock av vikt att det finns en sekretessreglering för dessa uppgifter. För att tillverkare ska vilja delta i en regulatorisk sandlåda krävs en tilltro till regulatoriska sandlådor för cyberresiliens och att känsliga uppgifter ges ett fullgott skydd.

11.9.2 En ny sekretessbestämmelse för uppgift om enskild i verksamhet som består i regulatoriska sandlådor för cyberresiliens

I syfte att säkerställa att regulatoriska sandlådor för cyberresiliens omfattas av en sekretessreglering föreslår utredningen att det införs en bestämmelse som utökar sekretessregleringen i 30 kap. 23 § OSL till att även omfatta verksamhet avseende regulatoriska sandlådor för cyberresiliens. Utredningen anser att en ny bestämmelse om detta kan placeras i 31 kap. OSL som innehåller bestämmelser om sekretess till skydd för enskild i annan verksamhet med anknytning till näringslivet. För att undvika att en regulatorisk sandlåda blir en konkurrensfördel för den som deltar samt för att främja innovation och utveckla regulatorisk tillämpning anser utredningen att bestämmelsen ska ha ett kvalificerat rakt skaderekvisit. Det innebär att det för sekretess krävs att den skada som kan antas uppkomma genom uppgiftens röjande ska vara avsevärd. Bestämmelsens tillämplighet begränsas således till fall där behovet av sekretess verkligen är kännbart. Den bör till exempel i regel kunna tillämpas i fall där en företagshemlighet annars skulle röjas. Uppgifter om affärs- eller driftförhållanden som affärsidkare gärna vill hålla för sig själva, men vars röjande inte kan antas få några nämnvärda ekonomiska konsekvenser, omfattas däremot inte av sekretess genom förslaget.

11.10 Sekretess till skydd för enskild i mål och ärenden hos domstol

Utredningens bedömning: Bestämmelserna i 36 kap. 2 § offentlighets- och sekretesslagen (2009:400) ger ett tillräckligt skydd för enskild i mål och ärenden hos domstol.

När det gäller skydd för enskild i mål och ärenden hos domstol finns i 36 kap. 2 § OSL en bestämmelse om sekretess för uppgift om en myndighets eller en enskilds affärs- eller driftförhållanden, uppfinningar och forskningsresultat, om det kan antas att den som uppgiften rör lider avsevärd skada om uppgiften röjs. För uppgift i en allmän handling gäller sekretessen i högst tjugo år.

Bestämmelserna utgör enligt utredningens mening tillräckligt skydd för enskilda i mål och ärenden hos domstol. Till exempel vid överklagan av de anmälda organens beslut enligt artikel 48 i EU:s cyberresiliensförordning.

Det saknas skäl att införa nya bestämmelser om sekretess till skydd för enskilda i mål och ärenden hos domstol.

11.11 Sekretess till skydd för det internationella samarbetet

Utredningens bedömning: Nuvarande sekretessreglering i 15 kap. 1 a § och 30 kap. 24 § offentlighets- och sekretesslagen (2009:400) innebär ett tillräckligt skydd för det internationella samarbetet enligt EU:s cyberresiliensförordning.

15 kap. 1 a § och 30 kap. 24 § OSL reglerar sekretess till skydd för det internationella samarbetet.

Enligt 15 kap. 1 a § OSL gäller sekretess för uppgift som en myndighet har fått från ett utländskt organ på grund av en bindande EU-rättsakt eller ett av EU ingånget eller av riksdagen godkänt avtal med en annan stat eller med en mellanfolklig organisation, om det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten eller avtalet försämras om uppgiften röjs. Motsvarande sekretess gäller för uppgift som en myndighet har inhämtat i syfte att överlämna den till ett utländskt organ i enlighet med en sådan rättsakt eller ett sådant avtal som avses i bestämmelsen. Sekretessen gäller i högst fyrtio år.

Uttrycket ”har fått från ett utländskt organ” innebär att uppgifter som en myndighet har fått från såväl utländska myndigheter som andra utländska organ omfattas av sekretessbestämmelsen. Att uppgiften finns hos myndigheten ”på grund av” en bindande EU-rättsakt eller ett av EU ingånget eller av riksdagen godkänt avtal innebär att endast sådana uppgifter som myndigheten har fått som en direkt följd av rättsakten eller avtalet träffas av bestämmelsen. Uppgifter som finns hos myndigheten av andra skäl än just på grund av rättsakten eller avtalet i fråga omfattas således inte. Med ”bindande EU-rättsakt” avses sådana rättsakter som gäller till följd av Sveriges medlemskap i EU, dvs. anslutningsfördragen samt förordningar, direktiv

och beslut som antas av EU:s institutioner. Det bör observeras att inte bara lagstiftningsakter, utan även delegerade akter och genomförandeakter kan ha en bindande verkan.¹⁵

Uppgiftens innehåll, art eller karaktär saknar betydelse för bestämmelsens tillämplighet. Bestämmelsen är tillämplig även i fråga om uppgifter om enskilda, om de finns hos myndigheten på grund av ett reglerat internationellt samarbete.¹⁶

Enligt 30 kap. 24 § OSL gäller sekretess, i den utsträckning riksdagen godkänt ett avtal om detta med en annan stat eller med en mellanfolklig organisation, hos en statlig myndighet i verksamhet som avses i 23 §, för sådan uppgift om en enskilds ekonomiska eller personliga förhållanden som myndigheten förfogar över på grund av avtalet. I begreppet avtal ingår EU-förordningar. Sekretessen gäller i högst tjugo år. Om en uppgift omfattas av regleringen i såväl 23 § som 24 § bör 24 § tillämpas i första hand.¹⁷

15 kap. 1 a § OSL föreskriver ett rakt skaderekvisit, dvs. det råder en presumtion för offentlighet. 30 kap. 24 § OSL ger ett starkt sekretesskydd för de angivna uppgifterna eftersom det inte finns något krav på att den enskilde ska lida skada om uppgifterna lämnas ut, dvs. sekretessen är absolut.

Om sekretess gäller enligt 15 kap. 1 a § eller 30 kap. 24 § OSL får de sekretessbrytande bestämmelserna i 10 kap. 5 c §, 15–27 §§ och 28 § första stycket inte tillämpas.

En förutsättning för att sekretess enligt 15 kap. 1 a § OSL ska gälla är att ett röjande av uppgiften kan antas försämra Sveriges möjlighet att delta i det internationella samarbete som avses i EU-rättsakten eller avtalet. Uttrycket syftar i detta sammanhang främst på möjligheten att få del av information i enlighet med EU-rättsakten eller avtalet, det vill säga att dra nytta av samarbetet. Bestämmelsen innebär att myndigheten i det enskilda fallet är skyldig att göra en självständig bedömning av vilka konsekvenser ett röjande kan antas få för det fortsatta samarbetet.¹⁸ En förutsättning för att sekretess enligt 30 kap. 24 § ska gälla är att avtalet eller rättsakten innehåller en klausul om att uppgifterna inte får lämnas vidare i det aktuella fallet. I den mån bestämmelser i EU:s cyberresiliensförordning inne-

¹⁵ Prop. 2012/13:192, *Sekretess i det internationella samarbetet*, s. 43.

¹⁶ Prop. 2012/13:192, *Sekretess i det internationella samarbetet*, s. 44.

¹⁷ RÅ 2007 ref. 45.

¹⁸ Prop. 2012/13:192, *Sekretess i det internationella samarbetet*, s. 44.

håller bestämmelser om konfidentialitet får dessa anses utgöra sådana sekretessklausuler.

15 kap. 1 a § kan aktualiseras för att sekretessbelägga uppgifter som svenska myndigheter mottar från ett utländskt organ, till exempel när CSIRT-enheten mottar sårbarhets- och incidentrapporter från Enisa och CSIRT-enheter i andra medlemsstater. Förutsättningen är att uppgiftsinnehavet är en direkt följd av EU:s cyberresiliensförordning. Det raka skaderekvisitet innebär att det råder en presumtion för offentlighet och förutsätter att myndigheten i varje enskilt fall, efter att ha beaktat om och i så fall hur EU:s cyberresiliensförordning reglerar frågan om sekretess, självständigt tar ställning till om ett utlämnande kan antas skada det framtida samarbetet.

30 kap. 24 § OSL kan aktualiseras för att sekretessbelägga uppgifter som svenska myndigheter förfogar över på grund av avtalet, till exempel uppgifter om ekonomiska aktörers affärs- och driftsförhållanden som myndigheten i sin marknadskontrollverksamhet förfogar över på grund av EU:s cyberresiliensförordning. Det kan även gälla uppgifter som marknadskontrollmyndigheten förfogar över enligt artikel 13.25 i EU:s cyberresiliensförordning¹⁹ och uppgifter som den anmälade myndigheten förfogar över enligt artikel 49.1 i EU:s cyberresiliensförordning²⁰. Bestämmelsen är inte begränsad till uppgifter som erhållits från utlandet utan den gäller också för uppgifter som inhämtats inom landet. Till skillnad från vad som gäller enligt 15 kap. 1 a § OSL gäller här absolut sekretess om en uppgift inte får lämnas ut enligt EU:s cyberresiliensförordning.

¹⁹ Artikel 13.25 i EU:s cyberresiliensförordning föreskriver följande. För att bedöma medlemsstaternas och unionens beroende av programvarukomponenter och i synnerhet av komponenter som klassificeras som programvara med fri och öppen källkod får Adco-gruppen besluta att genomföra en unionsomfattande beroendebedömning för specifika kategorier av produkter med digitala element. För detta ändamål får marknadskontrollmyndigheterna begära att tillverkare av sådana kategorier av produkter med digitala element tillhandahåller den relevanta programvaruförteckning som avses i bilaga I del II punkt 1. På grundval av denna information får marknadskontrollmyndigheterna förse Adco-gruppen med anonymiserad och aggregerad information om programvaruberoenden. Adco-gruppen ska lämna en rapport om resultaten av beroendebedömningen till den samarbetsgrupp som inrättats enligt artikel 14 i direktiv (EU) 2022/2555.

²⁰ Artikel 49.1 i EU:s cyberresiliensförordning föreskriver följande. De anmälda organen ska underrätta den anmälade myndigheten om följande: a) Avslag på ansökan om intyg, eller begränsning, tillfälligt tillbakadragande eller återkallelse av ett intyg. b) Omständigheter som inverkar på räckvidden och villkoren för anmälan. c) Begäran från marknadskontrollmyndigheterna om information om bedömningar av överensstämmelse. d) På begäran, bedömningar av överensstämmelse som gjorts inom ramen för anmälan och all annan verksamhet, inklusive gränsöverskridande verksamhet och underentreprenad.

Artikel 63.2 i EU:s cyberresiliensförordning föreskriver att, utan att det påverkar tillämpningen av artikel 63.1, information som utbyts på konfidentiell basis mellan marknadskontrollmyndigheterna och mellan marknadskontrollmyndigheter och kommissionen inte får lämnas ut utan föregående samtycke från den marknadskontrollmyndighet som ursprungligen lämnat informationen. En marknadskontrollmyndighet som motsätter sig ett utlämnande kan utgöra skäl till att sekretess gäller enligt 15 kap. 1 a § och 30 kap. 24 § OSL.

Frågan om sekretess för uppgifter till Enisa eller andra medlemsstater behandlas i avsnitt 11.14.

11.12 Sekretess till skydd för tillsyn samt av straffrättsliga och administrativa förfaranden

Utredningens bedömning: Bestämmelserna i 17 kap. 1 § och 18 kap. 1 § offentlighets- och sekretesslagen (2009:400) ger ett tillräckligt skydd för myndigheters tillsyn med mera samt för straffrättsliga och administrativa förfaranden.

När det gäller skydd för myndigheters verksamhet finns i 17 kap. 1 § OSL en bestämmelse om sekretess för uppgift om planläggning eller andra förberedelser för sådan inspektion, revision eller annan granskning som en myndighet ska göra, om det kan antas att syftet med granskningsverksamheten motverkas om uppgiften röjs. I 18 kap. 1 § OSL finns en bestämmelse om sekretess för uppgift som hänför sig till förundersökning i brottmål med mera.

Bestämmelserna utgör enligt utredningens mening tillräckligt skydd för allmänna intressen inför planerade tillsynsåtgärder samt avseende straffrättsliga och administrativa förfaranden och säkerställer på så sätt ett ändamålsenligt genomförande av EU:s cyberresiliensförordning.

Det saknas skäl att införa nya bestämmelser om sekretess till skydd för tillsyn samt till skydd av straffrättsliga och administrativa förfaranden.

11.13 Tystnadsplikt

Utredningens förslag: Den som deltar i verksamhet som utförs av ett privat organ för bedömning av överensstämmelse enligt EU:s cyberresiliensförordning får inte obehörigen röja eller utnyttja det som han eller hon fått kännedom om under det att uppgifterna utfördes.

Den som har tagit befattning med ett ärende som gäller marknadskontroll eller deltar i en regulatorisk sandlåda för cyberresiliens enligt EU:s cyberresiliensförordning får inte obehörigen röja eller utnyttja vad han eller hon har fått veta om någons affärs- eller driftförhållanden.

I det allmännas verksamhet tillämpas bestämmelserna i offentlighets- och sekretesslagen (2009:400).

Enligt 2 kap. 1 § OSL gäller förbudet att röja en uppgift myndigheter eller för en person som fått kännedom om uppgiften genom att för det allmännas räkning delta i en myndighets verksamhet på grund av anställning eller uppdrag hos myndigheten, på grund av tjänsteplikt eller på annan liknande grund. Bestämmelser om sekretess i OSL gäller således endast i det allmännas verksamhet.

Privata organ som utför bedömning av överensstämmelse omfattas därmed inte av 2 kap. 1 § OSL.²¹ Vidare kan det vid marknadskontroll och inom ramen för regulatoriska sandlådor för cyberresiliens som inrättas hos marknadskontrollmyndigheten uppstå situationer när uppgifter behöver hanteras av en vidare krets av personer än de som omfattas av 2 kap. 1 § OSL. Det kan till exempel gälla konsulter som anlitas i samband med vissa bedömningar av produkternas egenskaper eller laboratoriepersonal som utför tester.

I den privata sektorn gäller som huvudregel att den som disponerar över information i princip själv bestämmer om utlämnande av den till andra, med de begränsningar som dataskyddsregleringen ställer upp. För att säkerställa att alla som befattar sig med ett ärende som rör bedömning av överensstämmelse eller som biträder marknadskontrollmyndigheter, antingen inom ramen för ett ärende om marknadskontroll eller inom ramen för en regulatorisk sandlåda, bör en bestämmelse om tystnadsplikt införas i den svenska lagen som kom-

²¹ Skulle dock en myndighet anlitas inom ramen för bedömning av överensstämmelse gäller 31 kap. 12 § OSL.

pletterar EU:s cyberresiliensförordning. Bestämmelsen bör träda i kraft den 11 juni 2026, se vidare avsnitt 14.4.

Författningsreglerad tystnadsplikt utgör en inskränkning av yttrandefriheten. Den som bryter mot tystnadsplikten kan dömas för brott mot tystnadsplikten enligt 20 kap. 3 § brottsbalken.

Tystnadsplikten bör avgränsas med ett obehörighetsrekvisit vilket innebär att uppgifter kan lämnas ut med samtycke eller annars som en följd av en skyldighet i EU:s cyberresiliensförordning eller annan lag eller annan författning. Det möjliggör nödvändigt informationsutbyte mellan olika aktörer, till exempel mellan organet och marknadskontrollmyndigheten.

Det är av stor betydelse att ekonomiska aktörer känner förtroende för att de kan lämna uppgifter om sina ekonomiska förhållanden utan att känsliga uppgifter riskerar att lämnas ut till obehöriga. Det är lika viktigt oavsett om det är en myndighet eller en privat tjänsteleverantör som hanterar uppgifterna. Därför bedömer utredningen att behovet av tystnadsplikt för den som deltar eller har deltagit i sådan verksamhet väger tyngre än intresset av yttrandefrihet för dessa personer.

11.14 Sekretessbrytande bestämmelser och överföring av sekretess (informationsdelning)

Utredningens bedömning: CSIRT-enheten ska lämna de uppgifter som behövs för att en marknadskontrollmyndighet ska kunna fullgöra sina uppgifter enligt EU:s cyberresiliensförordning och anslutande föreskrifter.

I övrigt behövs inga nya bestämmelser för att en svensk myndighet ska kunna lämna information till andra myndigheter i enlighet med vad som krävs enligt bestämmelser i EU:s cyberresiliensförordning. Det gäller både nationellt och internationellt.

Bestämmelserna i EU:s cyberresiliensförordning ställer krav på informationsdelning nationellt och inom EU. Informationen behöver kunna utbytas mellan myndigheter utan att hindras av den sekretessreglering som föreligger enligt vad utredningen redovisat i föregående avsnitt. Enligt 8 kap. 1 § OSL får en uppgift som är sekretessbelagd enligt OSL inte röjas för enskilda eller för andra myndigheter,

om inte annat anges i OSL eller i lag eller förordning som OSL hänvisar till.

I detta avsnitt behandlas frågan om informationsdelning mellan myndigheter. Frågan om informationsdelning mellan CSIRT-enheten och enskilda behandlas i avsnitt 11.6.

11.14.1 Internationell informationsdelning

EU:s cyberresiliensförordning innehåller bestämmelser som förutsätter informationsdelning med kommissionen, Enisa och andra medlemsstater.

Enligt 8 kap. 3 § 1 OSL får en sekretessbelagd uppgift inte röjas för en utländsk myndighet eller en mellanfolklig organisation, om inte utlämnande sker i enlighet med särskild föreskrift i lag eller förordning.

Genom att skyldigheten till informationsdelningen följer av EU:s cyberresiliensförordning är kravet uppfyllt. Svenska myndigheter kan således i enlighet med vad som föreskrivs i EU:s cyberresiliensförordning lämna uppgifter till kommissionen, Enisa och andra medlemsstater. Det saknas därför skäl att införa nya sekretessbrytande bestämmelser.

Frågan om sekretess för uppgifter från kommissionen eller andra medlemsstater har behandlats i avsnitt 11.11.

11.14.2 Nationell informationsdelning

Sekretessbrytande bestämmelser

I 10 kap. OSL finns sekretessbrytande bestämmelser som kan tillämpas när svenska myndigheter ska dela sekretessbelagda uppgifter.

10 kap. 2 § OSL reglerar frågan om nödvändigt utlämnande. Enligt bestämmelsen hindrar inte sekretess att en uppgift lämnas till en enskild eller till en annan myndighet om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Lagrådet menar att bestämmelsen ska användas med restriktivitet och endast omständigheten att effektiviteten i myndighetens handlande sätts ned får inte leda till att sekretessen åsidosätts.²²

²² Prop. 1979/80:2 Del A, med förslag till sekretesslag m.m., (Lagrådets yttrande), s. 465.

I 10 kap. 27 § OSL, den så kallade generalklausulen, föreskrivs att en sekretessbelagd uppgift får lämnas mellan myndigheter om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda. Även 10 kap. 27 § OSL är avsedd att användas restriktivt.²³ Rutinmässigt utbyte av sekretessbelagda uppgifter mellan myndigheter ska dessutom i regel vara särskilt författningsreglerat.²⁴

Ytterligare en sekretessbrytande bestämmelse finns i 10 kap. 28 § OSL. Bestämmelsen innebär att sekretess inte hindrar att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av annan lag eller förordning.

Med tanke på att riksdagen överlätit beslutanderätten på normgivningsområdet till EU bör EU-förordningar kunna anses likställda med svensk lag. Utredningen bedömer att bestämmelserna om informationsdelning i EU:s cyberresiliensförordning är fråga om en sådan uppgiftsskyldighet som avses i 10 kap. 28 § OSL som innebär att myndigheter får lämna även sekretessbelagda uppgifter till andra myndigheter som anges i förordningen. Det saknas därför skäl att införa nya sekretessbrytande bestämmelser för de fall där EU:s cyberresiliensförordning ställer krav på informationsdelning.

Avseende den samverkan som enligt EU:s cyberresiliensförordning ska kunna ske mellan CSIRT-enheten och marknadskontrollmyndigheterna enligt artikel 52.5 i EU:s cyberresiliensförordning bedömer emellertid utredningen att det saknas ett krav på informationsdelning i förordningen. Artikel 52.5 föreskriver att marknadskontrollmyndigheterna får be CSIRT-enheten eller Enisa att ge tekniska råd i frågor som rör genomförandet och efterlevnaden av EU:s cyberresiliensförordning. Vid genomförandet av en utredning enligt artikel 54 får marknadskontrollmyndigheterna be CSIRT-enheten som utsetts till samordnare eller Enisa att tillhandahålla en analys till stöd för utvärderingar av överensstämmelse för produkter med digitala element. Artikeln riktar sig till marknadskontrollmyndigheterna och inte till CSIRT-enheten. Utredningen bedömer således gällande den samverkan som föreskrivs i artikel 52.5 i EU:s cyberresiliensförordning att det saknas en sådan uppgiftsskyldighet som avses i 10 kap. 28 § OSL som innebär att CSIRT-enheten får lämna även sekretessbelagda uppgifter till marknadskontrollmyndigheterna.

²³ Prop. 1979/80:2 Del A, med förslag till sekretesslag m.m., (Lagrådets yttrande), s. 465.

²⁴ Prop. 1979/80:2 Del A, med förslag till sekretesslag m.m., sid. 326.

Det får till följd att till exempel uppgifter i risk- och sårbarhetsanalyser med mera som är sekretessbelagda hos CSIRT-enheten enligt 18 kap. 13 § OSL inte kan lämnas till marknadskontrollmyndigheterna.

Utbyte av uppgifter är en förutsättning för att CSIRT-enheten och marknadskontrollmyndigheterna ska kunna samverka på så sätt som anges i artikel 52.5 i EU:s cyberresiliensförordning. Utredningen föreslår därför att en bestämmelse om uppgiftsskyldighet införs i förordningen med kompletterande bestämmelser till EU:s cyberresiliensförordning. Utredningen föreslår en uppgiftsskyldighet som innebär att CSIRT-enheten ska lämna de uppgifter som behövs för att marknadskontrollmyndigheterna ska kunna fullgöra sina uppgifter enligt EU:s cyberresiliensförordning.

Utredningen har i övrigt inte identifierat att det finns behov av ytterligare reglering kring informationsdelning för att säkerställa nationell samverkan.

Vidare vill utredningen uppmärksamma tillämpningen av 10 kap. 28 § OSL när det gäller sekretessregleringen till skydd för det internationella samarbetet i 15 kap. 1 a § OSL och 30 kap. 24 §. När det gäller sekretess enligt 15 kap. 1 a §, som gäller endast om det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten eller avtalet försämras om uppgiften röjs, ska den sekretessbrytande bestämmelsen 10 kap. 28 § OSL inte tillämpas. Sekretess enligt 30 kap. 24 § OSL är absolut och den sekretessbrytande bestämmelsen i 10 kap. 28 § OSL får inte tillämpas i strid med det aktuella avtalet. Regleringen hindrar inte att informationsdelning i enlighet med vad som anges i EU:s cyberresiliensförordning sker. Regleringen hindrar däremot att uppgifter lämnas till en annan myndighet utan stöd i EU:s cyberresiliensförordning.

Överföring av sekretess

När en myndighet överlämnar en uppgift som omfattas av sekretess följer inte sekretesskyddet automatiskt med till en mottagande myndighet.

Enligt 7 kap. 2 § OSL gäller sekretess för uppgiften hos den mottagande myndigheten endast om det följer av en primär sekretessbestämmelse som är tillämplig hos den mottagande myndigheten eller av en bestämmelse om överföring av sekretess.

Bestämmelser om överföring av sekretess som finns i 11 kap. OSL är inte tillämpliga vid den nationella informationsdelning som ska ske enligt EU:s cyberresiliensförordning. Utredningen bedömer dock att när uppgifter överlämnas görs det till myndigheterna i egenskap av tillsynsmyndigheter enligt andra regelverk och då gäller sekretess hos den mottagande myndigheten i enlighet med berörd myndighets primära sekretessbestämmelse enligt 9 § OSF (enligt utredningens förslag i avsnitt 11.8 eller enligt punkterna 99²⁵, 151²⁶, 153²⁷ och 166²⁸) eller enligt 32 kap. 1 § OSL²⁹.

Bestämmelserna i 30 kap. 23 § OSL, 9 § OSF och bilagan till OSF samt 32 kap. 1 § OSL tillförsäkrar enligt utredningens mening ett fullgott sekretesskydd för enskilda vid informationsutbyte mellan myndigheterna och det saknas skäl att införa nya bestämmelser om överföring av sekretess.

11.15 Behandling av personuppgifter

Utredningens bedömning: Myndigheter kommer att behandla personuppgifter när de utför uppgifter enligt EU:s cyberresiliensförordning och anslutande föreskrifter. Uppgiften att vara CSIRT-enhet, marknadskontrollmyndighet respektive anmälande myndighet är uppgifter av allmänt intresse som kommer att regleras i svensk rätt. Det finns rättslig grund för behandling av personuppgifter vid dessa myndigheter.

²⁵ Utredning, tillståndsgivning och tillsyn hos Post- och telestyrelsen.

²⁶ Marknadskontroll enligt Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011.

²⁷ Tillsyn enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster som enligt delbetänkandet *Nya regler om cybersäkerhet* (SOU 2024:18) föreslås ändras till tillsyn enligt lagen (2025:000) om cybersäkerhet.

²⁸ Utredning och tillsyn enligt Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) och lagen (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

²⁹ Sekretess gäller hos Integritetsskyddsmyndigheten i ärende om tillstånd eller tillsyn som enligt lag eller annan författning ska handläggas av myndigheten och i ärende om sådant bistånd som avses i Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter, för uppgift om en enskilds personliga eller ekonomiska förhållanden, om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs.

Vid tillämpningen av EU:s cyberresiliensförordning kan enskilda och myndigheter komma att behandla personuppgifter.

Enligt skäl 32 i EU:s cyberresiliensförordning bör förordningen inte påverka tillämpningen av förordning (EU) 2016/679³⁰ (EU:s dataskyddsförordning).

Enskilda som omfattas av EU:s cyberresiliensförordning måste, i förekommande fall, se till att uppfylla kraven både i EU:s cyberresiliensförordning och EU:s dataskyddsförordning, eller 9 kap. LEK om dessa bestämmelser i stället är tillämpliga, se även kapitel 13. Det gäller således ekonomiska aktörer samt förvaltare av programvara med fri och öppen källkod men även anmälda organ.

Behandlingen av personuppgifter som sker av myndigheter som utför uppgifter i enlighet med EU:s cyberresiliensförordning omfattas också av EU:s dataskyddsförordning. Det är nödvändigt att analysera hur EU:s cyberresiliensförordning förhåller sig till dataskyddsregleringen utifrån myndigheternas perspektiv.

Myndigheters behandling av personuppgifter

I samband med fullgörande av uppgifter enligt EU:s cyberresiliensförordning kommer myndigheter att behöva behandla personuppgifter.

För att myndigheter ska kunna behandla uppgifter och utbyta information med varandra krävs, förutom att informationen inte är sekretessbelagd eller att sekretessen kan brytas, att bestämmelser om behandling av personuppgifter hos myndigheterna ger stöd för att uppgifterna får behandlas.

EU:s dataskyddsförordning utgör grunden för generell personuppgiftsbehandling inom EU. Förordningen gäller i princip för all automatiserad behandling, samt i vissa fall manuell behandling, av personuppgifter. Personuppgifter är varje upplysning som avser en identifierad eller identifierbar fysisk person. Typiska personuppgifter är personnummer, namn och adress. Ett bolagsnummer är ofta inte en personuppgift men kan vara det om det handlar om ett enmansföretag. Personuppgiftsbehandling innefattar alla former av åtgärder med personuppgifter, exempelvis insamling, användning, utlämnande, spridning eller förstöring. Förordningen hindrar dock

³⁰ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

inte myndigheter att lämna ut allmänna handlingar enligt offentlighetsprincipen. En myndighet är inte skyldig att lämna ut allmänna handlingar på elektronisk väg men om det sker gäller dataskyddsförordningen för sådant utlämnande.

Den som behandlar personuppgifter är antingen personuppgiftsansvarig eller personuppgiftsbiträde. Personuppgiftsansvarig är den som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till. Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning. När uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom avtal.

För att en myndighets behandling av personuppgifter ska vara laglig måste det finnas en rättslig grund för behandlingen. Personuppgifter får endast behandlas om minst ett av det villkor som anges i artikel 6.1 a)–f) i EU:s dataskyddsförordning är uppfyllt. Dessa villkor utgör den rättsliga grunden för personuppgiftsbehandlingen. Uppräkningen av vad som kan utgöra rättslig grund för behandling av personuppgifter i artikel 6.1 är uttömmande. Av intresse för myndigheters verksamhet är framför allt artikel 6.1 e). Det utesluts dock inte att även andra rättsliga grunder enligt artikeln kan vara tillämpliga i vissa situationer.

Artikel 6.1 e) ger stöd för behandling av personuppgifter när behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Den rättsliga grunden som avses i artikel 6.1 e) måste enligt artikel 6.3 fastställas i enlighet med unionsrätten eller en medlemsstats nationella rätt. I förarbetena till dataskyddslagen, uttalar regeringen att alla uppgifter som riksdag eller regering gett i uppdrag åt statliga myndigheter att utföra är av allmänt intresse.³¹

Uppdraget som CSIRT-enhet, marknadskontrollmyndigheter respektive anmälände myndighet är uppgifter av allmänt intresse som kommer att regleras i svensk rätt. Myndigheterna kommer att utföra uppgifter som är av allmänt intresse och som följer av EU:s cyberresiliensförordning och anslutande föreskrifter. Det innebär att den rättsliga grunden i artikel 6.1 e) i EU:s dataskyddsförordning för behandling av personuppgifter kommer att vara tillämplig. Personuppgiftsbehandlingen bedöms nödvändig för att kunna utföra de uppgifter som anges i EU:s cyberresiliensförordning.

³¹ Prop. 2017/18:105, *Ny dataskyddslag*, s. 56 och 57.

Utredningen bedömer att det finns stöd i EU:s dataskyddsförordning och anslutande föreskrifter för myndigheternas behandling av personuppgifter som EU:s cyberresiliensförordning kan medföra. Personuppgiftsbehandling i samband med tillämpningen av EU:s cyberresiliensförordning får således anses vara förenlig med EU:s dataskyddsförordning.

Som redogörs för i avsnitt 11.13 kan uppgifter som samlas in i marknadskontrollverksamhet eller som behandlas inom ramen för regulatoriska sandlådor för cyberresiliens ibland hanteras av andra än marknadskontrollmyndigheterna själva, till exempel konsulter. Om det ingår behandling av personuppgifter i hanteringen är bestämmelserna om personuppgiftsbiträden tillämpliga och personuppgiftsbiträdesavtal ska upprättas.

12 Stöd till företag

12.1 Inledning

För att undvika att förordning (EU) 2024/2847¹ (EU:s cyberresiliensförordning) ska hämma näringslivet och innovation har utredningen i uppdrag att överväga vilka stödåtgärder och stödfunktioner som skulle kunna vara lämpliga för att bistå mikroföretag, små företag och medelstora företag. Utredningens uppdrag är att

- föreslå hur de åtgärder som avses i artikel 33 i EU:s cyberresiliensförordning kan genomföras i Sverige,
- föreslå lämpliga samarbetsformer eller forum där expertis och kunskap kan delas mellan såväl företag som offentlig-privata initiativ, och
- föreslå andra lämpliga stödåtgärder för mikroföretag, små företag och medelstora företag.

Artikel 33.1 och 33.2 i EU:s cyberresiliensförordning anger vilket stöd som får tillhandahållas av medlemsstaterna. Övriga delar av artikel 33 riktar sig till kommissionen eller rör specifikt frågan om det förenklade formuläret för den tekniska dokumentationen.

Enligt artikel 33.1 i EU:s cyberresiliensförordning ska medlemsstaterna, när så är lämpligt, vidta följande åtgärder som är anpassade till mikroföretags och små företags behov:

- a) Anordna särskild informations- och utbildningsverksamhet om tillämpningen av EU:s cyberresiliensförordning.

¹ Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen).

- b) Inrätta en särskild kanal för kommunikation med mikroföretag och små företag och, när så är lämpligt, lokala myndigheter för att ge råd och besvara frågor om genomförandet av EU:s cyberresiliensförordning.
- c) Stödja provning och bedömning av överensstämmelse, när så är lämpligt även med stöd av Europeiska kompetenscentrumet för cybersäkerhet (ECCC).

Enligt artikel 33.2 i EU:s cyberresiliensförordning får medlemsstaterna, när så är lämpligt, inrätta regulatoriska sandlådor för cyberresiliens. Sådana regulatoriska sandlådor ska tillhandahålla kontrollerade provmiljöer för innovativa produkter med digitala element för att underlätta utvecklingen, utformningen, valideringen och provningen av dem i syfte att uppfylla kraven i förordningen under en begränsad tidsperiod innan de släpps ut på marknaden. Kommissionen och, när så är lämpligt, Enisa får tillhandahålla tekniskt stöd, rådgivning och verktyg för inrättande och drift av regulatoriska sandlådor. De regulatoriska sandlådorna ska inrättas under marknadskontrollmyndigheternas direkta tillsyn, vägledning och stöd. Medlemsstaterna ska genom den särskilda administrativa samarbetsgruppen (Adco-gruppen) informera kommissionen och de andra marknadskontrollmyndigheterna om inrättandet av en regulatorisk sandlåda. De regulatoriska sandlådorna ska inte påverka de behöriga myndigheternas tillsynsbefogenheter och korrigerande befogenheter. Medlemsstaterna ska säkerställa öppen, rättvis och transparent tillgång till regulatoriska sandlådor, och i synnerhet underlätta tillgång för mikroföretag och små företag, inbegripet uppstartsföretag.

Skäl 23 i EU:s cyberresiliensförordning anger att effektiviteten i genomförandet av förordningen kommer att vara beroende av tillgången till lämpliga cybersäkerhetskunskaper. På unionsnivå konstaterades i olika programdokument och politiska dokument, inbegripet kommissionens meddelande Minska kompetensbristen på cybersäkerhetsområdet för att främja EU:s konkurrenskraft, tillväxt och resiliens av den 18 april 2023 och rådets slutsatser av den 22 maj 2023 om EU:s politik för cyberförsvar, kompetensbristen inom cybersäkerhet i unionen och behovet av att ta itu med sådana utmaningar som en prioriterad fråga, både inom den offentliga och den privata sektorn. För att säkerställa ett effektivt genomförande av EU:s cyberresiliensförordning bör medlemsstaterna se till att tillräckliga resur-

ser finns tillgängliga för lämplig personal vid marknadskontrollmyndigheterna och organen för bedömning av överensstämmelse för att de ska kunna utföra sina uppgifter enligt förordningen. Dessa åtgärder bör öka arbetskraftens rörlighet på cybersäkerhetsområdet och deras tillhörande karriärvägar. De bör också bidra till att göra cybersäkerhetsarbetskraften mer resilient och inkluderande, även när det gäller kön. Medlemsstaterna bör därför vidta åtgärder för att säkerställa att dessa uppgifter utförs av tillräckligt utbildade yrkesutövare med nödvändig cybersäkerhetskompetens. På samma sätt bör tillverkarna se till att deras personal har den kompetens som krävs för att fullgöra sina skyldigheter som fastställs i denna förordning. Medlemsstaterna och kommissionen bör, i enlighet med sina rättigheter och befogenheter och de särskilda uppgifter som de tilldelas genom förordningen, vidta åtgärder för att stödja tillverkare, särskilt mikroföretag och små och medelstora företag, inbegripet uppstartsföretag, även på områden såsom kompetensutveckling, i syfte att fullgöra de skyldigheter som fastställs i förordningen. Eftersom direktiv (EU) 2022/2555² (NIS 2-direktivet) ålägger medlemsstaterna att anta strategier för att främja och utveckla utbildning i cybersäkerhet och cybersäkerhetskompetens som en del av sina nationella strategier för cybersäkerhet, får medlemsstaterna, när de antar sådana strategier, också överväga om de ska ta itu med de kompetensbehov inom cybersäkerhet som följer av förordningen, inbegripet sådana som rör omskolning och kompetenshöjning.

Skäl 127 i EU:s cyberresiliensförordning föreskriver att det är viktigt att ge stöd till mikroföretag samt små och medelstora företag, inbegripet uppstartsföretag, vid genomförandet av förordningen och att begränsa de risker i samband med genomförandet som följer av bristande kunskap och expertis på marknaden, samt att underlätta för tillverkarna att fullgöra sina skyldigheter enligt förordningen. Programmet för ett digitalt Europa och andra relevanta unionsprogram tillhandahåller ekonomiskt och tekniskt stöd som gör att dessa företag kan bidra till tillväxten i unionens ekonomi och till en stärkt gemensam cybersäkerhetsnivå i unionen. ECCC och nationella samordningscentrum samt europeiska digitala innovationsknutpunkter som inrättas av kommissionen och medlems-

² Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

staterna på unionsnivå eller nationell nivå skulle också kunna stödja företag och organisationer inom den offentliga sektorn och bidra till genomförandet av förordningen. Inom ramen för sina respektive uppdrag och ansvarsområden skulle de kunna ge tekniskt och vetenskapligt stöd till mikroföretag samt små och medelstora företag, till exempel för testningsverksamhet och tredjepartsbedömningar av överensstämmelse. De skulle också kunna främja användningen av verktyg för att underlätta genomförandet av förordningen.

Artikel 10 i EU:s cyberresiliensförordning föreskriver vidare att vid tillämpningen av förordningen och för att tillgodose yrkesutövarnas behov, till stöd för genomförandet av förordningen, ska medlemsstaterna – när så är lämpligt med stöd av kommissionen, ECCC och Enisa och med full respekt för medlemsstaternas ansvar på utbildningsområdet – främja åtgärder och strategier som syftar till att

- a) utveckla cybersäkerhetskompetensen och skapa organisatoriska och tekniska verktyg för att säkerställa tillräcklig tillgång till kvalificerad arbetskraft för att stödja verksamheten vid marknadskontrollmyndigheterna och organen för bedömning av överensstämmelse,
- b) förbättra samarbetet mellan den privata sektorn, ekonomiska aktörer, bland annat genom omskolning eller kompetenshöjning för tillverkares anställda, konsumenter, utbildningsanordnare och även offentliga förvaltningar, och därmed utöka möjligheterna för unga att få jobb inom cybersäkerhetssektorn.

I detta kapitel behandlar utredningen frågan om lämpliga stödåtgärder och stödfunktioner för att bistå företag i deras regelefterlevnad.

Frågan om cybersäkerhetskompetens med mera vid och organen för bedömning av överensstämmelse och marknadskontrollmyndigheterna behandlas i kapitel 9.

12.2 Företagens utmaningar och behov av stöd

Avgörande för vad som skulle kunna utgöra lämpliga stödåtgärder och stödfunktioner för att bistå företag är en förståelse för vilka krav som ställs på företag enligt EU:s cyberresiliensförordning och vad det innebär för företag att efterleva kraven.

EU:s cyberresiliensförordning innehåller bestämmelser om skyldigheter för ekonomiska aktörer samt förvaltare av programvara

med fri och öppen källkod när det gäller cybersäkerheten för produkter med digitala element och i samband med processer för sårbarhetshantering under produkternas stödperiod samt regler för tillhandahållande på marknaden av produkterna. Förordningen krav gäller för samtliga produkter med digitala element.

Syftet med EU:s cyberresiliensförordning är att skapa förutsättningar för utveckling av säkra produkter med digitala element genom att säkerställa att hård- och mjukvara släpps ut på marknaden med färre sårbarheter och att tillverkare ska ta större ansvar för produkters cybersäkerhet genom deras livscykel. Förordningen syftar vidare till att konsumenter ska få tillräcklig information om cybersäkerheten för de produkter med digitala element som de köper och använder.

Kraven innebär att tillverkare ska ta cybersäkerhet i beaktande i designen och utvecklingen av produkter med digitala element. Därtill ska tillverkare granska säkerhetsaspekter under utvecklingsprocessen, ha transparens gentemot konsumenter gällande cybersäkerhetsaspekter samt försäkra säkerhetssupport och uppdateringar på ett proportionerligt sätt under produktens livscykel. För att efterleva bestämmelserna ställs krav på kompetens inom cybersäkerhet. Bland annat krävs att företag kan bedöma och dokumentera de cybersäkerhetsrisker som är förbundna med produkten och beakta resultatet av bedömningen under planerings-, utformnings-, utvecklings-, produktions-, leverans- och underhållsfaserna för produkten i syfte att minimera cybersäkerhetsriskerna, förhindra incidenter och minimera deras konsekvenser. Utifrån riskbedömningen, krävs det att företag säkerställer att produkten utformas, utvecklas och produceras i enlighet med de väsentliga cybersäkerhetskrav som fastställs i bilaga I del I innan den släpps ut på marknaden. Det krävs även att företagen kan avgöra vilken produktkategori produkten tillhör och att företaget genomför relevant förfarande för bedömning av överensstämmelse av produkten. Företag behöver vidare ta fram teknisk dokumentation för produkten och upprätta EU-försäkran om överensstämmelse. Produkten behöver även CE-märkas. När en produkt med digitala element släpps ut på marknaden, och under stödperioden, krävs det att företagen säkerställer att produktens, inbegripet dess komponenters, sårbarheter hanteras effektivt och i enlighet med de väsentliga cybersäkerhetskrav som fastställs

i bilaga I del II. Det krävs även att företag rapporterar eventuella sårbarheter och incidenter.

Genom EU:s cyberresiliensförordning regleras cybersäkerhet för produkttillverkare egentligen för första gången, utöver de bestämmelser som rör specifikt radioutrustning och som trädde i kraft den 1 augusti 2025 genom kommissionens delegerade förordning (EU) 2022/30³. Det finns ingen motsvarande befintlig reglering till EU:s cyberresiliensförordning, varken inom EU eller i Sverige, som ställer direkta krav på att samtliga produkter med digitala element ska utformas för att hantera risker som är specifikt kopplade till cybersäkerhetsområdet. Det finns dock närliggande och överlappande bestämmelser som reglerar andra aspekter av dessa produkter, eller verksamheter där produkterna används. EU:s cyberresiliensförordning har ett brett tillämpningsområde och innehåller krav som gäller i samband med tillverkning av produkterna, när produkterna sätts på marknaden och under produkternas livscykel. Att reglerna är baserade på det befintliga lagstiftningsramverket *New Legislative Framework (NLF)*⁴, där harmoniserade standarder fungerar som verktyg för att uppfylla föreskrivna krav, kan visserligen för vissa företag skapa igenkänning, tydlighet och förutsebarhet men det är inte alla produkter som tidigare omfattats av det ramverket. Utredningen bedömer att företag behöver stöd att identifiera tillämpliga bestämmelser, att efterleva de specifika krav som ställs i EU:s cyberresiliensförordning och att tillämpa den metodik som förordningen bygger på.

³ Kommissionens delegerade förordning (EU) 2022/30 av den 29 oktober 2021 om komplettering av Europaparlamentets och rådets direktiv 2014/53/EU vad gäller tillämpningen av de väsentliga krav som avses i artikel 3.3 d, e och f i det direktivet.

⁴ NLF grundar sig på Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93, Europaparlamentets och rådets beslut nr 768/2008/EG av den 9 juli 2008 om en gemensam ram för saluföring av produkter och upphävande av rådets beslut 93/465/EEG samt Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011.

12.3 EU:s cyberresiliensförordning

EU:s cyberresiliensförordning innehåller ett antal bestämmelser som är särskilt anpassade till små och medelstora företag. Förordningen innehåller även bestämmelser om stöd som ska erhållas från ett antal utpekade aktörer. De stödåtgärder och stödfunktioner till företag som utredningen har i uppdrag att lämna förslag kring ska komplettera detta.

12.3.1 Anpassningar och kompletterande reglering

Visst stöd till mikroföretag, små företag och medelstora företag ges genom att EU:s cyberresiliensförordning innehåller ett antal bestämmelser som är särskilt anpassade efter dessa företag. Mikroföretag och små företag får enligt artikel 33.5 i EU:s cyberresiliensförordning använda ett förenklat formulär för den tekniska dokumentationen. När det gäller förfaranden för bedömning av överensstämmelse och avgifter för detta är anmälda organ skyldiga att göra anpassningar för små och medelstora företag, se artiklarna 32.6, 39.12 och 47.2 i EU:s cyberresiliensförordning.

I tillägg till dessa bestämmelser kan nämnas att EU:s cyberresiliensförordning även innehåller anpassningar för mikroföretag, små företag och medelstora företag gällande regleringen kring administrativa sanktionsavgifter. Enligt artikel 64.5 i EU:s cyberresiliensförordning ska hänsyn tas till huruvida tillverkaren är ett mikroföretag eller ett småföretag eller medelstort företag, inbegripet ett uppstarts företag när administrativa sanktionsbelopp fastställs. Enligt artikel 64.10 i EU:s cyberresiliensförordning ska administrativa sanktionsavgifter inte tillämpas på mikroföretag eller små företag för en underlåtenhet att iaktta tidsfristen på 24 timmar avseende en tidig varning om aktivt utnyttjade sårbarheter eller allvarliga incidenter som påverkar säkerheten för produkten med digitala element (enligt artiklarna 14.2 a och 14.4 a) och inte heller på förvaltare av programvara med fri och öppen källkod för någon överträdelse av EU:s cyberresiliensförordning.

Utöver dessa regelanpassningar kommer visst stöd till företag att erhållas genom kompletteringar av bestämmelserna i EU:s cyberresiliensförordning. Här kan framför allt nämnas de harmoniserade standarder för de väsentliga cybersäkerhetskraven i bilaga I i EU:s

cyberresiliensförordning som nu utarbetas av ett antal europeiska standardiseringsorganisationer.

Utöver standarderna väntas kommissionen ta fram viss kompletterande lagstiftning.

Enligt artikel 7.4 i EU:s cyberresiliensförordning ska kommissionen senast den 11 december 2025 specificera den tekniska beskrivningen av de kategorier av viktiga respektive kritiska produkter med digitala element som anges i bilagor till förordningen.

Enligt artikel 13.24 i EU:s cyberresiliensförordning får kommissionen specificera formatet och de aspekter som ska ingå i den programvaruförteckning som avses i bilaga I del II punkt 1.

Enligt artikel 14.10 i EU:s cyberresiliensförordning får kommissionen ytterligare specificera formatet och förfarandena för de sårbarhets- och incidentrapporter som avses i artikel 14 samt i artiklarna 15 och 16.

Kommissionen får enligt artikel 27.2 i EU:s cyberresiliensförordning fastställa gemensamma specifikationer som omfattar tekniska krav vilka utgör ett sätt att uppfylla de väsentliga cybersäkerhetskrav som fastställs i bilaga 1.

Enligt artikel 30.6 i EU:s cyberresiliensförordning får kommissionen fastställa tekniska specifikationer för etiketter, piktogram eller andra märkningar som rör säkerheten för produkter med digitala element, deras stödperioder och mekanismer för att främja användningen av sådana och öka allmänhetens medvetenhet om säkerheten hos produkter med digitala element.

Enligt artikel 33.5 i EU:s cyberresiliensförordning ska kommissionen specificera det förenklade formuläret för teknisk dokumentation med inriktning på mikroföretags och små företags behov.

12.3.2 Stöd från ett antal utpekade aktörer

EU:s cyberresiliensförordning innehåller bestämmelser om att ett antal utpekade aktörer på olika sätt ska eller får tillhandahålla stöd till företag.

CSIRT-enheter som utsetts till samordnare

Enligt artikel 17.6 i EU:s cyberresiliensförordning ska de CSIRT-enheter som utsetts till samordnare tillhandahålla hjälptjänster⁵ i samband med rapporteringsskyldigheterna enligt artikel 14 till tillverkare, särskilt tillverkare som kan betecknas som mikroföretag eller små eller medelstora företag.

Marknadskontrollmyndigheter

Enligt artikel 52.10 i EU:s cyberresiliensförordning får marknadskontrollmyndigheterna ge ekonomiska aktörer vägledning och råd om genomförandet av denna förordning. Enligt artikel 52.12 ska marknadskontrollmyndigheterna när så är lämpligt underlätta samarbetet med berörda parter, inbegripet vetenskapliga organisationer samt forsknings- och konsumentorganisationer.

Kommissionen

Enligt artikel 26 i EU:s cyberresiliensförordning ska kommissionen, för att underlätta genomförandet av förordningen och säkerställa ett konsekvent genomförande, offentliggöra vägledning som ska vara till hjälp för de ekonomiska aktörerna vid tillämpningen av denna förordning, med särskilt fokus på att underlätta efterlevnaden för mikroföretag samt små och medelstora företag. I sådan vägledning ska kommissionen åtminstone ta upp

- förordningens tillämpningsområde (med särskilt fokus på lösningar för fjärrbehandling av data och programvara med fri och öppen källkod),
- tillämpningen av stödperioder med avseende på särskilda kategorier av produkter med digitala element,
- vägledning för tillverkare som omfattas av denna förordning och som också omfattas av annan unionsharmoniseringslagstiftning⁶, samt begreppet väsentlig ändring.

⁵ För vägledning kring begreppet ”hjälp-tjänster”, jämför den engelska språkversionen av cyberresiliensförordningen som använder begreppet ”helpdesk support”.

⁶ I skäl 30 och 53 anges att kommissionen bör tillhandahålla vägledning för att stödja tillverkare av produkter som omfattas av Europaparlamentets och rådets förordning (EU) 2023/1230 eller av delegerad förordning (EU) 2022/30 och som också är produkter med digitala element enligt definitionen i EU:s cyberresiliensförordning särskilt för att underlätta påvisandet av efterlevnaden av de båda förordningarna.

Vidare ska kommissionen upprätthålla en lättillgänglig förteckning över de delegerade akter och genomförandakter som antagits enligt EU:s cyberresiliensförordning.

Enligt artikel 33.4 i EU:s cyberresiliensförordning ska kommissionen tillkännage att ekonomiskt stöd inom ramen för unionens befintliga program är tillgängligt, särskilt för att minska den ekonomiska bördan för mikroföretag och små företag.

Till hjälp i kommissionens arbete har kommissionen inrättat en expertgrupp, *CRA Expert Group*, som bistår och ger råd i frågor som är relevanta för genomförandet av EU:s cyberresiliensförordning. I expertgruppen ingår myndighetsrepresentanter från Sverige.

Adco-gruppen

Enligt artikel 52.15 i EU:s cyberresiliensförordning ska en Adco-grupp inrättas för en enhetlig tillämpning av förordningen, enligt artikel 30.2 i förordning (EU) 2019/1020⁷. Adco-gruppen ska bestå av företrädare för de utsedda marknadskontrollmyndigheterna och, om så är lämpligt, företrädare för de centrala samordningskontoren. Adco-gruppen ska också behandla särskilda frågor som rör marknadskontroll rörande de skyldigheter som åläggs förvaltare av programvara med fri och öppen källkod.

Enligt artikel 52.16 i EU:s cyberresiliensförordning ska Adco-gruppen tillhandahålla vägledning som inbegriper vägledande stödperioder för kategorier av produkter med digitala element.

12.4 Nuvarande stöd till svenska företag inom cybersäkerhetsområdet

I Sverige finns ett antal myndigheter som arbetar med cybersäkerhet och som bland annat har i uppgift att ge stöd till företag. Dessa är Försvarets materielverk (FMV), Försvarets radioanstalt (FRA), Försvarsmakten, Myndigheten för samhällsskydd och beredskap (MSB), Polismyndigheten, Post- och telestyrelsen (PTS) samt Säkerhetspolisen.

⁷ Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011.

Utöver dessa myndigheter finns ett antal aktörer och funktioner i Sverige som bland annat har i uppgift att ge stöd till företag inom cybersäkerhetsområdet. Dessa är det nationella cybersäkerhetscentret (NCSC), Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE), den svenska kompetensgemenskapen Cybernoden Sverige och Cybercampus Sverige. Aktörerna och funktionerna omnämns särskilt i Nationell strategi för cybersäkerhet 2025–2029, Skr 2024/25:121, som aktörer som kan bidra till ökad cybersäkerhet.

12.4.1 Myndigheter som arbetar med cybersäkerhet

Myndigheten för samhällsskydd och beredskap

MSB har enligt 11 a–c §§ förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap ansvar för frågor om skydd mot olyckor, krisberedskap och civilt försvar, i den utsträckning inte någon annan myndighet har ansvaret. Myndigheten ska stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och regioner samt företag och organisationer. Detta görs till exempel genom Cybersäkerhetsrådgivningen (en tjänst som hjälper organisationer att anpassa informations- och cybersäkerhetsarbetet till sin verksamhet)⁸, ett metodstöd för informationssäkerhetsarbete (som genom vägledningar, verktyg, mallar, tips med mera förtydligar hur ett systematiskt säkerhetsarbete kan utformas utifrån standarderna om ledningssystem för informationssäkerhet, LIS), Cybersäkerhetskollen (med hjälp av vilken det går att mäta nivån på en verksamhets systematiska informations- och cybersäkerhetsarbete samt

⁸ Hösten 2024 bytte MSB:s rådgivningstjänst för systematiskt informationssäkerhetsarbete namn till Cybersäkerhetsrådgivningen. Det nya namnet speglar det utökade uppdrag som rådgivningen fått under 2024 och den utveckling som ska ske under 2025. Förutom frågor om systematiskt informationssäkerhetsarbete och NIS 2-frågor ska rådgivarna från och med 2025 även stötta i frågor kring hur verksamheter kan arbeta systematiskt och riskbaserat med tekniska säkerhetsåtgärder och cyberfysiska system. Rådgivarna kommer även att kunna ge information avseende stöd till forskning, innovation och kompetensförsörjning inom cybersäkerhet, inom ramen av NCC-SE.

ge stöd till förbättringsarbete)⁹ och årliga cybersäkerhetskonferenser (som syftar till att utgöra en plattform för kompetenshöjning, erfarenhetsutbyten och informationsdelning).

Myndigheten ansvarar även för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter (Sveriges nationella CSIRT-enhet, CERT-SE).

Myndigheten är vidare nationellt samordningscenter (NCC-SE) enligt artikel 6 i förordning (EU) 2021/887¹⁰ (CCCN-förordningen) samt, genom NCC-SE, ansvarig för samordning och inriktning av verksamheten i Cybernoden Sverige. Se mer om NCC-SE och Cybernoden Sverige i avsnitt 12.4.2.

Sedan 2024 handlägger även myndigheten ansökningar om bidrag enligt förordningen (2024:664) om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning. Beslut enligt förordningen kan överklagas till allmän förvaltningsdomstol. MSB får meddela föreskrifter om verkställigheten av förordningen.

Enligt förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster är MSB nationell kontaktpunkt (22 §) och CSIRT-enhet (12 §) och deltar i samarbetsgruppen som har inrättats enligt artikel 11 i direktiv (EU) 2016/1148¹¹ (23 §). MSB har enligt förordningen även ansvaret att leda ett samarbetsforum för tillsynsmyndigheterna och Socialstyrelsen samt mandat att meddela föreskrifter.

I betänkandet *Nya regler om cybersäkerhet* (SOU 2024:18) föreslås att MSB ska behålla dessa uppgifter samt även utgöra cyberkrishanteringsmyndighet. Betänkandet innehåller förslag för genomförandet av NIS 2-direktivet. Regeringen har i linje med förslagen i betänkandet gett MSB i uppdrag att vara behörig myndighet enligt NIS 2-direktivet gällande rollerna som gemensam kontaktpunkt, cyberkrishanteringsmyndighet, CSIRT-enhet samt som Sveriges representant i samarbetsgruppen (Fö2025/00387). Regeringsbeslutet fattades den

⁹ Nytt för 2024 var att organisationer som genomfört Cybersäkerhetskollen erbjöds en serie rådgivningssamtal som stöd i förbättringsarbetet utifrån deras resultat vilket ger en mer strukturerad och långsiktig rådgivning utifrån ett identifierat behov. Under 2025 kommer denna typ av långsiktig rådgivning utvecklas för fler områden.

¹⁰ Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum.

¹¹ Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

27 februari 2025 och gäller under året i avvaktan på att förslagen i betänkandet bereds.

Enligt förslagen i slutbetänkandet *Samlade förmågor för ökad cybersäkerhet* (SOU 2025:79) ska 11 a–11 c §§ upphöra att gälla den 1 juli 2026. Utredningens utgångspunkt är att en verksamhetsöverföring till FRA ska ske genom att uppgifter författningsmässigt överförs till FRA som myndighet men utföras inom ramen för NCSC:s verksamhet.

Försvarets radioanstalt

FRA har enligt 1 § förordningen (2007:937) med instruktion för Försvarets radioanstalt till uppgift att bedriva signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. Enligt 4 § ska FRA ha hög teknisk kompetens inom informationssäkerhetsområdet. FRA får efter begäran stödja sådana statliga myndigheter och enskilda verksamhetsutövare som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. Myndigheten ska särskilt kunna stödja insatser vid nationella kriser med it-inslag, medverka till identifieringen av inblandade aktörer vid it-relaterade hot mot samhällsviktiga system, genomföra it-säkerhetsanalyser och ge annat tekniskt stöd.

NCSC är sedan den 1 november 2024 en del av FRA, se mer om NCSC i avsnitt 12.4.2. Utöver FRA deltar även Försvarmakten, MSB, Polismyndigheten, Säkerhetspolisen, FMV och PTS som samverkansmyndigheter i centrets arbete. Av 4 a § förordningen (2007:937) med instruktion för Försvarets radioanstalt framgår att centret har till uppgift att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter.

Som ovan angetts föreslås i slutbetänkandet *Samlade förmågor för ökad cybersäkerhet* (SOU 2025:79) att uppgifter som i dag utförs av MSB enligt 11 a–c §§ förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap författningsmässigt ska överföras till FRA, men utföras inom ramen för NCSC:s verksamhet, från och med den 1 juli 2026.

Post- och telestyrelsen

PTS har enligt 1 och 4 §§ förordningen (2007:951) med instruktion för Post- och telestyrelsen ett samlat ansvar inom områdena post och elektronisk kommunikation. Myndigheten har bland annat till uppgift att främja tillgången till säkra och effektiva elektroniska kommunikationer, följa utvecklingen när det gäller säkerhet vid elektronisk kommunikation samt verka för robusta elektroniska kommunikationer och minska risken för störningar, inbegripet att upphandla förstärkningsåtgärder, och verka för ökad krishanteringsförmåga. PTS har även i uppgift att lämna råd och stöd till myndigheter, kommuner och regioner och till företag, organisationer och andra enskilda i frågor om nätsäkerhet. PTS är marknadskontrollmyndighet enligt radio-utrustningslagen (2016:392) och lagen (2023:254) om vissa produkters och tjänsters tillgänglighet.

I betänkandet *Anpassningar till AI-förordningen* (SOU 2025:101) föreslås ett system för marknadskontroll för förordning (EU) 2024/1689¹² (AI-förordningen) som består av flera marknadskontrollmyndigheter och där PTS ska vara marknadskontrollmyndighet med huvudsakligt ansvar för AI-förordningen. Utredningen har även föreslagit att PTS i denna egenskap ska vara samordnande marknadskontrollmyndighet.¹³

Försvarets materielverk

Enligt 1 § förordningen (2007:854) med instruktion för Försvarets materielverk ska verket bland annat upphandla varor, tjänster och byggentreprenader inom materielförsörjningsområdet samt att biträda Försvarsmakten i planeringen av materiel- och logistikförsörjningen.

FMV är enligt förordning (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt nationell myndighet för cybersäkerhetscertifiering. Inom ramen för den rollen bedriver myndigheten tillsyn, samverkan och annan informationsgivning rörande

¹² Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

¹³ Sid. 203–305.

tillämpning av certifieringsramverket i förordning (EU) 2019/881¹⁴ (EU:s cybersäkerhetsakt).

Försvarsmakten

Försvarsmaktens huvuduppgift är enligt 1 § förordningen (2007:1266) med instruktion för Försvarsmakten att försvara Sverige och allierade stater mot ett väpnat angrepp med utgångspunkt i det kollektiva försvaret inom Nato. Enligt 2 § ska Försvarsmakten främja Sveriges säkerhet och hävda Sveriges territoriella integritet. Myndigheten ska ha förmåga att värna Sveriges suveräna rättigheter och svenska intressen samt att förebygga och hantera konflikter och krig såväl nationellt som internationellt. Försvarsmakten ska med myndighetens befintliga förmåga och resurser kunna lämna stöd till civil verksamhet. Enligt 3 b § ska Försvarsmakten bedriva verksamhet enligt 1 § lagen (2000:130) om försvarsunderrättelseverksamhet samt leda och bedriva militär säkerhetstjänst vilket görs genom den Militära underrättelse- och säkerhetstjänsten (Must).

Enligt 1 och 2 §§ lagen (2000:130) om försvarsunderrättelseverksamhet ska försvarsunderrättelseverksamhet bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. Verksamheten ska fullgöras genom inhämtning, bearbetning och analys av information. Underrättelser ska rapporteras till berörda myndigheter.

Polismyndigheten

Enligt 2 § polislagen (1984:387) har polismyndigheten bland annat i uppgift att förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen eller säkerheten, utreda och beivra brott som hör under allmänt åtal samt lämna allmänheten skydd, upplysningar och annan hjälp, när sådant bistånd lämpligen kan ges av polisen.

¹⁴ Förordning (EU) 2019/881 om Europeiska unionens cybersäkerhetsbyrå och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (cybersäkerhetsakten).

Säkerhetspolisen

Säkerhetspolisen har enligt 3 § polislagen (1984:387) samt 1, 3 och 6 §§ förordningen (2022:1719) med instruktion för Säkerhetspolisen bland annat i uppgift att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot Sveriges säkerhet eller terrorbrott. Säkerhetspolisen bedriver i egenskap av säkerhetstjänst underrättelse- och säkerhetsarbete. Myndigheten får ge tekniskt stöd inom säkerhetsskydd. Myndigheten får dessutom ge råd för att förebygga brott mot Sveriges säkerhet eller andra särskilt viktiga samhällsintressen.

12.4.2 Andra aktörer och funktioner inom cybersäkerhetsområdet

Nationellt cybersäkerhetscenter

NCSC startade 2020 och är sedan 2024 en del av FRA. Inom NCSC samarbetar fler myndigheter som arbetar med cybersäkerhet. De myndigheter som ingår i samarbetet är FMV, FRA, Försvarmakten, MSB, Polismyndigheten, PTS samt Säkerhetspolisen (samverkansmyndigheterna). Det kan konstateras att NCSC sedan den 1 november 2024 är en del av FRA och därmed inte utgör ett myndighetsgemensamt samverkanscenter som tidigare.

Enligt 4 a § förordningen (2007:937) med instruktion för Försvarets radioanstalt har NCSC till uppgift att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter.

Den 22 april 2025 trädde förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt (NCSC-förordningen) i kraft. Enligt 2 § NCSC-förordningen ska NCSC utgöra en nationell plattform för samverkan och informationsutbyte mellan aktörer, såväl privata som offentliga, i frågor som rör cybersäkerhet. NCSC ska också vara en kontaktpunkt för sådana frågor. Enligt 3 § ska NCSC särskilt

- bidra till att samordna och harmonisera det nationella cybersäkerhetsarbetet,
- lämna råd och stöd till privata och offentliga aktörer i frågor om hot, sårbarheter och risker med koppling till cybersäkerhet,

- lämna råd och stöd till privata och offentliga aktörer vid it-incidenter,
- genomföra utbildningar, övningar och andra kompetenshöjande insatser inom cybersäkerhetsområdet,
- till privata och offentliga aktörer ta fram samlade lägesbilder av antagonistiska cyberhot och andra it-incidenter,
- bistå Regeringskansliet (Försvarsdepartementet) med samlade lägesbilder som bland annat innehåller bedömningar av hotnivån,
- vara en kontaktpunkt gentemot motsvarande funktioner i internationella sammanhang och utveckla samarbetet och informationsutbytet med dessa,
- rapportera till regeringen om förhållanden på cybersäkerhetsområdet som kan leda till behov av åtgärder samt lämna förslag på sådana åtgärder, och
- informera regeringen om relevanta förhållanden vid ett sådant hot eller annan incident som avses i 5 § andra stycket.

Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet och Cybernoden Sverige

Genom förordning (EU) 2021/887¹⁵ (CCCN-förordningen) inrättades Europeiska kompetenscentrumet för cybersäkerhet (ECCC) samt ett nätverk av nationella samordningscentrum. ECCC har i uppgift att bidra i genomförandet av cybersäkerhetsdelen av programmet för ett digitalt Europa och bidra till genomförandet av Horisont Europa. Medlemsstaterna ska gemensamt bidra till kompetenscentrumets och nätverkets arbete. Enligt ECCC:s arbetsprogram för åren 2025–2027 framgår att stöd ska lämnas bland annat till företag för att kunna efterleva kraven som ställs i EU:s regelverk inom cybersäkerhetsområdet.

I enlighet med CCCN-förordningen inrättades under 2022 Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE). MSB är enligt 11 c § förordningen (2008:1002) med instruktion för Myndigheten för samhälls-

¹⁵ Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum.

skydd och beredskap NCC-SE. Utvecklingen av verksamheten sker i samverkan med Verket för innovationssystem (Vinnova) och Myndigheten för digital förvaltning (DIGG). Enligt förslagen i slutbetänkandet *Samlade förmågor för ökad cybersäkerhet* (SOU 2025:79) ska uppgiften enligt 11 c §§ förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap författningsmässigt överföras till FRA men utföras inom ramen för NCSC:s verksamhet från och med den 1 juli 2026.

Vidare fastställs i CCCN-förordningen regler för upprättandet av en kompetensgemenskap för cybersäkerhet. MSB har valt att anlita RISE Research Institutes of Sweden AB (RISE) som uppdragstagare för att driva den svenska kompetensgemenskapen i form av Cybernoden Sverige i enlighet med CCCN-förordningens regler. NCC-SE ansvarar i samarbete med RISE för att driva Cybernoden Sverige. Närmare uppgifter för och styrning av Cybernoden i dess roll som den svenska kompetensgemenskapen regleras i ett särskilt avtal mellan MSB samt RISE.

NCC-SE:s uppgift

NCC-SE har till uppgift att främja samarbete mellan svenska forskningsinstitut, företag och myndigheter för utveckling av cybersäkerhetslösningar. Verksamheten ska även främja kontakt mellan svenska och europeiska forskare och företag, underlätta för svenska aktörer att svara på europeiska forsknings- och innovationsutlysningar samt stödja EU:s kompetenscentrum för cybersäkerhet (ECCC) i uppdraget för ökad cybersäkerhet inom EU. NCC-SE tillhandahåller i dag bland annat vägledningar för aktörer som vill söka EU-stöd, anordnar informationsträffar samt samordnar verksamheten i Cybernoden. MSB, genom NCC-SE, prövar frågor om stöd enligt förordningen (2024:664) om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning.

Cybernoden Sveriges uppgift

Cybernoden Sveriges primära syfte är att skapa en samverkansplattform i samhället, där aktörer med intresse och behov av innovation och forskning inom svensk cybersäkerhet kan mötas. Cybernoden är även en länk till den europeiska kompetensgemenskapen med möjlighet att få kunskap om EU-initiativ, delta i arbetsgrupper, påverka

européiska prioriteringar, nätverka och skapa samarbeten inom EU. Cybernoden är en plattform där akademien, näringslivet och offentlig sektor bygger upp samarbeten med målsättningen att initiera forskning och innovation inom cybersäkerhet. I Cybernodens uppdrag ingår att genomföra följande aktiviteter.

- driva ett forum med medlemmarna i den svenska kompetensgemenskapen,
- driva arbetsgrupper under forumet,
- regelbundet arrangera teknik- och innovationskonferenser samt rundabordssamtal,
- administrera och driva en webbplats för den svenska kompetensgemenskapen (dvs. cybernode.se) med en öppen del och medlemsidor som endast medlemmarna i den svenska kompetensgemenskapen har tillgång till,
- tillhandahålla stöd för och genomföra matchmaking-aktiviteter för bildandet av konsortier,
- utföra kommunikationsinsatser avseende den svenska kompetensgemenskapen i enlighet med inriktning från NCC-SE informationsansvarig, samt
- utföra övriga aktiviteter som specificeras i verksamhetsplanen för den svenska kompetensgemenskapen.

Cybercampus Sverige

Cybercampus Sverige inrättades 2024 och har fokus på forskning, innovationer och utbildningar. Det är en satsning och ett samarbete mellan universitet, institut, myndigheter och företag i hela Sverige. Kungliga Tekniska Högskolan (KTH) är huvudman för uppdraget att etablera och utveckla Cybercampus Sverige. Cybercampus Sverige utför forskning, innovation och utbildning för cybersäkerhet och försvar. Verksamheten ska möta behov som inte adresseras av någon av de andra aktörerna på cybersäkerhetsområdet, som stöd för alla samhällssektorer. Cybercampus Sverige syftar till ökad cybersäkerhet, att stärka samhällets försvarsförmåga och svensk konkurrenskraft.

12.5 Stöd till företag gällande regelefterlevnad av EU:s cyberresiliensförordning

Utredningens bedömning: Marknadskontrollmyndigheten som utses enligt EU:s cyberresiliensförordning och CSIRT-enheten bör ges i uppdrag att så tidigt som möjligt och före ikraftträdandet av EU:s cyberresiliensförordning tillhandahålla stöd till företag i syfte att förbereda företag att efterleva förordningens krav.

EU:s cyberresiliensförordning innebär att det införs harmoniserande cybersäkerhetskrav för produkter med digitala element, som gäller under produkternas livscykel, inom flertalet sektorer. För att undvika att EU:s cyberresiliensförordning ska hämma näringslivet och innovation samt säkerställa ett effektivt genomförande av förordningen och undvika risker som följer av bristande kunskap är det av vikt att företag ges förutsättningar och stöd att efterleva kraven i förordningen.

Artikel 33 i EU:s cyberresiliensförordning innehåller bestämmelser om stödåtgärder för företag. Vidare innehåller artikel 10 i EU:s cyberresiliensförordning bestämmelser om hur kompetensen i en cyberresilient digital miljö ska förbättras.

Som angetts i avsnitt 12.3 följer det av andra bestämmelser i EU:s cyberresiliensförordning att CSIRT-enheten och marknadskontrollmyndigheterna ska tillhandahålla visst stöd. CSIRT-enheten kommer att tillhandahålla stöd i samband med rapportering av sårbarheter och incidenter. Marknadskontrollmyndigheterna kommer att ge vägledning och råd samt vidta andra förebyggande åtgärder i syfte att produkter ska kunna uppfylla gällande krav.

Utredningen bedömer att stödet från CSIRT-enheten och marknadskontrollmyndigheterna är av vikt för att säkerställa företagens regelefterlevnad samt säkerställa en enhetlig och harmoniserad tillämpning av kraven i EU:s cyberresiliensförordning. Myndigheternas stöd kommer att kunna öka tydligheten kring regelverket och underlätta för företag och på så sätt undvika en onödig börda för företag.

Stödet kan bestå av allmän och generell information om gällande rätt, inklusive information om angränsande och överlappande regelverk, men kan även bestå av mallar, guider, checklistor, steg-för-steg-

processer, automatiserade stöd via online-tjänster med mera. Genom marknadskontrollansvaret och den samverkan som marknadskontrollmyndigheten har till uppgift att genomföra med andra myndigheter, såväl nationellt som i andra medlemsstater, och företrädare för organisationer och näringsliv i frågor som rör marknadskontroll får myndigheten stor kunskap om regelverket och dess tillämpning, följer arbetet som sker internationellt och får inblick i företagens behov av stöd. Utifrån det kan marknadskontrollmyndigheten bedöma vilket specifikt stöd som saknas och vad som bör tillhandahållas på nationell nivå. Det stöd som tillhandahålls kan behöva anpassas till olika branscher eller sektorer beroende på behov av stöd. Stödet kan även behöva tas fram tillsammans med bransch- eller intresseorganisationer.

CSIRT-enhetens och marknadskontrollmyndighetens stöd kan tillhandahållas direkt från respektive myndighet men kan även förmedlas genom andra befintliga kanaler och plattformar för att säkerställa att stödet når ut till alla berörda. Till exempel kan Tillväxtverkets sida verksam.se användas för visst stöd. [Verksam.se](https://verksam.se) är en hemsida på vilken myndigheter samlar information och tjänster för den som ska starta eller driver företag. Här finns övergripande information om produktsäkerhet, marknadskontroll och CE-märkning. Andra exempel för att nå ut till berörda aktörer är genom de plattformar som andra aktörer och funktioner inom cybersäkerhetsområdet tillhandahåller, såsom NCSC och Cybernoden Sverige.

Stöd som kan lämnas innan EU:s cyberresiliensförordning träder i kraft kan underlätta för företag genom att de så tidigt som möjligt förbereds på vad förordningen innebär för dem. Utredningen bedömer därför att det är av vikt att berörda myndigheter kan tillhandahålla stöd till företag i god tid och att dessa myndigheter därför bör ges i uppdrag att redan före ikraftträdandet av EU:s cyberresiliensförordning tillhandahålla stöd till företag. Utredningen gör bedömningen att ett sådant uppdrag, som gäller tiden före förordningens ikraftträdande, är tillräckligt att ges till marknadskontrollmyndigheten Post- och telestyrelsen, inte samtliga marknadskontrollmyndigheter, och till CSIRT-enheten.

Utredningen bedömer vidare att det stöd som CSIRT-enheten och marknadskontrollmyndigheten kommer att kunna tillhandahålla kan kompletteras med ytterligare mer specifikt stöd som är till nytta för företag. I det följande lämnar utredningen förslag på

stöd som utredningen bedömer är lämpligt för att bistå företag gällande regelefterlevnad av EU:s cyberresiliensförordning och som kompletterar det stöd som CSIRT-enheten och marknadskontrollmyndigheten kommer att bistå med.

12.5.1 Stödåtgärder enligt artikel 33.1

Utredningens bedömning: Myndigheten för samhällsskydd och beredskap (MSB) ska tillhandahålla och samordna stöd till små och medelstora företag enligt artikel 33.1 i EU:s cyberresiliensförordning.

MSB bör ges i uppdrag att så tidigt som möjligt och före ikraftträdandet av EU:s cyberresiliensförordning tillhandahålla stödet i syfte att förbereda små och medelstora företag att efterleva förordningens krav.

Som angetts i avsnitt 12.4 finns det i Sverige ett antal myndigheter som arbetar med cybersäkerhet och som bland annat har i uppgift att ge stöd till företag. Det finns vidare ett antal aktörer och funktioner i Sverige som har i uppgift att ge stöd till företag inom cybersäkerhetsområdet.

Utredningen bedömer att stödet som dessa olika aktörer, inom respektive aktörs uppdrag och ansvarsområde, tillhandahåller även är av stor vikt och kan bidra till genomförandet av EU:s cyberresiliensförordning. Utredningen bedömer att aktörerna har bred cybersäkerhetskompetens vilket så långt som möjligt bör nyttjas även för cyberresiliensförordningens genomförande. Cyberkompetens är en bristvara och blir allt viktigare. För att säkerställa kompetens och effektivitet är det bra att dra nytta av upparbetad kunskap samt befintliga strukturer och processer.

Utredningen bedömer att NCSC, Cybernoden Sverige och Cyber-campus Sverige är aktörer som inom ramen för deras nuvarande verksamhet generellt kan bidra till företagens regelefterlevnad av EU:s cyberresiliensförordning. NCSC kan i sin rådgivande verksamhet utgöra ett allmänt stöd till företag för regelefterlevnad av cyberresiliensförordningens krav. NCSC kan även fungera som plattform för att genomföra kompetenshöjande insatser som till exempel utbildningar och workshops för att höja kunskapen om EU:s cyberresiliensförordning. Cybernoden Sverige fungerar som

en digital mötesplats samt ett nätverk som samlar svenska företag och organisationer inom cybersäkerhetsområdet. På det sättet kan Cybernoden användas som en kanal för kommunikation till företag gällande sådant som rör EU:s cyberresiliensförordning. Via Cybernoden finns även möjlighet att utbilda och kompetensutveckla aktörer i frågor kopplade till EU:s cyberresiliensförordning. Cybercampus Sverige fungerar som en länk mellan svenska företag, relevanta myndigheter och internationell regelverksutveckling inom området genom aktiv omvärldsbevakning, kunskapsdelning och egna forskningsanknutna bidrag. Cybercampus fungerar därmed som ett centralt nav för kunskapsutveckling och kompetensförsörjning.

Utöver det generella cybersäkerhetsstödet som myndigheter och andra aktörer tillhandahåller och utöver det stöd som kommissionen, CSIRT-enheten och marknadskontrollmyndigheterna ska tillhandahålla enligt EU:s cyberresiliensförordning, anser utredningen att MSB bör ges i uppdrag att tillhandahålla stöd till små och medelstora företag, i enlighet med artikel 33.1, för att säkerställa regel efterlevnad av EU:s cyberresiliensförordning.

MSB har i dag i uppdrag att stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom område. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till bland annat företag. MSB tillhandahåller inom ramen för detta uppdrag redan i dag en rad olika stöd kopplade till cybersäkerhet, se vidare avsnitt 12.4.1. Utredningen bedömer att det stöd som behöver tillhandahållas för regel efterlevnad av EU:s cyberresiliensförordning i stor utsträckning kan hanteras inom ramen för de olika stöd som MSB redan i dag tillhandahåller. Till exempel kan cybersäkerhetsrådgivningen utökas till att omfatta EU:s cyberresiliensförordning. Inom ramen för cybersäkerhetskollen skulle det kunna skapas en mätning för provning och bedömning av överensstämmelse enligt EU:s cyberresiliensförordning. MSB är även NCC-SE. Genom NCC-SE kan riktade utlysningar för efterlevnad av EU:s cyberresiliensförordning inrättas. Inom ramen för redan etablerade strukturer kan NCC-SE, i enlighet med vad som anges i skäl 127 i EU:s cyberresiliensförordning, ge tekniskt och vetenskapligt stöd till mikroföretag samt små och medelstora företag, till exempel för testningsverksamhet och tredjepartsbedömningar av överensstämmelse. De skulle

också kunna främja användningen av verktyg för att underlätta genomförandet av förordningen.

Det kan innebära synergieffekter att samla uppgiften att tillhandahålla stöd hos MSB. MSB och NCC-SE verkar dessutom i nära samarbete med EU och andra medlemsstater och har en helhetsbild av EU:s regleringar inom cybersäkerhetsområdet. Det ger MSB och NCC-SE en bra överblick över det ekosystem inom vilket företag som ska tillämpa EU:s cyberresiliensförordning agerar inom och kan bidra till att uppnå en enhetlig och harmoniserad tillämpning av de krav som ställs. Det kan dessutom finnas fördelar med att uppgiften att lämna stöd särskiljs från uppgiften att utöva tillsyn.

Det stöd som MSB och NCC-SE ska tillhandahålla bör samordnas med det stöd som ska lämnas av andra aktörer såsom marknadskontrollmyndigheterna men även andra myndigheter som tillhandahåller stöd enligt angränsande cybersäkerhetsregleringar och annan närliggande reglering. Det är av vikt för att säkerställa att det lämnas ett enhetligt stöd där informationen som lämnas är korrekt och inte skiljer sig åt. Det är även viktigt för att undvika dubbelarbete och bristande effektivitet hos de aktörer som tillhandahåller stödet samt för att underlätta för företag så att det blir tydligt varifrån stödet kommer och för att undvika allt för många olika kanaler för kommunikation. Utredningen anser att MSB bör ges i uppdrag att samordna stödet till företag för regelefterlevnad av EU:s cyberresiliensförordning. MSB bedriver i dag en rad olika samarbetsforum och bör vara sammankallade för ett samarbetsforum med syfte att samordna stöd till företag för regelefterlevnad av EU:s cyberresiliensförordning. Forumet kan till exempel följa den modell som i dag finns inom ramen för NIS-regleringen i Sverige.

Utredningen föreslår att uppgiften att tillhandahålla och samordna stöd till företag regleras i en ny bestämmelse som införs i förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap. Utredningens bedömning är att denna nya arbetsuppgift, som MSB ska utföra genom ändringar i myndighetens instruktion, ska kunna utföras även inom ramen för NCC-SE:s verksamhet. Utredningen anser i tillägg att MSB ges i uppdrag att före ikraftträdandet för EU:s cyberresiliensförordning tillhandahålla stöd till företag i syfte att förbereda företag att efterleva förordningens krav. Utredningen har utformat förslaget efter dialog med MSB och NCC-SE.

Enligt förslagen i slutbetänkandet *Samlade förmågor för ökad cybersäkerhet* (SOU 2025:79) ska uppgifter som i dag utförs av MSB enligt 11 a–c §§ förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap författningsmässigt överföras till FRA men utförs inom ramen för NCSC:s verksamhet från och med den 1 juli 2026. Om dessa förslag beslutas bör uppdraget att tillhandahålla stöd till små och medelstora företag i enlighet med artikel 33.1 i EU:s cyberresiliensförordning ges till FRA i stället för MSB.

Det har till utredningen framförts att det kan finnas anledning att författningsreglera att övriga myndigheter som har i uppgift att ge stöd ska samverka med MSB och NCC-SE. Utredningen ser dock inget behov av att samordningen i sig författningsregleras. Myndigheter har ett generellt ansvar att samverka med varandra enligt förvaltningslagen (2017:900) och myndighetsförordningen (2007:515).

12.5.2 Regulatoriska sandlådor för cyberresiliens enligt artikel 33.2

Utredningens förslag: Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om regulatoriska sandlådor för cyberresiliens.

Utredningens bedömning: En marknadskontrollmyndighet får besluta om inrättande och drift av regulatoriska sandlådor för cyberresiliens enligt artikel 33.2 i EU:s cyberresiliensförordning. En marknadskontrollmyndighet får meddela föreskrifter om regulatoriska sandlådor för cyberresiliens.

Enligt artikel 33.2 i EU:s cyberresiliensförordning får medlemsstaterna, när så är lämpligt, inrätta regulatoriska sandlådor för cyberresiliens.

Regulatoriska sandlådor är ett policyinstrument som finns inom flera olika rättsområden. Regulatoriska sandlådor kan inrättas genom lagstiftning men kan även inrättas på eget initiativ av till exempel myndigheter inom ramen för myndighetens ordinarie arbetsuppgifter och uppdrag. Regulatoriska sandlådor är ett av flera verktyg

som ingår i kommissionens Better Regulation Toolbox¹⁶ och har introducerats i ett antal andra EU-regelverk som till exempel inom ramen för förordning (EU) 2024/1689¹⁷ (AI-förordningen) och förordning (EU) 2024/903¹⁸. Regulatoriska sandlådor kan ha gemensamma egenskaper men deras syfte och funktion avgörs inom ramen för de specifika förutsättningar som gäller respektive regulatorisk sandlåda.

Syftet med regulatoriska sandlådor för cyberresiliens är att tillhandahålla kontrollerade provmiljöer för innovativa produkter med digitala element för att underlätta utvecklingen, utformningen, valideringen och provningen av dem i syfte att uppfylla kraven i cyberresiliensförordningen under en begränsad tidsperiod innan de släpps ut på marknaden.

Det är medlemsstaterna som när så är lämpligt får inrätta regulatoriska sandlådor för cyberresiliens. Det är således inte obligatoriskt att inrätta regulatoriska sandlådor till skillnad mot vad som till exempel gäller inom ramen för AI-förordningen där det i stället är obligatoriskt för varje medlemsstat att upprätta minst en regulatorisk sandlåda för AI, enskilt eller tillsammans med andra medlemsstater.

Det anges inte i EU:s cyberresiliensförordning när det är lämpligt att inrätta regulatoriska sandlådor för cyberresiliens. Artikel 12.4 i EU:s cyberresiliensförordning föreskriver dock att tillverkare av produkter med digitala element vilka omfattas av EU:s cyberresiliensförordning och klassificeras som AI-system med hög risk enligt artikel 6 i AI-förordningen får delta i de regulatoriska sandlådor för AI som avses i artikel 57 i AI-förordningen. För att undvika dubbelarbete bör det enligt utredningen inte vara lämpligt att inrätta en regulatorisk sandlåda för cyberresiliens om en fråga kan hanteras inom en redan existerande regulatorisk sandlåda för AI. Vidare kan det vara olämpligt att hantera frågor som i stället kan hanteras av en konsultbyrå.

¹⁶ Ett dokument som kompletterar dokumentet Commission Staff Working Document the Better Regulation Guidelines, SWD(2021) 305 final.

¹⁷ Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

¹⁸ Europaparlamentets och rådets förordning (EU) 2024/903 av den 13 mars 2024 om åtgärder för en hög nivå av interoperabilitet inom den offentliga sektorn i hela unionen (förordning om ett interoperabelt Europa).

De regulatoriska sandlådorna för cyberresiliens ska inrättas under marknadskontrollmyndigheternas direkta tillsyn, vägledning och stöd. Medlemsstaterna ska genom Adco-gruppen informera kommissionen och de andra marknadskontrollmyndigheterna om inrättandet av en regulatorisk sandlåda. De regulatoriska sandlådorna ska inte påverka de behöriga myndigheternas tillsynsbefogenheter och korrigerande befogenheter. Medlemsstaterna ska säkerställa öppen, rättvis och transparent tillgång till regulatoriska sandlådor, och i synnerhet underlätta tillgång för mikroföretag och små företag, inbegripet uppstarts företag. Kommissionen och, när så är lämpligt, Enisa får tillhandahålla tekniskt stöd, rådgivning och verktyg för inrättande och drift av regulatoriska sandlådor.

Det är av vikt att förutsättningarna för regulatoriska sandlådor för cyberresiliens fastställs. Bland annat om den ska inrättas i digital eller fysisk form, om den ska gälla hårdvara eller mjukvara, vilka resurser som krävs för att genomföra sandlådan, vem som kan delta, vilka problem som ska lösas i sandlådan, vilka som ska involveras i driften av sandlådan, ansvar för eventuella skador som uppstår i sandlådan, hur länge sandlådan ska fortgå samt om projektet kan avslutas i förtid och förutsättningarna för det, vilken information som behöver delas i sandlådan och eventuell fråga om sekretess, sandlådans förhållande till myndighetens marknadskontroll samt om marknadskontrollmyndigheten ska inrätta sandlådan själv eller tillhandahålla en sandlåda genom upphandling.

Utredningen anser principiellt sett att regulatoriska sandlådor för cyberresiliens är en lämplig stödåtgärd för företag och att företag förtjänar möjligheten att kunna dra nytta av sådana sandlådor. Utredningen bedömer att det bör ankomma på marknadskontrollmyndigheterna att besluta om när regulatoriska sandlådor för cyberresiliens ska inrättas och under vilka förutsättningar samt meddela de föreskrifter som behövs.

För frågan om sekretess till skydd för enskild inom ramen för regulatoriska sandlådor för cyberresiliens se avsnitt 11.9.

13 Analys av berörda regelverk

13.1 Inledning

I kommittédirektiven anges att det finns ett behov av att identifiera vilka bestämmelser i svenska författningar som berörs av förordning (EU) 2024/2847¹ (EU:s cyberresiliensförordning) och analysera om de behöver upphävas, ändras eller om nya bestämmelser behövs med anledning av förordningen.

I direktiven framhålls som berörda författningar bland annat lagen (2022:482) om elektronisk kommunikation (LEK), produkt-säkerhetslagen (2004:451), konsumentköplagen (2022:260) (KKöpl) och konsumenttjänstlagen (1985:716) (KtjL). Analys av vilka bestämmelser i angivna författningar som omfattas av tillämpningsområdet för EU:s cyberresiliensförordning och om bestämmelserna behöver upphävas, ändras eller om nya bestämmelser behövs med anledning av förordningen redovisas nedan i berörda avsnitt. När det gäller frågan om potentiellt överlappande krav som följer av andra direkt tillämpliga EU-rättsakter bedömer utredningen att sådana krav i första hand måste hanteras i rättstillämpningen. I kapitel 4 finns en redogörelse för några mer centrala EU-rättsliga förordningar och direktiv på cyberområdet som har beröringspunkter med de nationella författningar som behandlas i detta kapitel.

¹ Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen).

13.2 Lagen (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt

Utredningens bedömning: EU:s cyberresiliensförordning har beröringspunkter med lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt. Det saknas skäl att upphäva, ändra eller införa nya bestämmelser i den lagen med anledning av EU:s cyberresiliensförordning.

Lagen (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt² kompletterar denna och reglerar enligt cybersäkerhetsakten nationell organisation, tillsyn, sanktionsavgifter och processuella frågor.

Det finns beröringspunkter och delvis överlappande krav i regelsystemen. Överlapp uppstår när samma sårbarhet i en certifierad produkt ska hanteras både enligt reglerna i EU:s cybersäkerhetsakt och EU:s cyberresiliensförordning, vilket kan medföra risk för dubbelrapportering och bristande samordning. Även tillsyn enligt EU:s cybersäkerhetsakt och marknadskontroll enligt EU:s cyberresiliensförordning kan beröra samma juridiska person (certifikatsinnehavare/tillverkare). Regelverken har samtidigt delvis olika fokus, även om de riktar sig mot samma aktör i form av tillverkare av en produkt med digitala element.

Det föreligger dock inte någon konflikt mellan regelverken. Regelverken kan tillämpas parallellt och i förekommande fall behöver kraven i båda regelverken uppfyllas. Det saknas därför skäl att lämna förslag på att upphäva, ändra eller införa nya bestämmelser i lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

² Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

13.3 Förslag till ny cybersäkerhetslag (NIS 2-direktivet)

Utredningens bedömning: EU:s cyberresiliensförordning har beröringspunkter med förslaget till ny cybersäkerhetslag. Det saknas skäl att föreslå att upphäva, ändra eller införa nya bestämmelser i den föreslagna lagen med anledning av EU:s cyberresiliensförordning.

I syfte att genomföra direktiv (EU) 2022/2555³ (NIS 2-direktivet) i svensk rätt föreslår regeringen att det ska införas en ny cybersäkerhetslag.⁴ Den nya lagen innebär att offentliga och enskilda verksamhetsutövare inom vissa utpekade sektorer bland annat ska vidta åtgärder för att skydda sina nätverks- och informationssystem samt rapportera betydande incidenter. Den nya lagen innehåller också regler om tillsyn och ingripandemöjligheter mot verksamhetsutövare som inte följer lagens bestämmelser. I lagens föreslås bestämmelser som bland annat anger syftet med lagen (1 kap. 1 §), definitioner (1 kap. 2 §), tillämpningsområde (1 kap. 3–8 §§), verksamhetsutövares skyldigheter (2 kap.), tillsyn (3 kap.), ingripanden (4 kap.) och överklagande (5 kap.). Den nya lagen föreslås träda i kraft den 15 januari 2026.

EU:s cyberresiliensförordning och den föreslagna cybersäkerhetslagen, som genomför NIS 2-direktivet har olika fokus och riktar sig mot olika aktörer. I direktivet finns krav på att berörda verksamhetsutövare (entiteter) ska vidta säkerhetsåtgärder (riskhanteringsåtgärder). Samtidigt finns krav på sårbarhets- och incidentrapportering, om än med delvis olika utgångspunkter, i båda regelverken. Det finns därför beröringspunkter och delvis överlappande krav i regelsystemen.

Det föreligger dock inte någon konflikt mellan regelverken. Regelverken kan tillämpas parallellt och i förekommande fall behöver kraven i båda regelverken uppfyllas. Det saknas därför skäl att lämna förslag på att upphäva, ändra eller införa nya bestämmelser i den

³ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

⁴ Prop. 2025/26:28 Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag.

föreslagna cybersäkerhetslagen med anledning av EU:s cyberresiliensförordning.

13.4 Dataskyddslagen (2018:218)

Utredningens bedömning: EU:s cyberresiliensförordning har beröringspunkter med lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. Det saknas skäl att upphäva, ändra eller införa nya bestämmelser i den lagen med anledning av EU:s cyberresiliensförordning.

Som redovisats i avsnitt 4.3.5 har EU:s cyberresiliensförordning beröringspunkter med förordning (EU) 2016/679⁵ (EU:s dataskyddsförordning). På motsvarande sätt som EU:s dataskyddsförordning syftar EU:s cyberresiliensförordning även till att säkerställa skydd för personuppgifter.

EU:s dataskyddsförordning kompletteras av lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). Dataskyddslagen innehåller bestämmelser om rättslig grund för behandling av personuppgifter, behandling av vissa kategorier av personuppgifter, användningsbegränsningar, begränsningar av vissa rättigheter och skyldigheter, tillsynsmyndighetens handläggning och beslut samt skadestånd och överklagande.

Det föreligger inte någon konflikt mellan regelverken. Regelverken kan tillämpas parallellt och i förekommande fall behöver kraven i båda regelverken uppfyllas. Det saknas därför skäl att upphäva, ändra eller införa nya bestämmelser i dataskyddslagen med anledning av EU:s cyberresiliensförordning.

⁵ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

13.5 Lagen (2022:482) om elektronisk kommunikation

Utredningens bedömning: EU:s cyberresiliensförordning har beröringspunkter med lagen (2022:482) om elektronisk kommunikation (LEK). Det saknas skäl att upphäva, ändra eller införa nya bestämmelser i LEK med anledning av EU:s cyberresiliensförordning.

Det finns beröringspunkter mellan EU:s cyberresiliensförordning och LEK. Utredningen bedömer att de delar i lagen som här är av intresse är bestämmelserna om rätt att använda radiosändare i 3 kap. LEK och bestämmelserna om säkerhet i 8 kap. LEK.

3 kap. LEK gäller den som vill använda radiosändare och 8 kap. LEK gäller tillhandahållare av elektroniska kommunikationsnät och -tjänster. Till skillnad från EU:s cyberresiliensförordning gäller bestämmelserna i LEK inte tillverkare men kan gälla för den som använder produkter med digitala element som omfattas av EU:s cyberresiliensförordning.

13.5.1 Rätt att använda radiosändare

3 kap. 1 § LEK föreskriver att det krävs tillstånd för att få använda radiosändare i Sverige. Bestämmelserna omfattar all frekvensanvändning, oavsett om den avser elektronisk kommunikation eller inte.

I 3 kap. 6 § första stycket LEK anges att tillstånd att använda radiosändare ska beviljas, om de förutsättningar som anges i punkterna 1–7 är uppfyllda. Enligt punkten 7 ska tillstånd beviljas om det kan antas att radioanvändningen inte kommer att orsaka skada för Sveriges säkerhet. För att möjliggöra en tillståndsgivning i de fall där det kan antas att radioanvändningen kommer att orsaka skada för Sveriges säkerhet har det i 3 kap. 12 § första stycket 9 LEK införts en bestämmelse som anger att tillstånd att använda radiosändare får förenas med villkor om krav som är av betydelse för Sveriges säkerhet. 3 kap. LEK möjliggör således för ingripande mot radioanvändning som kan orsaka skada för Sveriges säkerhet. I förarbetena anges att radioanvändning kan vara säkerhetshotande på grund av den tekniska utrustning som används och att det därför är

möjligt att ställa säkerhetskrav på teknisk utrustning, utesluta komponenter, leverantörer, operatörer och radioanvändare som inte håller en tillräckligt hög säkerhetsnivå.⁶

3 kap. LEK reglerar således användningen av radiosändare och inte produkter med digitala element i sig men en tillämpning av bestämmelserna i det enskilda fallet kan komma att påverka bland annat användning eller försäljning av produkter.

Enligt artikel 4 i EU:s cyberresiliensförordning får medlemsstaterna inte, med hänvisning till aspekter som omfattas av förordningen, hindra att produkter med digitala element som uppfyller kraven i förordningen tillhandahålls på marknaden. Vidare anges i skäl 52 i EU:s cyberresiliensförordning att de väsentliga cybersäkerhetskraven i förordningen inte bör påverka tillämpningen av samordnade säkerhetsriskbedömningar på unionsnivå av kritiska leveranskedjor som avses i artikel 22 i NIS 2-direktivet, som beaktar både tekniska och, när så är relevant, icke-tekniska riskfaktorer, såsom tredjelandas otillbörliga påverkan på leverantörer. De bör inte heller påverka medlemsstaternas rätt att fastställa ytterligare krav för att ta hänsyn till icke-tekniska faktorer för att säkerställa en hög resiliensnivå, inbegripet krav som definieras i kommissionens rekommendation (EU) 2019/534 av den 26 mars 2019 IT-säkerhet i 5G-nät, den EU-samordnade riskbedömningen av cybersäkerhet i 5G-nät och EU-verktygslådan för 5G-cybersäkerhet som överenskommit av samarbetsgruppen som inrättats enligt artikel 14 i NIS 2-direktivet.

Förbudet i artikel 4 i EU:s cyberresiliensförordning gäller endast om det sker med hänvisning till aspekter som omfattas av cyberresiliensförordningen. Bestämmelserna i 3 kap. LEK utgör inte något sådant hinder som avses i artikel 4 i EU:s cyberresiliensförordning. En ekonomisk aktör har således rätt att tillhandahålla en produkt på marknaden om reglerna i EU:s cyberresiliensförordning är uppfyllda. Däremot kan en produkts användning i enskilda fall påverkas av 3 kap. LEK när en radiotillståndshavare under vissa förutsättningar i villkor kan förbjudas att använda vissa produkter även om de aktuella produkterna i sig uppfyller kraven i cyberresiliensförordningen.

Trots den påverkan som 3 kap. LEK kan ha på produkter med digitala element som uppfyller kraven i EU:s cyberresiliensförord-

⁶ Prop. 2019/20:15 sid. 29 och 31.

ning så föreligger ingen konflikt mellan regelverken. Det saknas således anledning att upphäva, ändra eller införa nya bestämmelser i 3 kap. LEK med anledning av EU:s cyberresiliensförordning.

13.5.2 Säkerhetsåtgärder och incidentrapportering

8 kap. 1–4 §§ LEK innehåller bestämmelser om säkerhet i nät och tjänster. 8 kap. 6–9 §§ LEK innehåller bestämmelser om skydd av uppgifter vid tillhandahållande av tjänster. Bestämmelserna uppställer krav att tillhandahållare av elektroniska kommunikationsnät och -tjänster ska vidta säkerhetsåtgärder och rapportera incidenter.

Bestämmelserna i 8 kap. 1–4 §§ LEK utgör det svenska genomförandet av bestämmelserna om säkerhetsåtgärder och incidentrapportering i direktiv (EU) 2018/1772⁷ (kodexen). Bestämmelserna i 8 kap. 6–9 §§ LEK utgör det svenska genomförandet av motsvarande bestämmelser i direktiv (EG) 2002/58⁸ (e-dataskyddsdirektivet). E-dataskyddsdirektivet är ett direktiv som preciserar och kompletterar EU:s dataskyddsförordning. För en redogörelse av kodexen och e-dataskyddsdirektivet, se avsnitt 4.3.2 och 4.3.5.

NIS 2-direktivet upphäver bestämmelserna om säkerhetsåtgärder och incidentrapportering i kodexen (artikel 40 och 41) och ersätter dem med bestämmelserna som följer av NIS 2-direktivet. Genomförandet av NIS 2-direktivet i svensk rätt innebär att bestämmelserna om säkerhetsåtgärder och incidentrapportering, som har sin grund i kodexen och som återfinns i 8 kap. 1–4 §§ LEK, upphävs och ersätts av motsvarande bestämmelser i den föreslagna cybersäkerhetslagen (2025:000), se ovan avsnitt 13.3. E-dataskyddsdirektivet påverkas dock inte av NIS 2-direktivet och gäller fortsatt. Skyldigheten att vidta säkerhetsåtgärder och incidentrapportering i enlighet med vad som gäller enligt 8 kap. 6–9 §§ LEK kvarstår därför oförändrad när NIS 2-direktivet genomförs i svensk rätt.

Enligt 8 kap. 6 § LEK ska den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att uppgifter som

⁷ Europaparlamentets och rådets direktiv (EU) 2018/1772 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation.

⁸ Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation).

behandlas i samband med tillhandahållandet av tjänsten skyddas. Den som tillhandahåller ett allmänt elektroniskt kommunikationsnät ska vidta de åtgärder som är nödvändiga för att upprätthålla motsvarande skydd i nätet. Åtgärderna ska vara ägnade att säkerställa en nivå på säkerheten som, med hänsyn till tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för integritetsincidenter.

Enligt 8 kap. 8 § LEK ska den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst utan onödigt dröjsmål underrätta tillsynsmyndigheten om integritetsincidenter. Om en incident kan antas inverka negativt på de abonnenter eller användare som de behandlade uppgifterna berör, eller om tillsynsmyndigheten begär det, ska även dessa underrättas utan onödigt dröjsmål.

Om det vid tillhandahållande av en allmänt tillgänglig elektronisk kommunikationstjänst finns en särskild risk för bristande skydd av behandlade uppgifter, ska den som tillhandahåller tjänsten enligt 8 kap. 7 § LEK informera berörda abonnenter om risken. Om den som tillhandahåller tjänsten inte enligt 6 § är skyldig att vidta de åtgärder som avses där, ska abonnenterna informeras om hur och till vilken ungefärlig kostnad som risken kan elimineras.

Bestämmelserna i 8 kap. 6–9 §§ LEK syftar till att uppgifter som behandlas i samband med tillhandahållandet av elektroniska kommunikationsnät och -tjänster skyddas. Tillhandahållare är enligt bestämmelserna skyldiga att vidta åtgärder för att hantera risken för händelser som kan leda till oavsiktlig eller otillåten utplåning, förlust eller ändring eller otillåtet avslöjande av eller otillåten åtkomst till behandlade uppgifter. Även EU:s cyberresiliensförordning syftar till att säkerställa skydd för behandlade uppgifter. Produkter med digitala element får tillhandahållas på marknaden endast om de uppfyller de väsentliga cybersäkerhetskraven i bilaga 1 i EU:s cyberresiliensförordning. Kraven innebär bland annat att tillverkare ska säkerställa skydd mot obehörig åtkomst, skydda riktigheten hos och konfidentialiteten för behandlade uppgifter samt endast behandla uppgifter som är nödvändigt i förhållande till syftet med produkten ("uppgiftsminimiering"). Vidare innehåller både EU:s cyberresiliensförordning och 8 kap. LEK bestämmelser om skyldigheter att rapportera incidenter till myndigheter och skyldigheter att informera användare om incidenter.

EU:s cyberresiliensförordning och 8 kap. LEK innehåller som ovan angetts bestämmelser som båda syftar till att skydda behandlade uppgifter. Reglerna har dock olika tillämpningsområden genom att EU:s cyberresiliensförordning gäller för tillverkare och ställer krav på produkter med digitala element i sig medan 8 kap. LEK gäller tillhandahållare av elektroniska kommunikationsnät och -tjänster och ställer krav på näten och tjänsterna.

Även om LEK inte reglerar produkter med digitala element i sig kan bestämmelserna få en påverkan på användningen av sådana produkter vid tillhandahållandet av elektroniska kommunikationsnät och -tjänster. Tillhandahållare kan, som ett led i att säkerställa överensstämmelse med bestämmelserna i 8 kap. LEK, ställa säkerhetskrav på produkterna som används i tillhandahållarens verksamhet. Även tillsynsmyndighetens tillämpning av LEK kan i enskilda fall få en indirekt påverkan på säkerheten i produkter. EU:s cyberresiliensförordning kan bidra till att behandlade uppgifter skyddas och att likvärdiga krav ställs på tillverkare. EU:s cyberresiliensförordning kan även underlätta för tillhandahållare av elektroniska kommunikationsnät och -tjänster att efterleva kraven i 8 kap. LEK genom att produkterna utformas, utvecklas och produceras på ett sådant sätt att de i sig säkerställer ett skydd för behandlade uppgifter.

Trots den påverkan som 8 kap. LEK indirekt kan ha på produkter med digitala element så finns det inte någon konflikt mellan regelverken. Det saknas således anledning att upphäva, ändra eller införa nya bestämmelser i 8 kap. LEK med anledning av EU:s cyberresiliensförordning. Regelverken kan tillämpas parallellt och i förekommande fall behöver kraven i båda regelverken uppfyllas.

13.6 Radioutrustningslagen (2016:392)

Utredningens bedömning: EU:s cyberresiliensförordning har beröringspunkter med bestämmelserna i radioutrustningslagen (2016:392). Det saknas skäl att upphäva, ändra eller införa nya bestämmelser i radioutrustningslagen med anledning av EU:s cyberresiliensförordning.

Radioutrustningslagen (2016:392) innehåller bestämmelser om tillhandahållande av radioutrustning på marknaden och om viss använd-

ning av sådan utrustning. I LEK finns det bestämmelser om användning av radiosändare, se ovan avsnitt 13.5.1.

Som redovisats i avsnitt 4.3.6 är radioutrustningslagen med anslutande föreskrifter det svenska genomförandet av direktiv 2014/53/EU⁹ (radioutrustningsdirektivet).

Enligt 5 § radioutrustningslagen ska radioutrustning vara konstruerad och tillverkad så att den uppfyller väsentliga krav.

Väsentliga krav gällande cybersäkerhet finns i delegerade förordning (EU) 2022/30¹⁰. Inom andra områden som hälsa och säkerhet, elektromagnetisk kompatibilitet och spektrumanvändning är de väsentliga kraven som regleras i radioutrustningsdirektivet genomförda i Post- och telestyrelsen föreskrifter (PTSFS 2023:2) om radioutrustning.

Som redovisats i avsnitt 4.3.6 har kommissionen för avsikt att upphäva delegerade förordning (EU) 2022/30 när EU:s cyberresiliensförordning ska börja tillämpas.¹¹

Radioutrustningslagen i sig påverkas inte av detta och det föreligger ingen konflikt mellan den lagen och EU:s cyberresiliensförordning. Det saknas därför skäl att upphäva, ändra eller införa nya bestämmelser i radioutrustningslagen med anledning av EU:s cyberresiliensförordning. Regelverken kan tillämpas parallellt och i förekommande fall behöver kraven i båda regelverken uppfyllas.

13.7 Produktsäkerhetslagen (2004:451)

Utredningens bedömning: Av produktsäkerhetslagen (2004:451) framgår att lagen inte ska tillämpas på varor när det gäller risker som omfattas av särskilda säkerhetskrav i någon annan författning eller i en EU-förordning. EU:s förordning om allmän produktsäkerhet innehåller materiella bestämmelser om produkt-

⁹ Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG.

¹⁰ Kommissionens delegerade förordning (EU) 2022/30 av den 29 oktober 2021 om komplettering av Europaparlamentets och rådets direktiv 2014/53/EU vad gäller tillämpningen av de väsentliga krav som avses i artikel 3.3 d, e och f i det direktivet.

¹¹ Kommissionen har den 26 maj 2025 tagit fram ett utkast till förslag på delegerad förordning som avser att upphäva delegerade förordning (EU) 2022/30 från och med den 11 december 2027, se <https://circabc.europa.eu/ui/group/43315f45-aaa7-44dc-9405-a86f639003fe/library/12166519-54dd-4466-991b-7012d258f9d1/details>.

säkerhet som har samma syfte som produktsäkerhetslagen och ska tillämpas före den lagen.

Direktiv 2001/95/EG¹² (direktivet) har genomförts i svensk rätt huvudsakligen genom produktsäkerhetslagen (2004:451) och produktsäkerhetsförordningen (2004:469). Direktivet tillämpas uteslutande på varor som tillhandahålls i näringsverksamhet, med undantag för vissa typer av begagnade varor.

Produktsäkerhetslagen syftar till att säkerställa att varor och tjänster som tillhandahålls konsumenterna inte orsakar skada på person (1 §). Lagen tillämpas i fråga om varor och tjänster som tillhandahålls i näringsverksamhet och varor som tillhandahålls i offentlig verksamhet. En förutsättning är att varan eller tjänsten är avsedd för konsumenterna eller kan antas komma att användas av konsumenterna (2 § första stycket). Vad som sägs i lagen om näringsidkare och tillverkare gäller också den som i offentlig verksamhet tillhandahåller sådana varor som avses i första stycket. Lagen har alltså ett bredare tillämpningsområde än direktivet.

Av 4 § produktsäkerhetslagen framgår att bestämmelserna i 7–9, 11 och 12 §§ inte ska tillämpas på varor när det gäller risker som omfattas av särskilda säkerhetskrav i någon annan författning eller i en EU-förordning.

I kapitel 4 finns en redogörelse för förordning (EU) 2023/988¹³, som trädde i kraft 2023 och tillämpas fullt ut från den 13 december 2024. Förordningen ersätter det tidigare produktsäkerhetsdirektivet (2001/95/EG) och ställer det allmänna säkerhetskravet att endast säkra konsumentprodukter får släppas ut/tillhandahållas på marknaden. Förordningen ska tillämpas på alla produkter som tillhandahålls i en näringsverksamhet om de är avsedda för, eller kan förväntas under rimligen förutsebara förhållanden, att användas av konsumenterna, i den utsträckning det inte finns några särskilda bestämmelser med samma syfte i unionslagstiftningen som reglerar säkerheten för produkten i fråga (artikel 2.1 och 3.1). Om produkter omfattas av särskilda säkerhetskrav som följer av unionslagstiftning

¹² Europaparlamentets och rådets direktiv 2001/95/EG av den 3 december 2001 om allmän produktsäkerhet.

¹³ Europaparlamentets och rådets förordning (EU) 2023/988 av den 10 maj 2023 om allmän produktsäkerhet, ändring av Europaparlamentets och rådets förordning (EU) nr 1025/2012 och Europaparlamentets och rådets direktiv (EU) 2020/1828 och om upphävande av Europaparlamentets och rådets direktiv 2001/95/EG och rådets direktiv 87/357/EEG.

ska förordningen gälla bara de aspekter och risker som inte täcks av de särskilda säkerhetskraven. Det innebär att produkter som omfattas av harmoniserad unionslagstiftning inte ska omfattas av bestämmelserna om säkerhetskrav som finns i kapitel II när det gäller de risker som omfattas av den harmoniserade unionslagstiftningen. I den situationen tillämpas inte avsnitt 1 i kapitel III (Ekonomiska aktörers skyldigheter), och inte heller kapitlen V (Marknadskontroll och genomförande), VII (Kommissionens roll och samordning av kontrollen av efterlevnaden) eller IX–XI (Internationellt samarbete, Finansiella bestämmelser och Slutbestämmelser). Vissa produktkategorier är helt undantagna från tillämpningsområdet, bland annat läkemedel, livsmedel, levande växter och djur samt antikviteter (artikel 2.2).

I artikel 6.1 i förordning (EU) 2023/988 anges kriterier för att bedöma om en produkt är säker. I artikel 6.1 (g) anges krav som tar sikte på cybersäkerhet i produkten (se kapitel 4, avsnitt 4.4.).

När det krävs på grund av produktens art: lämpliga cybersäkerhets-egenskaper som är nödvändiga för att skydda produkten mot yttre påverkan, inbegripet tredje parter med avsikt att vålla skada, när en sådan påverkan kan inverka på produktens säkerhet, inbegripet eventuell förlust av sammankoppling.

En produkts säkerhet, dvs. för konsumenternas hälsa och säkerhet, ska bedömas även utifrån om produkten – när det är relevant för produkttypen – har tillräckliga cybersäkerhetsfunktioner för att motstå yttre angrepp som kan påverka dess säkra funktion.

Lex specialis-principen

Förordning (EU) 2023/988 är en horisontell ram för allmän produktsäkerhet och innehåller en konkurrensbestämmelse om förhållandet till annan lagstiftning. Som framgår ovan ska för en produkt som omfattas av särskilda säkerhetskrav i unionslagstiftning förordningens krav endast gälla de aspekter och risker som inte täcks av den särskilda lagstiftningen. EU:s cyberresiliensförordning utgör en sådan speciallagstiftning med avseende på cybersäkerhetsrisker hos produkter med digitala element (se artikel 11 i EU:s cyberresiliensförordning, avsnitt 4.4.3). Det innebär att för produkter med digitala element som omfattas av cyberresiliensförordningen

tar den förordningens detaljerade krav över vad gäller cybersäkerhetsaspekterna. Den generella regeln i angivna artikel 6.1 (g) i förordning (EU) 2023/988 kompletterar endast i den mån en cybersäkerhetsrelaterad risk för konsumentens hälsa eller säkerhet inte omfattas av regelverket i EU:s cyberresiliensförordning.

EU:s cyberresiliensförordning och tillämpning på produktsäkerhetskrav

EU:s cyberresiliensförordning gäller för produkter med digitala element, vilket definieras som en maskinvaru- eller programvaruprodukt inklusive dess fjärrdatabehandlingslösningar. Detta innebär att inte bara själva den fysiska eller digitala produkten omfattas, utan även tillhörande digitala tjänster som produkten är beroende av för att fungera korrekt. Enligt förordningen avses med fjärrdatabehandling av data databehandling på distans som utvecklats av (eller på uppdrag av) tillverkaren och vars avsaknad skulle hindra produkten från att utföra en av sina funktioner. Sådana integrerade fjärrtjänster (relaterade digitala tjänster), betraktas i dessa fall som en del av produkten och måste uppfylla cybersäkerhetskraven i förordningen.

I skäl 11 och 12 i EU:s cyberresiliensförordning ges exempel på när en tjänst faller inom förordningens tillämpningsområde. Om en smart enhet eller programvara kräver uppkoppling till en molnlösning eller databas som tillhandahålls av tillverkaren för att fullgöra en av sina grundläggande funktioner, så anses den tjänsten omfattad av förordningen som en fjärrdatabehandlingslösning. Bland annat nämns molnbaserade funktioner, till exempel en tillverkares molnplattform som gör det möjligt för användare att fjärrstyra enheten, som inkluderade i förordningens tillämpningsområde. Det innebär att tillverkaren måste garantera cybersäkerheten för hela systemet, dvs. både den fysiska produkten och den nödvändiga onlinetjänsten, under produktens livscykel.

Det är samtidigt viktigt att notera att inte alla tjänster online omfattas av förordningen. För att en molnlösning- eller onlinetjänst ska omfattas krävs att den uppfyller angivna definition, dvs. att tjänsten är framtagen av (eller för) tillverkaren och är nödvändig för produktens funktion. Fristående tjänster som inte är integrerade i produktens funktionalitet omfattas inte av förordningens tillämpnings-

område. I skäl 12 anges att till exempel webbplatser som inte stöder produktens funktion eller molntjänster utanför tillverkarens kontroll inte omfattas av EU:s cyberresiliensförordning. Sådana allmänna IKT-tjänster kan i stället omfattas av andra regelverk, exempelvis gäller NIS 2-direktivet för leverantörer av molntjänster som SaaS, PaaS eller IaaS.

EU:s cyberresiliensförordning adresserar således de tillverkarspecifika digitala tjänster som är inbyggda i produkten, medan fristående digitala tjänster regleras genom sektorspecifika lagar eller NIS 2-direktivet.

Sammanfattningsvis tillämpas EU:s cyberresiliensförordning på produkter med digitala element i vid mening, vilket även innefattar relaterade digitala tjänster, om dessa utgör en del av produktens avsedda funktion. Genom denna breda definition säkerställs att cybersäkerhetskraven omfattar hela ekosystemet kring en uppkopplad produkt, till exempel att tillverkaren måste hålla både produkten och dess molnlösning skyddade mot cyberhot och sårbarheter. Däremot undantas tjänster som ligger utanför tillverkarens ansvar eller inte är nödvändiga för funktionaliteten, eftersom de faller utanför förordningens syfte, men i stället kan omfattas av andra regelverk som till exempel NIS 2-direktivet.

Produktsäkerhetslagen

Som framgår ovan genomför produktsäkerhetslagen (2004:451) det tidigare direktivet om allmän produktsäkerhet och innehåller liknande krav som i den nya förordningen om allmän produktsäkerhet. Som anges ovan ersätter förordning (EU) 2023/988 överlappande nationella bestämmelser på området för konsumentprodukters säkerhet från december 2024.

Produktsäkerhetslagen, som under utredningsarbetet är föremål för revidering, kommer för närvarande främst att ha betydelse i den mån nationella kompletterande regler behövs som komplement till förordning (EU) 2023/988.

Utredningen bedömer mot bakgrund av det ovan angivna att det inte kommer att uppstå någon konflikt mellan regelverken vid tillämpningen. Det saknas därför skäl att lämna förslag på att upphäva,

ändra eller införa nya bestämmelser i produktsäkerhetslagen med anledning av EU:s cyberresiliensförordning.

13.8 Konsumentköplagen (2022:260)

Utredningens bedömning: EU:s cyberresiliensförordning har beröringspunkter med konsumentköplagen (2022:260) (KKöpl). Det finns ingen konflikt i normhierarkin och båda regelverken kan tillämpas parallellt. Det saknas skäl att upphäva, ändra eller införa nya bestämmelser i KKöpl med anledning av EU:s cyberresiliensförordning.

I utredningsdirektiven anges att EU:s cyberresiliensförordning kan medföra att säkerhetsrelaterade garantier och rättigheter som rör digitala produkter kan behöva integreras i konsumentköplagen (2022:260) (KKöpl).

13.8.1 EU:s cyberresiliensförordning

EU:s cyberresiliensförordning ska tillämpas på produkter med digitala element, dvs. produkter som kan ansluta direkt eller indirekt till en annan enhet eller ett nätverk. I cyberresiliensförordningen anges att produkten ska uppfylla väsentliga krav på cybersäkerhet, bland annat information till användare, riskbedömning, sårbarhetshantering, säkerhetsuppdateringar och fastställande av stödperiod.

I artikel 13.1 i EU:s cyberresiliensförordning anges att när en produkt med digitala element släpps ut på marknaden ska tillverkarna säkerställa att den har utformats, utvecklats och producerats i enlighet med de väsentliga cybersäkerhetskrav som fastställs i bilaga I i del I. Tillverkarna ska göra en bedömning av de cybersäkerhetsrisker som är förbundna med en produkt med digitala element och beakta resultatet av bedömningen under planerings-, utformnings-, utvecklings-, produktions-, leverans- och underhållsfaserna för en produkt med digitala element, för att minimera cybersäkerhetsriskerna, förhindra incidenter och minimera deras konsekvenser, inbegripet vad gäller användarnas hälsa och säkerhet (punkt 2). Bedömningen av cybersäkerhetsrisker ska dokumenteras och uppdateras

på lämpligt sätt under en stödperiod som ska fastställas i enlighet med punkt 8 i samma artikel. Bedömningen av cybersäkerhetsrisker ska ange huruvida, och i så fall på vilket sätt, de säkerhetskrav som anges i bilaga I del I punkt 2 är tillämpliga på den relevanta produkten med digitala element och hur dessa krav genomförs på grundval av bedömningen av cybersäkerhetsrisker. Det ska också anges hur tillverkaren tillämpar bilaga I del I punkt 1 och de krav på sårbarhetshantering som anges i bilaga I del II (punkt 3).

När en produkt med digitala element släpps ut på marknaden ska tillverkaren inkludera den bedömning av cybersäkerhetsrisker som avses i nämnda punkt 3 i den tekniska dokumentation som krävs enligt artikel 31 och bilaga VII.

När en produkt med digitala element släpps ut på marknaden, och under stödperioden, ska tillverkarna säkerställa att produktens, inbegripet dess komponenters, sårbarheter hanteras effektivt och i enlighet med de väsentliga cybersäkerhetskrav som fastställs i bilaga I del II.

Tillverkarna ska fastställa stödperioden så att den återspeglar den tidsperiod under vilken produkten förväntas vara i bruk, med särskilt beaktande av rimliga förväntningar från användarna, produktens art, inbegripet dess avsedda ändamål, samt relevant unionsrätt som fastställer livslängden för produkter med digitala element.

Stödperioden ska vara minst fem år. Om produkten med digitala element förväntas vara i bruk i mindre än fem år ska stödperioden motsvara den förväntade användningstiden.

Kommissionen får anta delegerade akter i enlighet med artikel 61 för att komplettera förordningen genom att specificera den minsta tillåtna stödperioden för specifika produktkategorier om uppgifter från marknadskontrollen tyder på otillräckliga stödperioder.

Tillverkarna ska inkludera den information som har beaktats för att fastställa stödperioden för en produkt med digitala element i den tekniska dokumentationen enligt bilaga VII.

Tillverkarna ska vidare säkerställa att varje säkerhetsuppdatering som avses i bilaga I del II punkt 8 och som har gjorts tillgänglig för användare under stödperioden förblir tillgänglig efter det att den har utfärdats i minst tio år eller under återstoden av stödperioden, beroende på vilken period som är längst (punkt 9). Innan en produkt med digitala element släpps ut på marknaden ska tillverkarna sammanställa den tekniska dokumentation som avses i artikel 31 (punkt 12).

13.8.2 Närmare om konsumentens rättigheter enligt konsumentköplagen

KKöpl innehåller bestämmelser om skydd för konsumenter när de köper varor av näringsidkare. Lagen är utformad för att implementera direktiv (EU) 2019/771¹⁴ (EU:s varudirektiv) respektive direktiv (EU) 2019/770¹⁵ (EU:s digitalköpsdirektiv) och omfattar utöver köp av en vara även köp av digitalt innehåll och digitala tjänster, inklusive varor med digitala delar.

I 1 kap. 1 § anges att i lagen finns bestämmelser om skydd för konsumenter vid köp av varor där köparen är konsument och säljaren är näringsidkare. Med näringsidkare avses i lagen säljaren, om inte något annat anges. Med konsument avses köparen. Med varor avses lösa saker, med eller utan digitala delar (se 2 §). Vidare anges att i 2–8 kap. finns reglerna om köp av varor, bland annat vad som utgör fel i vara och konsumentens rättigheter.

I 9 kap. 1 § finns regler om tillhandahållande av digitalt innehåll eller digitala tjänst. För digitalt innehåll på ett fysiskt medium ska 2 kap. 1 och 2 §§, 3 § första stycket och 5 och 6 §§ tillämpas, i stället för det som anges i paragrafens första och andra stycken. Av 9 kap. 4 § följer att för avtal om tillhandahållande av ett digitalt innehåll eller en digital tjänst gäller 4 kap. 1–4 §§ om krav på varan och 4 kap. 5–8 och 10–12 §§ om fel på varan. Vad gäller lagens krav på uppdateringar vid ett enstaka tillhandahållande av ett digitalt innehåll eller en digital tjänst gäller näringsidkarens skyldighet under den tid som konsumenten med fog kan förutsätta uppdateringar. Vid kontinuerligt tillhandahållande av ett digitalt innehåll eller en digital tjänst under en period gäller skyldigheten under tre år efter det att varan med digitala delar avlämnades eller den längre tid som avtalet löper under eller minst tre år för digitala delar, vilket grundas på EU:s minimikrav i direktivet.

¹⁴ Europaparlamentets och rådets direktiv (EU) 2019/771 av den 20 maj 2019 om vissa aspekter på avtal om försäljning av varor, om ändring av förordning (EU) 2017/2394 och direktiv 2009/22/EG samt om upphävande av direktiv 1999/44/EG (som fortsättningsvis benämns varudirektivet).

¹⁵ Europaparlamentets och rådets direktiv (EU) 2019/770 av den 20 maj 2019 om vissa aspekter på avtal om tillhandahållande av digitalt innehåll och digitala tjänster (som fortsättningsvis benämns digitaldirektivet).

13.8.3 Överväganden

Utredningen bedömer att en produkt med digitala element enligt definitionen i artikel 2 i EU:s cyberresiliensförordning omfattas av KKöPL:s tillämpningsområde och det finns skäl att analysera om bestämmelserna i cyberresiliensförordningen föranleder att de säkerhetsgarantier och rättigheter som följer av förordningen behöver integreras i KKöPL. EU:s cyberresiliensförordning omfattar produkter med digitala element som kan ansluta direkt eller indirekt till en annan enhet eller ett nätverk. Om en produkt med digitala element är helt fristående och inte kan kommunicera med andra enheter, torde den därför falla utanför förordningens tillämpningsområde. Det kan noteras att KKöPL inte ställer några krav på uppkoppling, till exempel internet- eller nätverksanslutning utan omfattar alla varor med digitala delar. Det finns således en överlappning av bestämmelserna i regelverken samtidigt som de skiljer sig åt i andra avseenden.

Utredningen bedömer att mer allmänt föreligger inte någon normkonflikt mellan bestämmelserna i EU:s cyberresiliensförordning och KKöPL. Vissa bestämmelser bör dock analyseras mer ingående i syfte att undersöka om den överlappning som finns medför att någon bestämmelse kan medföra oklarhet eller otydlighet vid rätts-tillämpningen. Det gäller i första hand bestämmelser i regelverken som rör krav på en vara med digitala delar samt skyldighet att lämna information och tillhandhålla säkerhetsuppdateringar.

Krav på varans beskaffenhet

EU:s cyberresiliensförordning innehåller bestämmelser om att en produkt med digitala element (varan) ska vara säker, dvs. uppfylla väsentliga krav på cybersäkerhet och stämma överens med de uppgifter som framgår av EU-försäkran och CE-märkningen för produkten. Av bestämmelserna i cyberresiliensförordningen framgår vad konsumenten kan förvänta sig för att produkten ska anses säker vad avser krav på cybersäkerhet i produkten med digitala element.

KKöPL innehåller allmänna krav på varors kvalitet och säkerhet. Enligt 4 kap. 1–2 §§ ska varan stämma överens med avtalet (subjektiva krav) och uppfylla vad konsumenten rimligen kan förvänta sig i fråga om bland annat hållbarhet, funktionalitet, kompatibilitet och

säkerhet (objektiva krav). Att säkerhet uttryckligen nämns innebär att varan (produkten) inte ska utgöra någon risk vid normal användning. Normalt avser detta fysisk säkerhet, till exempel att inga brandfarliga fel finns, men begreppet torde även få anses inbegripa egenskaper som rör cybersäkerhet i varan (produkten) om brister i dessa innebär en risk och kan orsaka skada. En vara som brister i cybersäkerhet, till exempel saknar grundläggande skydd eller har allvarliga sårbarheter, kan komma att avvika från vad konsumenten med fog kan förvänta sig av en sådan produkt, och kan därmed bedömas som felaktig enligt 4 kap. 2 § och 5 §.

Sammanfattningsvis kan noteras att när gäller krav på säkerhet i produkten/varan ställer artikel 13 i EU:s cyberresiliensförordning krav på cybersäkerhet i produkten med digitala element och KKöPL ställer krav på att varan med digitala delar ska uppfylla krav på säkerhet. De i förordningen ställda kraven på cybersäkerhet torde innebära att en produkt som uppfyller dessa krav även torde uppfylla krav på att varan ska vara säker enligt KKöPL, dvs. möter objektiva krav på cybersäkerhet i den aktuella varan med digitala delar.

De angivna bestämmelserna syftar till säkra och uppdaterade produkter för användare/konsumenter, men gör det ur olika perspektiv. Bestämmelserna överlappar till del och kompletterar även varandra. De kan tillämpas parallellt och det föreligger inte någon normkonflikt i detta avseende. Det saknas därför skäl att föreslå någon komplettering eller ändring till KKöPL i nu aktuellt hänseende.

Krav på säkerhetsuppdatering och stödperiod

När det gäller skyldigheten enligt artikel 13 i EU:s cyberresiliensförordning att lämna information och tillhandahålla uppdateringar under stödperioden kan noteras att det kommer att finnas ett betydande antal produkter med digitala element på marknaden som samtidigt torde utgöra en vara med digitala delar. Produkten kommer att omfattas av den stödperiod som anges av tillverkaren av produkten.

I sammanhanget sak noteras vad som föreskrivs om utformningen av stödperioden i artikel 13 och vad som gäller säljarens skyldighet att tillhandahålla uppdateringar enligt 4 kap. 4 § och 9 kap. 4 § KKöPL. Regleringen i 4 kap. 4 § är utformad efter vad

som anges i digitaldirektivet och för svensk del bestämdes tiden till tre år.

Med införandet av EU:s cyberresiliensförordning kommer det att finnas två olika regleringar med i vissa fall delvis olika tidsperioder med skyldighet att tillhandhålla säkerhetsuppdateringar, en som gäller för tillverkaren av en produkt med digitala element och en som gäller för säljaren av en vara med digitala delar (näringsidkaren).

Den i artikel 13.8 angivna stödperioden, under vilken tillverkaren är skyldig att lämna information, hantera sårbarheter och vid behov tillhandhålla uppdateringar som rör cybersäkerheten i produkten, är som huvudregel fem år, samtidigt som tillverkaren får ange stödperioden till såväl kortare som längre period beroende på bland annat produktens art och avsedda tillämpning.

Samtidigt innehåller 4 kap. 3 och 4 §§ KKöpl bestämmelser om information och krav på uppdateringar för varor med digitala delar, även om det kommer till uttryck på ett delvis annat sätt. Enligt dessa bestämmelser ska näringsidkaren före köpet upplysa konsumenten om sådana förhållanden som rör varans egenskaper eller användning som näringsidkaren känner till eller bör känna till och som konsumenten med fog kan räkna med att bli upplyst om, under förutsättning att informationen kan antas inverka på köpet. Vidare ska näringsidkaren se till att konsumenten informeras om och tillhandahålls säkerhetsuppdateringar och andra nödvändiga uppdateringar. Vid ett *enstaka* tillhandahållande av ett digitalt innehåll eller en digital tjänst gäller näringsidkarens skyldighet under den tid som konsumenten med fog kan förutsätta uppdateringar. Vid *kontinuerligt* tillhandahållande av ett digitalt innehåll eller en digital tjänst under en period gäller skyldigheten under *tre år* efter det att varan med digitala delar avlämnades eller den längre tid som avtalet löper. Den angivna begränsningen till tre år för skyldigheten att tillhandhålla uppdateringar vid kontinuerligt tillhandhållande kan således i vissa fall vara kortare än tillverkarens skyldighet att tillhandhålla uppdateringar enligt stödperioden för produkten.

Samtidigt ska varan med digitala delar uppdateras i den utsträckning det behövs för att uppfylla de krav som ställs i 2 § KKöpl när det gäller krav på cybersäkerhet. Denna uppdateringsskyldighet får anses utgöra ett objektivet krav på avtalsenlighet som konsumenten kan kräva ska fullgöras.

I detta sammanhang uppkommer även frågan om en EU-försäkran om överensstämmelse enligt artikel 28 och en CE-märkning enligt artikel 30 i EU:s cyberresiliensförordning kan anses utgöra en sådan "liknande utfästelse" som innebär att tillverkaren även enligt 4. kap 21 och 22 §§ KKöpl i köprättslig mening åtagit sig att under en viss tid svara för varan eller en del av varan eller för en egenskap hos varan under den i EU-försäkran angivna tiden.

EU-försäkran om överensstämmelse är en skriftlig försäkran från tillverkaren att produkten uppfyller tillämpliga krav på cybersäkerhet i förordningen och som utgör självdeklaration under tillverkarens eget ansvar. Ansvar för att intyga att kraven är uppfyllda ligger således i allmänhet hos tillverkaren. Med andra ord är en EU-försäkran rättsligt bindande för tillverkaren och CE-märkningen är den symbol som tillverkaren sätter på produkten (eller dess förpackning/manual) för att visa att produkten överensstämmer med alla tillämpliga EU-krav, inklusive krav på cybersäkerhet enligt EU:s cyberresiliensförordning. CE-märkningen fungerar som bevis på att kraven är uppfyllda, vilket möjliggör fri rörlighet för produkten på den inre marknaden. CE-märkningen är en obligatorisk uppgift som indikerar efterlevnad av lagstadgade minimikrav.

Genom krav på att tillverkaren anger och upprätthåller en stödperiod för säkerhetsuppdateringar uppkommer ett inslag av tidsbundet åtagande eftersom tillverkaren förbinder sig att avhjälpa sårbarheter och ge ut nödvändiga uppdateringar under stödperioden. Denna skyldighet är lagstadgad, men den kommuniceras också till konsumenten genom informationen om produkten där stödperiodens längd ska framgå. Därmed får konsumenten vid köpet information om att tillverkaren kommer att tillhandahålla säkerhetsuppdateringar till åtminstone angiven tidpunkt.

I 4 kap. 21 § KKöpl föreskrivs att en vara är felaktig om näringsidkaren eller någon annan för näringsidkarens räkning genom en garanti eller liknande utfästelse har åtagit sig att under en viss tid svara för varan eller en del av varan eller för en egenskap hos varan, och varan under den angivna tiden försämras i det avseende som utfästelsen omfattar. Det innebär att om säljaren eller till exempel tillverkaren på säljarens uppdrag garanterat en viss egenskap eller hållbarhet hos varan under en bestämd tid, så ska en försämring inom den tiden behandlas som ett fel i varan. Regeln tar sikte på

garantier och liknande löften som sträcker sig utöver den grundläggande avtalsenliga standarden.

Enligt 4 kap. 22 § KKöpl har konsumenten rätt att vända sig direkt mot den som lämnat garantin eller utfästelsen för att få det som utlovats. Särskilt nämns att om tillverkaren har åtagit sig att svara för varans hållbarhet under en viss tid, så har konsumenten alltid rätt att kräva att tillverkaren avhjälper felet eller företar omleverans (byte) om fel uppstår inom den utlovade tiden. Detta säkerställer att tillverkarens löften är direkt verkställbara av konsumenten, trots att konsumentens köpeavtal formellt är med säljaren. Det har i svensk rätt ansetts följa av allmänna avtalsrättsliga principer att en tillverkare som utfäster en garanti gentemot konsumenten måste infria sitt åtagande, även om tillverkaren inte är avtalspart i köpet.

Sammanfattningsvis torde slutsatsen kunna dras att EU-försäkringen och CE-märkning inte i sig torde utgöra några utfästelser eller åtaganden utöver vad som följer av de angivna rättsliga kraven som ligger till grund för en sådan försäkringen och utfästelse. Tillverkaren har endast åtagit sig att upprätthålla en egenskap, dvs. säkerhetsnivån genom uppdateringar, under en bestämd period. Om produkten under den perioden försämras i detta avseende, till exempel genom att säkerhetsbrister uppstår som inte åtgärdas eller att säkerhetsuppdateringar inte tillhandahålls, kan en situation uppstå där varan kan anse vara försämrad i jämförelse med vad som anges i stödperioden och konsekvensen enligt KKöpl torde då bli att varan kan anses felaktig. Konsumenten kan då kräva avhjälpande, prisavdrag, eller hävning mot säljaren, men torde även kunna vända sig direkt mot tillverkaren som kan anses ha lämnat utfästelse om uppdateringar med stöd av 4 kap. 22 §. Den senare regeln ger konsumenten rätt att vända sig till tillverkaren i enlighet med utfästelsens innehåll, i detta fall torde det innebära att kräva att tillverkaren tillhandahåller uppdateringar eller avhjälper säkerhetsfelet inom ramen för sin utfästelse. Den senare regeln ger konsumenten rätt att vända sig till tillverkaren i enlighet med utfästelsens innehåll, i detta fall torde det innebära att kräva att tillverkaren tillhandahåller uppdateringar eller avhjälper säkerhetsfelet inom ramen för sin utfästelse.

I sammanhanget kan noteras att KKöpl uttryckligen anger att om tillverkaren utfäst ansvar för varans hållbarhet en viss tid, kan konsumenten kräva avhjälpande eller omleverans direkt av tillver-

karen vid fel. En utebliven nödvändig säkerhetsuppdatering som leder till funktions- eller säkerhetsbrist torde kunna ses som att varans hållbarhet och/eller säkerhet brister i strid med tillverkarens utfästelse om stödperiod.

KKöpl:s garantiregel är utformad teknikneutralt och tar sikte på faktumet att säljaren/tillverkaren åtagit sig ett tidsbundet ansvar, inte nödvändigtvis på om åtagandet var juridiskt tvingande eller frivilligt i sin uppkomst. Det kan därför finnas skäl att anse den deklarerade stödperioden som en liknande utfästelse om varans egenskap under viss tid. Om tillverkaren skulle avbryta stöd innan den utlovade stödperioden eller underlåta att lämna uppdateringar så torde konsumenten kunna göra gällande att varan är felaktig även på denna grund.

Sammantaget bedömer utredningen att det saknas skäl att ändra eller komplettera KKöpl med anledning av bestämmelserna i EU:s cyberresiliensförordning. Ett klarläggande av eventuella oklarheter om den direkt rättsliga betydelsen av EU-försäkran och CE-märkning av en produkt med digitala element i konsumentköprättslig mening enligt KKöpl får enligt utredningens mening ske i rätts-tillämpningen.

I sammanhanget kan även noteras att i artikel 65 i EU:s cyberresiliensförordning¹⁶ anges att direktiv (EU) 2020/1828¹⁷ ska tillämpas på grupp-talan om ekonomiska aktörers överträdelse-er av bestämmelserna i denna förordning som skadar eller kan skada konsumenternas kollektiva intressen. Förordningens regelsystem i berörda delar kan anses röra konsumentintresset, vilket avspeglas i att förordningen listas i bilagan till direktiv (EU) 2020/1828. Direktivet

¹⁶ I skäl 124 anges att konsumenter bör ha rätt att hävda sina rättigheter med avseende på de skyldigheter som åläggs ekonomiska aktörer enligt denna förordning genom grupp-talan enligt Europaparlamentets och rådets direktiv (EU) 2020/1828 (33). För detta ändamål bör det i denna förordning föreskrivas att direktiv (EU) 2020/1828 är tillämpligt på grupp-talan om överträdelse-er av denna förordning som skadar eller kan skada konsumenters kollektiva intressen. Bilaga I till det direktivet bör därför ändras i enlighet med detta. Det åligger medlemsstaterna att säkerställa att dessa ändringar återspeglas i de införlivandeåtgärder som antas enligt det direktivet, även om antagandet av nationella införlivandeåtgärder i det avseendet inte är ett villkor för att det direktivet ska vara tillämpligt på sådan grupp-talan. Det direktivets tillämplighet på grupp-talan som väcks med avseende på ekonomiska aktörers överträdelse-er av bestämmelser i denna förordning som skadar eller skulle kunna skada konsumenters kollektiva intressen bör börja tillämpas från och med den 11 december 2027.

¹⁷ Europaparlamentets och rådets direktiv (EU) 2020/1828 av den 25 november 2020 om grupp-talan för att skydda konsumenters kollektiva intressen och om upphävande av direktiv 2009/22/EG (EUT L 409, 4.12.2020, s. 1).

har genomförts i lagen (2023:730) om grupptalan till skydd för konsumenters kollektiva intressen¹⁸.

13.9 Konsumenttjänstlagen (1985:716)

Utredningens bedömning: EU:s cyberresiliensförordning har beröringspunkter med konsumenttjänstlagen (1985:716) (KtjL). Det saknas skäl att upphäva, ändra eller införa nya bestämmelser i KtjL med anledning av EU:s cyberresiliensförordning.

I konsumenttjänstlagen (1985:716) (KtjL) regleras konsumenters rättigheter vid köp av tjänster. I kommittédirektiven anges att det finns ett behov av att identifiera vilka bestämmelser i KtjL som berörs av EU:s cyberresiliensförordning och analysera om de behöver upphävas, ändras eller om nya bestämmelser behövs med anledning av förordningen.

13.9.1 Närmare om konsumentens rättigheter i konsumenttjänstlagen

Konsumenttjänstlagen (KtjL) gäller tjänsteavtal där näringsidkaren arbetar på lös sak, fast egendom eller förvarar lös sak (1 §). Lagen innehåller dessutom ett uttryckligt undantag för arbete som en näringsidkare utför för att fullgöra ett avtal om köp av en lös sak, till exempel installation ingående i ett varuköp som en konsument gör, vilket betyder att sådana tjänstemoment omfattas av konsumentköplagen i stället för KtjL (2 §).¹⁹

¹⁸ Prop. 2022/23:136, bet. 2023/24:CU4, rskr. 2023/24:35, direktiv (EU) 2020/1828.

¹⁹ Med digital tjänst avses enligt KKöpl "en tjänst som gör det möjligt för konsumenten att skapa, bearbeta, lagra eller få tillgång till data i digital form, eller att utbyta data eller interagera på annat sätt med data i digital form". Exempel är molnlagring, strömmade media, sociala plattformar m.m. Efter genomförandet av EU:s digitalinnehållsdirektiv täcker konsumentköplagen nu även fristående digitala tjänster. 9 kap. KKöpl gäller generellt avtal där en näringsidkare åtar sig att tillhandahålla digitala tjänster åt konsumenten. Detta inkluderar både tjänster som levereras kontinuerligt över tid (t.ex. ett abonnemang på en streaming-tjänst) och sådana som levereras vid ett enskilt tillfälle (t.ex. en engångsnedladdningstjänst), i den mån de utgör digitala prestationer mot konsumenten. Konsumenttjänstlagen är inte avsedd att reglera denna typ av digitala nyttigheter; den är begränsad till traditionella tjänster som arbete på fysiska saker eller fastighet och förvaring. Under förarbetena diskuterades visserligen alternativet att hantera digitala tjänster inom ramen för konsumenttjänstlagen,

I 4 § KtjL anges att tjänsten ska utföras fackmässigt. Den får inte ske i strid med säkerhetsföreskrifter som syftar till att föremålet är tillförlitligt från säkerhetssynpunkt (5 §). En tjänst är felaktig om resultatet avviker från dessa krav (9 § p. 1–2). Näringsidkaren har även en upplysnings- och avrådningsplikt. Näringsidkaren ska avråda om tjänsten inte är till rimlig nytta (6 §) och upplysa om viktiga förhållanden som han känner till eller borde känna till (11 §). Oriktiga eller missledande uppgifter kan också medföra fel (10 §).

Vid fel kan konsumenten kräva avhjälpande, prisavdrag eller hävning (16–23 §§) samt skadestånd (31–33 §§). Reklamationsfrister finns i 17–18 §§.

Den tydligaste överlappningen med EU:s cyberresiliensförordning uppstår när en näringsidkare tillhandhåller en tjänst, exempelvis en installation eller reparation av en produkt med digitala element som konsumenten redan har köpt separat av en säljare. Kraven på cybersäkerhet i produkten anges i EU:s cyberresiliensförordning samtidigt som själva konsumentköpet regleras av KKöpl och KtjL tillämpas på själva tjänsten, om denna inte sker som en del av konsumentköpet.

Nedan behandlas de bestämmelser som utredningen bedömer har en koppling till och viss överlappning med EU:s cyberresiliensförordning.

Fackmässigt utförande

Av 4 § KtjL följer att näringsidkaren ska utföra tjänsten fackmässigt. Denne ska med tillbörlig omsorg ta till vara konsumentens intressen och samråda med denne i den utsträckning som det behövs och är möjligt. Om inte annat får anses avtalat så ingår det i tjänsten att näringsidkaren ska tillhandahålla behövligt material.

Enligt förarbete och praxis innebär fackmässighet att arbetet utförs i enlighet med god branschsed och gällande standarder inom området. Företaget ska ha rätt kompetens och uppfylla de krav som branschregler och eventuella myndighetsföreskrifter ställer. Kravet på fackmässighet är centralt vid bedömningen av fel i tjänsten, om

men regeringen valde att samla de nya reglerna i konsumentköplagen för att uppnå enhetlighet med EU-direktiven. Alltså ska avtal om fristående digitala tjänster bedömas enligt 9 kap. KKöpl, inte enligt KtjL.

resultatet inte uppfyller vad en kunnig fackman kunnat prestera, anses tjänsten felaktig.

Säkerhet

I 5 § KtjL anges att näringsidkaren ska särskilt iaktta att tjänsten inte utförs i strid mot sådana författningsföreskrifter eller myndighetsbeslut som väsentligen syftar till att säkerställa att föremålet för tjänsten är tillförlitligt från säkerhetssynpunkt, eller i strid mot förbud enligt 27 § produktsäkerhetslagen.

I sammanhanget kan noteras att enligt KtjL fullgörs prestationen normalt när tjänsten avslutas. Lagen innehåller således ingen motsvarighet till skyldigheten att i vissa fall fortlöpande tillhandahålla säkerhetsuppdateringar som finns i KKöpl. Det finns därför inget fortsatt ansvar för näringsidkaren för att produkten hålls uppdaterad och säker, om det inte särskilt anges i en eventuell garanti eller annars framgår av avtalet för tjänsten. Om näringsidkaren enligt avtal installerar en programvara ställer 4 § krav på att installationen görs fackmässigt och korrekt vid den tidpunkten. Eventuella senare uppdateringar skulle kräva ett separat avtal. Däremot kan noteras att om en näringsidkare åtagit sig under ett tjänsteavtal att leverera ett löpande underhåll av en produkt med digitalt element torde det betraktas som en del av uppdraget, men det är då ett avtalat fortlöpande åtagande mer än en lagstadgad generell uppdateringsplikt.

Näringsidkaren får inte heller utföra tjänsten på ett sätt som strider mot föreskrifter eller myndighetsbeslut som har till syfte att säkerställa att föremålet för tjänsten är tillförlitligt från säkerhetssynpunkt. De krav på cybersäkerhet i en produkt med digitala element som anges i EU:s cyberresiliensförordning torde utgöra en sådan säkerhetsföreskrift som omfattas av 5 § KtjL. Näringsidkaren bör därför inte vidta åtgärder som försätter produkten i strid mot kraven i förordningen. Om näringsidkaren utför tjänsten i strid med gällande säkerhetsföreskrifter kan det utgöra en överträdelse av 5 § KtjL. Näringsidkaren måste även beakta om en myndighet meddelat beslut om varan inte får säljas på grund av cybersäkerhetsrisk. Denne får inte bryta mot försäljningsförbud enligt produktsäkerhetslagen, till exempel om en produkt är förbjuden av säkerhetsskäl. Denna bestämmelse innebär att näringsidkaren måste följa

relevanta säkerhetsregler som rör produkten och tjänsten. 5 § skärper således kravet ur ett säkerhetsperspektiv, dvs. att tjänsten ska utföras så att produkten efter tjänsten är säkert att använda. I sammanhanget kan noteras att begreppet säkerhet bör tolkas mot bakgrund av den tekniska utvecklingen och att gränsen mellan fysisk säkerhet och cybersäkerhet kan bli flytande eftersom en sårbarhet i en produkt kan utnyttjas för att orsaka fysisk skada eller intrång i privatlivet. Det finns därför skäl att tolka cybersäkerhet som ingående i begreppet tillförlitligt från säkerhetssynpunkt.

Näringsidkarens skyldighet att avråda

Av 6 § KtjL framgår att om en tjänst med hänsyn till priset, värdet av föremålet för tjänsten eller andra särskilda omständigheter inte kan anses vara till rimlig nytta för konsumenten, ska näringsidkaren avråda från att låta utföra tjänsten. Om det först sedan tjänsten har börjat utföras visar sig att den inte kan anses vara till rimlig nytta för konsumenten eller att priset för tjänsten kan bli betydligt högre än den hade kunnat räkna med, ska näringsidkaren underätta konsumenten om förhållandet och begära hans anvisningar. Kan konsumenten inte anträffas eller får näringsidkaren av annan orsak inte anvisningar av denne inom rimlig tid, ska näringsidkaren avbryta påbörjat arbete. Detta gäller dock inte om det finns särskilda skäl att anta att konsumenten ändå önskar få tjänsten utförd. Detta är en informations- och omsorgsplikt som innebär att näringsidkaren förväntas informera kunden om denne beställer en tjänst som inte är ekonomiskt försvarbart eller ändamålsenligt. I detta sammanhang kan det innebära att om en konsument ber näringsidkaren att installera en produkt med digitala element kan det medföra en cybersäkerhetsrisk varför näringsidkaren torde behöva avråda från åtgärden. Vidare om konsumenten väljer en produkt som inte längre får säkerhetsuppdateringar torde bristen på säkerhet medföra att tjänsten inte är till rimlig nytta och näringsidkaren torde därför behöva upplysa konsumenten om riskerna och eventuellt rekommendera en annan lösning. Underlåter näringsidkaren att avråda trots skäl att anta att konsumenten annars inte skulle genomfört tjänsten, kan konsumenten aktualisera påföljder mot näringsidkaren.

Fel i tjänsten

I 9 § KtjL anges vad som avses med fel i tjänsten. Tjänsten ska anses felaktig, om resultatet avviker från

1. vad konsumenten med hänsyn till 4 § har rätt att kräva, även om avvikelsen beror på en olyckshändelse eller därmed jämförlig händelse,
2. sådana föreskrifter eller myndighetsbeslut som väsentligen syftar till att säkerställa att föremålet för tjänsten är tillförlitligt från säkerhetssynpunkt, eller
3. vad som därutöver får anses avtalat.

Tjänsten ska också anses felaktig, om den har utförts i strid mot förbud enligt 27 § produktsäkerhetslagen eller om näringsidkaren inte har utfört sådant tilläggsarbete som han är skyldig att utföra enligt 8 § tredje stycket.

Av paragrafen framgår att resultatet av tjänsten ska stämma överens med avtalet samt utföras fackmässigt. 9 § omfattar också att tjänsten ska uppfylla säkerhetskrav, dvs. om näringsidkaren bryter mot 5 § (säkerhetsreglerna) anses tjänsten felaktig.

I 10 § KtjL anges att tjänsten ska vidare anses felaktig, om resultatet avviker från sådana uppgifter av betydelse för bedömningen av tjänstens beskaffenhet eller ändamålsenlighet som kan antas ha inverkat på avtalet och som i samband med avtalets ingående eller annars vid marknadsföring har lämnats

1. av näringsidkaren,
2. av någon annan näringsidkare eller av en branschförening eller liknande organisation för näringsidkarens räkning, eller
3. av en leverantör av material till tjänsten eller av någon annan i tidigare led.

Det angivna gäller dock inte i fråga om uppgifter som i tid har rättats på ett tydligt sätt och inte heller om näringsidkaren varken kände till eller borde ha känt till uppgifterna.

Fel i tjänsten kan föreligga om till exempel efter ett köp av en produkt med digitala element en efterföljande installation eller konfiguration av produkten medför att den inte länge uppfyller kraven

på cybersäkerhet enligt EU:s cyberresiliensförordning, vilket torde medföra att resultatet inte motsvarar vad konsumenten har rätt att kräva. I linje med HD:s avgörande NJA 2013 s.1174 bär dock inte näringsidkaren ansvar för fel som orsakats av felaktiga uppgifter eller instruktioner från konsumenten. Om till exempel konsumenten uttryckligen begärt av näringsidkaren att inte uppdatera till exempel programvaran för att få behålla viss funktion, och detta medför en sårbarhet i produkten, kan felet anses bero på konsumentens anvisning och därmed inte ge rätt till påföljder enligt 10 §.

Av 11 § KtjL följer att tjänsten ska även anses felaktig, om näringsidkaren i annat fall än som avses i 6 § första stycket före avtalets ingående har underlåtit att upplysa konsumenten om ett sådant förhållande rörande tjänstens beskaffenhet eller ändamålsenlighet som näringsidkaren kände till eller borde ha känt till och som han insåg eller borde ha insett vara av betydelse för konsumenten. En förutsättning för att tjänsten ska anses felaktig är dock att underlåtenheten kan antas ha inverkat på avtalet.

Näringsidkaren har således en upplysningsplikt mot konsumenten som i sammanhanget innebär att näringsidkaren ska informera konsumenten om förhållanden som rör till exempel krav på cybersäkerhet (säkerhetsuppdatering) i produkten som tjänsten omfattar och som kan antas vara av betydelse för konsumenten.

Av 12 § KtjL följer att frågan om tjänsten är felaktig ska bedömas med hänsyn till förhållandena vid den tidpunkt då uppdraget avslutades. Avser tjänsten en sak som har överlämnats till näringsidkaren eller som av annan orsak befinner sig i hans besittning, anses uppdraget avslutat först när saken har kommit i konsumentens besittning.

Garanti och liknande utfästelse

I 14 § KtjL anges att om näringsidkaren genom en garanti eller liknande utfästelse åtagit sig att under en viss tid efter den tidpunkt som anges i 12 § svara för resultatet av tjänsten och försämrats det utfästa resultatet under den angivna tiden, ska tjänsten anses felaktig. Det gäller dock inte om näringsidkaren gör sannolikt att försämringen beror på en olyckshändelse eller därmed jämförlig hän-

delse eller på vanvård, onormalt brukande eller något liknande förhållande på konsumentens sida.

Påföljder vid fel

Om tjänsten är felaktig har konsumenten rätt till olika påföljder enligt vad som anges i 16 § KtjL. Konsumenten har rätt att kräva avhjälpande, dvs. att näringsidkaren kostnadsfritt rättar till felet. Om avhjälpande inte sker eller inte är möjligt, kan konsumenten få prisavdrag eller i allvarliga fall häva avtalet. Dessutom kan skadestånd utgå för skador som felet orsakat, till exempel om en vårdslöst utförd installation förstört utrustning eller data.

13.9.2 Överväganden

KtjL i omfattar i första hand avtal om tjänster som avser arbete på bland annat fysiska saker. KtjL kan beröras av regleringen i EU:s cyberresiliensförordning i de fall en tjänst utförs på en produkt med digitala element, och som inte omfattas av KKöpl, till exempel när en näringsidkare installerar, konfigurerar, uppdaterar eller reparerar en produkt med digitala element. I dessa fall blir kravet på cybersäkerhet vid tjänstens utförande en aspekt av tjänstens kvalitet och konsumenten har rimlig förväntan att tjänsten utförs på ett säkert sätt så att inte nya sårbarheter introduceras eller befintliga skydd försämrats. KtjL innehåller allmänna krav på fackmässighet och omsorg som redan kan tolkas täcka säkerhetsaspekter (4 §). Fackmässigt innebär att tjänsten ska utföras enligt god yrkessed och branschstandard. Detta bör tolkas som att en näringsidkare ska följa föreskrivna krav och standarder på cybersäkerhet i produkten vid utförande av tjänsten. Vidare innehåller 5 § en uttrycklig regel om säkerhet, dvs. näringsidkaren ska särskilt iaktta att tjänsten inte utförs i strid med föreskrifter eller myndighetsbeslut som syftar till att föremålet för tjänsten är tillförlitligt ur säkerhetssynpunkt, och inte heller i strid med förbud enligt produktsäkerhetslagen. Denna bestämmelse kräver att tjänsteutövaren följer gällande säkerhetsregler vid utförandet av tjänsten. Om det exempelvis finns rekommendationer från myndigheter eller bindande standarder om hur en viss typ av installation ska ske säkert, så måste näringsidkaren följa dem. Om närings-

idkaren bryter mot vad som följer av krav och standarder för cybersäkerhet i produkter med digitala element vid utförandet av tjänsten torde tjänsten kunna bedömas som felaktig enligt 9 § eftersom resultatet avviker från gällande säkerhetsföreskrifter och även från vad konsumenten har rätt att kräva vid utförandet av tjänsten. Även brister i näringsidkarens rådgivningsansvar mot konsumenten enligt 6 § kan medföra att fel i tjänsten föreligger och att konsumenten kan aktualisera påföljder. På motsvarande sätt som gäller vid konsumentköp av en vara med digital del har konsumenten rätt till påföljder om en tjänst är felaktig, dvs. om resultatet inte är fackmässigt eller strider mot säkerhetsföreskrifter. Konsumenten kan då kräva avhjälpande, prisavdrag eller häva avtalet, samt i vissa fall kräva skadestånd om konsumenten lider skada på grund av näringsidkarens oaktsamhet vid utförandet av tjänsten.

Utredningen konstaterar att det finns viss överlappning mellan regelverken i EU:s cyberresiliensförordning och KtjL. EU:s cyberresiliensförordning medför dock inte att det uppkommer garantier och rättigheter som i sig medför att KtjL bör ändras eller kompletteras. Utredningen bedömer att det inte heller i övrigt föreligger någon konflikt i normhierarkin. Det saknas därför skäl att föreslå att KtjL behöver ändras eller kompletteras med anledning av bestämmelserna i EU:s cyberresiliensförordning.

14 Övriga frågor

14.1 Inledning

I detta kapitel behandlas ett antal övriga frågor. Det handlar om EU-försäkran om överensstämmelse, gemensam kontaktpunkt för rapportering av sårbarheter och incidenter samt ikraftträdande- och övergångsbestämmelser.

14.2 EU-försäkran om överensstämmelse

Utredningens bedömning: En EU-försäkran om överensstämmelse eller en förenklad EU-försäkran om överensstämmelse som avses i artikel 28 i EU:s cyberresiliensförordning ska vara skriven på svenska eller engelska.

En tillverkare ska upprätta en EU-försäkran om överensstämmelse om produkten med digitala element uppfyller kraven i förordning (EU) 2024/2847¹ (EU:s cyberresiliensförordning) (artikel 13.12). Genom att upprätta en EU-försäkran om överensstämmelse tar tillverkaren ansvar för att produkten med digitala element uppfyller de krav som fastställs i förordningen (artikel 28.4). Tillverkaren ska antingen lämna en kopia av EU-försäkran om överensstämmelse eller en förenklad EU-försäkran om överensstämmelse tillsammans med produkten med digitala element. Om en förenklad EU-försäkran om överensstämmelse lämnas ska den innehålla den exakta webbadress där det går att få tillgång till hela texten till EU-försäkran om överensstämmelse (artikel 13.20). En EU-försäkran eller en förenklad

¹ Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen)

EU-försäkrans ska utformas enligt en mall och tillhandahållas på de språk som krävs av den medlemsstat där produkten med digitala element släpps ut på marknaden eller tillhandahålls på marknaden (artikel 28.2).

Utöver svenska bör en EU-försäkrans även kunna upprättas på engelska. Det minskar den administrativa bördan för tillverkaren och minskar även risken för att en översättning av EU-försäkrans till svenska blir ofullständig eller missvisande. En EU-försäkrans ska därför kunna vara skriven antingen på svenska eller engelska.

14.3 Gemensam kontaktpunkt för rapportering av sårbarheter och incidenter

Utredningens bedömning: Utredningen bedömer att frågan om en gemensam kontaktpunkt för rapportering av sårbarheter och incidenter inte är något som kan hanteras inom denna utrednings uppdrag men anser att en sådan samordning behöver övervägas i det fortsatta arbetet med regelförenkling i den utsträckning det är möjligt och lämpligt.

Det har till utredningen framförts att olika rapporteringskrav som fastställs i EU-rättsakter avseende sårbarheter och incidenter är handelshindrande och utgör en administrativ börda för företag. Rapporteringskraven skiljer sig åt (till exempel gällande när i tiden en incident ska rapporteras och till vilken myndighet rapporten ska inges) och en och samma aktör kan vara skyldig att rapportera en incident enligt flera olika rättsakter. Det finns därför ett behov av regelförenkling och inrättandet av en one-stop-shop för rapportering.

I skäl 72 i EU:s cyberresiliensförordning anges att medlemsstaterna uppmuntras överväga att tillhandahålla gemensamma kontaktpunkter på nationell nivå för olika rapporteringskrav i syfte att förenkla rapporteringen av den information som krävs enligt denna förordning, med beaktande av andra kompletterande rapporteringskrav som fastställs i unionsrätten², samt för att minska den admi-

² Här nämns rapporteringskraven enligt förordning (EU) 2016/679, förordning (EU) 2022/2554, direktiv 2002/58/EG samt direktiv (EU) 2022/2555.

nistrativa bördan för entiteterna.³ I skälet nämns rapporteringskraven i förordning (EU) 2016/679⁴ (EU:s dataskyddsförordning), förordning (EU) 2022/2554⁵ (Dora-förordningen), direktiv 2002/58/EG⁶ (e-dataskyddsdirektivet) och direktiv (EU) 2022/2555⁷ (NIS 2-direktivet).

Det finns i dag ingen gemensam kontaktpunkt i Sverige för de olika rapporteringskrav som fastställs i unionsrätten. NIS 2-direktivet är ännu inte genomfört i Sverige och därför gäller fortfarande rapporteringskraven enligt lagen (2018:1174) om informations-säkerhet för samhällsviktiga och digitala tjänster (NIS-lagen), lagen (2022:482) om elektronisk kommunikation (LEK) och förordning (EU) nr 910/2014⁸ (eIDAS-förordningen). Rapporter enligt NIS-lagen lämnas till Myndigheten för samhällsskydd och beredskap (MSB). Rapporter enligt LEK och eIDAS-förordningen lämnas till Post- och telestyrelsen (PTS). Rapporter enligt NIS 2-direktivet föreslås i delbetänkandet *Nya regler om cybersäkerhet* (SOU 2024:18) lämnas till MSB. I slutbetänkandet *Samlade förmågor för ökad cybersäkerhet* (SOU 2025:79) föreslår dock den utredningen att uppgiften att ta emot sådana rapporter ska överföras till Försvarets radioanstalt. Vidare lämnas rapporter enligt EU:s dataskyddsförordning till Integritetsskyddsmyndigheten. Rapporter enligt e-dataskyddsdirektivet

³ Det anges vidare i skälet att användningen av sådana nationella gemensamma kontaktpunkter för att rapportera säkerhetsincidenter enligt förordning (EU) 2016/679 och direktiv 2002/58/EG inte bör påverka tillämpningen av bestämmelserna i förordning (EU) 2016/679 och direktiv 2002/58/EG, särskilt de som rör oberoendet för de myndigheter som avses i dessa. Vid inrättandet av den gemensamma rapporteringsplattform som avses i den här förordningen bör Enisa beakta möjligheten att integrera de nationella slutpunkter för elektronisk anmälan som avses i den här förordningen i nationella gemensamma kontaktpunkter som också kan integrera andra anmälningar som krävs enligt unionsrätten.

⁴ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

⁵ Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011.

⁶ Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation).

⁷ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

⁸ Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

lämnas till PTS. Rapporter enligt Dora-förordningen lämnas till Finansinspektionen.

Utöver detta lämnas rapporter enligt förordning (EU) 2019/881⁹ (EU:s cybersäkerhetsakt) till Försvarets materielverk. Rapporter enligt förordning (EU) 2024/1689¹⁰ (AI-förordningen) ska lämnas till marknadskontrollmyndigheterna enligt den förordningen.

Utredningen bedömer att frågan om en gemensam kontaktpunkt inte är något som kan hanteras inom denna utrednings uppdrag men anser att en sådan samordning behöver övervägas i det fortsatta arbetet med regelförenkling i den utsträckning det är möjligt och lämpligt. Se även avsnitt 4.5 om EU:s arbete med regelförenkling på det digitala området.

14.4 Ikraftträdande- och övergångsbestämmelser

Utredningens förslag: De föreslagna bestämmelserna om vilken myndighet som är anmälände myndighet, om att anmälände myndighet får meddela vissa föreskrifter, om tystnadsplikt för den som deltar i verksamhet som utförs av ett privat organ för bedömning av överensstämmelse och om överklagande i lagen med kompletterande bestämmelser till EU:s cyberresiliensförordning (kompletteringslagen) ska träda i kraft den 11 juni 2026. Övriga bestämmelser i kompletteringslagen ska träda i kraft den 11 december 2027.

Den föreslagna bestämmelsen om sekretess till skydd för enskild inom ramen för regulatoriska sandlådor för cyberresiliens i offentlighets- och sekretesslagen (2009:400) ska träda i kraft den 11 december 2027. Övriga föreslagna bestämmelser i den lagen ska träda i kraft den 11 september 2026.

Utredningens bedömning: De föreslagna bestämmelserna om vilken myndighet som är anmälände myndighet och om att anmälände myndighet får meddela vissa föreskrifter i förordningen

⁹ Förordning (EU) 2019/881 om Europeiska unionens cybersäkerhetsbyrå och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (cybersäkerhetsakten).

¹⁰ Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

med kompletterande bestämmelser till EU:s cyberresiliensförordning (kompletteringsförordningen) ska träda i kraft den 11 juni 2026. Den föreslagna bestämmelsen om ord och uttryck (som definierar vad som avses med CSIRT-enhet) samt den föreslagna upplysningsbestämmelsen om vilken myndighet som är CSIRT-enhet i kompletteringsförordningen ska träda i kraft den 11 september 2026. Övriga föreslagna bestämmelser i kompletteringsförordningen ska träda i kraft den 11 december 2027.

Den föreslagna bestämmelsen om sekretess för diarium över sårbarhets- och incidentrapporter i offentlighets- och sekretessförordningen (2009:641) ska träda i kraft den 11 september 2026. Den föreslagna bestämmelsen om sekretess till skydd för enskild vid marknads kontroll och utredning i samma förordning ska träda i kraft den 11 december 2027.

Den föreslagna bestämmelsen i förordning om ändring i förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap ska träda i kraft den 11 december 2027.

Det krävs inga övergångsbestämmelser.

Artikel 71.2 föreskriver att EU:s cyberresiliensförordning ska tillämpas från och med den 11 december 2027. Artikel 14 ska dock tillämpas från och med den 11 september 2026 och kapitel IV (artiklarna 35–51) ska tillämpas från och med den 11 juni 2026.

Artikel 14 i EU:s cyberresiliensförordning innehåller bestämmelser om tillverkarnas rapporteringsskyldigheter avseende sårbarheter och incidenter. Kapitel IV (artiklarna 35–51) innehåller bestämmelser om anmälade myndighet och anmälan av organ för bedömning av överensstämmelse.

Utredningen har föreslagit ett antal bestämmelser som kompletterar artikel 14 i EU:s cyberresiliensförordning. Det gäller den föreslagna bestämmelsen om ord och uttryck (som definierar vad som avses med CSIRT-enhet) samt den föreslagna upplysningsbestämmelsen om vilken myndighet som är CSIRT-enhet i förordningen med kompletterande bestämmelser till EU:s cyberresiliensförordning (kompletteringsförordningen) (se kapitel 8). Det gäller även de föreslagna bestämmelserna om sekretess till skydd för sårbarhets- och incidentrapporter i offentlighets- och sekretesslagen (2009:400) (OSL) samt i offentlighets- och sekretessförordningen (2009:641)

(OSF) (se avsnitt 11.6). I enlighet med vad som följer av EU:s cyberresiliensförordning ska dessa föreslagna bestämmelser träda i kraft den 11 september 2026.

Utredningen har föreslagit ett antal bestämmelser som kompletterar kapitel IV (artiklarna 35–51) i EU:s cyberresiliensförordning. Det gäller de föreslagna bestämmelserna om vilken myndighet som är anmälade myndighet, om att anmälade myndighet får meddela vissa föreskrifter, om tystnadsplikt för den som deltar i verksamhet som utförs av ett privat organ för bedömning av överensstämmelse och om överklagande i lagen med kompletterande bestämmelser till EU:s cyberresiliensförordning (kompletteringslagen) och kompletteringsförordningen (se avsnitt 6.7, 6.8 och avsnitt 11.13). I enlighet med vad som följer av EU:s cyberresiliensförordning ska dessa föreslagna bestämmelser träda i kraft den 11 juni 2026. När det gäller överklagandebestämmelsen är det beslut av den anmälade myndigheten som behöver kunna överklagas från och med den 11 juni 2026 vilket gör att bestämmelsen behöver träda i kraft detta datum.

Övriga föreslagna bestämmelser i kompletteringslagen, kompletteringsförordningen, OSL, OSF samt i förordning om ändring i förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap kompletterar andra bestämmelser i EU:s cyberresiliensförordning. I enlighet med vad som följer av EU:s cyberresiliensförordning ska dessa övriga föreslagna bestämmelser träda i kraft den 11 december 2027.

Övergångsbestämmelser finns i artikel 69 i EU:s cyberresiliensförordning.

Artikel 69.1 föreskriver att EU-typkontrollintyg och beslut om godkännande som utfärdats avseende cybersäkerhetskrav för produkter med digitala element som omfattas av annan unionsharmoniseringslagstiftning än denna förordning ska fortsätta att gälla till och med den 11 juni 2028, såvida de inte löper ut före den dagen, eller något annat anges i sådan annan unionsharmoniseringslagstiftning, i vilket fall de förblir giltiga enligt den lagstiftningen.

Artikel 69.2 föreskriver att produkter med digitala element som har släppts ut på marknaden före den 11 december 2027 ska omfattas av kraven som anges i denna förordning endast om de, från och med den dagen, är föremål för en väsentlig ändring.

Artikel 69.3 föreskriver att som avvikelse till artikel 69.2 ska de skyldigheter som fastställs i artikel 14 tillämpas på alla produkter med

digitala element som omfattas av denna förordnings tillämpningsområde och som har släppts ut på marknaden före den 11 december 2027. Skyldigheten att rapportera sårbarheter och incidenter i artikel 14 gäller således samtliga produkter som finns på marknaden, även sådana som har släppts ut på marknaden före detta datum.

Utredningen bedömer att det saknas skäl att införa några övergångsbestämmelser.

15 Konsekvensutredning

15.1 Inledning

Utredningen ska i enlighet med kommittéförordningen (1998:1474) och förordningen (2024:183) om konsekvensutredningar redovisa konsekvenserna av de förslag som lämnas i betänkandet.

Utredningen ska innehålla en beskrivning av kostnadsmässiga och andra relevanta konsekvenser för bland annat staten och enskilda. Därutöver ska den innehålla en redogörelse för vilka åtgärder som har vidtagits för att förslagen inte ska medföra mer långtgående kostnader eller begränsningar än nödvändigt för att uppnå dess syften, en bedömning av om särskild hänsyn behöver tas när det gäller tidpunkten för ikraftträdande och om det finns behov av speciella informationsinsatser samt en beskrivning av hur och när konsekvenserna av förslagen kan utvärderas.

Konsekvensutredningen ska innehålla en bedömning av om förslagen överensstämmer med eller går utöver de skyldigheter som följer av Sveriges anslutning till EU.

Av utredningens direktiv framgår särskilt att utredningen ska redovisa förslagens konsekvenser ur ett jämställdhetsperspektiv och för den personliga integriteten. Utredningen ska också bedöma vilka konsekvenser standardiseringsarbetet, som följer av förslagen, kan antas medföra för berörda myndigheter, företag och andra nationella organisationer. Utredaren ska särskilt redogöra för vilka ekonomiska konsekvenser de förslag som lämnas kan få för mikroföretag, små företag och medelstora företag.

I de inledande kapitlen har utredningen redovisat bakgrunden till de lämnade förslagen och de behov som bedöms finnas för den kompletterande lagen och förordningen. Även alternativa lösningar har redovisat i relevanta delar. Bedömningar i fråga om ikraftträdande

finns i avsnitt 14.4. Det som redovisats i de angivna kapitlen upprepas inte här.

I detta kapitel ska konsekvenserna av utredningens förslag redovisas. Förslagen om åtgärder och kompletterande författningsbestämmelser syftar till att anpassa svensk lagstiftning till bestämmelserna i EU:s cyberresiliensförordning och säkerställa att unionsrätten får avsedd effekt. EU:s cyberresiliensförordning är direkt tillämplig i medlemsstaterna. Det kan därför inledningsvis konstateras att de konsekvenser som uppstår för samhället och de aktörer som berörs huvudsakligen är en direkt följd av den bakomliggande EU-förordningen och inte av utredningens förslag.

15.1.1 Kommissionens konsekvensbedömning

De konsekvenser som följer av de direkt tillämpliga bestämmelserna i EU:s cyberresiliensförordning redovisas i kommissionens konsekvensbedömningsrapport (SWD(2022) 282 final). För att säkerställa att ansvariga myndigheter ges förutsättningar att utföra sina uppgifter som följer av EU:s cyberresiliensförordning behöver dock vissa nationella konsekvenser som följer direkt av EU:s cyberresiliensförordning behandlas.

Det finns flera svårigheter och osäkerhetsfaktorer när det gäller att bedöma konsekvenserna av EU:s cyberresiliensförordning. Regelverket har ännu inte trätt i kraft och är fortfarande under utveckling. Även andra angränsande regelverk inom cyber- och produktsäkerhetsområdet är fortfarande under utveckling. Det pågår dessutom ett arbete med uppbyggnad och omorganisation av svenska funktioner inom cybersäkerhetsområdet. Vidare finns en osäkerhet kring antalet tillsynsobjekt samt omfattningen av den framtida sårbarhets- och incidentrapporteringen samt kring behovet av stöd.

15.1.2 Underlag till konsekvensutredningen

Företaget Governo AB har på utredningens uppdrag genomfört en utredning och analys av förutsättningar, eventuella utmaningar och kostnader för ekonomiska aktörer, organ för bedömning av överensstämmelse och den föreslagna marknadskontrollmyndigheten Post- och telestyrelsen (PTS) med anledning av genomförandet av EU:s

cyberresiliensförordning. Rapporten finns i sin helhet som bilaga 3 i betänkandet.

När det gäller konsekvenser för CSIRT-enheten och ett antal andra funktioner som i dag finns hos Myndigheten för samhällsskydd och beredskap (MSB) men som föreslås flyttas över till Försvarets radioanstalt (FRA)¹ har utredningen begärt underlag från dessa myndigheter som visar kostnader och andra konsekvenser för funktionerna. MSB har inkommit med ett sådant underlag som den myndigheten har berett tillsammans med FRA.

Governo AB:s rapport och underlaget från MSB ligger till grund för utredningens konsekvensutredning i dessa delar.

15.2 Övergripande om utredningens förslag

EU:s cyberresiliensförordning är till alla delar bindande och direkt tillämplig i varje medlemsstat. Det innebär att förordningens bestämmelser ska tillämpas direkt på samma sätt som nationella författningar.

Utredningens förslag om kompletterande nationell lagstiftning syftar till att anpassa svensk rätt till bestämmelserna i EU:s cyberresiliensförordning och säkerställa att unionsrätten får avsedd effekt.

Utredningen lämnar förslag på vilka myndigheter som ska utses till att vara anmälände myndighet och marknadskontrollmyndighet. Utredningen lämnar även förslag om myndigheternas befogenheter och möjlighet att besluta om sanktioner, även mot myndigheter, för överträdelse av regelverket. Vidare föreslås vissa processuella bestämmelser, bland annat om överklagande och det införs en rätt att få ett beslut omprövat och överklaga ett beslut av ett organ för bedömning av överensstämmelse. Utredningen lämnar förslag om bemyndiganden att meddela föreskrifter i vissa fall. Därutöver lämnas förslag om ändring i offentlighets- och sekretesslagen (2009:400) och om stöd till företag.

Utredningens förslag är en konsekvens av Sveriges medlemskap i EU. Förslaget bedöms överensstämma med de skyldigheter som följer av Sveriges medlemskap i EU och följer kraven på medlemsstaterna i förordningen. Effekten av om någon reglering inte kommer till stånd (nollalternativet) blir således att Sverige inte följer skyldigheterna enligt EU-rätten. Det leder även till att bestämmelserna i

¹ Se kapitel 8 och slutbetänkandet *Samlade förslag för ökad cybersäkerhet* (SOU 2025:79).

EU:s cyberresiliensförordning inte följs och att förordningens syfte därmed inte uppnås. Det kan även leda till att kommissionen inleder ett överträdelseärende mot Sverige.

15.3 Vem berörs av förslagen?

Utredningens förslag om stöd till företag, marknadskontrollmyndigheternas befogenheter, överklagande och sanktioner berör ekonomiska aktörer, det vill säga tillverkare, tillverkares representanter, importörer och distributörer, samt förvaltare av programvara med fri och öppen källkod.

Utredningens förslag berör även Styrelsen för ackreditering och teknisk kontroll (Swedac) som enligt förslaget ska utses till anmälände myndighet.

Utredningens förslag berör vidare PTS som enligt förslaget ska utses till marknadskontrollmyndighet. Det berör även de marknadskontrollmyndigheter som ska utses enligt förordning (EU) 2024/1689² (AI-förordningen). Indirekt berörs även Tullverket, när det gäller kontroll av produkter som förs in på unionsmarknaden.

Förslaget berör även MSB, anmälda organ, Sveriges domstolar och Polismyndigheten. Det finns dock ett förslag att Försvarets radioanstalt (FRA) från och med den 1 juli 2026 ska överta uppgifter som i dag utförs av MSB.³ Om förslaget beslutas gäller vad som sägs i konsekvensutredningen om MSB i stället FRA.

För det fall myndigheter tillhandahåller produkter med digitala element berör utredningens förslag dessa på samma sätt som andra företag som tillhandahåller sådana produkter. De effekter av förslagen som redovisas i denna konsekvensutredning gäller därmed även dessa aktörer.

² Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

³ Se kapitel 8 och slutbetänkandet *Samlade förmågor för ökad cybersäkerhet* (SOU 2025:79).

15.3.1 Uppskattning av antalet ekonomiska aktörer samt förvaltare av programvara med fri och öppen källkod

EU:s cyberresiliensförordning är tillämplig på alla produkter med digitala element som tillhandahålls på marknaden och vars avsedda ändamål eller rimligen förutsebara användning omfattar en direkt eller indirekt logisk eller fysisk dataanslutning till en enhet eller ett nät.

EU:s cyberresiliensförordning uppställer skyldigheter för ekonomiska aktörer samt förvaltare av programvara med fri och öppen källkod för att få tillhandahålla produkter med digitala element på marknaden.

Det är i dagsläget svårt att på ett tillförlitligt sätt beräkna hur många fysiska eller juridiska personer som berörs av regelverket i egenskap av ekonomiska aktörer eller förvaltare av programvara med fri och öppen källkod.

Governo AB har på utredningens uppdrag gjort en uppskattning hur många svenska tillverkare, importörer och distributörer samt produkter som omfattas av EU:s cyberresiliensförordning. Att göra en sådan uppskattning är komplicerad och beroende av en mängd antaganden. Governo AB har utgått från den metod som använts i kommissionens konsekvensbedömningsrapport (2022, SWD(2022) 282 final) för att få en konsekvent och likvärdig behandling av materian även om metoden kräver en del teoretiska förenklingar jämfört med de komplexa produktområden som egentligen föreligger. Hur uppskattningen har genomförts och vilka antaganden som har gjorts framgår av Governo AB:s rapport.

Sammanfattningsvis uppskattar Governo AB, utifrån kommissionens konsekvensbedömningsrapport, antalet svenska tillverkare av mjukvara som omfattas av EU:s cyberresiliensförordning till 27 178 och antalet tillverkare av hårdvara som omfattas av förordningen till 10 192, vilket sammantaget blir 37 370 tillverkare. Governo AB tydliggör dock i rapporten den stora osäkerheten som finns i beräkningarna och sammanfattar därför att det rimligtvis bör kunna antas att antalet svenska tillverkare som omfattas av EU:s cyberresiliensförordning ligger någonstans inom spannet 24 000–38 000 företag.

Governo AB uppskattar i enlighet med kommissionens uppskattning att 99,58 procent av tillverkarna är små- och medelstora företag vilket innebär att 37 213⁴ tillverkare är små- eller medelstora företag.

När det gäller att beräkna antalet produkter som svenska tillverkare tillverkar är även denna bedömning komplicerad och behäftad med osäkerheter. Governo AB uppskattar sammanfattningsvis att viktiga produkter, klass I och II, utgör 8 procent av alla produkter (2 990 stycken), kritiska produkter utgör 2 procent av alla produkter (747 stycken) samt övriga produkter utgör 90 procent av alla produkter (33 370 stycken).

Governo AB uppskattar antalet förvaltare av programvara med fri och öppen källkod i Sverige till 300.

Governo AB uppskattar antalet svenska importörer av produkter med digitala element till 12 718. Vidare uppskattar Governo AB antalet svenska distributörer av produkter med digitala element till 10 467. Det finns även vissa allmänt inriktade butiker som kan ha produkter med digitala element i sitt sortiment, till exempel stora livsmedelsbutiker, vilket innebär att antalet svenska distributörer sannolikt kan göra att antalet är något eller några hundratal butiker utöver det antalet som anges.

Sammanfattningsvis kan utredningen konstatera att bedömningen av antalet svenska ekonomiska aktörer som omfattas av EU:s cyber-resiliensförordning utgår från ett osäkert underlag och att antalet berörda produkter och ekonomiska aktörer därför kan vara av både större och mindre omfattning än de som nu redovisas, även om slutsatsen kan dras att det är en betydande mängd produkter med digitala element och ekonomiska aktörer som berörs.

⁴ 99,58 procent av 37 370.

15.4 Ekonomiska konsekvenser för ekonomiska aktörer samt förvaltare av programvara med fri och öppen källkod

15.4.1 Ekonomiska konsekvenser för ekonomiska aktörer samt förvaltare av programvara med fri och öppen källkod till följd av EU:s cyberresiliensförordning

EU:s cyberresiliensförordning väntas ge ekonomiska konsekvenser för ekonomiska aktörer samt förvaltare av programvara med fri och öppen källkod. Förordningens innehåll och konsekvenser i sig ingår dock inte i utredningens uppdrag att bedöma men som ovan angetts finns det anledning att behandla dessa för att kunna bedöma konsekvenserna för berörda myndigheter.

Syftet med EU:s cyberresiliensförordning är att fastställa villkor för utvecklingen av säkra produkter med digitala element genom att säkerställa att hårdvaru- och programvaruprodukter som släpps ut på marknaden har färre sårbarheter och att tillverkarna tar säkerheten på allvar under produktens hela livscykel. Den syftar också till att skapa förutsättningar för att användarna ska kunna ta hänsyn till cybersäkerheten när de väljer och använder produkter med digitala element, exempelvis genom att öka transparensen när det gäller stödperioden för produkter med digitala element som släpps ut på marknaden.

I kommissionens konsekvensbedömningsrapport (2022, SWD (2022) 282 final) redovisas vilka fördelar samt vilka kostnader och andra konsekvenser som EU:s cyberresiliensförordning innebär.

Governo AB har på utredningens uppdrag uppskattat konsekvenserna för svenska ekonomiska aktörer samt förvaltare av programvara med fri och öppen källkod.

För tillverkare innebär EU:s cyberresiliensförordning kostnader för upprättande av teknisk dokumentation, CE-märkning och dylikt, för rapporteringsskyldighet, för cybersäkerhet i produktionen, för personella resurser samt i tillämpliga fall för bedömning av överensstämmelse av anmält organ.

För förvaltare av programvara med fri och öppen källkod innebär EU:s cyberresiliensförordning kostnader för upprättande av cybersäkerhetspolicy och rapporteringsskyldighet.

För importörer och distributörer är den främsta kostnaden relaterad till anpassningskostnader för att sätta sig in i de nya rättsliga kraven och etablering av systematiska processer för efterlevnad av regelverket.

Governo AB redovisar i sin rapport kostnaderna, uppdelade på engångskostnader och återkommande (årliga) kostnader, för de ekonomiska aktörerna samt förvaltare av programvara med fri och öppen källkod.

15.4.2 Ekonomiska konsekvenser för ekonomiska aktörer samt förvaltare av programvara med fri och öppen källkod till följd av utredningens förslag

Utredningens bedömning: Utredningens förslag väntas inte medföra några kostnader för ekonomiska aktörer eller förvaltare av programvara med fri och öppen källkod.

Utredningen lämnar förslag om stöd till företag, marknadskontrollmyndigheternas befogenheter, överklagande och sanktioner. Dessa förslag berör helt eller delvis ekonomiska aktörer, det vill säga tillverkare, tillverkares representanter, importörer och distributörer, samt förvaltare av programvara med fri och öppen källkod.

De förslag som utredningen lämnar om stöd till företag syftar till att underlätta regelefterlevnad samt begränsa företagets kostnader och andra negativa effekter. Frågan behandlas i kapitel 12.

De förslag som utredningen lämnar om marknadskontrollmyndigheternas befogenheter, överklagande respektive sanktionssystem syftar till att ge goda förutsättningar för sakkunnig marknadskontroll. Sanktionssystemet har föreslagits på ett sätt som ska ge effektiva och förutsebara konsekvenser av bristande efterlevnad. Bestämmelserna tydliggör för ekonomiska aktörer vilka sanktioner som kan bli aktuella vid överträdelser och under vilka förutsättningar avgift kan beslutas. Eftersom en sanktionsavgift kan uppgå till höga belopp beroende på bland annat överträdelsens allvar kan förslagen även förväntas leda till en bättre regelefterlevnad. Detta stärker på sikt företagets konkurrenskraft och skapar bättre och mer rättvisa spelregler för företagandet.

Utredningens förslag väntas därför inte medföra några kostnadsökningar för ekonomiska aktörer eller förvaltare av programvara med fri och öppen källkod.

15.5 Särskilt om ekonomiska konsekvenser för små och medelstora företag

Utredningens bedömning: EU:s cyberresiliensförordning väntas ge ekonomiska konsekvenser för företag. Små och medelstora företag riskerar att relativt sett påverkas i större utsträckning än större företag. De förslag utredningen lämnar om stöd till små och medelstora företag syftar till att undvika att EU:s cyberresiliensförordning ska hämma näringslivet och innovation.

När det gäller tillverkare som är små eller medelstora företag uppger Governo AB att dessa aktörer riskerar att relativt sett påverkas i större utsträckning än större företag. Stora företag kommer ha större möjligheter att fördela engångskostnader för att sätta sig in i nya regleringar. Brist på medvetenhet och kompetens inom cybersäkerhetsområdet kan skapa ett konsultberoende för mindre aktörer. De mindre företagens begränsade laboratoriekapacitet, både vad gäller resurser och kompetens, kan potentiellt innebära att de måste använda externa testlaboratorier eller kontrollorgan för att säkerställa efterlevnad för produkter som faller under de lägre riskklasserna i EU:s cyberresiliensförordning. För de företag som tidigare inte arbetat strukturerat med cybersäkerhet kan kostnaderna bli särskilt betungande, eftersom de både måste stärka sin utvecklingskapacitet och avsätta resurser för löpande uppföljning och rapportering. Samtidigt kan en utebliven anpassning innebära att de inte längre får tillträde till EU:s inre marknad, vilket gör att efterlevnaden av EU:s cyberresiliensförordning blir en strategiskt avgörande fråga även för de minsta aktörerna.

Governo AB anger att importörer och distributörer som är små och medelstora företag kan komma att påverkas särskilt av EU:s cyberresiliensförordning, inte minst eftersom de ofta saknar omfattande resurser och expertis inom cybersäkerhet och regelefterlevnad. Importörer som tar in produkter från tillverkare utanför EU bär ett direkt ansvar för att dessa uppfyller kraven i förordningen, även om

de själva inte har insyn i tillverkarens processer eller tekniska kapacitet. Detta innebär att de måste utveckla rutiner för att granska dokumentation, säkerställa CE-märkning och vid behov inhämta försäkringar om att sårbarheter hanteras, trots att de i praktiken kan ha begränsad möjlighet att bedöma detta. Bristen på resurser och systematiska processer gör att kostnaderna för utbildning, administrativa kontroller och eventuell förstärkning av personalstyrkan kan väga tungt i förhållande till företagets storlek. För dessa aktörer kan EU:s cyberresiliensförordning därför innebära både en organisatorisk och ekonomisk utmaning, där riskerna främst ligger i att inte upptäcka brister i importerade produkter och därmed själva hållas ansvariga.

De förslag utredningen lämnar om stöd till små och medelstora företag syftar till att undvika att EU:s cyberresiliensförordning ska hämma näringslivet och innovation. Frågan behandlas i kapitel 12.

15.6 Ekonomiska konsekvenser för Swedac

Utredningens bedömning: Utredningens förslag att Swedac ska vara anmälande myndighet bedöms inte medföra ökade kostnader. Utredningens förslag i övrigt som rör Swedac bör finansieras inom befintlig ram.

Utredningen föreslår att Swedac ska utses till anmälande myndighet enligt artikel 36 i EU:s cyberresiliensförordning. Frågan behandlas i kapitel 6.

Den nationella ackrediteringsmyndigheten Swedac har redan i dag i uppgift att ansvara för ackreditering av organ för bedömning av överensstämmelse enligt förordning (EU) 2019/881⁵. Jämfört med de uppgifter myndigheten utför i dag skiljer sig ansvaret enligt EU:s cyberresiliensförordning åt endast i begränsad omfattning.

Ett organ som vill bli ackrediterat och anmält som organ enligt artikel 42 och artikel 43 i EU:s cyberresiliensförordning ska lämna in en ansökan till anmälande myndighet, som prövar och bedömer

⁵ Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

om organet uppfyller de krav som ställs i EU:s cyberresiliensförordning och förordning (EG) nr 765/2008⁶ samt lagen (2011:791) om ackreditering och teknisk kontroll med tillhörande förordning jämte föreskrifter som Swedac meddelat.

Ackrediteringsförfarandet vid Swedac finansieras av kundernas avgifter, som ska täcka samtliga kostnader för ackreditering. Anmälningförfarandet är anslagsfinansierat.

Av Governo AB:s rapport framgår att endast ett fåtal organ för bedömning av överensstämmelse för närvarande uttrycker intresse av att bli ackrediterade och anmälda, samtidigt som behovet av sådana organ kan förändras med anledning av en ökad efterfrågan på sådana tjänster. Eftersom verksamheten när det gäller ackreditering är avgiftsfinansierad bör denna verksamhet därför inte nu kräva ytterligare finansiella resurser. Anmälningförfarandet är anslagsfinansierat och bedöms inledningsvis kunna finansieras inom befintlig ram, dock kan frågan om ytterligare resurser behöva övervägas efter en tid efter ikraftträdandet av bestämmelserna om anmälan av organ för bestämning av överensstämmelse. Förslaget att Swedac ska ges i uppdrag att föreslå lämpliga åtgärder för att säkerställa att ett anmält organs ärenden kan behandlas av ett annat anmält organ bedöms inte heller kräva ytterligare resurser utan bedöms kunna utföras inom ram.

15.7 Ekonomiska konsekvenser för anmälda organ för bedömning av överensstämmelse

Utredningens bedömning: Utredningens förslag medför inte ökade kostnader för anmälda organ för bedömning av överensstämmelse.

EU:s cyberresiliensförordning ställer krav på anmälda organ för bedömning av överensstämmelse. Kraven följer av olika rättigheter och skyldigheter som följer av förordningen och som därför inte är en följd av utredningens förslag. Konsekvenserna redogörs för i kommissionens konsekvensbedömningsrapport (SWD(2022) 282 final).

⁶ Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93.

Utredningen lämnar förslag om ändring av beslut, överklagande och tystnadsplikt. Dessa förslag berör anmälda organ för bedömning av överensstämmelse. Utredningens förslag väntas inte medföra några kostnadsökningar för organen.

15.8 Ekonomiska konsekvenser för CSIRT-enheten

Utredningens förslag: EU:s cyberresiliensförordning väntas ge ökade kostnader för CSIRT-enheten. Det medför ett ökat finansieringsbehov hos Myndigheten för samhällsskydd och beredskap motsvarande 4 miljoner kronor för år 2026 och 7 miljoner årligen från 2027. Kostnaderna föreslås finansieras med anslag.

EU:s cyberresiliensförordning definierar vad som avses med CSIRT-enhet samt vilka uppgifter CSIRT-enheten har. Utredningen har således varken haft i uppdrag att utse CSIRT-enhet eller att införa skyldigheter för CSIRT-enheten.

I Sverige är MSB i dag CSIRT-enhet. Det finns dock ett förslag att FRA ska vara CSIRT-enhet från och med den 1 juli 2026.⁷

Utredningen har endast föreslagit att det i förordningen med kompletterande bestämmelser till EU:s cyberresiliensförordning ska införas en upplysningsbestämmelse som anger var i nationell rätt det finns bestämmelser om vilken myndighet som är CSIRT-enhet. Frågan behandlas i kapitel 8.

Utredningens förslag innebär således i sig inte några konsekvenser för CSIRT-enheten. Mot bakgrund av de uppgifter som åläggs CSIRT-enheten enligt EU:s cyberresiliensförordning, utöver de uppgifter som redan följer av NIS 2-direktivet, är det enligt utredningen av vikt att säkerställa att den nationella organiseringen och behovet av resurser är dimensionerade för att hantera samtliga dessa uppgifter. I syfte att säkerställa att den svenska CSIRT-enheten ges förutsättningar, i form av tekniska och finansiella resurser och personalresurser, för att på ett effektivt sätt kunna utföra de uppgifter som den tilldelas enligt EU:s cyberresiliensförordning väljer dock utredningen att här redovisa konsekvenserna för den svenska CSIRT-enheten som följer av skyldigheterna i förordningen.

⁷ Se kapitel 8 och slutbetänkandet *Samlade förmågor för ökad cybersäkerhet* (SOU 2025:79).

EU:s cyberresiliensförordning ålägger CSIRT-enheten ett antal uppgifter i tillägg till de uppgifter som redan följer av NIS 2-direktivet, se vidare avsnitt 8.3. Sammanfattningsvis är CSIRT-enheten mottagare av sårbarhets- och incidentrapporter, har en operativ roll i att analysera och följa upp rapporterade sårbarheter och incidenter, ska bistå med teknisk analys samt vid behov informera och samverka med andra berörda aktörer som marknadskontrollmyndigheterna, EU:s cybersäkerhetsbyrå (Enisa), med flera. Uppgifterna syftar till att stötta samhället, både företag och myndigheter samt att hantera och förebygga it-incidenter.

Den svenska CSIRT-enheten har redan i dag omfattande uppgifter att stötta samhället i arbetet med att hantera och förebygga it-incidenter. Dessa uppgifter är likartade dem som följer av EU:s cyberresiliensförordning. EU:s cyberresiliensförordning får dock till följd att betydligt fler aktörer omfattas av rapporteringsskyldigheterna och att rapporteringsskyldigheten, till skillnad från NIS-regleringen, inte rör sårbarheter och incidenter i nätverks- och informationssystem utan i produkter med digitala element. Cyberresiliensförordningens breda tillämpningsområde kan komma att medföra en omfattande sårbarhets- och incidentrapportering till CSIRT-enheten samt efterfrågan av mer stöd. Dessutom får EU:s cyberresiliensförordning till följd att CSIRT-enheten behöver samverka med en ny kategori av tillsynsmyndighet i form av marknadskontrollmyndigheterna.

Konsekvenserna för CSIRT-enheten är beroende av i vilken utsträckning som företag och marknadskontrollmyndigheter efterfrågar stöd och hur många sårbarhets- och incidentrapporter som inkommer till enheten. Det kan noteras att EU:s cyberresiliensförordning har ett brett tillämpningsområde eftersom förordningen omfattar en mycket stor mängd produkter som dessutom väntas öka framöver samt att sårbarhets- och incidentrapporteringen även omfattar produkter som släppts på marknaden före förordningens ikraftträdande. Även om den obligatoriska sårbarhets- och incidentrapporteringen endast omfattar aktivt utnyttjade sårbarheter och inträffade incidenter är det möjligt för vem som helst att också frivilligt inkomma med rapporter om eventuella sårbarheter, cyberhot, eventuella incidenter och tillbud.

Av MSB:s årsrapport om it-incidentrapportering 2024⁸ framgår att antalet inkomna it-incidentrapporter minskade under 2024. Totalt rapporterades 319 it-incidenter från 163 enskilda organisationer in till MSB. Under 2024 rapporterades 170 incidenter från statliga myndigheter, vilket fortsätter en trend av ett minskat inrapporterade incidenter från statliga myndigheter som pågått sedan 2018. Under 2024 rapporterades 149 incidenter från leverantörer av samhällsviktiga tjänster och vissa digitala tjänster (NIS-leverantörer), vilket är en marginell ökning som fortsätter en ökande trend. MSB har under en längre tid bedömt att det förekommer ett stort mörkertal i it-incidentrapporteringen.

Under 2024 har flera stora sårbarheter i olika it-produkter påträffats, vilket bidragit till att antalet hanterade ärenden hos den svenska CSIRT-enheten CERT-SE fortsatt att öka och uppgick till 17 500, en ökning på nästan 20 procent jämfört med 2023. CERT-SE har under året hanterat flera större cybersäkerhetsincidenter, inklusive utpressningsvirus- och överbelastningsangrepp mot svenska myndigheter, banker och samhällsaktörer samt riktade nätfiskekampanjer. Under året har CERT-SE även stärkt förmågan att hantera it-incidenter inom Sverige och förmågan till automatiserad omvärldsbevakning, exempelvis genom funktionen för Automatiska Notifieringar av Tekniska Sårbarheter (ANTS). Under 2024 skickades 37 500 notifieringar till ANTS-anslutna organisationer.

MSB har till utredningen inkommit med underlag som beretts med FRA. I underlaget beskriver MSB vad en utveckling och anpassning av CSIRT-enheten till EU:s cyberresiliensförordning innebär och kostar för myndigheten.

MSB uppger att myndigheten planerar en förmågehöjning kring samordnad delgivning av information om sårbarheter (CVD) för att från och med första kvartalet 2026 kunna svara upp mot uppgifterna som följer av artikel 12 i NIS 2-direktivet. Förmågehöjningen innebär en uppdatering av rutiner och processer, kompetensförsörjning samt extern kommunikation kring CVD. För att möta kraven i EU:s cyberresiliensförordning kommer myndigheten i detta även inarbeta de nya mandat och arbetsuppgifter som den förordningen för med sig. EU:s cyberresiliensförordning innebär ett tillskott av CVD-ärenden vilket gör att myndighetens befintliga ambitioner i förmågehöjningen be-

⁸ Verktyg för ökad motståndskraft och stärkt civilt försvar, Årsrapport it-incidentrapportering 2024, MSB2563 – mars 2025.

höver justeras upp för att hantera ökade volymer. MSB uppger att myndigheten även behöver ta höjd för de nya åtaganden som åläggs verksamheten, däribland de hjälptjänster som ska tillhandahållas till tillverkare. MSB:s tolkning är att tjänsterna ska hjälpa tillverkaren att förstå rapporteringsskyldigheter och tillvägagångssätt för rapportering och kan realiseras genom stöttande dokumentation och beskrivningar på hemsida samt vägledning via telefon och mejl. MSB:s erfarenhet från implementeringen av NIS-direktivet och pågående implementering av NIS 2-direktivet är att sådant stöd utgör en resursintensiv uppgift. Därutöver ska CSIRT-enheten tillhandahålla stöd till marknadskontrollmyndigheterna. MSB uppger att det stöd som aktualiseras kommer att belasta personal med den kompetens som behövs i CVD-ärenden. MSB uppger att myndigheten behöver ha en dialog med marknadskontrollmyndigheterna för att stämma av förväntningar och behov av stöd för att dimensionera sin förmåga korrekt. Vidare uppger MSB att myndigheten internationellt är engagerade i EU CSIRTs Networks arbetsgrupp kring CVD som även stöttar Enisa i arbetet med både EU:s sårbarhetsdatabas och det gemensamma rapporteringsverktyget för EU:s cyberresiliensförordning (Single Reporting Platform). Genom fortsatt aktivt deltagande i arbetsgruppen och bevakning av arbetet med det gemensamma rapporteringsverktyget tillser MSB integration mot svenska system och intressenter (rapportörer, MSB och marknadskontrollmyndigheterna). I detta ingår även att följa vad nationella slutpunkter för elektronisk anmälan innebär i praktisk tillämpning för att tidigt fånga upp stora krav och säkerställa erforderlig nationell implementering.

MSB uppger att det kommer att uppstå sannolika utmaningar i att snabbt bygga upp personalstyrkan med rätt kompetens. CVD-processen är en kunskapsintensiv process som kräver kvalificerad personal med kompetens inom bland annat server-klient-lösningar, webbapplikationer, respektive erfarenhet av utveckling eller penetrationstestning, områden där det är känt att arbetsmarknaden har svårare att möta upp med kompetens. Rapporteringen ska börja tillämpas den 11 september 2026, således drygt en månad efter att den nationella CSIRT-enheten föreslås överföras från MSB till FRA. Att verksamheten precis varit igenom en verksamhetsöverföring ställer ännu högre krav på MSB:s förberedelser som behöver inledas så snart som möjligt.

MSB har inkommit med beräkningarna över kostnaderna för de åtgärder som myndigheten bedömer behöver vidtas för att anpassa CSIRT-enheten till kraven i EU:s cyberresiliensförordning, uppdelade på initiala och löpande kostnader. Dessa avser en miniminivå för att bygga upp en grundläggande förmåga på CSIRT-enheten för att hantera de nya uppgifter som följer av EU:s cyberresiliensförordning. MSB noterar att kostnaderna kan komma att bli högre när EU:s cyberresiliensförordning tillämpas fullt ut i Sverige. Kostnaderna redovisas i nedanstående två tabeller.

Tabell 15.1 Initiala kostnader

Initiala kostnader	tkr
Integration mellan Single Report Platform och den svenska rapporteringsportalen	200
Anskaffning av analysverktyg för kod	1 000
Utbildning i, integration av, samt etablera förmåga kring analysverktyg	200
Resurser för att bygga upp och etablera förmåga, både avseende hjälptjänster och CVD-hantering*	3 000

*) Det tar tid att rekrytera de specialister som behövs till CVD-analys, därför behöver denna rekrytering påbörjas tidigt i processen för att nå full bemanning enligt tabellen nedan så snabbt som möjligt.

Källa: Myndigheten för samhällsskydd och beredskap.

Tabell 15.2 Löpande kostnader

Löpande kostnader	tkr
Resurser som bemannar hjälptjänster motsvarande två heltidstjänster	2 000
Specialister till analys av CVD-ärenden och stöd till marknadskontrollmyndighet/erna motsvarande tre heltidstjänster	4 500
Löpande kompetensutveckling och internationellt erfarenhetsutbyte inom CVD-analys	150
Drift-, förvaltning- och licenskostnader av integrationer, system och verktyg	240

Källa: Myndigheten för samhällsskydd och beredskap.

Som redovisats ovan är det i nuläget mycket svårt att uppskatta antalet ekonomiska aktörer som kommer omfattas av EU:s cyberresiliensförordning. Av detta följer att det inte heller går att beräkna antalet incidenter eller hur omfattande behovet av hjälptjänster är på ett tillförlitligt sätt. Samtidigt träder bestämmelserna om sårbarhets- och incidentrapportering i EU:s cyberresiliensförordning i kraft den 11 september 2026 och utredningen föreslår dessutom att CSIRT-

enheten ska tillhandahålla de hjälptjänster som anges i förordningen så tidigt som möjligt och före ikraftträdandet av EU:s cyberresiliensförordning i syfte att förbereda företag att efterleva förordningens krav. Därför bör den myndighet som är CSIRT-enhet ha utökade resurser från 2026 för att kunna hantera rapportering och hjälptjänster.

Utredningen bedömer dock att det finns vissa samordningsvinster när det gäller sårbarhets- och incidentrapportering eftersom samma myndighet redan hanterar sårbarhets- och incidentrapporter enligt den föreslagna lagen om cybersäkerhet. När det gäller hjälptjänster är utredningens bedömning att samma samordningsvinster inte gör sig gällande mot bakgrund av att de ekonomiska aktörerna är en helt ny kategori aktörer jämfört med de aktörer som regleras i den föreslagna cybersäkerhetslagen. Vidare är majoriteten av aktörerna små företag som kan ha begränsad kompetens inom cybersäkerhetsområdet. Dessutom saknas ännu den gemensamma rapporteringsplattform som kommissionen ska inrätta (bestämmelserna om denna träder i kraft först den 11 december 2027). Utredningens bedömning är att den myndighet som är CSIRT-enhet behöver få medel för att verksamheten enligt EU:s cyberresiliensförordning ska kunna förberedas. Resursbehovet kan inte finansieras inom befintlig ram. Utredningen gör mot bakgrund av ovanstående och underlaget från MSB den sammantagna bedömningen att MSB behöver tillföras 4 miljoner kronor för år 2026 och med en permanent ökning av anslaget med 7 miljoner kronor från och med 2027. Kostnaderna föreslås finansieras med anslag.

15.9 Ekonomiska konsekvenser för Myndigheten för samhällsskydd och beredskap – stöd till företag

Utredningens förslag: Utredningens förslag om stöd till företag enligt artikel 33.1 i EU:s cyberresiliensförordning innebär ökade kostnader för Myndigheten för samhällsskydd och beredskap. Det medför ett ökat finansieringsbehov motsvarande 6 miljoner kronor årligen från 2026. Kostnaderna föreslås finansieras med anslag.

Utredningen har föreslagit att MSB ska tillhandahålla och samordna stöd till företag enligt artikel 33.1 i EU:s cyberresiliensförordning. Utredningen har också föreslagit att MSB bör ges ett regeringsuppdrag att så tidigt som möjligt och före ikraftträdandet av EU:s cyberresiliensförordning tillhandahålla stödet. Frågan behandlas i kapitel 12.

MSB har till utredningen inkommit med underlag som uppskattar konsekvenser samt visar vad en utveckling och anpassning av verksamheten till EU:s cyberresiliensförordning innebär för myndigheten. Beräkningarna avser enligt MSB en miniminivå för att bygga upp en grundläggande förmåga på myndigheten att hantera de nya uppgifter som följer av EU:s cyberresiliensförordning. MSB ser därför att kostnaderna för myndigheten kan komma att bli högre när förordningen väl tillämpas fullt ut i Sverige.

MSB bedömer att myndigheten kommer att behöva rekrytera personal motsvarande fyra heltidstjänster till en kostnad av 6 miljoner kronor i syfte att stärka CSIRT-enheten, NCC-SE samt de funktioner som bland annat ansvarar för Cybersäkerhetsrådgivningen, MSB:s metodstöd för informations-säkerhetsarbete, Cybersäkerhetskollen och Cybersäkerhetskonferensen. MSB uppger att för att kunna tillhandahålla stöd inom cybersäkerhetsområdet, inklusive stöd enligt EU:s cyberresiliensförordning, behöver myndigheten rekrytera kompetens som inte finns på myndigheten i dag.

Utredningen bedömer att behovet av stöd till företag som stort, i synnerhet vad avser små och medelstora företag. Utredningen anser att det är av yttersta vikt att tillräckliga resurser ges för stödjande och kunskapshöjande insatser för att undvika att näringslivet och innovation hämmas.

EU:s cyberresiliensförordning träder i kraft den 11 december 2027 och utredningen föreslår att MSB ska tillhandahålla stöd till företag så tidigt som möjligt och före ikraftträdandet av EU:s cyberresiliensförordning i syfte att förbereda företag att efterleva förordningens krav. Därför bör MSB ha utökade resurser från 2026 för att kunna påbörja arbetet. Utredningen gör mot bakgrund av ovanstående och underlaget från MSB den sammantagna bedömningen att MSB behöver tillföras en permanent ökning av anslaget med 6 miljoner kronor från och med 2026. Resursbehovet kan inte finansieras inom befintlig ram.

15.10 Ekonomiska konsekvenser för marknadskontrollmyndigheterna

Utredningens förslag: EU:s cyberresiliensförordning och utredningens förslag innebär nya arbetsuppgifter för marknadskontrollmyndigheterna. Det medför ett ökat finansieringsbehov hos Post- och telestyrelsen motsvarande 10 miljoner kronor för år 2026 och 20 miljoner årligen från och med 2027. Kostnaderna föreslås finansieras med anslag.

Utredningen föreslår att PTS ska vara marknadskontrollmyndighet enligt EU:s cyberresiliensförordning. Frågan behandlas i kapitel 9.

För produkter med digitala element som omfattas av EU:s cyberresiliensförordning och som klassificeras som AI-system med hög risk enligt artikel 6 i AI-förordningen ska dock de marknadskontrollmyndigheter som utsetts enligt AI-förordningen vara de myndigheter som ansvarar för den marknadskontroll som föreskrivs i EU:s cyberresiliensförordning (artikel 52.14 i EU:s cyberresiliensförordning).

Betänkandet *Anpassningar till AI-förordningen* (SOU 2025:101) föreslår Arbetsmiljöverket, Boverket, Elsäkerhetsverket, Finansinspektionen, Integritetsskyddsmyndigheten (IMY), Kemikalieinspektionen, Konsumentverket, Läkemedelsverket, MSB, PTS och Transportstyrelsen som marknadskontrollmyndigheter enligt AI-förordningen.⁹ Den utredningens arbete har pågått parallellt och det har därför inte varit möjligt att beakta resultaten av utredningen i denna konsekvensutredning. Konsekvenserna till följd av EU:s cyberresiliensförordning och utredningens förslag för de myndigheter som ska utses som marknadskontrollmyndigheter enligt AI-förordningen har inte kunnat beaktats inom ramen för utredningens arbete. Konsekvenserna för dessa myndigheter bör beaktas i det fortsatta lagstiftningsarbetet. I detta sammanhang redovisas endast konsekvenserna för PTS.

Artikel 52.8 i EU:s cyberresiliensförordning anger att medlemsstaterna ska säkerställa att de utsedda marknadskontrollmyndigheterna har tillräckliga ekonomiska och tekniska resurser, inbegripet vid behov verktyg för automatisk databehandling samt personal-

⁹ Se s. 225–305.

resurser med nödvändig cybersäkerhetskompetens för att kunna fullgöra sina uppgifter enligt denna förordning.

De ekonomiska konsekvenserna för PTS och övriga marknadskontrollmyndigheter följer till största delen direkt av EU:s cyberresiliensförordning och inte av utredningens förslag. De förändringar som utredningens förslag för med sig i kostnadsavseende kan antas vara marginella.

15.10.1 Ekonomiska konsekvenser för marknadskontrollmyndigheterna – marknadskontroll

EU:s grundstruktur för marknadskontroll, som sedan länge finns etablerad, bygger på att det som huvudregel är tillverkarens ansvar att en produkt uppfyller gällande krav och det krävs inte någon förhandskontroll av produkten från myndighetshåll innan den släpps ut på marknaden. För att säkerställa att produkter på marknaden överensstämmer med gällande krav används i stället marknadskontroll, se vidare kapitel 9.

Governo AB bedömer att uppbyggnadsfasen för den nya marknadskontrolluppgiften med anledning av EU:s cyberresiliensförordning kommer att medföra kostnader för dels att bygga upp och etablera den nya funktionen för marknadskontroll (till exempel i form av kompetensuppbyggnad och nyrekryteringar), dels att etablera den nya marknadskontrollfunktionen i en extern kontext (till exempel i form av samverkan och informationsinsatser). Med ett antagande om att den nya marknadskontrollfunktionen skulle komma att omfatta cirka sex till tolv årsarbetskrafter bedömer Governo AB att kostnaderna för marknadskontrollmyndighetens interna insatser för att bygga upp och etablera den nya funktionen skulle uppgå till ett belopp mellan tre och sex miljoner kronor samt kostnaderna för att etablera den nya marknadskontrollfunktionen i en extern kontext skulle uppgå till ett belopp mellan cirka en och två miljoner kronor. Sammantaget bedömer Governo AB att kostnaderna för uppbyggnadsfasen för den nya marknadskontrolluppgiften kommer att uppgå till mellan fyra och åtta miljoner kronor.

När det sedan gäller kostnader för den löpande verksamheten uppger Governo AB att kostnaden för marknadskontrollen beror på hur många kontroller som görs. Med nuvarande kunskapsläge är det svårt att bedöma hur många produkter som bör kontrolleras och

hur många kontroller som bör göras. Governo AB:s ansats har varit att först försöka ange ett ”nollalternativ”, dvs. säga en minsta nivå för hur stora resurser den nya marknadskontrollfunktionens löpande verksamhet bedöms kräva. Denna nivå har sedan ställts mot två – i varierande grad – mer expansiva alternativ. Sammanfattningsvis bedömer Governo att den löpande verksamheten avseende den nya marknadskontrolluppgiften uppgår till mellan 10 och 20 miljoner kronor per år.

Utredningens förslag är att PTS ska utses till marknadskontrollmyndighet enligt EU:s cyberresiliensförordning. Förslaget innebär utökade och flera nya arbetsuppgifter för PTS. Ansvaret kommer att omfatta en stor mängd produkter, som med teknikutvecklingen med största sannolikhet kommer att öka ytterligare framöver, och sträcka sig över alla samhällets sektorer. I marknadskontrollansvaret ingår även att lämna information och ge stöd till företag. Behovet av stöd bedöms som stort, särskilt vad avser små och medelstora företag. Även om PTS har erfarenhet av marknadskontroll och har kompetens inom cybersäkerhetsområdet så innebär utredningens förslag nya arbetsuppgifter för myndigheten. Utredningen bedömer att marknadskontroll enligt EU:s cyberresiliensförordning är komplext och avviker från sedvanlig marknadskontroll av produkter genom att även omfatta bland annat produkternas livscykel. PTS saknar även tidigare erfarenhet av att etablera regulatoriska sandlådor. Dessutom ställer förordningen långtgående krav på samverkan med andra aktörer och stöd till företag inom ett område där det råder brist på cybersäkerhetskompetens. Utöver det kan resursbehovet påverkas av förändringar i regelverket genom harmoniserade standarderna samt genom kommissionens delegerade akter och genomförandeakter. Utredningen bedömer därför att marknadskontrollverksamheten kan bli resurskrävande.

Utredningen gör mot bakgrund av ovanstående och Governo AB:s rapport den sammantagna bedömningen att cirka 12 årsarbetskrafter krävs för marknadskontrollverksamhetens uppbyggnad och genomförande även om den bedömningen är förenad med viss osäkerhet. Marknadskontrollverksamheten bedöms inte kunna finansieras inom befintlig ram. PTS bedöms behöva tillföras 10 miljoner kronor för år 2026 och med en permanent ökning av anslaget med 20 miljoner kronor från och med 2027. Marknadskontrollen ska kunna påbörjas i december 2027 och det är av vikt att medel tillförs

myndigheten redan 2026 och 2027 eftersom ett omfattande arbete krävs för att bygga upp och förbereda verksamheten samt tillhandahålla stöd till företag i syfte att säkerställa att EU:s cyberresiliensförordning inte hämmar näringsliv och innovation. Kostnaderna föreslås finansieras med anslag. Frågan om utvärdering av finansieringen behandlas i avsnitt 15.18.

Alternativ finansiering

Utredningen har även övervägt om ett alternativ till anslagsfinansierad marknadskontroll är att införa en avgiftsfinansierad marknadskontroll. I dessa fall antingen som en engångsavgift som tas ut för varje kontroll eller att avgifter erläggs av alla ekonomiska aktörer, dvs. kollektivet.

Ett system med engångsavgift innebär att den som åtgärden riktas mot står för myndighetens hela kostnad för kontrollen. Ett system med årliga avgifter innebär att alla i kollektivet ingående ekonomiska aktörer som marknadskontrollen riktas mot tillsammans finansierar myndigheternas arbete med marknadskontrollen.

Frågan om olika former av finansiering har övervägts i flera andra utredningar, bland annat i betänkandet *Informationssäkerhet för samhällsviktiga och digitala tjänster* (SOU 2017:36) som behandlar genomförandet av direktiv (EU) 2016/1148¹⁰ (NIS-direktivet) samt i betänkandet *Nya regler om cybersäkerhet* (SOU 2024:18) som behandlar genomförandet av direktiv (EU) 2022/2555¹¹ (NIS 2-direktivet). Även Statskontoret har belyst frågor om lämplig finansiering när det gäller NIS- och NIS 2-direktiven.¹²

En förutsättning för att finansiera tillsyn med årliga avgifter är att det finns information om de verksamheter som omfattas av kontroller. En tillsynsavgift bör även motsvaras av en tydlig motprestation, uppfattas som rättvis och inte vara konkurrenssnedvridande. Avgifterna bör vara förutsebara, lätta att förstå och ge incitament till avsedda beteenden hos de som ska kontrolleras.

¹⁰ Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

¹¹ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

¹² Statskontoret (2018:7), Tillsyn enligt NIS-direktivet – kostnader och finansiering, samt Statskontoret (2025:8), Tillsynsmyndigheternas kostnader till följd av NIS2-direktivet.

När det gäller lämplig modell för avgifter för marknadskontroll enligt EU:s cyberresiliensförordning kan till en början noteras att det finns ett mycket stort antal ekonomiska aktörer som omfattas av kontrollen och att det med nuvarande ordning inte finns förutsättningar att få kännedom om alla individuella ekonomiska aktörer, eftersom det i de flesta fall inte finns någon skyldighet att anmäla till en myndighet att man bedriver verksamhet som omfattas av förordningens tillämpningsområde. Det saknas redan härigenom förutsättningar att påföra enskilda ekonomiska aktörer en skyldighet att erlägga en årlig avgift för marknadskontroll. Det kan även noteras att det inte finns stöd i EU:s cyberresiliensförordning för att ålägga alla ekonomiska aktörer en skyldighet att anmäla när en produkt med digitala element sätts på den inre marknaden.

I sammanhanget ska noteras att förslaget om anslagsfinansiering hindrar inte marknadskontrollmyndigheterna att ta ut vissa avgifter för marknadskontroll enligt förordning (EU) 2019/1020¹³ (EU:s marknadskontrollförordning). Det innebär att marknadskontrollmyndigheten från den relevanta ekonomiska aktören i det enskilda fallet får återkräva kostnader för sin verksamhet i de fall en bristande överensstämmelse föreligger. De kostnader som avses får inkludera kostnader för att utföra provning, kostnader för att vidta åtgärder i enlighet med artikel 28.1 och 28.2 i EU:s marknadskontrollförordning, kostnader för lagring och kostnader för verksamhet avseende produkter som befunnits inte överensstämma med kraven och som undergår korrigerande åtgärder innan de övergår till fri omsättning eller släpps ut på marknaden. Det rör sig således endast av vissa av de kostnader som är hänförliga till marknadskontroll, inte hela marknadskontrollverksamheten. Det finns i denna modell således även ett behov av anslagsfinansiering. Frågan behandlas även i kapitel 9. Vidare ska noteras att en enhetlig finansiering med anslag underlättar även budgetering och resursplanering samt skapar tydligare ekonomiska ramar för marknadskontrollarbetet.

Som utredningen anför ovan framstår därför en modell med anslagsfinansiering, med möjlighet att i det enskilda fallet ta ut avgifter för kontroll, som den mest ändamålsenliga och kostnadseffektiva modellen att finansiera marknadskontrollen.

¹³ Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011.

En senare utvärdering av finansiering bör dock enligt utredningens bedömning göras, se vidare avsnitt 15.18.

15.10.2 Ekonomiska konsekvenser för marknadskontrollmyndigheterna – stöd till företag och regulatoriska sandlådor

Enligt EU:s cyberresiliensförordning får marknadskontrollmyndigheterna ge ekonomiska aktörer vägledning och råd om genomförandet av förordningen. De ska även, när så är lämpligt, underlätta samarbetet med berörda parter, inbegripet vetenskapliga organisationer samt forsknings- och konsumentorganisationer. Enligt utredningens förslag bör PTS ges i uppdrag att så tidigt som möjligt och före ikraftträdandet av EU:s cyberresiliensförordning tillhandahålla stöd till företag i syfte att förbereda företag att efterleva förordningens krav. Vidare föreslår utredningen att PTS i syfte att stödja företag får besluta om inrättande och drift av regulatoriska sandlådor. Frågan behandlas i kapitel 12.

Att informera om gällande regelverk är en del av marknadskontrollansvaret och kostnaderna för detta utgör ingen tillkommande kostnad utan ingår som en del i de kostnader som redovisats gällande marknadskontrolluppgiften. Även om förslag avseende stödåtgärder innebär en viss kostnad för myndigheten förväntas stödåtgärderna underlätta tillämpningen av förordningen och förväntas därmed även bidra till en effektivare marknadskontroll för myndigheten.

15.10.3 Ekonomiska konsekvenser för Post- och telestyrelsen – förbättra kompetensen i en cyberresilient digital miljö samt öka tillgång på organ för bedömning av överensstämmelse

Förslagen att PTS ska ges i uppdrag att ta fram förslag som främjar åtgärder och strategier för att utveckla cybersäkerhetskompetens och skapa organisatoriska och tekniska verktyg för att säkerställa tillräcklig tillgång till kvalificerad arbetskraft för att stödja verksamheten vid organ för bedömning av överensstämmelse och marknadskontrollmyndigheterna och att verka för en ökad nationell tillgång på organ för bedömning av överensstämmelse bedöms inte kräva

ytterligare resurser utan bedöms kunna utföras inom befintlig ekonomisk ram.

15.11 Ekonomiska konsekvenser för Tullverket

Utredningens bedömning: EU:s cyberresiliensförordning får konsekvenser för Tullverket. De kostnader som uppstår bör finansieras inom befintlig ekonomisk ram.

Tullverket har i uppdrag att utföra kontroll av produkter som förs in på unionsmarknaden. De produkter som omfattas av EU:s cyberresiliensförordning och som kan bli föremål för Tullverkets kontroll omfattas visserligen redan av annan produkt- och marknadskontrollagstiftning men utredningen bedömer att EU:s cyberresiliensförordning kan komma att leda till att Tullverket behöver genomföra fler kontroller och riskbedömningar än i dag. Frågan behandlas i kapitel 9. Det kommer i sin tur medföra resursmässiga och ekonomiska konsekvenser. Utredningen bedömer att dessa kostnader bör kunna hanteras inom befintliga ekonomiska ramar.

15.12 Ekonomiska konsekvenser för Polismyndigheten

Utredningens bedömning: Utredningens förslag kan få konsekvenser för Polismyndigheten. De eventuella kostnader som uppstår bör finansieras inom befintlig ekonomisk ram.

Enligt utredningens förslag ska Polismyndigheten under vissa förutsättningar och på begäran av marknadskontrollmyndigheterna lämna den hjälp som behövs vid marknadskontroll. Frågan behandlas i kapitel 9.

Detta förväntas ske endast i undantagsfall. De eventuella ökade kostnader som kan uppkomma med anledning av förslagen bör kunna hanteras inom befintliga ekonomiska ramar.

15.13 Ekonomiska konsekvenser för Sveriges domstolar

Utredningens förslag: Utredningens förslag kan få konsekvenser för Sveriges domstolar. De eventuella kostnader som uppstår bör finansieras inom befintlig ekonomisk ram.

Beslut som fattas av anmälda organ för bedömning av överensstämmelse enligt EU:s cyberresiliensförordning ska kunna överklagas till allmän förvaltningsdomstol. Frågan behandlas i kapitel 6.

Som ovan framgår är det förenat med svårigheter att uppskatta antal produkter med digitala element som kommer att kräva bedömning av överensstämmelse av sådana organ. Även om andelen utgör en mindre del av berörda produkter kan förutsättas att ett antal beslut av dessa organ kan komma att bli föremål för överprövning i domstol och att antalet kan komma att öka när regelverket tillämpats en tid. Överklagade beslut kommer också att i vissa fall innehålla komplexa tekniska förhållanden som kan komma att kräva sakkunnig expertis i domstolen. Utredningen föreslår samtidigt att överklagade ska ske till allmän förvaltningsdomstol vilket medför en spridning av målen på befintliga domstolar. Sammantaget bedöms de allmänna domstolarna initialt kunna handlägga mål om överklagande inom befintlig ram samtidigt som eventuell måltillströmning kan aktualisera ett ökat resursbehov hos domstolarna.

Även beslut som fattas av Swedac ska kunna överklagas till allmän förvaltningsdomstol. Frågan behandlas i kapitel 6. Det kan förväntas leda till en något ökad måltillströmning hos domstolarna. Utredningen bedömer att antalet sådana mål är begränsade och att domstolarna kan hantera dessa mål inom befintliga ekonomiska ramar.

Marknadskontrollmyndigheterna får fatta beslut om marknadskontrollåtgärder och sanktioner. Frågan behandlas i kapitel 9 och 10. Besluten kan förväntas leda till domstolsprövning i ett antal fall. Som framgår ovan är det förenat med svårigheter att bedöma antal ekonomiska aktörer samt även produkter som kan bli aktuella för marknadskontroll.

Den angivna konsultrapporten indikerar att det är ett stort antal företag och produkter som omfattas av EU:s cyberresiliensförordning och som därför är underkastade marknadskontroll. Avgörande för bedömningen av beslut som kan förväntas överklagas och måltillströmningen hos allmänna domstolar är omfattningen av mark-

nadskontrollen. Initialt bedöms antalet överklaganden av marknadskontrollmyndighetens beslut vara begränsat men kan komma att öka när regelverket har tillämpats en tid. Det kan således förväntas leda till en något ökad måltillströmning hos domstolarna. Även dessa mål kan i vissa fall innehålla komplexa tekniska förhållanden som kräver sakkunnig expertis hos domstolen. Sammantaget gör utredningen bedömningen att de eventuella ökade kostnader som kan uppkomma med anledning av förslaget att beslut av en marknadskontrollmyndighet ska överklagas till allmän förvaltningsdomstol initialt kan hanteras inom befintliga ekonomiska ramar men den faktiska måltillströmningen bör följas upp.

15.14 Konsekvenser för det kommunala självstyret

Utredningens bedömning: Utredningens förslag har ingen påverkan på den kommunala självstyrelsen.

Utredningen bedömer att förslagen inte inskränker den kommunala självstyrelsen eller innebär förändringar av kommunala befogenheter eller skyldigheter, respektive grunderna för kommunernas eller regionernas organisation eller verksamhetsformer.

15.15 Konsekvenser med anledning av standardiseringsarbetet

Utredningens bedömning: Standardiseringsarbetet till följd av EU:s cyberresiliensförordning kan få konsekvenser för Post- och telestyrelsen. De eventuella kostnader som uppstår bör kunna finansieras inom befintlig ekonomisk ram.

Som framgår av avsnitt 7.6 har utredningen gjort bedömningen att det inte finns några åtgärder som i närtid kan vidtas för att kunna påverka standardiseringsarbetet för EU:s cyberresiliensförordning. De intressenter som är tillgängliga bedöms redan delta i arbetet. Det finns därför inga förslag från utredningens sida som medför konsekvenser för berörda myndigheter, företag eller andra nationella orga-

nisationer. Däremot anser utredningen att det är lämpligt att de svenska standardiseringsorganen, inom ramen för sin återsrapporteringsskyldighet, utvärderar vilka effekter det ökade statsbidraget till svenska standardiseringsorganisationer för 2025 har medfört. För att skyndsamt kunna medverka vid ny lagstiftning som förutsätter harmoniserade standarder bör de svenska standardiseringsorganen och övriga intressenter arbeta mer långsiktigt. Frågan behandlas i kapitel 7.

De åtgärder som anges i mål 4 i den Nationella strategin för cybersäkerhet kan antas bidra till ökad rekrytering av experter på framtida standardiseringsområden. Utredningen anser dock att behoven bör fortsatt särskilt beaktas vid uppföljning och uppdatering av den strategin.

Sammantaget bedömer utredningen att behovet av åtgärder för ett strategiskt och mer långsiktigt arbete med rekrytering av experter på framtida områden omhändertas i tillräcklig omfattning i regeringens nationella strategier på området.

Som framgår av avsnitt 9.6.7 deltar PTS redan i standardiseringsarbetet inom cybersäkerhetsområdet. De eventuella ökade kostnader som kan uppkomma med anledning av standardiseringsarbetet till följd av EU:s cyberresiliensförordning bör kunna hanteras inom befintliga ekonomiska ramar.

15.16 Konsekvenser för jämställdhet och den personliga integriteten

Utredningens bedömning: Utredningens förslag förväntas inte få några konsekvenser för jämställdheten mellan kvinnor och män.

Förslagen i detta betänkande bedöms inte ha särskilda konsekvenser för jämställdheten mellan kvinnor och män eller för den personliga integriteten. Konsekvenserna för grundläggande fri- och rättigheter är snarare en följd av EU:s cyberresiliensförordning än av utredningens förslag. Däremot bidrar förslagen till att de positiva konsekvenserna som förväntas av EU:s cyberresiliensförordning uppnås ur ett svenskt perspektiv genom att kraven i förordningen följs.

15.17 Särskild hänsyn till tidpunkt för ikraftträdande och behov av speciella informationsinsatser

Utredningens förslag om regeringsuppdrag till myndigheterna avseende stöd till företag (se kapitel 12) bör ges så tidigt som möjligt och före ikraftträdandet av EU:s cyberresiliensförordning. Utredningens övriga förslag bör träda i kraft samtidigt som bestämmelserna i EU:s cyberresiliensförordning. EU:s cyberresiliensförordning ska tillämpas från och med den 11 december 2027. Artikel 14, om den obligatoriska sårbarhets- och incidentrapporteringen, ska dock tillämpas från och med den 11 september 2026 samt kapitel IV, om anmälan av organ för bedömning av överensstämmelse, ska tillämpas från och med den 11 juni 2026.

Utredningens förslag kommer att remitteras före det att beslut fattas. Berörda aktörer kommer då att få ta del av förslagen och få möjlighet att yttra sig över dem. Det bedöms inte i övrigt finnas behov av några speciella informationsinsatser med anledning av de föreslagna kompletterande bestämmelserna. Däremot finns det ett behov av informationsinsatser i god tid om EU:s cyberresiliensförordning i sin helhet, vilket är bakgrunden till utredningens förslag i dessa delar, se kapitel 12.

15.18 Utvärdering av konsekvenserna

Som utredningen tidigare framhållit är det förenat med vissa svårigheter att fullt ut bedöma konsekvenserna i flera olika avseenden för berörda ekonomiska aktörer och myndigheter genom införandet av regelverket i EU:s cyberresiliensförordning. Konsekvensbedömningen grundas på flera okända faktorer och antaganden om den fortsatta utvecklingen av bland annat marknadsförhållanden och tillämpningen av marknadskontrollen. Det föreligger därför skäl att efter en tid genomföra en utvärdering av konsekvenserna av regelverkets genomförande. En utvärdering av konsekvenserna som följer av utredningens förslag och EU:s cyberresiliensförordning är framför allt aktuell i fråga om behovet av stöd till berörda företag samt resursbehov och finansiering hos berörda myndigheter och domstolarna.

En utvärdering av konsekvenserna för berörda myndigheter och domstolarna kan dock aktualiseras först när regelverket som helhet

finns på plats, dvs. när harmoniserade standarder samt delegerade akter och genomförandeakter är beslutade och när myndigheternas kostnader och andra eventuella konsekvenser blivit kända.

En av fortsatt resursbehov och finansiering bör därför enligt utredningens bedömning göras när regelverket som helhet finns på plats och myndigheterna verksamhet kopplat till EU:s cyberresiliensförordning har pågått en period. Eftersom förordningen i dess helhet ska tillämpas från den 11 december 2027 bör en utvärdering påbörjas 2030.

16 Författningskommentar

16.1 Förslaget till lag med kompletterande bestämmelser till EU:s cyberresiliensförordning

Inledande bestämmelser

1 § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen), i denna lag benämnd EU:s cyberresiliensförordning.

Ord och uttryck i denna lag har samma betydelse som i EU:s cyberresiliensförordning.

I paragrafen anges lagens innehåll.

Övervägandena finns i avsnitt 2.5, 3.3 och 10.2.

Av *första stycket* framgår att syftet med lagen är att komplettera förordning (EU) 2024/2847 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen). Lagen kompletterar EU:s cyberresiliensförordning och kan därför inte tillämpas fristående från den. Hänvisningarna till EU:s cyberresiliensförordning är i huvudsak dynamiska. Det innebär att hänvisningen avser EU:s cyberresiliensförordning i den vid varje tidpunkt gällande lydelsen. I artikel 15–18 görs dock hänvisning till EU:s cyberresiliensförordning i den ursprungliga lydelsen. Det framgår även att förordning (EU) 2024/2847 i lagen benämns EU:s cyberresiliensförordning.

Andra stycket innehåller en upplysning om att ord och uttryck i lagen har samma betydelse som i EU:s cyberresiliensförordning. I artikel 3 i EU:s cyberresiliensförordning finns definitioner.

Anmälande myndighet av organ för bedömning av överensstämmelse

2 § Den myndighet som regeringen bestämmer är anmälande myndighet enligt EU:s cyberresiliensförordning.

Paragrafen innehåller bestämmelser om anmälande myndighet av organ för bedömning av överensstämmelse.

Övervägandena finns i avsnitt 6.8.

I artikel 36.1 i EU:s cyberresiliensförordning anges att varje medlemsstat ska utse en anmälande myndighet med ansvar för att inrätta och genomföra de förfaranden som krävs vid bedömning, utseende och anmälan av organ för bedömning av överensstämmelse och vid kontroll, inklusive överensstämmelse med artikel 41.

I paragrafen anges att regeringen bestämmer anmälande myndighet enligt artikel 36.1 i EU:s cyberresiliensförordning.

3 § I Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och upphävande av förordning (EEG) nr 339/93 och i lagen (2011:791) om ackreditering och teknisk kontroll finns allmänna bestämmelser om ackreditering av organ för bedömning av överensstämmelse.

Bestämmelser om ackreditering och anmälan av organ för bedömning av överensstämmelse finns i lagen (2011:791) om ackreditering och teknisk kontroll och i föreskrifter som har meddelats i anslutning till den lagen.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om förfarandena vid bedömning, utseende och anmälan av organ för bedömning och för övervakning av dessa enligt artikel 39–43 samt anmälda organs informationsskyldighet enligt artikel 49 och delta i sektorsövergripande grupp enligt artikel 51 i EU:s cyberresiliensförordning.

Paragrafen innehåller upplysningsbestämmelser om ackreditering och anmälan av organ av bedömning av överensstämmelse. Paragrafen innehåller även bestämmelser om anmälda organ.

Övervägandena finns i avsnitt 6.7 och 6.8.

Första stycket innehåller en upplysning om att ackreditering sker enligt förordning (EG) nr 765/2008 och lagen (2011:791) om ackreditering och teknisk kontroll, som kompletterar den förordningen.

Andra stycket innehåller en upplysning om att det i lagen (2011:791) om ackreditering och teknisk kontroll och i föreskrifter som har meddelats i anslutning till den lagen finns bestämmelser

om ackreditering och anmälan av organ för bedömning av överensstämmelse enligt EU:s cyberresiliensförordning.

Enligt *tredje stycket* får regeringen eller den myndighet som regeringen bestämmer meddela de ytterligare föreskrifter om ackreditering och om anmälan av organ för bedömning av överensstämmelse enligt artikel 39–43 i EU:s cyberresiliensförordning. Bestämmelsen ger stöd för att meddela de kompletterande föreskrifter som kan behövas för ackreditering och anmälan av organ för bedömning av överensstämmelse enligt EU:s cyberresiliensförordning. Bestämmelsen ger även stöd för att meddela kompletterande föreskrifter för anmälda organs informationsskyldighet enligt artikel 49 och deltagande i sektorsövergripande grupp enligt artikel 51 i EU:s cyberresiliensförordning.

Marknadskontroll

4 § Bestämmelser om marknadskontroll finns i Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011.

Paragrafen innehåller en upplysningsbestämmelse om marknadskontroll.

Överväganden finns i avsnitt 9.8.1.

Av paragrafen framgår att bestämmelser om marknadskontroll finns i Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordning (EG) nr 765/2008 och (EU) nr 305/2011 (EU:s marknadskontrollförordning).

Marknadskontrollmyndighet

5 § Den myndighet eller de myndigheter som regeringen bestämmer är marknadskontrollmyndighet.

Av artikel 52.14 i EU:s cyberresiliensförordning framgår att för produkter med digitala element som omfattas av EU:s cyberresiliensförordning och som klassificeras som AI-system med hög risk enligt artikel 6 i Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) ska de marknadskontrollmyndigheter som utsetts enligt förordning (EU) 2024/1689 vara de myndigheter som ansvarar för den marknadskontroll som föreskrivs i EU:s cyberresiliensförordning.

Paragrafen innehåller bestämmelser om vilka myndigheter som är marknadskontrollmyndighet.

Överväganden finns i avsnitt 9.5.4 och 9.8.1.

Paragrafens *första stycke* anger att den myndighet eller de myndigheter som regeringen bestämmer är marknadskontrollmyndigheter.

Av *andra stycket* följer att enligt artikel 52.14 i EU:s cyberresiliensförordning är de myndigheter som utses enligt Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) marknadskontrollmyndigheter för cyberresilienskrav för produkter med digitala element som klassificeras som AI-system med hög risk.

Marknadskontrollmyndighetens befogenheter

6 § Vid marknadskontroll enligt förordning (EU) 2019/1020 har en marknadskontrollmyndighet befogenhet att enligt

1. artikel 14.4 a–14.4 c kräva att ekonomiska aktörer eller förvaltare av programvara med fri och öppen källkod ska tillhandahålla handlingar, specifikationer, data eller uppgifter,

2. artikel 14.4 d utföra oanmälda inspektioner på plats och fysiska kontroller av produkter,

3. artikel 14.4 e få tillträde till lokaler, mark eller transportmedel,

4. artikel 14.4 f inleda undersökningar på eget initiativ,
5. artikel 14.4 g kräva att ekonomiska aktörer eller förvaltare av programvara med fri och öppen källkod ska vidta lämpliga åtgärder för att få en bristande överensstämmelse att upphöra eller att eliminera en risk,
6. artikel 14.4 h själv vidta åtgärder,
7. artikel 14.4 j införskaffa, inspektera och demontera varuprover, och
8. artikel 14.4 k kräva att innehåll på ett onlinegränssnitt ska avlägsnas, att en varning ska visas eller att åtkomsten ska begränsas.

Befogenheten enligt första stycket 8 gäller inte i fråga om databaser som omfattas av tryckfrihetsförordningens eller yttrandefrihetsgrundlagens skydd.

När ändrade förhållanden ger anledning till det, ska en marknadskontrollmyndighet besluta att åtgärder enligt första stycket 8 inte längre behöver gälla.

Paragrafen innehåller bestämmelser om en marknadskontrollmyndighets befogenheter enligt EU:s marknadskontrollförordning.

Överväganden finns i avsnitt 9.8.2.

I *första stycket* anges att en marknadskontrollmyndighet i enlighet med artikel 14.4 a-14.4 h samt 14.4 j och 14.4 k i EU:s marknadskontrollförordning har befogenheter att kräva handlingar, specifikationer, data eller uppgifter, att utföra oanmälda inspektioner på plats och fysiska kontroller av produkter, att få tillträde till lokaler, mark eller transportmedel, att inleda undersökningar på eget initiativ, att kräva åtgärder för att få en bristande överensstämmelse att upphöra eller att eliminera en risk, att själv vidta åtgärder, att införskaffa, inspektera och demontera varuprover samt att kräva att innehåll på ett onlinegränssnitt begränsas.

Andra stycket innehåller en begränsning av befogenheten enligt artikel 14.4 k som följer av grundlag. Befogenheten gäller inte i fråga om databaser som omfattas av tryckfrihetsförordningens eller yttrandefrihetsgrundlagens skydd. De databaser som bestämmelsen tar sikte på regleras i den så kallade bilageregeln i 1 kap. 5 och 6 §§ tryckfrihetsförordningen och den så kallade databasregeln i 1 kap. 4 § yttrandefrihetsgrundlagen.

Av *tredje stycket* följer att när ändrade förhållanden ger anledning till det, ska marknadskontrollmyndigheten besluta att skyldigheten att vidta en åtgärd enligt artikel 14.4 k inte längre ska gälla. Ändrade förhållanden kan exempelvis vara att en produkt har korrigerats så att den inte längre utgör en cybersäkerhetsrisk.

Alla hänvisningar till en ekonomisk aktör enligt EU:s marknadskontrollförordning ska förstås som att de inkluderar förvaltare av

fri och öppen programvara enligt artikel 3.14 i EU:s cyberresiliensförordning.

7 § En marknadskontrollmyndighet får införskaffa ett varuprov under dold identitet enligt artikel 14.4 j i förordning (EU) 2019/1020 endast om det är nödvändigt för att syftet med kontrollen ska uppnås. Myndigheten ska underrätta den ekonomiska aktören eller förvaltaren av programvara med fri och öppen källkod om att införskaffandet har skett under dold identitet, så snart det går utan att syftet med åtgärden går förlorat.

Paragrafen innehåller bestämmelser om en marknadskontrollmyndighets befogenhet att införskaffa ett varuprov under dold identitet.

Överväganden finns i avsnitt 9.8.2.

En marknadskontrollmyndighet får endast införskaffa ett varuprov under dold identitet om det är nödvändigt för syftet med kontrollen ska uppnås. Att införskaffa ett varuprov under dold identitet kan till exempel vara nödvändigt om marknadskontrollmyndigheten annars inte har möjlighet att få tillgång till ett varuprov, eller annars inte får tillgång till ett varuprov som är representativt för de produkter som den ekonomiska aktören tillhandahåller. Vidare anges att efter införskaffandet ska myndigheten underrätta den ekonomiska aktören eller förvaltaren av fri och öppen programvara om det, så snart det går utan att syftet med åtgärden går förlorat. I vissa situationer kan det finnas skäl att skjuta upp underrättelsen en tid för att syftet med införskaffandet under dold identitet inte ska gå förlorat. Det kan till exempel finnas anledning att vänta med att underrätta den ekonomiska aktören eller förvaltaren av fri och öppen programvara till dess att leveransen av en produkt har skett och marknadskontrollmyndigheten har haft möjlighet att kontrollera produkten.

Befogenheten att införskaffa varuprover under dold identitet är tillämpliga både vid köp i fysisk butik och vid digitala köp. Om myndigheten agerar i eget namn är det inte fråga om att den agerar med dold identitet. I en fysisk butik kan ett införskaffande av varuprover under dold identitet till exempel gå till så att myndighetsföreträdaren inte klargör att införskaffandet sker för marknadskontrollmyndighetens räkning. Myndighetsföreträdaren uppträder som en vanlig kund och talar inte om att införskaffandet görs inom ramen för myndighetens kontrollverksamhet. Vid digitala köp kan en myndighetsföreträdare till exempel använda sig av påhittade namn och kontaktuppgifter för att införskaffa varuprover. En beställning kan

exempelvis ske med leverans till en boxadress eller ett centrallager. I senare fallet kan marknadskontrollmyndigheten sedan göra en separat beställning från centrallagret till myndighetens egen adress och på så sätt undvika att den ekonomiska aktören eller förvaltaren av programvara med fri och öppen källkod får kännedom om vart produkten slutligen levereras.

Förelägganden och vite

8 § En marknadskontrollmyndighet får besluta de förelägganden som behövs i ett enskilt fall för att EU:s cyberresiliensförordning, denna lag, anslutande föreskrifter och förordning (EU) 2019/1020 ska följas.

Ett beslut om föreläggande enligt första stycket eller 6 § får förenas med vite.

Paragrafen innehåller bestämmelser om förelägganden och vite.

Överväganden finns i avsnitten 9.8.3.

Första stycket innehåller bestämmelser om att en marknadskontrollmyndighet får besluta de förelägganden som behövs för att EU:s cyberresiliensförordning, denna lag, anslutande föreskrifter och EU:s marknadskontrollförordning ska följas.

Andra stycket reglerar marknadskontrollmyndighetens möjlighet att förena beslut om förelägganden med vite.

För viten tillämpas lagen (1985:206) om viten.

Omedelbar verkställighet

9 § En marknadskontrollmyndighet får när den fattar beslut enligt 6 eller 8 §§ bestämma att beslutet ska gälla omedelbart.

Paragrafen innehåller bestämmelser om omedelbar verkställighet av vissa beslut.

Överväganden finns i avsnitt 9.8.3.

Bestämmelsen innebär att marknadskontrollmyndigheten får bestämma att dess beslut enligt 6 § eller 8 § ska gälla omedelbart.

Hjälp av Polismyndigheten

10 § Polismyndigheten ska på begäran av marknadskontrollmyndigheten lämna den hjälp som behövs när myndigheten vidtar åtgärder enligt 6 §.

Hjälp enligt första stycket får begäras endast om

1. det på grund av särskilda omständigheter kan befaras att åtgärden inte kan utföras utan att en polismans särskilda befogenheter enligt 10 § polislagen (1984:387) behöver tillgripas, eller

2. det annars finns synnerliga skäl.

Paragrafen innehåller bestämmelser om en marknadskontrollmyndighets möjlighet att begära hjälp av Polismyndigheten för att vidta åtgärder för marknadskontroll enligt artikel 14.4 a–14.4. h samt 14.4 j och 14.4 k i EU:s marknadskontrollförordning.

Överväganden finns i avsnitt 9.8.4.

En förutsättning för en begäran är att det på grund av särskilda omständigheter kan befaras att en åtgärd inte kan utföras utan att en polismans särskilda befogenheter enligt 10 § polislagen (1984:387) behöver användas, eller om det annars finns synnerliga skäl.

Det är marknadskontrollmyndigheten som har att pröva om det finns förutsättningar att begära hjälp av Polismyndigheten. Synnerliga skäl kan till exempel finnas om det finns en överhängande risk för att produkter eller handlingar kommer att förstöras och man inte kan avvakta med att verkställigheten löses på annat sätt.

Föreskrifter om regulatoriska sandlådor

11 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om regulatoriska sandlådor för cyberresiliens.

Paragrafen innehåller en bestämmelse om föreskriftsrätt om regulatoriska sandlådor.

Övervägandena finns i avsnitt 12.5.2.

Genom bestämmelsen bemyndigas regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om regulatoriska sandlådor.

Tystnadsplikt

12 § Den som deltar i verksamhet som utförs av ett privat organ för bedömning av överensstämmelse enligt EU:s cyberresiliensförordning får inte obehörigen röja eller utnyttja det som han eller hon fått kännedom om under det att uppgifterna utfördes.

Den som har tagit befattning med ett ärende som gäller marknadskontroll eller deltar i en regulatorisk sandlåda för cyberresiliens enligt EU:s cyberresiliensförordning får inte obehörigen röja eller utnyttja vad han eller hon har fått veta om någons affärs- eller driftförhållanden.

I det allmännas verksamhet tillämpas bestämmelserna i offentlighets- och sekretesslagen (2009:400).

Paragrafen innehåller bestämmelser om tystnadsplikt.

Överväganden finns i avsnitt 11.13.

Enligt *första stycket* innebär tystnadsplikten att den som deltar i verksamhet som utförs av ett privat organ för bedömning av överensstämmelse i enlighet med EU:s cyberresiliensförordning inte obehörigen får röja eller utnyttja det som han eller hon fått kännedom om under det att uppgifterna utfördes. Organ för bedömning av överensstämmelse kan vara privaträttsliga aktörer, till exempel ett aktiebolag. Tystnadsplikten innebär att personer som deltar i organet för bedömning av överensstämmelses verksamhet inte får avslöja eller utnyttja det han eller hon fått kännedom om under det att uppgifterna utfördes.

Enligt *andra stycket* innebär tystnadsplikten att de som omfattas inte obehörigen får avslöja eller utnyttja vad de har fått veta om någons affärs- eller driftförhållanden i samband med att de utfört marknadskontrolluppgifter eller deltar i en regulatorisk sandlåda för cyberresiliens. Det kan förekomma att uppgifter i ett ärende om marknadskontroll eller i en verksamhet som består i en regulatorisk sandlåda för cyberresiliens hanteras av personer utanför det allmännas verksamhet som inte omfattas av regleringen i offentlighets- och sekretesslagen. En marknadskontrollmyndighet kan exempelvis behöva anlita tekniska experter som är verksamma vid externa laboratorier som drivs i privat regi.

Tystnadsplikten gäller såväl under som efter någons deltagande i verksamhet som omfattas av bestämmelsens tillämpningsområde. Den som bryter mot tystnadsplikten kan dömas för brott mot tystnadsplikten enligt 20 kap. 3 § brottsbalken.

I *tredje stycket* finns det en upplysning om att bestämmelserna i offentlighets- och sekretesslagen (2009:400) tillämpas i stället för första och andra styckets regler om tystnadsplikt när det gäller den verksamhet som marknadskontrollmyndigheten bedriver eller ett offentligt organ för bedömning av överensstämmelse utför i det allmännas verksamhet.

Avgifter

13 § Av lagen (2014:140) med bemyndigande att meddela vissa föreskrifter om marknadskontroll av varor och annan närliggande tillsyn framgår att föreskrifter för avgifter för kontroll enligt förordning (EU) 2019/1020 får meddelas.

Paragrafen innehåller en upplysningsbestämmelse om avgifter.

Överväganden finns i avsnitt 9.8.5.

Av paragrafen framgår var det finns ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om avgifter enligt 15 § i EU:s marknadskontrollförordning.

Ändring av beslut av privata organ för bedömning av överensstämmelse

14 § Ett privat organ för bedömning av överensstämmelse ska ändra ett beslut som det har meddelat, om

1. organet anser att beslutet är uppenbart felaktigt i något väsentligt hänseende på grund av att det har tillkommit nya omständigheter eller av någon annan anledning, och

2. beslutet kan ändras snabbt och enkelt och utan att det blir till nackdel för någon enskild.

Paragrafen innehåller bestämmelser om ändring av beslut av privata organ för bedömning av överensstämmelse.

Övervägandena finns i avsnitt 6.13.3.

Paragrafen har sin redaktionella förebild i 38 § förvaltningslagen.

Av paragrafen framgår att privata organ för bedömning av överensstämmelse har en skyldighet att ändra ett beslut när beslutet är uppenbart felaktigt på grund av nya omständigheter eller av någon

annan anledning och beslutet kan ändras snabbt och enkelt utan att det blir till nackdel för någon enskild.

Sanktionsavgift

15 § En marknadskontrollmyndighet ska besluta att ta ut sanktionsavgift vid överträdelse av artikel 13 och 14 samt väsentliga cybersäkerhetskrav i bilaga I i EU:s cyberresiliensförordning och anslutande föreskrifter.

Avgiftens storlek ska bestämmas med tillämpning av artikel 64.5 i EU:s cyberresiliensförordning.

Sanktionsavgiften ska bestämmas till högst 15 000 000 euro eller, om överträdelsen begås av ett företag, till 2,5 procent av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

Sanktionsavgiften för en myndighet ska bestämmas till högst 10 000 000 kronor.

Paragrafen innehåller bestämmelser om administrativa sanktionsavgifter för överträdelser av bestämmelser som anges i artikel 64.2 i EU:s cyberresiliensförordning.

Övervägandena finns i avsnitt 10.3.1–10.3.3.

I *första stycket* anges att marknadskontrollmyndigheten ska besluta att ta ut sanktionsavgift vid överträdelser som avses i artikel 64.2 i EU:s cyberresiliensförordning och anslutande föreskrifter i den ursprungliga lydelsen. I artikeln anges att sanktionsavgift ska ta ut för bristande efterlevnad av de skyldigheter som anges i artikel 13 och 14 samt de väsentliga cybersäkerhetskrav som anges i bilaga I i EU:s cyberresiliensförordning. I artikel 13 anges tillverkares skyldigheter. I artikel 14 anges tillverkarnas rapporteringsskyldigheter. I bilaga I del I anges väsentliga cybersäkerhetskrav avseende egenskaper hos produkter med digitala element och i del II anges krav på sårbarhetshantering. Strikt ansvar för överträdelser gäller. Det innebär att det inte krävs att det föreligger någon form av uppsåt eller vårdslöshet hos den som gjort sig skyldig till överträdelsen.

I *andra stycket* anges att avgiftens storlek ska bestämmas med tillämpning av artikel 64.5 i EU:s cyberresiliensförordning. I den artikeln anges att vid beslut om storleken på den administrativa sanktionsavgiften i varje enskilt fall ska alla relevanta omständigheter i den specifika situationen beaktas och vederbörlig hänsyn ska tas till överträdelsens art, allvarlighetsgrad och varaktighet samt dess

konsekvenser. Vidare ska beaktas huruvida administrativa sanktionsavgifter redan har påförts av samma eller andra marknadskontrollmyndigheter på samma ekonomiska aktör för en liknande överträdelse, och storleken på företaget, särskilt när det gäller mikroföretag, små och medelstora företag, inbegripet uppstartsföretag, och marknadsandelen för den ekonomiska aktör som begått överträdelsen.

I *tredje stycket* anges att sanktionsavgiften ska bestämmas till högst 15 000 000 euro eller, om överträdelsen begås av företag, till 2,5 procent av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

I *fjärde stycket* anges att sanktionsavgiften för en myndighet ska bestämmas till högst 10 000 000 kronor.

16 § En marknadskontrollmyndighet ska besluta att ta ut en sanktionsavgift vid överträdelse av artikel 18–23, 28, 30.1–30.4, 31.1–31.4, 32.1–32.3, 33.5 och 53 i EU:s cyberresiliensförordning och anslutande föreskrifter.

Avgiftens storlek ska bestämmas med tillämpning av artikel 64.5 i EU:s cyberresiliensförordning.

Sanktionsavgiften ska bestämmas till högst 10 000 000 euro eller, om överträdelsen begås av ett företag, upp till 2 procent av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

Sanktionsavgiften för en myndighet ska bestämmas till högst 5 000 000 kronor.

Paragrafen innehåller bestämmelser om administrativa sanktionsavgifter för överträdelser av bestämmelser som anges i artikel 64.3 i EU:s cyberresiliensförordning.

Övervägandena finns i avsnitt 10.3.1–10.3.3.

I *första stycket* anges att marknadskontrollmyndigheten ska besluta att ta ut sanktionsavgift vid överträdelser som avses i artikel 64.3 i EU:s cyberresiliensförordning och anslutande föreskrifter i den ursprungliga lydelsen. I artikeln anges att sanktionsavgift ska ta ut för bristande efterlevnad av de skyldigheter som anges i artikel 18–23, artikel 28, artikel 30.1–30.4, artikel 31.1–31.4, artikel 32.1–32.3, artikel 33.5 och artikel 53.

I artikel 18 finns bestämmelser om tillverkarens representanter. I artikel 19 finns bestämmelser om importörens skyldigheter. I artikel 20 finns bestämmelser om distributörens skyldigheter. I artikel 21 finns bestämmelser som gäller för både importörer och distributörer. I artikel 22 finns andra fall där tillverkarnas skyldigheter gäl-

ler. I artikel 23 finns bestämmelser om identifiering av ekonomiska aktörer. I artikel 28 finns bestämmelser om EU-försäkran om överensstämmelse. I artikel 30.1–30.4 finns bestämmelser för anbringande av CE-märkning. I artikel 31.1–31.4 finns bestämmelser om teknisk dokumentation. I artikel 32.1–32.3 finns bestämmelser om förfaranden för bedömning av överensstämmelse för produkter med digitala element. I artikel 33.5 finns bestämmelser om mikroföretags och små företags skyldigheter att tillhandahålla dokumentation. I artikel 53 finns bestämmelser om tillgång till data och dokumentation.

Strikt ansvar för överträdelser gäller. Det innebär att det inte krävs att det föreligger någon form av uppsåt eller vårdslöshet hos den som gjort sig skyldig till överträdelsen.

I *andra stycket* anges att avgiftens storlek ska bestämmas med tillämpning av artikel 64.5 i EU:s cyberresiliensförordning, se författningskommentaren till 15 §.

I *tredje stycket* anges att sanktionsavgiften ska bestämmas till högst 10 000 000 euro eller, om överträdelsen begås av företag, till 2 procent av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

I *fjärde stycket* anges att sanktionsavgiften för en myndighet ska bestämmas till högst 5 000 000 kronor.

17 § en anmälade myndigheten ska besluta att ta ut en sanktionsavgift vid överträdelse av artikel 39, 41, 47 och 49 i EU:s cyberresiliensförordning och anslutande föreskrifter.

Avgiftens storlek ska bestämmas med tillämpning av artikel 64.5 i EU:s cyberresiliensförordning.

Sanktionsavgiften ska bestämmas till högst 10 000 000 euro eller, om överträdelsen begås av ett företag, upp till 2 procent av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

Sanktionsavgiften för en myndighet ska bestämmas till högst 5 000 000 kronor.

Paragrafen innehåller bestämmelser om administrativa sanktionsavgifter för överträdelser av bestämmelser som anges i artikel 64.3 i EU:s cyberresiliensförordning och anslutande föreskrifter i den ursprungliga lydelsen.

Övervägandena finns i avsnitt 10.3.1–10.3.3.

I *första stycket* anges att den anmälade myndigheten ska besluta att ta ut sanktionsavgift vid överträdelser som avses i artikel 64.3 i EU:s cyberresiliensförordning och anslutande föreskrifter i den ursprungliga lydelsen. I artikeln anges att sanktionsavgift ska ta ut för bristande efterlevnad av de skyldigheter som anges i artikel 39, artikel 41, artikel 47 och artikel 49.

I artikel 39 finns bestämmelser om krav på anmälda organ. I artikel 41 finns bestämmelser om dotterbolag och underentreprenörer till anmälda organ. I artikel 47 finns bestämmelser om anmälda organs operativa skyldigheter. I artikel 49 finns bestämmelser om anmälda organs informationsskyldighet.

Strikt ansvar för överträdelser gäller. Det innebär att det inte krävs att det föreligger någon form av uppsåt eller vårdslöshet hos den som gjort sig skyldig till överträdelsen.

I *andra stycket* anges att avgiftens storlek ska bestämmas med tillämpning av artikel 64.5 i EU:s cyberresiliensförordning, se författningskommentaren till 15 §.

I *tredje stycket* anges att sanktionsavgiften ska bestämmas till högst 10 000 000 euro eller, om överträdelsen begås av företag, till 2 procent av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

I *fjärde stycket* anges att sanktionsavgiften för en myndighet ska bestämmas till högst 5 000 000 kronor.

18 § En marknadskontrollmyndighet ska besluta att ta ut en sanktionsavgift vid överträdelse av artikel 64.4 i EU:s cyberresiliensförordning och anslutande föreskrifter.

Avgiftens storlek ska bestämmas med tillämpning av artikel 64. 5 i EU:s cyberresiliensförordning.

Sanktionsavgiften ska bestämmas till högst 5 000 000 euro eller, om överträdelsen begås av ett företag, upp till 1 procent av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

Sanktionsavgiften för en myndighet ska bestämmas till högst 2 500 000 kronor.

Paragrafen innehåller bestämmelser om administrativa sanktionsavgifter för överträdelser av bestämmelser som anges i artikel 64.4 i EU:s cyberresiliensförordning och anslutande föreskrifter i den ursprungliga lydelsen.

Övervägandena finns i avsnitt 10.3.1–10.3.3.

I *första stycket* anges att marknadskontrollmyndigheten ska besluta att ta ut sanktionsavgift vid överträdelser som avses i artikel 64.4 i EU:s cyberresiliensförordning och anslutande föreskrifter i den ursprungliga lydelsen. I artikeln anges att sanktionsavgift ska ta ut för tillhandahållande av oriktig, ofullständig eller vilseledande information till anmälda organ och till marknadskontrollmyndigheter som svar på en begäran. Strikt ansvar för överträdelser gäller. Det innebär att det inte krävs att det föreligger någon form av uppsåt eller vårdslöshet hos den som gjort sig skyldig till överträdelsen.

I *andra stycket* anges att avgiftens storlek ska bestämmas med tillämpning av artikel 64.5 i EU:s cyberresiliensförordning, se författningskommentaren till 15 §.

I *tredje stycket* anges att sanktionsavgiften ska bestämmas till högst 5 000 000 euro eller, om överträdelsen begås av företag, till 1 procent av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.

I *fjärde stycket* anges att sanktionsavgiften för en myndighet ska bestämmas till högst 2 500 000 kronor.

19 § Den anmälade myndigheten och en marknadskontrollmyndighet får avstå från att ta ut en sanktionsavgift när överträdelsen bedöms som ringa eller ursäktlig, eller om det annars med hänsyn till omständigheterna vore oskäligt att besluta om en sanktion.

Paragrafen innehåller bestämmelser om när den anmälade myndigheten och marknadskontrollmyndigheten får besluta att avstå från att ta ut en sanktionsavgift.

Övervägandena finns i avsnitt 10.3.1.

En sanktionsavgift behöver inte tas ut när överträdelsen bedöms som ringa eller ursäktlig, eller om det annars med hänsyn till omständigheterna vore oskäligt att besluta om en sanktion. Vad som är ringa fall måste bedömas utifrån situationen i det enskilda fallet. Typiskt sett kan det vara fråga om ett åsidosättande som har haft mindre allvarliga konsekvenser, till exempel att produkten har tillhandahållits på marknaden endast i begränsad omfattning. Det kan

också handla om mindre allvarliga överträdelse av de formella krav som följer av EU:s cyberresiliensförordning, till exempel att tillverkaren eller importören har underlåtit att på produkten ange någon av de uppgifter som föreskrivs. Det kan även vara fråga om fall där en sanktionsavgift har påförts med stöd av en annan författning för samma överträdelse.

20 § Sanktionsavgiften ska betalas till den anmälade myndigheten eller marknadskontrollmyndigheten inom 30 dagar från det att beslutet om att ta ut sanktionsavgift fick laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas i tid, ska den anmälade myndigheten och marknadskontrollmyndigheten lämna den obetalda avgiften för indrivning.

Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

En sanktionsavgift tillfaller staten.

Paragrafen innehåller bestämmelser om betalning av sanktionsavgift.

Övervägandena finns i 10.4.

I *första stycket* anges att en sanktionsavgift ska betalas till den anmälade myndigheten och marknadskontrollmyndigheten inom 30 dagar från det att beslutet om att ta ut sanktionsavgift fick laga kraft eller inom den längre tid som anges i beslutet.

I *andra stycket* anges att om sanktionsavgiften inte betalas i tid, ska den anmälade myndigheten och marknadskontrollmyndigheten lämna den obetalda avgiften för indrivning.

Av *tredje stycket* framgår att bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

I *fjärde stycket* anges att sanktionsavgiften tillfaller staten.

21 § Innan den anmälade myndigheten och marknadskontrollmyndigheten beslutar om sanktionsavgift ska den som avgiften ska tas ut av få tillfälle att yttra sig. Om så inte har skett inom två år från det att överträdelsen ägde rum får någon sanktionsavgift inte beslutas.

Ett beslut om sanktionsavgift ska delges.

Paragrafen innehåller bestämmelser om när en sanktionsavgift får beslutas och krav på delgivning.

Övervägandena finns i avsnitt 10.4.

Första stycket innebär att om kommunikation enligt förvaltningslagen med den som avgiften ska tas ut av inte har gjorts inom två år från den dag då överträdelsen ägde rum, får en sanktionsavgift inte tas ut. Bevisbördan för att kommunikation har genomförts ligger på den anmälade myndigheten och marknadskontrollmyndigheten.

Av *andra stycket* framgår att ett beslut om sanktionsavgift ska delges. Det innebär att myndigheten ska använda sig av de metoder för delgivning som regleras i delgivningslagen (2010:1932).

22 § En beslutad sanktionsavgift ska falla bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Paragrafen innehåller bestämmelser om preskription av sanktionsavgifter.

Övervägandena finns i avsnitt 10.4.

Bestämmelsen innebär att betalning av beslutad avgift inte kan krävas efter det att fem år gått sedan beslutet fick laga kraft. En beslutad sanktionsavgift ska falla bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

23 § En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande vid vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

Paragrafen innehåller bestämmelser om förbud mot sanktionsavgifter i vissa fall.

Övervägandena finns i avsnitt 10.3.4.

Enligt paragrafen får en sanktionsavgift inte beslutas om överträdelsen omfattas av ett föreläggande vid vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet. Paragrafen syftar till att förhindra att samma överträdelse blir föremål för dubbla prövningar och sanktioner. Om ett beslut om vitesföreläggande har meddelats och en domstolsprocess inletts om utdömande av vitet är marknadskontrollmyndigheten enligt bestämmelsen förhindrad att besluta om sanktionsavgift för samma överträdelse. Bestämmelsen hindrar inte att en överträdelse först kan bli föremål för ett vitesföreläggande och i ett senare skede beslut om sanktionsavgift, under förutsättning att någon ansökan om utdömande av vitet inte

har gjorts. En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande vid vite om överträdelsen ligger till grund för en ansökan om utdömande av vitet.

Överklagande

24 § Ett beslut av en förvaltningsmyndighet eller ett anmält organ enligt EU:s cyberresiliensförordning, denna lag och anslutande föreskrifter får överklagas till allmän förvaltningsdomstol.

En myndighet får överklaga en förvaltningsmyndighets eller ett anmält organs beslut.

Förvaltningsmyndigheten eller det anmälda organet ska vid överklagande vara motpart i domstolen.

Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Paragrafen innehåller bestämmelser om överklagande av beslut.

Övervägandena finns i avsnitt 6.14 och 9.8.6.

I *första stycket* anges att beslut av en förvaltningsmyndighet eller ett anmält organ för bedömning av överensstämmelse enligt EU:s cyberresiliensförordning, denna lag och anslutande föreskrifter får överklagas till allmän förvaltningsdomstol. Med förvaltningsmyndighet avses den anmälande myndigheten och en marknadskontrollmyndighet. I fråga om förfarandet vid överklagande av beslut av privata organ för bedömning av överensstämmelse finns bestämmelser i lagen (1986:1142) om överklagande av beslut av enskilda organ med offentliga förvaltningsuppgifter.

I *andra stycket* anges att en myndighet får överklaga en förvaltningsmyndighets eller ett anmält organs beslut eftersom en myndighet skulle kunna vara en ekonomisk aktör och till exempel kan påföras en sanktionsavgift enligt 15–18 §§ i denna lag.

Av *tredje stycket* framgår att den förvaltningsmyndighet eller det anmälda organet som fattat beslutet ska vid överklagande vara motpart i domstolen.

Enligt *fjärde stycket* krävs det prövningstillstånd vid överklagande till kammarrätten.

I lagen finns ikraftträdandebestämmelser.

Överväganden finns i avsnitt 14.4.

Bestämmelserna i 2 och 3 §§ om anmälande myndighet och om att anmälande myndighet får meddela vissa föreskrifter, bestämmelserna i 12 § första stycket om tystnadsplikt för den som deltar i

verksamhet som utförs av ett privat organ för bedömning av överensstämmelse samt bestämmelserna om överklagande i 24 § träder i kraft den 11 juni 2026. Övriga bestämmelser träder i kraft den 11 december 2027.

16.2 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

18 kap.

Sårbarhets- och incidentrapporter enligt förordning (EU) 2024/2847

8 d § Sekretess gäller för uppgift i en sårbarhets- eller incidentrapport enligt artikel 14 eller 15 i Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen) samt för uppgift om vilka åtgärder som har vidtagits till följd av cyberhotet, tillbudet, sårbarheten eller incidenten om det inte står klart att uppgiften kan röjas utan skada för tillverkaren av produkten med digitala element eller för förvaltaren av programvara med fri och öppen källkod i den mån denne deltar i utvecklingen av produkter med digitala element, för den som ingett rapporten, för användaren eller för den verksamhet där den aktuella produkten används eller för de åtgärder som tillverkaren eller förvaltaren av programvara med fri och öppen källkod vidtagit motverkas.

För uppgift i en allmän handling gäller sekretessen i högst fyrtio år.

Paragrafen, som är ny, innehåller bestämmelser om sekretess för uppgifter i sårbarhets- och incidentrapporter enligt artikel 14 och 15 i EU: cyberresiliensförordning samt för uppgifter om åtgärder som vidtagits till följd av cyberhotet, tillbudet, sårbarheten eller incidenten.

Överväganden finns i avsnitt 11.6.

Enligt *första stycket* skyddas uppgifter i rapporterna samt uppgifter om vilka åtgärder som har vidtagits till följd av cyberhotet, tillbudet, sårbarheten eller incidenten. Paragrafen har ett omvänt skaderekvisit vilket innebär att en uppgift inte ska lämnas ut om det inte står klart att uppgiften kan röjas utan att tillverkaren av produkten med digitala element, förvaltaren av programvara med fri och öppen källkod i den mån denne deltar i utvecklingen av produkter med digitala element, den som ingett rapporten eller för an-

vändaren eller för den verksamhet där den aktuella produkten används skadas eller syftet med den vidtagna åtgärden motverkas. Genom bestämmelsen kan sekretess till exempel gälla för uppgifter om en rapports förekomst, uppgifter som beskriver en sårbarhet eller incident, uppgift om vidtagna korrigerande eller riskreducerande åtgärder eller uppgift om att sådana åtgärder inte vidtagits alls samt uppgift om vem som har rapporterat. Sekretess gäller oaktat inom vilken offentlig verksamhet rapporten finns i.

Enligt *andra stycket* gäller sekretessen i högst fyrtio år.

Sekretessbrytande bestämmelse

8 e § Sekretess enligt 18 kap. 8 d § hindrar inte CSIRT-enheten att underätta användarna av produkter med digitala element enligt vad som anges i artikel 14.8 i förordning (EU) 2024/2847 eller att informera allmänheten enligt vad som anges i artikel 17.2 i förordning (EU) 2024/2847.

Paragrafen, som är ny, innehåller bestämmelser som bryter sekretessen i 8 d §.

Överväganden finns i avsnitt 11.6.

Bestämmelsen ger CSIRT-enheten möjlighet att lämna sekretesskyddade uppgifter till användare av produkten med digitala element enligt vad som anges i artikel 14.8 i EU:s cyberresiliensförordning eller till allmänheten enligt vad som anges i artikel 17.2 i EU:s cyberresiliensförordning.

19 § Den tystnadsplikt som följer av 5–7, 8, 8 d, 9 och 10 §§, 11 § första stycket, 12, 12 a och 13 §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befodringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol, undersökningsledare eller åklagare eller inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Den tystnadsplikt som följer av 17 § inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befodringsföretag, hemlig avlyssning av elektronisk kom-

munikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol eller åklagare.

Att den tystnadsplikt som följer av 1–3 §§ i vissa fall inskränker rätten att meddela och offentliggöra uppgifter utöver det som anges i andra stycket följer av 7 kap. 10 §, 12–18 §§, 20 § 3 och 22 § första stycket 1 och andra stycket tryckfrihetsförordningen samt 5 kap. 1 § och 4 § första stycket 1 och andra stycket yttrandefrihetsgrundlagen.

Paragrafen innehåller bestämmelser om rätten att meddela och offentliggöra uppgifter.

Överväganden finns i avsnitt 11.6.

Första stycket ändras så att den nya 8 d § omfattas av uppräkningsen som görs där. Rätten att meddela och offentliggöra uppgifter får därmed inte företräde framför den tystnadsplikt som följer av 8 d §.

31 kap.

Regulatorisk sandlåda för cyberresiliens

25 b § *Sekretess gäller i verksamhet avseende regulatorisk sandlåda för cyberresiliens enligt artikel 33 i förordning (EU) 2024/2847 för uppgift om en enskilds affärs- eller driftförhållanden, uppfinningar eller forskningsresultat om det kan antas att den enskilde lider avsevärd skada om uppgiften röjs.*

För uppgift i en allmän handling gäller sekretessen i högst tjugo år.

Paragrafen, som är ny, innehåller bestämmelser om sekretess i verksamhet avseende regulatorisk sandlåda för cyberresiliens enligt artikel 33 i EU:s cyberresiliensförordning.

Överväganden finns i avsnitt 11.9.

Enligt *första stycket* skyddas uppgifter om en enskilds affärs- eller driftförhållanden, uppfinningar eller forskningsresultat. Paragrafen har ett kvalificerat rakt skaderekvisit vilket innebär att en uppgift ska lämnas ut om det inte står klart att det innebär avsevärd skada för den enskilde om uppgiften röjs.

Enligt *andra stycket* gäller sekretessen i högst tjugo år.

I lagen finns ikraftträdandebestämmelser.

Överväganden finns i avsnitt 14.4.

Bestämmelsen om sekretess till skydd för enskild inom ramen för regulatoriska sandlådor för cyberresiliens träder i kraft den 11 december 2027. Övriga föreslagna bestämmelser träder i kraft den 11 september 2026.

Referenser

Offentliga tryck

Propositioner

Prop. 1979/80:2, Del A, *Förslag till sekretesslag m.m.*

Prop. 2003/04:93, *Några frågor om sekretess, m.m.*

Prop. 2004/05:5, *Vårt framtida försvar.*

Prop. 2010/11:80, *Ny lag om ackreditering och teknisk kontroll.*

Prop. 2012/13:192, *Sekretess i det internationella samarbetet.*

Prop. 2016/17:180, *En modern och rättssäker förvaltning – ny förvaltningslag.*

Prop. 2017/18:89, *Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetskylldslag.*

Prop. 2017/18:105, *Ny dataskyddslag.*

Prop. 2017/18:235, *Följändringar till ny förvaltningslag.*

Prop. 2020/21:186, *Kompletterande bestämmelser till EU:s Cybersäkerhetsakt.*

Prop. 2021/22:238, *Anpassningar till EU:s marknadskontrollförordning – del 2.*

Prop. 2022/23:116 *Ett granskningssystem för utländska direktinvesteringar till skydd för svenska säkerhetsintressen.*

Prop. 2025/26:28, *Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag.*

Lagrådsremiss *Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag*, 2025.

Skrivelser

Skr. 2024/25:121, *Nationell strategi för cybersäkerhet 2025–2029*.

Statens offentliga utredningar

SOU 2010:29 *En ny förvaltningslag*.

SOU 2017:6 *Marknadskontrollmyndigheter – befogenheter och sanktionsmöjligheter*.

SOU 2017:36 *Informationssäkerhet för samhällsviktiga och digitala tjänster*.

SOU 2020:58 *EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering*.

SOU 2021:63 *Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem*.

SOU 2022:24 *Materielförsörjningsstrategi*.

SOU 2024:18 *Nya regler om cybersäkerhet*.

SOU 2024:64 *Motståndskraft i samhällsviktiga tjänster*.

SOU 2025:79 *Samlade förmågor för ökad cybersäkerhet*.

SOU 2025:101 *Anpassningar till AI-förordningen*.

Beslut

Regeringskansliets (Finansdepartementet) beslut den 18 oktober 2024. Direktiv: Kompletterande bestämmelser till EU-förordningen om allmän produktsäkerhet och reglering av säkerhetskrav för produkter som inte omfattas av förordningen.

Regeringsbeslut av den 19 december 2024 (UD2024/17860), Riktlinjer för budgetåret 2025 avseende Svenska institutet för standarder (SIS), Sveriges konsument- och arbetstagarråd (SKA-rådet), Svensk Elstandard (SEK), Svenska informations- och telekommunikationsstandardiseringen (ITS).

Europaparlamentets och rådets beslut nr 768/2008/EG av den 9 juli 2008 om en gemensam ram för saluföring av produkter och upphävande av rådets beslut 93/465/EEG.

Beslut av Europaparlamentets presidium av den 15 april 2013 om bestämmelserna för Europaparlamentets hantering av sekretessbelagd information (EUT C 96, 1.4.2014, s. 1).

Kommissionens beslut (EU, Euratom) 2015/444 av den 13 mars 2015 om säkerhetsbestämmelser för skydd av säkerhetsskydds-klassificerade EU-uppgifter (EUT L 72, 17.3.2015, s. 53).

Rapporter

Statskontoret (2018:7) *Tillsyn enligt NIS-direktivet – kostnader och finansiering*.

Statskontoret (2025:8) *Tillsynsmyndigheternas kostnader till följd av NIS2-direktivet*.

Myndigheten för samhällsskydd och beredskap, *Verktyg för ökad motståndskraft och stärkt civilt försvar, Årsrapport it-incident-rapportering 2024*.

Övrigt

Regeringens strategi för standardisering,
<https://www.regeringen.se/informationsmaterial/2018/07/regeringens-strategi-for-standardisering/>.

Europeiska kommissionen (gemensamt meddelande) *The UE's Cybersecurity Strategy for the Digital Decade*, JOIN(2020) 18 final, 2020.

Europeiska kommissionen, *Impact Assessment Report, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU)*.

Europeiska kommissionen *Den digitala helheten – digital omnibus*, uppmaning att inkomma med synpunkter, 2025.

Europeiska kommissionen, *Commission Staff Working Document Executive Summary of the Evaluation of the New Legislative Framework* {SWD (2022) 364 final}.

Enisa rapport: *Good practices for supply chain cybersecurity*, June, 2023.

Europeiska kommissionen, *Meddelande från kommissionen, 2022 års blåbok om genomförandet av EU:s produktbestämmelser*, 2022.

Europeiska kommissionen, Meddelande från kommissionen till Europaparlamentet, rådet, europeiska ekonomiska och sociala kommittén samt regionkommittén: *Den inre marknaden: vår europeiska hemmamarknad i en osäker värld En strategi för att göra den inre marknaden enkel, sömlös och stark*, COM (2025) 500 final.

Europeiska kommissionen, Kommissionens arbetsprogram 2025: *Gemensamma framsteg: En djärvare, enklare och snabbare union*, bilagorna 1–5, COM (2025).

Europeiska kommissionen, Meddelande om genomförande och förenkling, *Ett enklare och snabbare EU*, 2025.

Europeiska kommissionen *Översyn av EU:s cybersäkerhetsakt*, offentligt samråd, 2025.

Europeiska kommissionen *Strategin för den europeiska dataunionen*, offentligt samråd, 2025.

Enisa guidelines document supporting Commission Implementing Regulation (EU) 2024/482. EUCC Scheme – *Guidelines on Vulnerability Management and Disclosure*, version 1.1, 2025.

Danelius, m.fl. *Mänskliga rättigheter i europeisk praxis* (2023, version 6, JUNO).

Holmberg m.fl. *Grundlagarna* (7 mars 2019, version 3A, JUNO).

von Essen, *Förvaltningsprocesslagen* (5 mars 2025, JUNO).

Kommittédirektiv 2024:119

Kompletterande bestämmelser till EU:s cyberresiliensförordning

Beslut vid regeringssammanträde den 28 november 2024.

Sammanfattning

En särskild utredare ska analysera behovet av och föreslå åtgärder och kompletterande författningsbestämmelser som behövs i syfte att anpassa svensk rätt till EU:s cyberresiliensförordning.

Utredaren ska bl.a.

- analysera om befintliga bestämmelser i nationell rätt behöver upphävas eller ändras eller om nya bestämmelser behövs med anledning av förordningen,
- föreslå vilken befintlig myndighet eller vilka befintliga myndigheter som ska utses till nationell marknadskontrollmyndighet,
- föreslå vilken befintlig myndighet som ska utses till anmälände myndighet med ansvar för att bl.a. inrätta och genomföra de förfaranden som krävs för bedömning, utseende och anmälan av organ för bedömning av överensstämmelse, och
- lämna de förslag, inklusive författningsförslag, i övrigt som är nödvändiga eller annars bedöms lämpliga för att komplettera förordningen.

Uppdraget ska redovisas senast den 15 december 2025.

EU-förordningen

Europaparlamentet och rådet har antagit förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen), i fortsättningen benämnd EU:s cyberresiliensförordning. Förordningen träder i kraft den 10 december 2024 och ska tillämpas fr.o.m. 11 december 2027. Artikel 14 ska dock tillämpas fr.o.m. den 11 september 2026 och kapitel IV (artiklarna 35–51) ska tillämpas fr.o.m. den 11 juni 2026.

Syftet med förordningen är att skapa förutsättningar för utveckling av säkra produkter med digitala element genom att säkerställa att hård- och mjukvara släpps ut på marknaden med färre sårbarheter och att tillverkare ska ta större ansvar för produkters cybersäkerhet genom deras livscykel. Förordningen syftar vidare till att konsumenter ska få tillräcklig information om cybersäkerheten för de produkter med digitala element som de köper och använder. Ekonomiska operatörer, vilka i huvudsak är tillverkare, importörer och distributörer, ska följa de cybersäkerhetskrav förordningen anger för alla produkter med digitala element, för att de ska kunna tillhandahållas på den inre marknaden.

Kraven innebär att tillverkare ska ta cybersäkerhet i beaktande i designen och utvecklingen av produkter med digitala element. Därtill ska tillverkare granska säkerhetsaspekter under utvecklingsprocessen, ha transparens gentemot konsumenter gällande cybersäkerhetsaspekter samt försäkra säkerhetssupport och uppdateringar på ett proportionerligt sätt under produktens livscykel. Regelefterlevnad uppvisas genom en konformitetsbedömning och i vissa fall certifiering.

Uppdraget att identifiera berörda svenska regelverk

Det finns ett behov av att identifiera vilka bestämmelser i svenska författningar som berörs av EU:s cyberresiliensförordning samt att analysera om de behöver upphävas eller ändras eller om nya bestämmelser behövs med anledning av förordningen.

Produktsäkerhetslagen (2004:451) syftar till att säkerställa att produkter som tillhandahålls på marknaden är säkra för konsumenter. EU:s cyberresiliensförordning ställer krav på säkerhet i digitala pro-

dukter, vilket kan medföra ett behov av att ändra produktsäkerhetslagen för att inkludera krav i fråga om cybersäkerhet och sårbarhet i digitala produkter. Även Europaparlamentets och rådets förordning (EU) 2023/988 av den 10 maj 2023 om allmän produktsäkerhet, ändring av Europaparlamentets och rådets förordning (EU nr 1025/2012 och Europaparlamentets och rådets direktiv (EU) 2020/1828 och om upphävande av Europaparlamentets och rådets direktiv 2001/95/EG och rådets direktiv 87/357/EEG, i fortsättningen benämnd EU-förordningen om allmän produktsäkerhet, som börjar tillämpas den 13 december 2024, kan behöva beaktas vid denna bedömning.

Lagen (2022:482) om elektronisk kommunikation innehåller bl.a. bestämmelser om säkerhet och integritet inom sektorn för elektronisk kommunikation. Bestämmelserna kan bl.a. ställa krav på säkerheten i nätverksutrustning och programvara som motsvarar kraven i bilaga III i EU:s cyberresiliensförordning. Förordningens bestämmelser kan därför medföra ett behov av ändringar i denna lag för att inkludera nya krav på cybersäkerhet och hantering av sårbarheter i den tekniska infrastrukturen.

I konsumentköplagen (2022:260) och konsumenttjänstlagen (1985:716) regleras konsumenters rättigheter vid köp av varor och tjänster. EU:s cyberresiliensförordning kan medföra att säkerhetsrelaterade garantier och rättigheter för digitala produkter behöver integreras i dessa lagar.

Av artikel 2.7 i EU:s cyberresiliensförordning framgår dock att förordningen inte tillämpas på produkter med digitala element som utvecklats eller ändrats uteslutande för ändamål som rör nationell säkerhet eller försvarsändamål eller på produkter som utformats specifikt för att behandla säkerhetsskyddsklassificerade uppgifter.

Utredaren ska därför

- identifiera vilka bestämmelser i svensk rätt som omfattas av tillämpningsområdet för EU:s cyberresiliensförordning,
- analysera om bestämmelserna behöver upphävas eller ändras eller om nya bestämmelser behövs med anledning av förordningen,
- ta ställning till behovet av undantag från befintliga eller föreslagna bestämmelser med hänsyn till nationell säkerhet eller skydd av andra väsentliga statliga funktioner,

- kartlägga potentiellt överlappande krav som följer av andra EU-rättsakter, bl.a. Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet), Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) och Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), och
- lämna nödvändiga författningsförslag.

Uppdraget att föreslå sanktionsbestämmelser

Medlemsstaterna ska enligt EU:s cyberresiliensförordning fastställa regler om sanktioner för överträdelser av förordningen. Detta avser bristande efterlevnad av de cybersäkerhetskrav som anges i bilaga I i förordningen. Sanktionerna ska vara effektiva, proportionella och avskräckande.

Utredaren ska därför

- analysera vilka sanktioner som behövs för att uppfylla kravet på sanktioner vid överträdelse av förordningen, och
- lämna nödvändiga författningsförslag.

Uppdraget att utse nationell marknadskontrollmyndighet och anmälände myndighet

EU:s cyberresiliensförordning ställer krav på att medlemsstaterna ska utse en eller flera nationella marknadskontrollmyndigheter för att säkerställa ett effektivt genomförande av förordningen. Medlemsstaterna får utse en befintlig eller en ny myndighet till att vara mark-

nadskontrollmyndighet enligt förordningen. Flera myndigheter arbetar med marknads- och produktkontroll utifrån olika regelverk, exempelvis Post- och telestyrelsen, Statens energimyndighet och Elsäkerhetsverket.

Medlemsstaterna ska vidare utse en anmälände myndighet med ansvar för att inrätta och genomföra de förfaranden som krävs för bedömning, utseende och anmälan av organ för bedömning av överensstämmelse och för övervakning av dessa.

Utredaren ska därför

- föreslå vilken befintlig myndighet eller vilka befintliga myndigheter som ska utses till nationell marknadskontrollmyndighet för Sveriges räkning,
- föreslå vilken befintlig myndighet som ska utses till anmälände myndighet med ansvar för att bl.a. inrätta och genomföra de förfaranden som krävs för bedömning, utseende och anmälan av organ för bedömning av överensstämmelse,
- analysera om det finns möjligheter att samordna marknadskontrollen med andra regelverk, och
- föreslå de författningsändringar och andra åtgärder som krävs för att föreslagna myndigheter ska kunna vidta de åtgärder som följer av förordningen.

Uppdraget att lämna förslag om stöd för regelfterlevnad till mikroföretag, små företag och medelstora företag

Mikroföretag, små företag och medelstora företag har ofta särskilda utmaningar gällande regelfterlevnad av förordningar när det gäller resurser och kunskap. EU:s cyberresiliensförordning ställer krav på medlemsstaterna att, när så är lämpligt, vidta vissa stödåtgärder för mikroföretag, små företag och medelstora företag. För att undvika att förordningen ska hämma näringslivet och innovation ska utredningen överväga vilka stödåtgärder och stödfunktioner som skulle kunna vara lämpliga för att bistå dessa företag.

Utredaren ska därför

- föreslå hur de åtgärder som avses i artikel 33 i EU:s cyberresiliensförordning kan genomföras i Sverige,

- föreslå lämpliga samarbetsformer eller forum där expertis och kunskap kan delas mellan såväl företag som offentlig-privata initiativ, och
- föreslå andra lämpliga stödåtgärder för mikroföretag, små företag och medelstora företag.

Uppdraget att lämna anslutande förslag

Om det som en följd av utredarens förslag i övrigt bedöms nödvändigt, får utredaren ta upp och lämna förslag i närliggande frågor.

Allmänna utgångspunkter för uppdragets genomförande

Utredaren ska vid utformningen av sina förslag noga beakta skyddet för grundläggande fri- och rättigheter, däribland yttrande- och informationsfriheten samt äganderätten, behovet av att upprätthålla ett högt skydd för den nationella säkerheten och för produkter som har utvecklats uteslutande för ändamål som rör nationell säkerhet eller försvarsändamål. Utredarens förslag ska även utformas utifrån kostnads-effektivitet och så att företagens och myndigheternas totala regelbörda och kostnader inte ökar mer än nödvändigt. Utredaren ska ta medborgarnytta, effektivitet och konkurrenskraft i beaktning.

Konsekvensbeskrivningar

Utredaren ska i enlighet med kommittéförordningen (1998:1474) och förordningen (2024:183) om konsekvensutredningar bedöma och beskriva förslagens ekonomiska och samhällsekonomiska konsekvenser, samt konsekvenser i övrigt för enskilda, företag och det allmänna. Utredaren ska bl.a. beskriva och beräkna eventuella offentligfinansiella konsekvenser, däribland eventuella konsekvenser för berörda myndigheter. Utredaren ska beräkna hur statens inkomster och utgifter påverkas. Om förslag som lämnas medför offentligfinansiella kostnader, ska förslag till finansiering lämnas. Utredaren ska även redovisa förslagens konsekvenser ur ett jämställdhetsperspektiv och för den personliga integriteten.

Processerna för att ta fram standarder kan komma att innebära ett omfattande åtagande både i fråga om resurser och personal för bl.a. deltagande i arbetskommittéer. Utredaren ska bedöma vilka konsekvenser standardiseringsarbetet som följer av förslagen kan antas medföra för berörda myndigheter, företag och andra nationella organisationer.

Mikroföretag, små företag och medelstora företag är särskilt sårbara för risken att omfattande regelverk hämmar affärsverksamheten. Utredaren ska därför särskilt redogöra för vilka ekonomiska konsekvenser de förslag som lämnas kan få för mikroföretag, små företag och medelstora företag.

Kontakter och redovisning av uppdraget

Utredaren ska ha en dialog med och inhämta upplysningar från Post- och telestyrelsen, Försvarets materielverk, Myndigheten för samhällsskydd och beredskap, Statens energimyndighet, Elsäkerhetsverket och Styrelsen för ackreditering och teknisk kontroll (Swedac). Utredaren ska även, i den utsträckning som bedöms lämplig, ha en dialog med och inhämta upplysningar från övriga berörda myndigheter, näringslivet, Implementeringsrådet och organisationer som berörs av uppdraget.

Utredaren ska hålla sig informerad om och beakta annat relevant arbete som bedrivs inom Regeringskansliet, exempelvis uppdraget åt en sakkunnig att analysera behovet av kompletterande bestämmelser till EU-förordningen om allmän produktsäkerhet, och i internationella forum med anledning av genomförandet av EU:s cyberresiliensförordning. Detta inkluderar t.ex. Europeiska unionens cybersäkerhetsbyrå (Enisa) och högnivåforumet för europeisk standardisering. Utredaren bör, om det bedöms lämpligt och främjar uppdraget, också undersöka hur andra medlemsstater planerar att genomföra förordningen.

Uppdraget ska redovisas senast den 15 december 2025.

(Finansdepartementet)

2024/2847

20.11.2024

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2024/2847

av den 23 oktober 2024

om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av
förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828
(cyberresiliensförordningen)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ⁽¹⁾,

efter att ha hört Regionkommittén,

i enlighet med det ordinarie lagstiftningsförfarandet ⁽²⁾, och

av följande skäl:

- (1) Cybersäkerhet är en av de största utmaningarna för unionen. Antalet och mångfalden av uppkopplade enheter kommer att öka exponentiellt under de kommande åren. Cyberattacker är en fråga av allmänintresse eftersom de har en avgörande inverkan inte bara på unionens ekonomi utan även på demokratin liksom på konsumenternas säkerhet och hälsa. Det är därför nödvändigt att stärka unionens strategi när det gäller cybersäkerhet, ta upp frågan om cyberresiliens på unionsnivå och förbättra den inre marknadens funktionssätt genom att fastställa en enhetlig rättslig ram för väsentliga cybersäkerhetskrav för utsläppande av produkter med digitala element på marknaden i unionen. Två stora problem som ökar kostnaderna för användarna och samhället bör lösas: en låg cybersäkerhetsnivå för produkter med digitala element, vilket visas av utbredda sårbarheter och ett otillräckligt och inkonsekvent tillhandahållande av säkerhetsuppdateringar för att åtgärda dessa sårbarheter, samt användarnas bristfälliga förståelse och tillgång till information, vilket hindrar dem från att välja produkter med tillräckliga cybersäkerhetsfunktioner eller att använda dem på ett säkert sätt.
- (2) Denna förordning syftar till att fastställa randvillkor för utvecklingen av säkra produkter med digitala element genom att säkerställa att hårdvaru- och programvaruprodukter som släpps ut på marknaden har färre sårbarheter och att tillverkarna tar säkerheten på allvar under produktens hela livscykel. Den syftar också till att skapa förutsättningar för att användarna ska kunna ta hänsyn till cybersäkerheten när de väljer och använder produkter med digitala element, exempelvis genom att öka transparensen när det gäller stödperioden för produkter med digitala element som släpps ut på marknaden.
- (3) Den relevanta unionsrätt som för närvarande gäller omfattar flera uppsättningar övergripande regler som behandlar vissa aspekter av cybersäkerheten från olika synvinklar, inbegripet åtgärder för att förbättra säkerheten i den digitala leveranskedjan. Den befintliga unionsrätten om cybersäkerhet, inbegripet Europaparlamentets och rådets förordning (EU) 2019/881 ⁽³⁾ och Europaparlamentets och rådets direktiv (EU) 2022/2555 ⁽⁴⁾ täcker inte på ett direkt sätt obligatoriska krav avseende säkerheten för produkter med digitala element.

⁽¹⁾ EUT C 100, 16.3.2023, s. 101.

⁽²⁾ Europaparlamentets ståndpunkt av den 12 mars 2024 (ännu inte offentliggjord i EUT) och rådets beslut av den 10 oktober 2024.

⁽³⁾ Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).

⁽⁴⁾ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80).

- (4) Den befintliga unionsrätten är visserligen tillämplig på vissa produkter med digitala element, men det finns inget övergripande unionsregelverk med övergripande cybersäkerhetskrav för alla produkter med digitala element. De olika rättsakter och initiativ som hittills har vidtagits på unionsnivå och nationell nivå åtgärdar endast delvis de identifierade cybersäkerhetsrelaterade problemen och riskerna, vilket ger upphov till ett lapptäcke av lagar på den inre marknaden som ökar rättsosäkerheten för både tillverkare och användare av dessa produkter och innebär att det blir onödigt betugande för företag och organisationer som måste uppfylla många olika krav och skyldigheter för samma typer av produkter. Cybersäkerheten för dessa produkter har en särskilt stark gränsöverskridande dimension, eftersom produkter med digitala element som tillverkas i en medlemsstat eller ett tredjeland ofta används av organisationer och konsumenter på hela den inre marknaden. Därmed är det nödvändigt att reglera detta område på unionsnivå för att säkerställa ett harmoniserat regelverk och rättssäkerhet för användare, organisationer och företag, inbegripet mikroföretag och små och medelstora företag enligt definitionen i bilagan till kommissionens rekommendation 2003/361/EG⁽⁷⁾. Unionens regelverk bör harmoniseras genom ett införande av övergripande cybersäkerhetskrav för produkter med digitala element. Rättslig förutsebarhet för ekonomiska aktörer och användare liksom harmoniseringen på den inre marknaden och proportionaliteten för mikroföretag samt små och medelstora företag, vilket skapar hållbarare villkor för ekonomiska operatörer som vill komma in på den marknaden bör säkerställas i hela unionen.
- (5) När det gäller mikroföretag och små och medelstora företag bör bestämmelserna i bilagan till rekommendation 2003/361/EG tillämpas i sin helhet vid fastställandet av vilken kategori ett företag omfattas av. Vid beräkningen av personalstyrkan och de finansiella taken för att fastställa företagskategorierna bör därför bestämmelserna i artikel 6 i bilagan till rekommendation 2003/361/EG om fastställande av uppgifter för ett företag med hänsyn till särskilda typer av företag, såsom partnerföretag eller anknutna företag, också tillämpas.
- (6) Kommissionen bör ge vägledning för att hjälpa ekonomiska aktörer, särskilt mikroföretag och små och medelstora företag, vid tillämpningen av denna förordning. Sådan vägledning bör bland annat omfatta denna förordnings tillämpningsområde, särskilt distansbehandling av data och dess konsekvenser för utvecklare av programvara med fri och öppen källkod, tillämpningen av de kriterier som används för att fastställa stödperioder för produkter med digitala element, samspillet mellan denna förordning och annan unionsrätt och begreppet väsentlig ändring.
- (7) På unionsnivå har särskilda EU-cybersäkerhetskrav efterlysts för digitala eller uppkopplade produkter med digitala element, exempelvis det gemensamma meddelandet från kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik av den 16 december 2020 med titeln *EU:s strategi för cybersäkerhet för ett digitalt decennium*, rådets slutsatser av den 2 december 2020 om cybersäkerhet för uppkopplade enheter och av den 23 maj 2022 om utvecklingen av Europeiska unionens arbete på cyberområdet och Europaparlamentets resolution av den 10 juni 2021 om EU:s strategi för cybersäkerhet för ett digitalt decennium⁽⁸⁾, och flera tredjeländer håller på att vidta åtgärder för att åtgärda denna fråga på eget initiativ. I slutrapporten från konferensen om Europas framtid efterlyste medborgarna "En starkare roll för EU när det gäller att motverka cybersäkerhetshot". För att unionen ska kunna spela en ledande internationell roll på cybersäkerhetsområdet är det viktigt att utarbeta ett ambitiöst regelverk.
- (8) För att höja den allmänna cybersäkerhetsnivån för alla produkter med digitala element som släpps ut på den inre marknaden är det nödvändigt att införa målinriktade och teknikneutrala väsentliga cybersäkerhetskrav för dessa produkter vilka ska tillämpas övergripande.
- (9) Under vissa omständigheter kan alla produkter med digitala element vilka är integrerade i eller anslutna till ett större elektroniskt informationssystem fungera som en attackvektor för fientliga aktörer. Det innebär att även hårdvara eller programvara som anses vara mindre kritisk kan underlätta en inledande kompromettering av en enhet eller ett nät, vilket gör det möjligt för fientliga aktörer att få privilegierad åtkomst till ett system eller att röra sig lateralt mellan system. Tillverkarna bör därför säkerställa att alla produkter med digitala element utformas och utvecklas i enlighet med de väsentliga cybersäkerhetskrav som fastställs i denna förordning. Denna skyldighet avser både produkter som kan anslutas fysiskt via hårdvarugränssnitt och produkter som ansluts logiskt, t.ex. via nätslutningsuttag, rör, filer, programmeringsgränssnitt eller andra typer av programvarugränssnitt. I och med att cyberhot kan spridas via olika produkter med digitala element tills de når ett visst mål, exempelvis genom att sammanlänka flera olika attacker mot sårbarheter, bör tillverkarna också säkerställa cybersäkerheten för produkter som endast indirekt ansluts till andra enheter eller nät.

⁽⁷⁾ Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

⁽⁸⁾ EUT C 67, 8.2.2022, s. 81.

- (10) Genom att cybersäkerhetskrav fastställs för utsläppandet på marknaden av produkter med digitala element är syftet att dessa produkters cybersäkerhet ska förbättras för både konsumenter och företag. Dessa krav kommer också att säkerställa att cybersäkerhet tas i beaktande genom leveranskedjorna som helhet, för att göra slutprodukterna med digitala element och deras komponenter säkrare. Detta innefattar krav för utsläppandet på marknaden av konsumentprodukter med digitala element vilka är avsedda för sårbara konsumenter, exempelvis leksaker och babyövervakningssystem. Konsumentprodukter med digitala element som i denna förordning kategoriseras som viktiga produkter med digitala element utgör en högre cybersäkerhetsrisk genom att de utför en funktion som medför en betydande risk för negativa effekter i fråga om intensitet och förmåga att skada hälsan, tryggheten eller säkerheten för användarna av sådana produkter, och bör genomgå ett striktare förfarande för bedömning av överensstämmelse. Detta är tillämpligt på sådana produkter som smarta hemprodukter med säkerhetsfunktioner, inbegripet smarta dörrlås, babyövervakningssystem och larmsystem, uppkopplade leksaker och kroppsburen medicinsk teknik. De striktare förfaranden för bedömning av överensstämmelse som andra produkter med digitala element som i denna förordning kategoriseras som viktiga eller kritiska produkter med digitala element måste genomgå kommer dessutom att bidra till att förhindra att konsumenterna kan komma att påverkas negativt av utnyttjandet av sårbarheter.
- (11) Syftet med denna förordning är att säkerställa en hög cybersäkerhetsnivå för produkter med digitala element och deras integrerade lösningar för fjärrbehandling av data. Sådana lösningar för fjärrbehandling av data bör definieras som all databehandling på distans för vilken programvaran har utformats och utvecklats av tillverkaren av den berörda produkten med digitala element eller för dennes räkning, och vars avsaknad skulle innebära att produkten med digitala element inte skulle kunna utföra en av sina grundläggande funktioner. Detta tillvägagångssätt säkerställer att tillverkarna på lämpligt sätt säkrar sådana produkter i sin helhet, oavsett om uppgifterna behandlas eller lagras lokalt på användarens enhet eller på distans av tillverkaren. Samtidigt omfattas fjärrbehandling eller fjärrlagring av denna förordnings tillämpningsområde endast i den mån det är nödvändigt för att en produkt med digitala element ska kunna utföra sina funktioner. Sådan fjärrbehandling eller fjärrlagring omfattar situationer där en mobilapplikation kräver tillgång till ett programmeringsgränssnitt eller en databas som tillhandahålls genom en tjänst som utvecklats av tillverkaren. I ett sådant fall omfattas tjänsten av denna förordnings tillämpningsområde som en lösning för fjärrbehandling av uppgifter. Kraven på lösningar för fjärrdatabehandling som omfattas av denna förordning innebär därför inte några tekniska, operativa eller organisatoriska åtgärder som syftar till att hantera riskerna för säkerheten i en tillverkarens nätverks- och informationssystem som helhet.
- (12) Molnlösningar utgör lösningar för fjärrdatabehandling i den mening som avses i denna förordning endast om de uppfyller definitionen som fastställs i denna förordning. Till exempel omfattar denna förordning molnaktiverade funktioner som tillhandahålls av en tillverkare av enheter för smarta hem som gör det möjligt för användare att fjärrkontrollera enheten. Å andra sidan omfattas webbplatser som inte stöder funktionen hos en produkt med digitala element, eller molntjänster som utformats och utvecklats utanför en tillverkarens ansvar för en produkt med digitala element, inte av denna förordnings tillämpningsområde. Direktiv (EU) 2022/2555 är tillämpligt på molntjänster och molntjänstmodeller, som Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) eller Infrastructure-as-a-Service (IaaS). Entiteter som tillhandahåller molntjänster i unionen och som räknas som medelstora företag enligt artikel 2 i bilagan till rekommendation 2003/361/EG, eller överskrider de tak för medelstora företag som anges i punkt 1 i den artikeln, omfattas av det direktivets tillämpningsområde.
- (13) I linje med målet för denna förordning, som är att avlägsna hinder för den fria rörligheten för produkter med digitala element, får medlemsstaterna inte, med hänvisning till aspekter som omfattas av denna förordning, hindra att produkter med digitala element som uppfyller kraven i denna förordning tillhandahålls på marknaden. I frågor som harmoniseras genom denna förordning kan medlemsstaterna därför inte införa ytterligare cybersäkerhetskrav för tillhandahållande på marknaden av produkter med digitala element. Varje entitet, offentlig eller privat, kan dock fastställa ytterligare krav utöver dem som fastställs i denna förordning för upphandling eller användning av produkter med digitala element för sina specifika ändamål, och kan därför välja att använda produkter med digitala element som uppfyller strängare eller mer specifika cybersäkerhetskrav än de som är tillämpliga för tillhandahållande på marknaden enligt denna förordning. Utan att det påverkar tillämpningen av Europaparlamentets och rådets direktiv 2014/24/EU (*) och 2014/25/EU (**) bör medlemsstaterna, vid upphandling av produkter med digitala element som måste uppfylla de väsentliga cybersäkerhetskrav som fastställs i denna förordning, inbegripet de som

(*) Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EG (EUT L 94, 28.3.2014, s. 65).

(**) Europaparlamentets och rådets direktiv 2014/25/EU av den 26 februari 2014 om upphandling av enheter som är verksamma på områdena vatten, energi, transporter och posttjänster och om upphävande av direktiv 2004/17/EG (EUT L 94, 28.3.2014, s. 243).

rör sårbarhetshantering, säkerställa att sådana krav beaktas i upphandlingsprocessen och att tillverkarnas förmåga att effektivt tillämpa cybersäkerhetsåtgärder och hantera cyberhot också beaktas. I direktiv (EU) 2022/2555 fastställs dessutom riskhanteringsåtgärder för cybersäkerhet för de väsentliga och viktiga entiteter som avses i artikel 3 i det direktivet som kan medföra säkerhetsåtgärder i leveranskedjan som kräver att sådana entiteter använder produkter med digitala element som uppfyller strängare cybersäkerhetskrav än de som fastställs i denna förordning. I enlighet med direktiv (EU) 2022/2555 och i linje med dess princip om minimiharmonisering kan medlemsstaterna därför införa ytterligare cybersäkerhetskrav för väsentliga eller viktiga entiteters användning av produkter för informations- och kommunikationsteknik (IKT) enligt det direktivet för att säkerställa en högre cybersäkerhetsnivå, förutsatt att sådana krav är förenliga med medlemsstaternas skyldigheter enligt unionsrätten. Frågor som inte omfattas av denna förordning kan omfatta icke-tekniska faktorer som rör produkter med digitala element och deras tillverkare. Medlemsstaterna kan därför fastställa nationella åtgärder, inbegripet begränsningar för produkter med digitala element eller leverantörer av sådana produkter, som tar hänsyn till icke-tekniska faktorer. Nationella åtgärder som rör sådana faktorer måste vara förenliga med unionsrätten.

- (14) Denna förordning bör inte påverka medlemsstaternas ansvar att skydda den nationella säkerheten, i enlighet med unionsrätten. Medlemsstaterna bör kunna låta produkter med digitala element som är upphandlade eller används för ändamål som rör nationell säkerhet- eller försvar omfattas av ytterligare åtgärder, förutsatt att sådana åtgärder är förenliga med medlemsstaternas skyldigheter enligt unionsrätten.
- (15) Denna förordning är tillämplig på ekonomiska aktörer endast med avseende på produkter med digitala element som tillhandahålls på marknaden och därmed levereras för distribution eller användning på unionsmarknaden i samband med kommersiell verksamhet. Tillhandahållande inom ramen för en kommersiell verksamhet kan kännetecknas inte bara av att det tas ut en avgift för en produkt med digitala element utan också av att en avgift tas ut för tekniska stödtjänster när detta inte enbart tjänar till att täcka faktiska kostnader, när syftet är att monetarisera, till exempel genom att tillhandahålla en programvaruplattform som tillverkaren använder för att monetarisera andra tjänster, genom att som ett villkor för användning kräva behandling av personuppgifter för andra syften än uteslutande för att förbättra programvarans säkerhet, kompatibilitet eller interoperabilitet, eller genom att ta emot donationer som överstiger kostnaderna för utformning, utveckling och tillhandahållande av en produkt med digitala element. Att ta emot donationer utan avsikt att göra vinst bör inte betraktas som en kommersiell verksamhet.
- (16) Produkter med digitala element som tillhandahålls som en del av tillhandahållandet av en tjänst för vilka en avgift tas ut enbart för att täcka de faktiska kostnader som är direkt kopplade till driften av den tjänsten, såsom kan vara fallet med vissa produkter med digitala element som tillhandahålls av enheter inom offentlig förvaltning, bör inte i sig anses utgöra kommersiell verksamhet vid tillämpningen av denna förordning. Dessutom bör produkter med digitala element som utvecklas eller ändras av en offentlig förvaltningsentitet uteslutande för dess eget bruk inte anses vara tillgängliggjord på marknaden i den mening som avses i denna förordning.
- (17) Programvara och data som delas öppet och som användarna fritt kan komma åt, använda, modifiera och redistribuera, eller modifierade versioner av dem, kan bidra till forskning och innovation på marknaden. För att främja utvecklingen och spridningen av programvara med fri och öppen källkod, särskilt av mikroföretag och små och medelstora företag, inbegripet uppstarts företag, enskilda personer, ideella organisationer och akademiska forskningsorganisationer, bör tillämpningen av denna förordning på produkter med digitala element som klassificeras som programvara med fri och öppen källkod och som tillhandahålls för distribution eller användning i samband med kommersiell verksamhet ta hänsyn till de olika utvecklingsmodellerna för programvara som distribueras och utvecklas inom ramen för licenser för programvara med fri och öppen källkod.
- (18) Med programvara med fri och öppen källkod avses programvara vars källkod delas öppet och vars licensiering ger alla rättigheter att göra den fritt tillgänglig, samt möjlig att använda, ändra och omfördela. Programvara med fri och öppen källkod utvecklas, underhålls och distribueras öppet, inbegripet via onlineplattformar. När det gäller ekonomiska aktörer som omfattas av denna förordning bör endast programvara med fri och öppen källkod som tillhandahålls på marknaden och som därför levereras för distribution eller användning i samband med kommersiell verksamhet omfattas av denna förordnings tillämpningsområde. De omständigheter under vilka produkten med digitala element har utvecklats, eller hur utvecklingen har finansierats, bör inte beaktas vid fastställandet av huruvida denna verksamhet är av kommersiell eller icke-kommersiell karaktär. Mer specifikt bör tillhandahållandet av produkter med digitala element som klassificeras som programvara med fri och öppen källkod och som inte monetariseras av deras tillverkare inte betraktas vara en kommersiell verksamhet vid tillämpningen av denna

förordning och för de ekonomiska aktörer som omfattas av dess tillämpningsområde, för att säkerställa en tydlig åtskillnad mellan utvecklings- och leveransfaserna. Dessutom bör tillhandahållande av produkter med digitala element som klassificeras som komponenter för programvara med fri och öppen källkod och som är avsedda att integreras av andra tillverkare i deras egna produkter med digitala element betraktas som tillhandahållande på marknaden endast om komponenten monetariseras av dess ursprungliga tillverkare. Till exempel bör enbart det faktum att en programvaruprodukt med fri och öppen källkod med digitala element får ekonomiskt stöd från tillverkare, eller att tillverkarna bidrar till utvecklingen av en sådan produkt, inte i sig fastställa att verksamheten är av kommersiell karaktär. Dessutom bör själva det faktum att en produkt regelbundet släpps ut inte i sig leda till slutsatsen att en produkt med digitala element tillhandahålls inom ramen för kommersiell verksamhet. Slutligen bör utveckling av produkter med digitala element som betraktas som programvara med fri och öppen källkod av ideella organisationer inte betraktas som kommersiell verksamhet vid tillämpningen av denna förordning, förutsatt att organisationen är inrättad på ett sätt som säkerställer att alla intäkter efter kostnader används för att uppnå icke-vinstdrivande mål. Denna förordning är inte tillämplig på fysiska eller juridiska personer som bidrar med källkod till produkter med digitala element som klassificeras som programvara med fri och öppen källkod och som inte omfattas av deras ansvar.

- (19) Med tanke på hur viktigt det är för cybersäkerheten hos många produkter med digitala element som klassificeras som programvara med fri och öppen källkod och som offentliggörs men inte tillhandahålls på marknaden i den mening som avses i denna förordning, bör juridiska personer som ger varaktigt stöd för utvecklingen av sådana produkter som är avsedda för kommersiell verksamhet och som spelar en viktig roll för att säkerställa dessa produkters bärkraft (förvaltare av programvara med fri och öppen källkod) omfattas av ett förenklat och skräddarsytt regelverk. Förvaltare av programvara med fri och öppen källkod omfattar vissa stiftelser samt enheter som utvecklar och publicerar programvara med fri och öppen källkod i ett affärssammanhang, inbegripet icke-vinstdrivande enheter programvara med fri och öppen källkod. Regelverket bör ta hänsyn till deras särskilda karaktär och förenlighet med den typ av skyldigheter som införs. Det bör endast omfatta produkter med digitala element som klassificeras som programvara med fri och öppen källkod och som i slutändan är avsedda för kommersiell verksamhet, såsom integrering i kommersiella tjänster eller i monetariserade produkter med digitala element. Vid tillämpningen av det regelverket omfattar en avsikt om integrering i monetariserade produkter med digitala element fall där tillverkare som integrerar en komponent i sina egna produkter med digitala element antingen bidrar till utvecklingen av den komponenten på ett regelbundet sätt eller tillhandahåller regelbundet ekonomiskt stöd för att säkerställa en programvaruprodukts kontinuitet. Tillhandahållandet av varaktigt stöd till utvecklingen av en produkt med digitala element omfattar, men är inte begränsat till, hysande och förvaltning av samarbetsplattformar för programvaruutveckling, hysande av källkod eller programvara, styrning eller förvaltning av produkter med digitala element som klassificeras som fri och öppen programvara med fri och öppen källkod samt styrning av utvecklingen av sådana produkter. Eftersom det förenklade och skräddarsydda regelverket inte ålägger dem som agerar som förvaltare av programvara med fri och öppen källkod samma skyldigheter som dem som agerar som tillverkare enligt denna förordning, bör de inte ha rätt att fästa CE-märkningen på produkter med digitala element vars utveckling de stöder.
- (20) Enbart hysande av produkter med digitala element i öppna databaser, inbegripet genom paketförvaltare eller på samarbetsplattformar, utgör inte i sig tillhandahållande på marknaden av en produkt med digitala element. Leverantörer av sådana tjänster bör betraktas vara distributörer endast om de tillhandahåller sådan programvara på marknaden och därmed tillhandahåller den för distribution eller användning på unionsmarknaden i samband med kommersiell verksamhet.
- (21) För att stödja och underlätta tillbörlig aktsamhet hos tillverkare som i sina produkter med digitala element integrerar komponenter för programvara med fri och öppen källkod som inte omfattas av de väsentliga cybersäkerhetskrav som fastställs i denna förordning bör kommissionen kunna inrätta frivilliga program för säkerhetsintyg, antingen genom en delegerad akt som kompletterar denna förordning eller genom att enligt artikel 48 i förordning (EU) 2019/881 begära en europeisk ordning för cybersäkerhetscertifiering som tar hänsyn till särdragen hos utvecklingsmodellerna för programvara med fri och öppen källkod. Programmen för säkerhetsintyg bör utformas på ett sådant sätt att inte bara fysiska eller juridiska personer som utvecklar eller bidrar till utvecklingen av en produkt med digitala element som klassificeras som programvara med fri och öppen källkod kan initiera eller finansiera ett säkerhetsintyg, utan även tredje parter, såsom tillverkare som integrerar sådana produkter i sina egna produkter med digitala element, användare eller offentliga förvaltningar på unionsnivå och nationell nivå.
- (22) Med tanke på målen för offentlig cybersäkerhet i denna förordning och för att förbättra medlemsstaternas situationsmedvetenhet när det gäller unionens beroende av programvarukomponenter, särskilt av komponenter för potentiell programvara med fri och öppen källkod, bör en särskild administrativ samarbetsgrupp (Adco-grupp) som inrättas genom denna förordning kunna besluta att gemensamt genomföra en beroendebedomning på unionsnivå. Marknadskontrollmyndigheterna bör kunna begära att tillverkare av kategorier av produkter med digitala element som inrättats av Adco-gruppen lämnar in de mjukvaruförteckningar som de har framställt enligt denna förordning. För att skydda sekretessen för mjukvaruförteckningar bör marknadskontrollmyndigheterna lämna relevant information om beroendeförhållanden till Adco-gruppen på ett anonymiserat och aggregerat sätt.

SV

EUT L, 20.11.2024

- (23) Effektiviteten i genomförandet av denna förordning kommer också att vara beroende av tillgången till lämpliga cybersäkerhetskunskaper. På unionsnivå konstaterades i olika programdokument och politiska dokument, inbegripet kommissionens meddelande *Minska kompetensbristen på cybersäkerhetsområdet för att främja EU:s konkurrenskraft, tillväxt och resiliens* av den 18 april 2023 och rådets slutsatser av den 22 maj 2023 om EU:s politik för cyberförsvar, kompetensbristen inom cybersäkerhet i unionen och behovet av att ta itu med sådana utmaningar som en prioriterad fråga, både inom den offentliga och den privata sektorn. För att säkerställa ett effektivt genomförande av denna förordning bör medlemsstaterna se till att tillräckliga resurser finns tillgängliga för lämplig personal vid marknadskontrollmyndigheterna och organen för bedömning av överensstämmelse för att de ska kunna utföra sina uppgifter enligt denna förordning. Dessa åtgärder bör öka arbetskraftens rörlighet på cybersäkerhetsområdet och deras tillhörande karriärvägar. De bör också bidra till att göra cybersäkerhetsarbetskraften mer resiliënt och inkluderande, även när det gäller kön. Medlemsstaterna bör därför vidta åtgärder för att säkerställa att dessa uppgifter utförs av tillräckligt utbildade yrkesutövare med nödvändig cybersäkerhetskompetens. På samma sätt bör tillverkarna se till att deras personal har den kompetens som krävs för att fullgöra sina skyldigheter som fastställs i denna förordning. Medlemsstaterna och kommissionen bör, i enlighet med sina rättigheter och befogenheter och de särskilda uppgifter som de tilldelas genom denna förordning, vidta åtgärder för att stödja tillverkare, särskilt mikroföretag och små och medelstora företag, inbegripet uppstarts företag, även på områden såsom kompetensutveckling, i syfte att fullgöra de skyldigheter som fastställs i denna förordning. Eftersom direktiv (EU) 2022/2555 ålägger medlemsstaterna att anta strategier för att främja och utveckla utbildning i cybersäkerhet och cybersäkerhetskompetens som en del av sina nationella strategier för cybersäkerhet, får medlemsstaterna, när de antar sådana strategier, också överväga om de ska ta itu med de kompetensbehov inom cybersäkerhet som följer av denna förordning, inbegripet sådana som rör omskolning och kompetenshöjning.
- (24) Ett säkert internet är avgörande för att kritiska infrastrukturer och samhället som helhet ska kunna fungera. Direktiv (EU) 2022/2555 syftar till att säkerställa en hög cybersäkerhetsnivå för tjänster som tillhandahålls av väsentliga och viktiga entiteter som avses i artikel 3 i det direktivet, inbegripet leverantörer av digital infrastruktur som stöder kärnfunktioner för ett öppet internet eller säkerställer internetåtkomst och tillhandahåller internettjänster. Det är därför viktigt att de produkter med digitala element som behövs för att leverantörer av digital infrastruktur ska kunna säkerställa ett fungerande internet utvecklas på ett säkert sätt och att de uppfyller väletablerade internetsäkerhetsstandarder. Denna förordning, som är tillämplig på alla uppkopplingsbara hårdvaru- och programvaruprodukter, syftar också till att främja att leverantörer av digital infrastruktur uppfyller leveranskedjekraven enligt direktiv (EU) 2022/2555 genom att säkerställa att de produkter med digitala element som de använder för tillhandahållandet av sina tjänster utvecklas på ett säkert sätt och att de har tillgång till säkerhetsuppdateringar i rätt tid för sådana produkter.
- (25) I Europaparlamentets och rådets förordning (EU) 2017/745 ⁽⁹⁾ fastställs regler om medicintekniska produkter och i Europaparlamentets och rådets förordning (EU) 2017/746 ⁽¹⁰⁾ fastställs regler om medicintekniska produkter för in vitro-diagnostik. De förordningarna behandlar cybersäkerhetsrisker enligt särskilda tillvägagångssätt som också behandlas i den här förordningen. Närmare bestämt fastställs i förordningarna (EU) 2017/745 och (EU) 2017/746 väsentliga krav för medicintekniska produkter som fungerar genom ett elektroniskt system eller som själva utgörs av programvara. Viss icke-inbyggd programvara och ett livscykelperspektiv täcks också av dessa förordningar. Dessa krav innebär att tillverkarna ska utveckla och bygga sina produkter genom att tillämpa riskhanteringsprinciper och genom att fastställa krav på it-säkerhetsåtgärder, samt motsvarande förfaranden för bedömning av överensstämmelse. Vidare finns det sedan december 2019 särskilda riktlinjer för cybersäkerheten för medicintekniska produkter, som ger tillverkarna av medicintekniska produkter, däribland för in vitro-diagnostik, vägledning för hur alla berörda väsentliga krav som anges i bilaga I till dessa förordningar ska uppfyllas när det gäller cybersäkerhet. Produkter med digitala element på vilka någon av dessa förordningar är tillämpliga bör därför inte omfattas av den här förordningen.
- (26) Produkter med digitala element som utvecklas eller ändras uteslutande för ändamål som rör nationell säkerhet eller försvar eller produkter som är särskilt utformade för att behandla säkerhetsskyddsklassificerade uppgifter omfattas inte av denna förordnings tillämpningsområde. Medlemsstaterna uppmanas att säkerställa samma eller en högre skyddsnivå för dessa produkter som för de produkter som omfattas av denna förordnings tillämpningsområde.

⁽⁹⁾ Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter, om ändring av direktiv 2001/83/EG, förordning (EG) nr 178/2002 och förordning (EG) nr 1223/2009 och om upphävande av rådets direktiv 90/385/EEG och 93/42/EEG (EUT L 117, 5.5.2017, s. 1).

⁽¹⁰⁾ Europaparlamentets och rådets förordning (EU) 2017/746 av den 5 april 2017 om medicintekniska produkter för in vitro-diagnostik och om upphävande av direktiv 98/79/EG och kommissionens beslut 2010/227/EU (EUT L 117, 5.5.2017, s. 176).

- (27) Genom Europaparlamentets och rådets förordning (EU) 2019/2144 ⁽¹¹⁾ fastställs krav för typgodkännande av fordon och deras system och komponenter, som innebär att vissa cybersäkerhetskrav införs, inbegripet när det gäller användning av ett certifierat ledningssystem för cybersäkerhet och uppdateringar av programvara, som täcker organisationspolicyer och processer för cybersäkerhetsrisker under hela livscykeln för fordon, utrustning och tjänster i enlighet med tillämpliga Förenta nationernas (FN) föreskrifter om tekniska specifikationer och cybersäkerhet, i synnerhet FN-föreskrift nr 155 – Enhetliga bestämmelser om godkännande av fordon med avseende på cybersäkerhet och ledningssystem för cybersäkerhet ⁽¹²⁾, och föreskrivs särskilda förfaranden för bedömning av överensstämmelse. På luftfartsområdet är huvudsyftet för Europaparlamentets och rådets förordning (EU) 2018/1139 ⁽¹³⁾ att fastställa och upprätthålla en hög och enhetlig säkerhetsnivå inom den civila luftfarten i unionen. Förordningen ger en ram för väsentliga krav på luftvärdighet för luftfartsprodukter, delar och utrustning, inbegripet programvara som inbegriper skyldigheten att skydda sig mot informationssäkerhetshot. Certifieringsförfarandena enligt förordning (EU) 2018/1139 säkerställer den assurancesnivå som eftersträvas i den här förordningen. Produkter med digitala element som omfattas av förordning (EU) 2019/2144 och produkter som certifierats i enlighet med förordning (EU) 2018/1139 bör därför inte omfattas av de väsentliga cybersäkerhetskrav och förfaranden för bedömning av överensstämmelse som fastställs i den här förordningen.
- (28) Genom denna förordning fastställs övergripande cybersäkerhetsregler som inte är sektorspecifika eller specifika för vissa produkter med digitala element. Sektors- eller produktspecifika unionsregler kan dock införas, med krav som omfattar alla eller vissa risker som täcks av de väsentliga cybersäkerhetskraven enligt denna förordning. I sådana fall får tillämpningen av denna förordning på sådana produkter med digitala element som omfattas av andra unionsregler, där krav fastställs avseende alla eller vissa risker som täcks av de väsentliga cybersäkerhetskrav som anges i denna förordning, begränsas eller uteslutas när en begränsning eller ett uteslutande är förenligt med den allmänna rättsliga ram som är tillämplig på dessa produkter och när sektorsreglerna ger minst samma skyddsnivå som denna förordning. Kommissionen bör ges befogenhet att anta delegerade akter för att komplettera denna förordning genom att identifiera sådana produkter och regler. För befintlig unionsrätt på vilken denna typ av begränsning eller uteslutande bör tillämpas, omfattar denna förordning särskilda bestämmelser som klargör dess förhållande till den unionsrätten.
- (29) För att säkerställa att produkter med digitala element som tillhandahålls på marknaden kan repareras ändamålsenligt och deras hållbarhet förlängas bör ett undantag göras för reservdelar. Undantaget bör omfatta både reservdelar som har till syfte att reparera befintliga produkter som tillhandahålls före den dag då denna förordning börjar tillämpas och reservdelar som redan har genomgått ett förfarande för bedömning av överensstämmelse enligt denna förordning.
- (30) I kommissionens delegerade förordning (EU) 2022/30 ⁽¹⁴⁾ anges att ett antal väsentliga krav som anges i artikel 3.3 d, e och f i Europaparlamentets och rådets direktiv 2014/53/EU ⁽¹⁵⁾ avseende skada på nät och missbruk av nätresurser, personuppgifter och integritet samt bedrägeri ska tillämpas på viss radioutrustning. I kommissionens genomförandebeslut C(2022) 5637 av den 5 augusti 2022 om en standardiseringsbegäran till Europeiska standardiseringskommittén och Europeiska kommittén för elektroteknisk standardisering fastställs krav för utarbetandet av särskilda standarder som ytterligare specificerar hur de tre väsentliga kraven bör hanteras. De väsentliga cybersäkerhetskrav som anges i denna förordning omfattar alla aspekter av de väsentliga krav som avses i artikel 3.3 d, e och f i direktiv 2014/53/EU. De väsentliga cybersäkerhetskrav som anges i denna förordning är dessutom
- ⁽¹¹⁾ Europaparlamentets och rådets förordning (EU) 2019/2144 av den 27 november 2019 om krav för typgodkännande av motorfordon och deras släpvagnar samt de system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, med avseende på deras allmänna säkerhet och skydd för personer i fordonet och oskyddade trafikanter, om ändring av Europaparlamentets och rådets förordning (EU) 2018/858 och om upphävande av Europaparlamentets och rådets förordningar (EG) nr 78/2009, (EG) nr 79/2009 och (EG) nr 661/2009 samt kommissionens förordningar (EG) nr 631/2009, (EU) nr 406/2010, (EU) nr 672/2010, (EU) nr 1003/2010, (EU) nr 1005/2010, (EU) nr 1008/2010, (EU) nr 1009/2010, (EU) nr 19/2011, (EU) nr 109/2011, (EU) nr 458/2011, (EU) nr 65/2012, (EU) nr 130/2012, (EU) nr 347/2012, (EU) nr 351/2012, (EU) nr 1230/2012 och (EU) 2015/166 (EUT L 325, 16.12.2019, s. 1).
- ⁽¹²⁾ EUT L 82, 9.3.2021, s. 30.
- ⁽¹³⁾ Europaparlamentets och rådets förordning (EU) 2018/1139 av den 4 juli 2018 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 2111/2005, (EG) nr 1008/2008, (EU) nr 996/2010, (EU) nr 376/2014 och direktiv 2014/30/EU och 2014/53/EU, samt om upphävande av Europaparlamentets och rådets förordningar (EG) nr 552/2004 och (EG) nr 216/2008 och rådets förordning (EEG) nr 3922/91 (EUT L 212, 22.8.2018, s. 1).
- ⁽¹⁴⁾ Kommissionens delegerade förordning (EU) 2022/30 av den 29 oktober 2021 om komplettering av Europaparlamentets och rådets direktiv 2014/53/EU vad gäller tillämpningen av de väsentliga krav som avses i artikel 3.3 d, e och f i det direktivet (EUT L 7, 12.1.2022, s. 6).
- ⁽¹⁵⁾ Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG (EUT L 153, 22.5.2014, s. 62).

anpassade till syftena för kraven på särskilda standarder som omfattas av den standardiseringsbegäran. När kommissionen upphäver eller ändrar delegerad förordning (EU) 2022/30 med följden att den upphör att gälla för vissa produkter som omfattas av denna förordning, bör kommissionen och de europeiska standardiseringsorganisationerna, i samband med förberedelserna och utarbetandet av harmoniserade standarder för att underlätta genomförandet av denna förordning, ta hänsyn till det standardiseringsarbete som utförts inom ramen för genomförandebeslut C(2022)5637. Under övergångsperioden för tillämpningen av den här förordningen bör kommissionen ge vägledning till tillverkare som omfattas av den här förordningen och som också omfattas av delegerad förordning (EU) 2022/30 för att underlätta påvisandet av efterlevnaden av de båda förordningarna.

- (31) Europaparlamentets och rådets direktiv (EU) 2024/2853⁽¹⁶⁾ kompletterar denna förordning. Genom det direktivet fastställs skadeståndsansvar för produkter med säkerhetsbrister så att skadelidande kan kräva ersättning när en skada har orsakats av produkter med säkerhetsbrister. Där fastställs principen att tillverkaren av en produkt har skadeståndsansvaret för skador som orsakats av säkerhetsbrister i produkten oavsett om tillverkaren agerat oaksamt (strikt ansvar). När sådana säkerhetsbrister består av en brist på säkerhetsuppdateringar efter att produkten släppts ut på marknaden och detta orsakar skada kan tillverkarens skadeståndsansvar utlösas. Tillverkarnas skyldigheter avseende tillhandahållandet av sådana säkerhetsuppdateringar bör fastställas i denna förordning.
- (32) Denna förordning bör inte påverka tillämpningen av Europaparlamentets och rådets förordning (EU) 2016/679⁽¹⁷⁾, inbegripet när det gäller bestämmelser om inrättandet av certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd som syftar till att visa att personuppgiftsansvarigas och personuppgiftsbiträdens databehandling uppfyller kraven i den förordningen. Sådan behandling kan vara inbyggd i en produkt med digitala element. Inbyggt dataskydd och dataskydd som standard samt allmän cybersäkerhet är viktiga aspekter av förordning (EU) 2016/679. Genom att skydda konsumenter och organisationer från cybersäkerhetsrisker bidrar de väsentliga cybersäkerhetskrav som fastställs i den här förordningen till att förbättra skyddet av personuppgifter och individens personliga integritet. När det gäller både standardiseringen och certifieringen av cybersäkerhetsaspekter bör synergier övervägas genom samarbete mellan kommissionen, europeiska standardiseringsorganisationer, Europeiska unionens cybersäkerhetsbyrå (Enisa), Europeiska dataskyddsstyrelsen, som inrättats genom förordning (EU) 2016/679, och de nationella tillsynsmyndigheterna med ansvar för dataskydd. Synergier mellan den här förordningen och unionens dataskyddsrätt bör också skapas på områdena marknads kontroll och kontroll av efterlevnaden. Därför bör de nationella marknads kontrollmyndigheter som utses enligt den här förordningen samarbeta med de myndigheter som utövar tillsyn över tillämpningen av unionens dataskyddsrätt. De sistnämnda bör också ha tillgång till information av relevans för utförandet av deras uppgifter.
- (33) I den mån deras produkter omfattas av denna förordning bör leverantörer av europeiska digitala identitetsplånböcker som avses i artikel 5a.2 i Europaparlamentets och rådets förordning (EU) nr 910/2014⁽¹⁸⁾ uppfylla både de övergripande väsentliga cybersäkerhetskrav som fastställs i den här förordningen och de särskilda säkerhetskrav som fastställs i artikel 5a i förordning (EU) nr 910/2014. För att främja efterlevnad bör de leverantörerna kunna visa att europeiska digitala identitetsplånböcker uppfyller de krav som fastställs i den här förordningen och i förordning (EU) nr 910/2014 genom att låta certifiera sina produkter inom en europeisk ordning för cybersäkerhetscertifiering som inrättas inom ramen för förordning (EU) 2019/881 och för vilket kommissionen genom delegerade akter har specificerat en presumtion om överensstämmelse med den här förordningen, i den mån som certifikatet, eller delar av detta, täcker dessa krav.
- (34) Vid integrering av komponenter från tredje parter i produkter med digitala element under utformnings- och utvecklingsfasen bör tillverkarna, för att säkerställa att produkterna utformas, utvecklas och tillverkas i enlighet med de väsentliga cybersäkerhetskrav som fastställs i denna förordning, iakta tillbörlig aktsamhet med avseende på dessa komponenter, inbegripet komponenter av programvara med fri och öppen källkod som inte har tillhandahållits på

⁽¹⁶⁾ Europaparlamentets och rådets direktiv (EU) 2024/2853 av den 23 oktober 2024 om skadeståndsansvar för produkter med säkerhetsbrister och om upphävande av rådets direktiv 85/374/EEG (EUT L, 2024/2853, 18.11.2024, ELI: <http://data.europa.eu/eli/dir/2024/2853/oj>).

⁽¹⁷⁾ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

⁽¹⁸⁾ Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73).

marknaden. Den lämpliga nivån på tillbörlig aktsamhet beror på arten av och nivån på den cybersäkerhetsrisk som är förknippad med en viss komponent, och bör i detta syfte beakta en eller flera av följande åtgärder: Kontrollera, när så är relevant, att tillverkaren av en komponent har påvisat överensstämmelse med denna förordning, inbegripet genom att kontrollera om komponenten redan är försedd med CE-märkning. Kontrollera att en komponent får regelbundna säkerhetsuppdateringar, till exempel genom att kontrollera dess säkerhetshistorik. Kontrollera att en komponent är fri från sårbarheter som registrerats i den europeiska sårbarhetsdatabas som inrättats enligt artikel 12.2 i direktiv (EU) 2022/2555 eller andra allmänt tillgängliga sårbarhetsdatabaser, eller utföra ytterligare säkerhetstester. De skyldigheter att hantera sårbarheter som fastställs i denna förordning och som tillverkare måste uppfylla när de släpper ut en produkt med digitala element på marknaden och för stödperioden, gäller för produkter med digitala element i sin helhet, inbegripet alla integrerade komponenter. Om tillverkaren av en produkt med digitala element vid utövandet av tillbörlig aktsamhet identifierar en sårbarhet i en komponent, inbegripet i en komponent med fri och öppen källkod, bör den informera den person eller entitet som tillverkar eller underhåller komponenten, åtgärda och avhjälpa sårbarheten och, i tillämpliga fall, förse personen eller entiteten med den tillämpliga säkerhetsåtgärden.

- (35) Omedelbart efter övergångsperioden för tillämpningen av denna förordning kan en tillverkare av en produkt med digitala element som integrerar en eller flera komponenter från tredje parter som också omfattas av denna förordning inte kunna kontrollera, som en del av sin skyldighet att visa tillbörlig aktsamhet, att tillverkarna av dessa komponenter har visat överensstämmelse med denna förordning, till exempel genom att kontrollera om komponenterna redan är CE-märkta. Detta kan vara fallet om komponenterna har integrerats innan denna förordning blir tillämplig på tillverkarna av dessa komponenter. I sådana fall bör en tillverkare som integrerar sådana komponenter visa tillbörlig aktsamhet på andra sätt.
- (36) Produkter med digitala element bör vara försedda med en CE-märkning som på ett synligt, läsligt och outplånligt sätt visar att de överensstämmer med denna förordning, så att de omfattas av den fria rörligheten på den inre marknaden. Medlemsstaterna bör inte sätta upp omotiverade hinder för utsläppandet på marknaden av produkter med digitala element som uppfyller kraven i denna förordning och är försedda med en CE-märkning. Dessutom bör medlemsstaterna vid mässor, utställningar och demonstrationer eller liknande evenemang inte förhindra presentation eller användning av en produkt med digitala element som inte uppfyller kraven i denna förordning, inbegripet prototyper, förutsatt att produkten presenteras med en synlig skylt som tydligt anger att produkten inte uppfyller kraven i denna förordning och att den inte får tillhandahållas på marknaden förrän den gör det.
- (37) För att säkerställa att tillverkarna kan släppa ut programvara i testsyfte innan deras produkter med digitala element genomgår en bedömning av överensstämmelse bör medlemsstaterna inte hindra tillhandahållandet av ofärdig programvara, såsom alfaversioner, betaversioner eller lanseringskandidater, förutsatt att inte färdigställd programvara endast görs tillgänglig så lång tid som de behöver för att testa den och få återkoppling. Tillverkarna bör säkerställa att programvara som görs tillgänglig under de villkoren endast släpps ut efter att en riskbedömning har gjorts och att den i möjligaste mån uppfyller de säkerhetskrav som enligt denna förordning föreskrivs för egenskaper hos produkter med digitala element. Tillverkarna bör också i möjligaste mån uppfylla sårbarhetshanteringskraven. Tillverkarna bör inte tvinga användare att uppdatera till versioner som endast släpps ut i testsyfte.
- (38) För att säkerställa att produkter med digitala element inte utgör cybersäkerhetsrisker för personer och organisationer när de släpps ut på marknaden bör väsentliga cybersäkerhetskrav fastställas för sådana produkter. Dessa väsentliga cybersäkerhetskrav, inbegripet krav på hantering av sårbarhetshantering, är tillämpliga för varje enskild produkt med digitala element när den släpps ut på marknaden, oavsett om produkten med digitala element tillverkas som en enskild enhet eller i serie. För en produkttyp bör till exempel varje enskild produkt med digitala element ha fått alla säkerhetsprogramfixar eller uppdateringar som finns tillgängliga för att hantera relevanta säkerhetsfrågor när den släpps ut på marknaden. När produkterna med digitala element senare, fysiskt eller digitalt, ändras på ett sätt som tillverkaren inte förutsett i den ursprungliga riskbedömningen och som kan innebära att de inte längre uppfyller de relevanta väsentliga cybersäkerhetskraven, bör ändringen betraktas som väsentlig. Exempelvis kan programvarureparationer betraktas som underhållsåtgärder, förutsatt att de inte ändrar en produkt med digitala element som redan släppts ut på marknaden på ett sådant sätt att överensstämmelsen med de tillämpliga kraven kan påverkas eller att det avsedda ändamål för vilken produkten har bedömts kan ändras.
- (39) Precis som vid fysiska reparationer eller ändringar bör en produkt med digitala element anses vara väsentligt ändrad genom en programvaruändring om programvaruuppdateringen ändrar produktens avsedda ändamål och dessa ändringar inte förutsågs av tillverkaren i den ursprungliga riskbedömningen, eller om farans art har ändrats eller

nivån på cybersäkerhetsrisken har ökat på grund av programvaruuppdateringen, och den uppdaterade versionen av produkten tillhandahålls på marknaden. Om en säkerhetsuppdatering, som är utformad för att minska cybersäkerhetsnivån för en produkt med digitala element, inte ändrar det avsedda ändamålet för en produkt med digitala element anses det inte vara en väsentlig ändring. Detta omfattar vanligtvis situationer där säkerhetsuppdateringar endast medför smärre justeringar av källkoden. Detta kan till exempel vara fallet om en säkerhetsuppdatering åtgärdar en känd sårbarhet, inbegripet genom att ändra funktioner eller prestanda hos en produkt med digitala element enbart i syfte att minska cybersäkerhetsrisken. På samma sätt bör en mindre funktionsuppdatering, såsom en visuell förbättring eller tillägg av nya piktogram eller språk i användargränssnittet, inte i allmänhet betraktas som en väsentlig ändring. Omvänt gäller att om en funktionsuppdatering ändrar de ursprungligen avsedda funktionerna eller typen eller prestandan för en produkt med digitala element och uppfyller de ovannämnda kriterierna, bör den betraktas vara en väsentlig ändring, eftersom tillägg av nya funktioner vanligtvis leder till en bredare angreppsytta, vilket ökar cybersäkerhetsrisken. Detta kan till exempel vara fallet när ett nytt indatatelement läggs till i en applikation, vilket kräver att tillverkaren säkerställer lämplig validering av indata. Vid bedömningen av om en uppdatering av objektet betraktas vara en väsentlig ändring är det inte relevant om den tillhandahålls som en separat uppdatering eller i kombination med en säkerhetsuppdatering. Kommissionen bör ge vägledning för fastställandet av vad som utgör en väsentlig ändring.

- (40) Med tanke på programvaruutvecklingens upprepande karaktär bör tillverkare som har släppt ut efterföljande versioner av en programvaruprodukt på marknaden till följd av en senare betydande ändring av den produkten kunna tillhandahålla säkerhetsuppdateringar under stödperioden endast för den version av programvaruprodukten som de senast har släppt ut på marknaden. De bör endast kunna göra detta om användarna av de relevanta tidigare produktversionerna har kostnadsfri tillgång till den produktversion som senast släpptes ut på marknaden och inte ådrar sig ytterligare kostnader för att anpassa den maskin- eller programvarumiljö där de använder produkten. Detta kan till exempel vara fallet när en uppgradering av ett stationärt operativsystem inte kräver ny hårdvara, såsom en snabbare centralenhet eller mer minne. Tillverkaren bör dock under stödperioden fortsätta att uppfylla andra krav på hantering av sårbarheter, såsom att ha en policy för samordnad delgivning av information om sårbarheter eller åtgärder för att underlätta utbytet av information om potentiella sårbarheter för alla efterföljande väsentligt ändrade versioner av den programvara som släpps ut på marknaden. Tillverkarna bör kunna tillhandahålla mindre säkerhets- eller funktionsuppdateringar som inte utgör en väsentlig ändring endast av den senaste versionen eller underversionen av en programvaruprodukt som inte har ändrats väsentligt. Om en hårdvaruprodukt, till exempel en smarttelefon, inte är kompatibel med den senaste versionen av det operativsystem som den ursprungligen levererades med, bör tillverkaren samtidigt fortsätta att tillhandahålla säkerhetsuppdateringar åtminstone för den senaste kompatibla versionen av operativsystemet under stödperioden.
- (41) I linje med det vedertagna begreppet väsentlig ändring för produkter som regleras genom unionsharmoniseringslagstiftning, är det, vid en väsentlig ändring som kan påverka överensstämmelsen med denna förordning hos produkten med digitala element eller om produktens avsedda ändamål ändras, lämpligt att produktens överensstämmelse kontrolleras och att den, om tillämpligt, genomgår en ny bedömning av överensstämmelse. Om tillverkaren låter göra en bedömning av överensstämmelse som involverar tredje part bör en förändring som kan leda till en väsentlig ändring i tillämpliga fall anmälas till denna tredje part.
- (42) Om en produkt med digitala element är föremål för *renovering*, *underhåll* och *reparation* av en produkt med digitala element, enligt definitionen i artikel 2.18, 2.19 och 2.20 i Europaparlamentets och rådets förordning (EU) 2024/1781⁽¹⁹⁾, medför detta inte nödvändigtvis en väsentlig ändring av produkten, exempelvis om det avsedda ändamålet och de avsedda funktionerna inte ändras och risknivån inte påverkas. Tillverkarens uppgradering av en produkt med digitala element kan dock medföra ändringar av produktens utformning och utveckling och skulle därför kunna påverka dess avsedda ändamål och uppfyllande av de krav som fastställs i den här förordningen.
- (43) Produkter med digitala element bör anses vara viktiga om de negativa konsekvenserna av utnyttjandet av potentiella sårbarheter i produkten kan vara allvarliga på grund av, bland annat, cybersäkerhetsrelaterade funktioner eller en funktion som medför en betydande risk för negativa effekter i fråga om dess intensitet och förmåga att störa, kontrollera eller orsaka skada på ett stort antal andra produkter eller på användarnas hälsa, säkerhet eller skydd genom direkt manipulering, såsom en central systemfunktion, inbegripet nätförvaltning, konfigurationsstyrning, virtualisering eller behandling av personuppgifter. I synnerhet kan sårbarheter i produkter med digitala element som har en cybersäkerhetsrelaterad funktion, såsom starthanterare, medföra att säkerhetsproblem sprids i hela

⁽¹⁹⁾ Europaparlamentets och rådets förordning (EU) 2024/1781 av den 13 juni 2024 om upprättande av en ram för att fastställa ekodesignkrav för hållbara produkter, om ändring av direktiv (EU) 2020/1828 och förordning (EU) 2023/1542 och om upphävande av direktiv 2009/125/EG (EUT L, 2024/1781, 28.6.2024, ELI: <http://data.europa.eu/eli/reg/2024/1781/oj>).

leveranskedjan. Allvarlighetsgraden i en cybersäkerhetsincident kan också öka när produkten primärt utför en central systemfunktion, inbegripet nätförvaltning, konfigurationsstyrning, virtualisering eller behandling av personuppgifter.

- (44) Vissa kategorier av produkter med digitala element bör omfattas av striktare förfaranden för bedömning av överensstämmelse, med bevarande av proportionaliteten. Därför bör viktiga produkter med digitala element delas in i två klasser som återspeglar produktkategoriernas cybersäkerhetsrisknivå. En incident som involverar viktiga produkter med digitala element som omfattas av i klass II skulle kunna få större negativa konsekvenser än en incident som involverar viktiga produkter med digitala element i klass I, exempelvis på grund av produkternas cybersäkerhetsrelaterade funktion eller utförandet av en annan funktion som medför en betydande risk för negativa effekter. Som en indikation på sådana större negativa effekter skulle produkter med digitala element som omfattas av klass II antingen kunna utföra en cybersäkerhetsrelaterad funktion eller en annan funktion som medför en betydande risk för negativa effekter som är högre än för dem som förtecknas i klass I, eller uppfylla båda ovannämnda kriterier. Viktiga produkter med digitala element som omfattas av klass II bör därför omfattas av ett striktare förfarande för bedömning av överensstämmelse.
- (45) Viktiga produkter med digitala element som avses i denna förordning bör förstås som produkter som har kärnfunktionen hos en kategori av viktiga produkter med digitala element som anges i denna förordning. I denna förordning anges exempelvis kategorier av produkter med digitala element som genom sina kärnfunktioner definieras som brandväggar eller intrångsdetektions- eller intrångsskyddssystem i klass II. Därmed bör brandväggar och intrångsdetektions- eller intrångsskyddssystem genomgå en obligatorisk tredjepartsbedömning av överensstämmelse. Detta är inte fallet för andra produkter med digitala element som inte kategoriseras som viktiga produkter med digitala element som kan integrera brandväggar eller intrångsdetektions- eller intrångsskyddssystem. Kommissionen bör anta en genomförandeakt för att specificera den tekniska beskrivningen av de kategorier av viktiga produkter med digitala element som omfattas av klasserna I och II som anges i denna förordning.
- (46) De kategorier av kritiska produkter med digitala element som anges i denna förordning har en cybersäkerhetsrelaterad funktion och en funktion som medför en betydande risk för negativa effekter i fråga om intensitet och förmåga att störa, kontrollera eller skada ett stort antal andra produkter med digitala element genom direkt manipulation. Dessutom anses dessa kategorier av produkter med digitala element vara kritiska beroenden för de väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555. De kategorier av kritiska produkter med digitala element som anges i en bilaga till denna förordning använder redan i stor utsträckning olika former av certifiering, och omfattas också av det europeiska gemensamma kriteriebaserade systemet för cybersäkerhetscertifiering (EUCC) som anges i kommissionens genomförandeförordning (EU) 2024/482⁽²⁹⁾. För att säkerställa ett gemensamt tillräckligt cybersäkerhetsskydd för kritiska produkter med digitala element i unionen skulle det därför kunna vara lämpligt och proportionellt att genom en delegerad akt låta sådana produktkategorier omfattas av obligatorisk europeisk cybersäkerhetscertifiering om det redan finns en relevant europeisk ordning för cybersäkerhetscertifiering som omfattar dessa produkter och en bedömning av de potentiella marknadseffekterna av den planerade obligatoriska certifieringen har utförts av kommissionen. Bedömningen bör beakta både utbuds- och efterfrågesidan, inbegripet huruvida det finns tillräcklig efterfrågan på de berörda produkterna med digitala element från både medlemsstaterna och användarna för att europeisk cybersäkerhetscertifiering ska krävas, samt de ändamål för vilka produkterna med digitala element är avsedda att användas, inbegripet det kritiska beroendet av dem hos väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555. Bedömningen bör också analysera de potentiella effekterna av den obligatoriska certifieringen på dessa produkters tillgänglighet på den inre marknaden och medlemsstaternas kapacitet och beredskap att genomföra de relevanta europeiska ordningarna för cybersäkerhetscertifiering.
- (47) Delegerade akter som kräver obligatorisk europeisk cybersäkerhetscertifiering bör fastställa de produkter med digitala element som har kärnfunktionen hos en kategori av kritiska produkter med digitala element som anges i denna förordning och som ska omfattas av obligatorisk certifiering, samt den assurancesnivå som krävs, som åtminstone bör vara "väsentlig". Den assurancesnivå som krävs bör stå i proportion till den nivå av cybersäkerhetsrisk som är förknippad med produkten med digitala element. Om produkten med digitala element till exempel har kärnfunktionen hos en kategori av kritiska produkter med digitala element som anges i denna förordning och är

⁽²⁹⁾ Kommissionens genomförandeförordning (EU) 2024/482 av den 31 januari 2024 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller antagande av den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC) (EUT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

avsedd för användning i en känslig eller kritisk miljö, såsom produkter avsedda för användning av väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555, får den kräva högsta assurancesnivå.

- (48) För att säkerställa ett gemensamt tillräckligt cybersäkerhetsskydd i unionen för produkter med digitala element som har kärnfunktionen hos en kategori av kritiska produkter med digitala element som anges i denna förordning, bör kommissionen också ges befogenhet att anta delegerade akter för att ändra denna förordning genom att lägga till eller stryka kategorier av kritiska produkter med digitala element, för vilka tillverkare skulle kunna åläggas att erhålla ett europeiskt cybersäkerhetscertifikat inom ramen för en europeisk ordning för cybersäkerhetscertifiering, enligt förordning (EU) 2019/881 för att visa överensstämmelse med denna förordning. En ny kategori av kritiska produkter med digitala element kan läggas till dessa kategorier om det finns ett kritiskt beroende av dem hos de väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555 eller om incidenter eller utnyttjade sårbarheter kan leda till avbrott i kritiska leveranskedjor. När kommissionen bedömer behovet av att lägga till eller stryka kategorier av kritiska produkter med digitala element genom en delegerad akt bör den kunna beakta huruvida medlemsstaterna på nationell nivå har identifierat produkter med digitala element som har en avgörande roll för resiliensen hos de väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555 och som i allt högre grad drabbas av cyberattacker i leveranskedjan, med potentiella allvarliga störande effekter. Dessutom bör kommissionen kunna beakta resultatet av den samordnade säkerhetsriskbedömning av kritiska leveranskedjor på unionsnivå som genomförts i enlighet med artikel 22 i direktiv (EU) 2022/2555.
- (49) Kommissionen bör se till att ett brett spektrum av berörda parter rådfrågas på ett strukturerat och regelbundet sätt vid utarbetandet av åtgärder för genomförandet av denna förordning. Detta bör särskilt vara fallet när kommissionen bedömer behovet av potentiella uppdateringar av förteckningarna över kategorier av viktiga eller kritiska produkter med digitala element, där relevanta tillverkare bör rådfrågas och deras synpunkter beaktas för att analysera cybersäkerhetsriskerna samt balansen mellan kostnader och fördelar med att beteckna sådana produktkategorier som viktiga eller kritiska.
- (50) Denna förordning behandlar cybersäkerhetsrisker på ett målinriktat sätt. Produkter med digitala element kan dock utgöra andra säkerhetsrisker som inte alltid rör cybersäkerheten men som kan vara en konsekvens av en säkerhetsöverträdelse. Dessa risker bör även fortsättningsvis regleras av annan relevant unionsharmoniseringslagstiftning än denna förordning. Om ingen annan del av unionsharmoniseringslagstiftningen än denna förordning är tillämplig bör de omfattas av Europaparlamentets och rådets förordning (EU) 2023/988⁽²¹⁾. Mot bakgrund av denna förordnings fokus och som en avvikelse från artikel 2.1 tredje stycket b i förordning (EU) 2023/988, bör kapitel III avsnitt 1, kapitel V och VII och kapitel IX–XI i förordning (EU) 2023/988 tillämpas på produkter med digitala element med avseende på säkerhetsrisker som inte omfattas av den här förordningen, om produkterna inte omfattas av särskilda krav enligt andra bestämmelser i annan unionsharmoniseringslagstiftning än den här förordningen i den mening som avses i artikel 3.27 i förordning (EU) 2023/988.
- (51) Produkter med digitala element som klassificeras som AI-system med hög risk enligt definitionen i artikel 6 i Europaparlamentets och rådets förordning (EU) 2024/1689⁽²²⁾ och som omfattas av den här förordningen bör uppfylla de väsentliga cybersäkerhetskrav som fastställs i den här förordningen. När sådana AI-system med hög risk uppfyller de väsentliga cybersäkerhetskrav som anges i den här förordningen bör de anses uppfylla de cybersäkerhetskrav som fastställs i artikel 15 i förordning (EU) 2024/1689 i den mån som dessa krav omfattas av en EU-försäkran om överensstämmelse som utfärdats enligt den här förordningen, eller delar av denna. För detta ändamål bör vid bedömningen av cybersäkerhetsriskerna i samband med en produkt med digitala element som klassificeras som ett AI-system med hög risk enligt förordning (EU) 2024/1689 under planerings-, utformnings-, utvecklings-, produktions-, leverans- och underhållsfaserna för en sådan produkt, i enlighet med den här förordningen, risker för ett AI-systems cyberresiliens beaktas när det gäller obehöriga tredje parter försök att ändra dess användning, beteende eller prestanda, inbegripet AI-specifika sårbarheter såsom dataförgiftning eller

⁽²¹⁾ Europaparlamentets och rådets förordning (EU) 2023/988 av den 10 maj 2023 om allmän produktsäkerhet, ändring av Europaparlamentets och rådets förordning (EU) nr 1025/2012 och Europaparlamentets och rådets direktiv (EU) 2020/1828 och om upphävande av Europaparlamentets och rådets direktiv 2001/95/EG och rådets direktiv 87/357/EEG (EUT L 135, 23.5.2023, s. 1).

⁽²²⁾ Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) (EUT L 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).

kontradiktoriska angrepp, samt, i relevanta fall, risker för grundläggande rättigheter, i enlighet med förordning (EU) 2024/1689. När det gäller de förfaranden för bedömning av överensstämmelse avseende väsentliga cybersäkerhetskrav för en produkt med digitala element som omfattas av den här förordningen och klassificeras som ett AI-system med hög risk, bör artikel 43 i förordning (EU) 2024/1689 tillämpas som regel i stället för relevanta bestämmelser i den här förordningen. Denna regel bör dock inte leda till att den nödvändiga assurancesnivån sänks för viktiga eller kritiska produkter med digitala element enligt den här förordningen. Med avvikelse från den regeln bör därför också AI-system med hög risk som omfattas av förordning (EU) 2024/1689 och som också kategoriseras som viktiga eller kritiska produkter med digitala element enligt den här förordningen, och på vilka förfarandet för bedömning av överensstämmelse baserat på intern kontroll enligt bilaga VI i förordning (EU) 2024/1689 är tillämpligt, omfattas av den här förordningens bestämmelser om förfarandena för bedömning av överensstämmelse i den mån som de väsentliga cybersäkerhetskrav som anges i den här förordningen berörs. När det gäller alla andra aspekter som omfattas av förordning (EU) 2024/1689, bör i sådana fall relevanta bestämmelser om bedömning av överensstämmelse baserad på intern kontroll vilka fastställs i bilaga VI till den förordningen tillämpas.

- (52) För att förbättra säkerheten för produkter med digitala element som släpps ut på den inre marknaden är det nödvändigt att fastställa väsentliga cybersäkerhetskrav som är tillämpliga på sådana produkter. Dessa väsentliga cybersäkerhetskrav bör inte påverka tillämpningen av samordnade säkerhetsriskbedömningar på unionsnivå av kritiska leveranskedjor som avses i artikel 22 i direktiv (EU) 2022/2555, som beaktar både tekniska och, när så är relevant, icke-tekniska riskfaktorer, såsom tredjelandets otillbörliga påverkan på leverantörer. De bör inte heller påverka medlemsstaternas rätt att fastställa ytterligare krav för att ta hänsyn till icke-tekniska faktorer för att säkerställa en hög resiliensnivå, inbegripet krav som definieras i kommissionens rekommendation (EU) 2019/534⁽²³⁾, den EU-samordnade riskbedömningen av cybersäkerhet i 5G-nät och EU-verktygsplådan för 5G-cybersäkerhet som överenskommit av samarbetsgruppen som inrättats enligt artikel 14 i direktiv (EU) 2022/2555.
- (53) Tillverkare av produkter som omfattas av Europaparlamentets och rådets förordning (EU) 2023/1230⁽²⁴⁾ och som också är produkter med digitala element enligt definitionen i den här förordningen bör uppfylla både de väsentliga cybersäkerhetskrav som fastställs i den här förordningen och de grundläggande hälso- och säkerhetskraven i förordning (EU) 2023/1230. De väsentliga cybersäkerhetskrav som anges i den här förordningen och vissa väsentliga krav som anges i förordning (EU) 2023/1230 skulle kunna hantera liknande cybersäkerhetsrisker. Överensstämmelse med de väsentliga cybersäkerhetskrav som anges i den här förordningen skulle därför kunna underlätta efterlevnaden av de grundläggande krav som även omfattar vissa cybersäkerhetsrisker enligt förordning (EU) 2023/1230, särskilt de som rör skydd mot korruption samt säkerhet och tillförlitlighet hos de kontrollsystem som anges i avsnitten 1.1.9 och 1.2.1 i bilaga III till den förordningen. Sådana synergier måste påvisas av tillverkaren, till exempel genom att i förekommande fall tillämpa harmoniserade standarder eller andra tekniska specifikationer som omfattar relevanta väsentliga cybersäkerhetskrav efter en riskbedömning som omfattar dessa cybersäkerhetsrisker. Tillverkaren bör också följa de tillämpliga förfaranden för bedömning av överensstämmelse som anges i den här förordningen och i förordning (EU) 2023/1230. Kommissionen och de europeiska standardiseringsorganisationerna bör i det förberedande arbetet för genomförandet av den här förordningen och förordning (EU) 2023/1230 och de därmed sammanhängande standardiseringsprocesserna främja enhetlighet i hur cybersäkerhetsriskerna ska bedömas och hur dessa risker ska omfattas av harmoniserade standarder med avseende på de relevanta väsentliga kraven. Kommissionen och de europeiska standardiseringsorganisationerna bör särskilt beakta den här förordningen vid förberedelserna och utarbetandet av harmoniserade standarder för att underlätta genomförandet av förordning (EU) 2023/1230, särskilt när det gäller cybersäkerhetsaspekter i samband med skydd mot förvanskning samt säkerhet och tillförlitlighet i kontrollsystemen som anges i avsnitten 1.1.9 och 1.2.1 i bilaga III till den förordningen. Kommissionen bör tillhandahålla vägledning för att stödja tillverkare som omfattas av den här förordningen och som också omfattas av förordning (EU) 2023/1230, särskilt för att underlätta påvisandet av överensstämmelse med relevanta grundläggande krav som fastställs i den här förordningen och förordning (EU) 2023/1230.
- (54) För att säkerställa att produkter med digitala element är säkra både när de släpps ut på marknaden och under den tid som produkten med digitala element förväntas vara i bruk, är det nödvändigt att fastställa väsentliga cybersäkerhetskrav för sårbarhetshantering och väsentliga cybersäkerhetskrav för egenskaperna hos produkter med digitala element. Tillverkarna bör uppfylla alla väsentliga cybersäkerhetskrav som rör sårbarhetshantering under

⁽²³⁾ Kommissionens rekommendation (EU) 2019/534 av den 26 mars 2019 om it-säkerhet i 5G-nät (EUT L 88, 29.3.2019, s. 42).

⁽²⁴⁾ Europaparlamentets och rådets förordning (EU) 2023/1230 av den 14 juni 2023 om maskiner och om upphävande av Europaparlamentets och rådets direktiv 2006/42/EG och rådets direktiv 73/361/EEG (EUT L 165, 29.6.2023, s. 1).

produktens hela stödperiod och de bör fastställa vilka andra väsentliga cybersäkerhetskrav på produkttegenskaper som är relevanta för den berörda typen av produkt med digitala element. Därför bör tillverkarna göra en bedömning av vilka cybersäkerhetsrisker som är förbundna med en produkt med digitala element, för att identifiera relevanta risker och relevanta väsentliga cybersäkerhetskrav för att tillhandahålla sina produkter med digitala element utan kända sårbarheter som kan utnyttjas och som kan påverka dessa produkters säkerhet och tillämpa lämpliga harmoniserade standarder, gemensamma specifikationer eller europeiska eller internationella standarder.

- (55) I de fall då vissa väsentliga cybersäkerhetskrav inte är tillämpliga på en produkt med digitala element ska tillverkaren inkludera en tydlig motivering till detta i bedömningen av cybersäkerhetsrisker inbegripet i den tekniska dokumentationen. Detta kan vara fallet om ett väsentligt cybersäkerhetskrav är oförenligt med beskaffenheten hos en produkt med digitala element. Till exempel kan det avsedda ändamålet med en produkt med digitala element kräva att tillverkaren följer allmänt erkända interoperabilitetsstandarder även om dess säkerhetsdetaljer inte längre anses vara den senaste tekniken. På samma sätt kräver annan unionsrätt att tillverkarna tillämpar särskilda interoperabilitetskrav. Om ett väsentligt cybersäkerhetskrav inte är tillämpligt på en produkt med digitala element, men tillverkaren har identifierat cybersäkerhetsrisker i samband med det väsentliga cybersäkerhetskravet, bör tillverkaren vidta åtgärder för att hantera dessa risker på andra sätt, till exempel genom att begränsa produktens avsedda ändamål till tillförlitliga miljöer eller genom att informera användarna om dessa risker.
- (56) En av de viktigaste åtgärderna som användarna ska vidta för att skydda sina produkter med digitala element från cyberattacker är att installera de senaste tillgängliga säkerhetsuppdateringarna så snart som möjligt. Tillverkarna bör därför utforma sina produkter och införa processer för att säkerställa att produkter med digitala element omfattar funktioner som möjliggör anmälan, distribution, nedladdning och installation av automatiska säkerhetsuppdateringar, särskilt när det gäller konsumentprodukter. De bör också ge möjlighet att godkänna nedladdning och installation av säkerhetsuppdateringar som ett sista steg. Användarna bör behålla möjligheten att avaktivera automatiska uppdateringar, med en tydlig och lättanvänd mekanism som stöds av tydliga instruktioner om hur användarna kan fransäga sig dem. De krav avseende automatiska uppdateringar som anges i en bilaga till denna förordning är inte tillämpliga på produkter med digitala element som främst är avsedda att integreras som komponenter i andra produkter. De är inte heller tillämpliga på produkter med digitala element för vilka användarna inte rimligen skulle förvänta sig automatiska uppdateringar, inbegripet produkter med digitala element som är avsedda att användas i IKT-nätverk för yrkesmässigt bruk, särskilt i kritiska miljöer och industrimiljöer där en automatisk uppdatering skulle kunna störa verksamheten. Oavsett om en produkt med digitala element är utformad för att få automatiska uppdateringar eller inte bör tillverkaren informera användarna om sårbarheter och göra säkerhetsuppdateringar tillgängliga utan dröjsmål. Om en produkt med digitala element har ett användargränssnitt eller liknande tekniska medel som möjliggör direkt interaktion med användarna bör tillverkaren använda sådana funktioner för att informera användarna om att deras produkt med digitala element har nått slutet av stödperioden. Anmälningar bör begränsas till vad som är nödvändigt för att säkerställa ett effektivt mottagande av denna information och bör inte ha en negativ inverkan på användarupplevelsen av produkten med digitala element.
- (57) För att förbättra insynen i processer för sårbarhetshantering och för att säkerställa att användarna inte är skyldiga att installera nya funktionsuppdateringar enbart i syfte att ta emot de senaste säkerhetsuppdateringarna, bör tillverkarna, när det är tekniskt möjligt, säkerställa att nya säkerhetsuppdateringar tillhandahålls separat från funktionsuppdateringar.
- (58) I det gemensamma meddelandet *Europeisk strategi för ekonomisk säkerhet* från kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik av den 20 juni 2023 anges att unionen måste maximera fördelarna med sin ekonomiska öppenhet och samtidigt minimera riskerna med ekonomiskt beroende av högriskleverantörer, genom en gemensam strategisk ram för unionens ekonomiska säkerhet. Beroenden av högriskleverantörer av produkter med digitala element kan utgöra en strategisk risk som måste hanteras på unionsnivå, särskilt om produkterna med digitala element är avsedda för användning av väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555. Sådana risker kan vara kopplade till, men inte begränsas till, den jurisdiktion som är tillämplig på tillverkaren, egenskaperna hos dess företagsägande och kopplingarna till kontrollen till en tredjelandsgovernment där den är etablerad, särskilt om ett land ägnar sig åt ekonomiskt spionage eller oansvarigt statligt beteende i cyberrymden och dess lagstiftning tillåter godtycklig tillgång till alla typer av företagsverksamhet eller uppgifter, inbegripet kommersiellt känsliga uppgifter, och kan införa skyldigheter för underrättelseändamål utan demokratiska kontroller och motvikt, tillsynsmekanismer, rättssäkerhet eller rätt att överklaga till en oberoende domstol. Vid fastställandet av betydelsen av en cybersäkerhetsrisk i den mening som avses i denna förordning bör kommissionen och marknadskontrollmyndigheterna, i enlighet med sina ansvarsområden enligt

denna förordning, också beakta icke-tekniska riskfaktorer, särskilt de som fastställts till följd av samordnade säkerhetsriskbedömningar av kritiska leveranskedjor på unionsnivå som genomförts i enlighet med artikel 22 i direktiv (EU) 2022/2555.

- (59) För att säkerställa säkerheten för produkter med digitala element efter deras utsläppande på marknaden bör tillverkarna fastställa stödperioder som bör återspegla den tid som produkten med digitala element förväntas vara i bruk. Vid fastställandet av en stödperiod bör en tillverkare särskilt ta hänsyn till rimliga förväntningar från användarna, produktens beskaffenhet samt relevant unionsrätt som fastställer livslängden för produkter med digitala element. Tillverkarna bör också kunna ta hänsyn till andra relevanta faktorer. Kriterierna bör tillämpas på ett sätt som säkerställer proportionalitet vid fastställandet av stödperioden. På begäran bör en tillverkare förse marknadskontrollmyndigheterna med den information som beaktades för att fastställa stödperioden för en produkt med digitala element.
- (60) Den stödperiod under vilken tillverkaren säkerställer en effektiv hantering av sårbarheter bör vara minst fem år, såvida inte livslängden för produkten med digitala element är kortare än fem år, och i sådana fall bör tillverkaren säkerställa sårbarhetshanteringen under den livslängden. Om den tid som produkten med digitala element rimligen förväntas vara i bruk är längre än fem år, vilket ofta är fallet för maskinvarukomponenter såsom moderkort eller mikroprocessorer, nätverksenheter såsom routrar, modem eller växlar samt programvara såsom operativsystem eller videoredigeringsverktyg, bör tillverkarna följaktligen säkerställa längre stödperioder. I synnerhet produkter med digitala element som är avsedda att användas i industriella miljöer, såsom industriella styrsystem, används ofta under betydligt längre perioder. En tillverkare bör kunna fastställa en stödperiod på mindre än fem år endast om detta är motiverat på grund av beskaffenheten av den berörda produkten med digitala element och om produkten förväntas användas i mindre än fem år, och i sådana fall bör stödperioden motsvara den förväntade användningstiden. Exempelvis skulle livslängden för en kontaktspårningsapplikation som är avsedd att användas under en pandemi kunna begränsas till pandemins varaktighet. Dessutom kan vissa programvaruapplikationer av naturliga skäl endast göras tillgängliga på grundval av en abonnemangsmodell, särskilt om applikationen inte är tillgänglig för användaren och följaktligen inte längre används när abonnemanget löper ut.
- (61) När produkter med digitala element når slutet av sina stödperioder bör tillverkarna, för att säkerställa att sårbarheter kan hanteras efter stödperiodens slut, överväga att frigöra källkoden för sådana produkter med digitala element, antingen till andra företag som åtar sig att utvidga tillhandahållandet av tjänster för sårbarhetshantering, eller till allmänheten. Om tillverkare frigör källkoden till andra företag bör de kunna skydda äganderätten till produkten med digitala element och förhindra att källkoden sprids till allmänheten, till exempel genom avtalsarrangemang.
- (62) För att säkerställa att tillverkare i hela unionen fastställer liknande stödperioder för jämförbara produkter med digitala element bör Adco-gruppen offentliggöra statistik över de genomsnittliga stödperioder som fastställs av tillverkarna för kategorier av produkter med digitala element och utfärda riktlinjer som anger lämpliga stödperioder för sådana kategorier. För att säkerställa ett harmoniserat tillvägagångssätt på hela den inre marknaden bör kommissionen dessutom kunna anta delegerade akter för att specificera minsta tillåtna stödperioder för specifika produktkategorier i de fall då de uppgifter som tillhandahålls av marknadskontrollmyndigheterna tyder på att de stödperioder som fastställs av tillverkarna systematiskt inte stämmer överens med kriterierna för att fastställa stödperioderna enligt denna förordning, eller att tillverkare i olika medlemsstater på ett omotiverat sätt fastställer olika stödperioder.
- (63) Tillverkarna bör inrätta en gemensam kontaktpunkt som gör det möjligt för användarna att enkelt kommunicera med dem, inbegripet i syfte att rapportera och ta emot information om sårbarheter hos produkten med digitala element. De bör göra den gemensamma kontaktpunkten lättillgänglig för användarna och tydligt ange dess tillgänglighet och hålla denna information uppdaterad. Om tillverkarna väljer att erbjuda automatiserade verktyg, t. ex. chattbotar, bör de också erbjuda ett telefonnummer eller andra digitala kontaktmöjligheter, såsom en e-postadress eller ett kontaktformulär. Den gemensamma kontaktpunkten bör inte uteslutande förlita sig på automatiserade verktyg.
- (64) Tillverkarna bör tillhandahålla sina produkter med digitala element på marknaden med en säker standardkonfiguration och tillhandahålla användarna säkerhetsuppdateringar utan kostnad. Tillverkarna bör endast kunna avvika från dessa väsentliga cybersäkerhetskrav när det gäller skräddarsydda produkter som är anpassade för ett visst ändamål och för en viss företagsanvändare och om både tillverkaren och användaren uttryckligen har samtyckt till en annan uppsättning avtalsvillkor.

SV

EUT L, 20.11.2024

- (65) Tillverkarna bör samtidigt, via den gemensamma rapporteringsplattformen, anmäla aktivt utnyttjade sårbarheter i produkter med digitala element samt allvarliga incidenter som påverkar dessa produkters säkerhet till både den enhet för hantering av it-säkerhetsincidenter (CSIRT-enhet) som utsetts till samordnare och till Enisa. Anmälningarna bör lämnas in med hjälp av slutpunkten för elektronisk anmälan hos en CSIRT-enhet som utsetts till samordnare och bör samtidigt vara tillgängliga för Enisa.
- (66) Tillverkarna bör anmäla aktivt utnyttjade sårbarheter för att säkerställa att de CSIRT-enheter som utsetts till samordnare, och Enisa, har en adekvat överblick över sådana sårbarheter och förses med den information som de behöver för att utföra sina uppgifter som anges i direktiv (EU) 2022/2555 och höja den allmänna cybersäkerhetsnivån för de väsentliga och viktiga entiteter som avses i artikel 3 i det direktivet, och för att säkerställa att marknadskontrollmyndigheterna fungerar effektivt. I och med att de flesta produkter med digitala element saluförs på hela den inre marknaden bör varje utnyttjad sårbarhet i en produkt med digitala element anses som ett hot mot en fungerande inre marknad. Enisa bör, i samförstånd med tillverkaren, meddela åtgärdade sårbarheter till den europeiska sårbarhetsdatabas som inrättats enligt artikel 12.2 i direktiv (EU) 2022/2555. Den europeiska sårbarhetsdatabasen kommer att hjälpa tillverkarna att upptäcka kända sårbarheter i deras produkter som kan utnyttjas, för att säkerställa att säkra produkter tillhandahålls på marknaden.
- (67) Tillverkarna bör också anmäla alla allvarliga incidenter som påverkar säkerheten för produkter med digitala element till den CSIRT-enhet som utsetts till samordnare och Enisa. För att säkerställa att användarna kan reagera snabbt på allvarliga incidenter som påverkar säkerheten för deras produkter med digitala element, bör tillverkarna också underrätta sina användare om alla sådana incidenter och, om tillämpligt, om eventuella korrigeringande åtgärder som användarna kan vidta för att begränsa konsekvenserna av incidenten, exempelvis genom att offentliggöra relevant information på sina webbplatser eller, om tillverkaren kan kontakta användarna och det är motiverat med tanke på cybersäkerhetsriskerna, genom att vända sig direkt till användarna.
- (68) Aktivt utnyttjade sårbarheter rör fall där en tillverkare fastställer att en säkerhetsöverträdelse som påverkar dess användare eller någon annan fysisk eller juridisk person har orsakats av en fientlig aktör som utnyttjar en brist i en av de produkter med digitala element som tillverkaren tillhandahåller på marknaden. Exempel på sådana sårbarheter skulle kunna vara svagheter i en produkts identifierings- och autentiseringsfunktioner. Sårbarheter som upptäcks utan ont uppsåt för att i god tro testa, utreda, korrigera eller delge information i syfte att stödja systemägarens och dess användares säkerhet eller trygghet bör inte omfattas av kravet på obligatorisk anmälan. Allvarliga incidenter som påverkar säkerheten för produkten med digitala element avser å andra sidan situationer där en cybersäkerhetsincident påverkar tillverkarens utvecklings-, produktions- eller underhållsprocesser på ett sådant sätt att det skulle kunna leda till en ökad cybersäkerhetsrisk för användare eller andra personer. En sådan allvarlig incident skulle kunna vara en situation då en angripare har lyckats införa en skadlig kod i den kanal genom vilken tillverkaren släpper säkerhetsuppdateringar till användarna.
- (69) För att säkerställa att anmälningar snabbt kan spridas till alla relevanta CSIRT-enheter som utsetts till samordnare och för att tillverkare ska kunna lämna in en enda anmälan i varje skede av anmälningsprocessen, bör Enisa inrätta en gemensam rapporteringsplattform med nationella slutpunkter för elektronisk anmälan. Den dagliga driften av den gemensamma rapporteringsplattformen bör skötas och upprätthållas av Enisa. De CSIRT-enheter som utsetts till samordnare bör informera sina respektive marknadskontrollmyndigheter om anmälda sårbarheter eller incidenter. Den gemensamma rapporteringsplattformen bör utformas på ett sådant sätt att den säkerställer konfidentialitet för anmälningar, särskilt när det gäller sårbarheter för vilka en säkerhetsuppdatering ännu inte är tillgänglig. Enisa bör dessutom införa förfaranden för att hantera information på ett säkert och konfidentiellt sätt. På grundval av sin insamlade information bör Enisa vartannat år utarbeta en teknisk rapport om nya trender i fråga om cybersäkerhetsrisker i produkter med digitala element, och lämna den till samarbetsgruppen enligt artikel 14 i direktiv (EU) 2022/2555.
- (70) Under exceptionella omständigheter, och särskilt på begäran av tillverkaren, bör den CSIRT-enhet som utsetts till samordnare och som först tar emot anmälan kunna besluta att skjuta upp spridningen av den till de andra relevanta CSIRT-enheter som utsetts till samordnare via den gemensamma rapporteringsplattformen, om detta kan motiveras på grundval av cybersäkerhetsrelaterade skäl och under en tidsperiod som är absolut nödvändig. Den CSIRT-enhet som utsetts till samordnare bör omedelbart informera Enisa om beslutet att skjuta upp spridningen och skälen till detta samt när den avser att återuppta spridningen av anmälan. Kommissionen bör genom en delegerad akt utarbeta specifikationer om villkoren för när cybersäkerhetsrelaterade skäl kan tillämpas och bör samarbeta med det CSIRT-nätverk som inrättats enligt artikel 15 i direktiv (EU) 2022/2555, och med Enisa när det gäller att utarbeta utkastet till delegerad akt. Exempel på cybersäkerhetsrelaterade skäl är en pågående samordnad delgivning av information om sårbarheter eller situationer då en tillverkare snabbt förväntas tillhandahålla en riskreducerande åtgärd och då cybersäkerhetsriskerna med en omedelbar spridning via den gemensamma rapporteringsplattformen väger tyngre än fördelarna. På begäran av den CSIRT-enhet som utsetts till samordnare bör Enisa kunna stödja denna

CSIRT-enhet i tillämpningen av cybersäkerhetsrelaterade skäl när det gäller att skjuta upp spridningen av anmälan på grundval av den information Enisa har mottagit från den CSIRT-enheten om beslutet att undanhålla en anmälan utifrån dessa cybersäkerhetsrelaterade skäl. Under särskilt exceptionella omständigheter bör Enisa dessutom inte få alla uppgifter som rör en anmälan om en aktivt utnyttjad sårbarhet samtidigt. Detta skulle vara fallet om tillverkaren i sin anmälan anger att den anmälda sårbarheten aktivt har utnyttjats av en fiendlig aktör och att den, enligt tillgänglig information, inte har utnyttjats i någon annan medlemsstat än den där CSIRT-enheten har utsetts till samordnare och till vilken tillverkaren har anmält sårbarheten, när all omedelbar fortsatt spridning av den anmälda sårbarheten sannolikt skulle leda till tillhandahållande av information vars utlämnande skulle strida mot den medlemsstatens väsentliga intressen, eller när den anmälda sårbarheten utgör en överhängande hög cybersäkerhetsrisk till följd av den fortsatta spridningen. I sådana fall kommer Enisa endast att få samtidig tillgång till information om att tillverkaren har gjort en anmälan och till generell information om den berörda produkten med digitala element, information om den allmänna karaktären av utnyttjandet och information om att dessa säkerhetsskäl har angetts av tillverkaren och att det fullständiga innehållet i anmälan därför undanhålls. Den fullständiga anmälan bör sedan göras tillgänglig för Enisa och andra relevanta CSIRT-enheter som utsetts till samordnare när den CSIRT-enhet som utsetts till samordnare och som först tar emot anmälan konstaterar att dessa säkerhetsskäl, som utgör ovanligt exceptionella omständigheter enligt denna förordning, inte längre föreligger. Om Enisa, på grundval av den tillgängliga informationen, anser att det finns en systemrisk som påverkar säkerheten på den inre marknaden bör Enisa rekommendera den mottagande CSIRT-enheten att sprida den fullständiga anmälan till de andra CSIRT-enheter som utsetts till samordnare och till Enisa själv.

- (71) När tillverkarna anmäler en aktivt utnyttjad sårbarhet eller en allvarlig incident som påverkar säkerheten för produkten med digitala element bör de ange hur känslig de anser att den anmälda informationen är. Den CSIRT-enhet som utsetts till samordnare och som först tar emot anmälan bör ta hänsyn till denna information när den bedömer huruvida anmälan ger upphov till exceptionella omständigheter som motiverar att spridningen av anmälan till de andra relevanta CSIRT-enheter som utsetts till samordnare på grundval av motiverade cybersäkerhetsrelaterade skäl skjuts upp. Den bör också ta hänsyn till denna information när den bedömer huruvida anmälan om en aktivt utnyttjad sårbarhet ger upphov till ovanligt exceptionella omständigheter som motiverar att den fullständiga anmälan inte samtidigt görs tillgänglig för Enisa. Slutligen bör CSIRT-enheter som utsetts till samordnare kunna beakta denna information när de fastställer lämpliga åtgärder för att begränsa de risker som härrör från sådana sårbarheter och incidenter.
- (72) För att förenkla rapporteringen av den information som krävs enligt denna förordning, med beaktande av andra kompletterande rapporteringskrav som fastställs i unionsrätten, såsom förordning (EU) 2016/679, Europaparlamentets och rådets förordning (EU) 2022/2554⁽²⁵⁾, Europaparlamentets och rådets direktiv 2002/58/EG⁽²⁶⁾ och direktiv (EU) 2022/2555, samt för att minska den administrativa bördan för entiteterna, uppmuntras medlemsstaterna att överväga att tillhandahålla gemensamma kontaktpunkter på nationell nivå för sådana rapporteringskrav. Användningen av sådana nationella gemensamma kontaktpunkter för att rapportera säkerhetsincidenter enligt förordning (EU) 2016/679 och direktiv 2002/58/EG bör inte påverka tillämpningen av bestämmelserna i förordning (EU) 2016/679 och direktiv 2002/58/EG, särskilt de som rör oberoendet för de myndigheter som avses i dessa. Vid inrättandet av den gemensamma rapporteringsplattform som avses i den här förordningen bör Enisa beakta möjligheten att integrera de nationella slutpunkter för elektronisk anmälan som avses i den här förordningen i nationella gemensamma kontaktpunkter som också kan integrera andra anmälningar som krävs enligt unionsrätten.
- (73) Vid inrättandet av den gemensamma rapporteringsplattform som avses i denna förordning och för att dra nytta av tidigare erfarenheter bör Enisa samråda med unionens andra institutioner eller byråer som förvaltar plattformar eller databaser som omfattas av stränga säkerhetskrav, såsom Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-LISA). Enisa bör också analysera eventuell komplementaritet med den europeiska sårbarhetsdatabas som inrättats enligt artikel 12.2 i direktiv (EU) 2022/2555.
- (74) Tillverkare och andra fysiska och juridiska personer bör på frivillig basis, till en CSIRT-enhet som utsetts till samordnare eller Enisa, kunna anmäla eventuella sårbarheter i en produkt med digitala element, cyberhot som skulle

⁽²⁵⁾ Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1).

⁽²⁶⁾ Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (EGT L 201, 31.7.2002, s. 37).

kunna påverka riskprofilen för en produkt med digitala element, eventuella incidenter som påverkar säkerheten för produkten med digitala element samt tillbud som skulle ha kunnat leda till en sådan incident.

- (75) Medlemsstaterna bör sträva efter att i största möjliga utsträckning ta itu med de utmaningar som sårbarhetsforskare ställs inför, inbegripet deras potentiella utsatthet för straffrättsligt ansvar, i enlighet med nationell rätt. Med tanke på att fysiska och juridiska personer som forskar om sårbarheter skulle kunna riskera straff- och civilrättsligt ansvar i vissa medlemsstater uppmantras medlemsstaterna att anta riktlinjer för icke-lagföring av forskare inom informationssäkerhet och befrielse från civilrättsligt ansvar för deras verksamhet.
- (76) Tillverkare av produkter med digitala element bör införa samordnade policyer för information om sårbarheter för att underlätta individers eller entiteters rapportering av sårbarheter, antingen direkt till tillverkaren eller indirekt, och anonymt om så begärs, via CSIRT-enheter som utsetts till samordnare för att åstadkomma en samordnad delgivning av information om sårbarheter i enlighet med artikel 12.1 i direktiv (EU) 2022/2555. Tillverkarnas samordnade policy för offentliggörande av sårbarheter bör specificera en strukturerad process där sårbarheter rapporteras till en tillverkare på ett sådant sätt att tillverkaren kan diagnostisera och åtgärda dessa sårbarheter innan mer detaljerad sårbarhetsinformation lämnas ut till tredje part eller till allmänheten. Tillverkarna bör också överväga att offentliggöra sin säkerhetspolicy i maskinläsbart format. I och med att information om sårbarheter som kan utnyttjas hos allmänt använda produkter med digitala element kan säljas till höga priser på den svarta marknaden bör tillverkare av sådana produkter som ett led i sina samordnade policyer för information om sårbarheter kunna använda program för att ge incitament till rapportering av sårbarheter genom att säkerställa att individer eller entiteter får erkännande och ersättning för sina insatser. Detta avser så kallade buggbelöningsprogram.
- (77) För att underlätta sårbarhetsanalys bör tillverkarna identifiera och dokumentera de komponenter som ingår i produkter med digitala element, inbegripet genom att utarbeta en programvaruförteckning. En programvaruförteckning kan förse dem som tillverkar, köper och driver programvara med information som förbättrar deras förståelse av leveranskedjan, vilket har många fördelar, framför allt att det hjälper tillverkare och användare att spåra kända nya sårbarheter och cybersäkerhetsrisker. Det är särskilt viktigt att tillverkarna säkerställer att deras produkter med digitala element inte innehåller sårbara komponenter som utvecklats av tredje part. Tillverkarna bör inte vara skyldiga att offentliggöra programvaruförteckningen.
- (78) Ett företag som bedriver verksamhet online inom ramen för de nya komplexa affärsmodeller som hänger samman med onlineförsäljning kan tillhandahålla en rad olika tjänster. Beroende på arten av de tjänster som tillhandahålls i samband med en viss produkt med digitala element kan samma entitet omfattas av olika kategorier av affärsmodeller eller ekonomiska aktörer. Om en entitet tillhandahåller endast onlinebaserade förmedlingstjänster för en viss produkt med digitala element och endast är leverantör av en onlinemarknadsplats, enligt definitionen i artikel 3.14 i förordning (EU) 2023/988, kan den inte kategoriseras som någon typ av ekonomisk aktör enligt definitionen i den här förordningen. Om samma entitet är leverantör av en onlinemarknadsplats och även agerar som ekonomisk aktör enligt definitionen i den här förordningen vid försäljningen av särskilda produkter med digitala element, bör den omfattas av de skyldigheter som fastställs i den här förordningen för den typen av ekonomisk aktör. Om till exempel leverantören av en onlinemarknadsplats också distribuerar en produkt med digitala element betraktas denna leverantör, med avseende på försäljningen av den produkten, som distributör. Och även när entiteten i fråga säljer sina egna märkesprodukter med digitala element betraktas den som tillverkare och måste därmed följa de tillämpliga kraven för tillverkare. Vissa entiteter kan också betraktas som leverantörer av distributionstjänster enligt definitionen i artikel 3.11 i Europaparlamentets och rådets förordning (EU) 2019/1020⁽⁷⁾ om de erbjuder sådana tjänster. I sådana fall måste en bedömning göras i varje enskilt fall. Med tanke på den framträdande roll som onlinemarknadsplatser har när det gäller att möjliggöra elektronisk handel bör de sträva efter att samarbeta med medlemsstaternas marknadskontrollmyndigheter för att hjälpa till att säkerställa att produkter med digitala element som köps via onlinemarknadsplatser uppfyller de cybersäkerhetskrav som fastställs i den här förordningen.
- (79) För att underlätta bedömningen av överensstämmelse med de krav som fastställs i denna förordning bör det finnas en presumtion om överensstämmelse för produkter med digitala element som överensstämmer med harmoniserade standarder som omsätter de väsentliga cybersäkerhetskrav som anges i denna förordning till detaljerade tekniska

⁽⁷⁾ Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011 (EUT L 169, 25.6.2019, s. 1).

specifikationer och som antas i enlighet med Europaparlamentets och rådets förordning (EU) nr 1025/2012 ⁽²⁶⁾. Den förordningen fastställer ett förfarande för invändningar mot harmoniserade standarder som inte helt uppfyller kraven som anges i den här förordningen. Standardiseringsförfarandet bör säkerställa en balanserad representation av intressen och ett aktivt deltagande av berörda parter i det civila samhället, inbegripet konsumentorganisationer. Internationella standarder som stämmer överens med den nivå av cybersäkerhetsskydd som eftersträvas genom de väsentliga cybersäkerhetskrav som fastställs i den här förordningen bör också beaktas, för att underlätta utvecklingen av harmoniserade standarder och genomförandet av den här förordningen samt för att underlätta efterlevnaden för företag, särskilt mikroföretag samt små och medelstora företag och företag som är verksamma på global nivå.

- (80) En snabb utveckling av harmoniserade standarder under övergångsperioden för tillämpningen av denna förordning och tillgängligheten före den dag då denna förordning börjar tillämpas kommer att vara särskilt viktigt för ett effektivt genomförande av den. Detta gäller särskilt viktiga produkter med digitala element som omfattas av klass I. Tillgängliga harmoniserade standarder kommer att göra det möjligt för tillverkarna av sådana produkter att bedöma överensstämmelsen via förfarandet för intern kontroll, och flaskhalsar och förseningar kan därför undvikas när organ för bedömning av överensstämmelse utför sitt arbete.
- (81) Genom förordning (EU) 2019/881 inrättas en frivillig europeisk ram för cybersäkerhetscertifiering av IKT-produkter, IKT-processer och IKT-tjänster. De europeiska ordningarna för cybersäkerhetscertifiering förser användarna med en gemensam tillförlitlig ram för användning av produkter med digitala element vilka omfattas av den här förordningens tillämpningsområde. Den här förordningen bör följaktligen skapa synergier med förordning (EU) 2019/881. För att underlätta bedömningen av överensstämmelse med kraven i den här förordningen, när det gäller produkter med digitala element som är certifierade eller för vilka en försäkras om överensstämmelse har utfärdats inom en europeisk ordning för cybersäkerhet enligt förordning (EU) 2019/881 som har identifierats av kommissionen i en genomförandeakt, bör det finnas en presumtion om överensstämmelse med de väsentliga cybersäkerhetskraven i den här förordningen i den mån som det europeiska cybersäkerhetscertifikatet eller försäkras om överensstämmelse – eller delar av dessa – täcker dessa krav. Behovet av nya europeiska ordningar för cybersäkerhetscertifiering av produkter med digitala element bör bedömas i ljuset av den här förordningen, inbegripet när unionens löpande arbetsprogram utarbetas i enlighet med förordning (EU) 2019/881. Om det behövs ett nytt system som omfattar produkter med digitala element, bland annat för att underlätta efterlevnaden av den här förordningen, kan kommissionen begära att Enisa utarbetar förslag till certifieringsordning i enlighet med artikel 48 i förordning (EU) 2019/881. Sådana framtida europeiska ordningar för cybersäkerhet som omfattar produkter med digitala element bör beakta de väsentliga cybersäkerhetskrav och förfaranden för bedömning av överensstämmelse som fastställs i den här förordningen och främja efterlevnaden av den här förordningen. För europeiska ordningar för cybersäkerhetscertifiering som träder i kraft innan den här förordningen träder i kraft kan ytterligare specifikationer behövas om detaljerade aspekter av hur en presumtion om överensstämmelse kan tillämpas. Kommissionen bör, genom delegerade akter, ha befogenhet att specificera på vilka villkor de europeiska ordningarna för cybersäkerhetscertifiering kan användas för att visa överensstämmelse med de väsentliga cybersäkerhetskrav som fastställs i den här förordningen. För att undvika onödiga administrativa bördor bör det inte finnas någon skyldighet för tillverkarna att genomföra en tredjepartsbedömning av överensstämmelse i enlighet med den här förordningen för motsvarande krav om ett europeiskt cybersäkerhetscertifikat har utfärdats enligt sådana europeiska ordningar för cybersäkerhetscertifiering, på åtminstone assuransnivån "betydande".
- (82) Vid ikraftträdandet av genomförandeförordning (EU) 2024/482 som avser produkter som omfattas av den här förordningens tillämpningsområde, såsom säkerhetsmoduler i maskinvara och mikroprocessorer, bör kommissionen genom en delegerad akt kunna specificera hur EUCC ger en presumtion om överensstämmelse med de väsentliga cybersäkerhetskrav som anges i den här förordningen eller delar av dessa. En sådan delegerad akt får dessutom specificera hur ett certifikat som utfärdas inom ramen för EUCC befriar tillverkaren från skyldigheten att genomföra en tredjepartsbedömning av överensstämmelse som krävs enligt den här förordningen för de motsvarande kraven.
- (83) Den nuvarande europeiska standardiseringsramen, som bygger på de principer enligt den nya metoden som fastställs i rådets resolution av den 7 maj 1985 om en ny metod för teknisk harmonisering och standarder och på förordning (EU) nr 1025/2012, utgör automatiskt ramen för utarbetande av standarder som föreskriver en presumtion om överensstämmelse med de relevanta väsentliga cybersäkerhetskraven i den här förordningen. Europeiska standarder bör vara marknadsdrivna, ta hänsyn till allmänintresset och de politiska mål som tydligt anges i kommissionens begäran till en eller flera europeiska standardiseringsorganisationer att utarbeta harmoniserade standarder inom en fastställd tidsfrist, och bör bygga på samförstånd. I avsaknad av relevanta hänvisningar till harmoniserade standarder

⁽²⁶⁾ Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut nr 1673/2006/EG (EUT L 316, 14.11.2012, s. 12).

bör kommissionen dock kunna anta genomförandeakter för att fastställa gemensamma specifikationer för de väsentliga cybersäkerhetskrav som anges i den här förordningen, förutsatt att den på lämpligt sätt respekterar de europeiska standardiseringsorganisationernas roll och funktioner, som en exceptionell reservlösning för att underlätta tillverkarens skyldighet att uppfylla dessa väsentliga cybersäkerhetskrav, om standardiseringsprocessen blockerats eller om fastställandet av lämpliga harmoniserade standarder försenas. Om en sådan försening beror på den tekniska komplexiteten hos standarden i fråga bör kommissionen beakta detta innan den överväger att fastställa gemensamma specifikationer.

- (84) I syfte att så effektivt som möjligt fastställa gemensamma specifikationer som omfattar de väsentliga cybersäkerhetskrav som fastställs i denna förordning bör kommissionen involvera berörda parter i processen.
- (85) *Rimlig tid* avser, när det gäller offentliggörandet av en hänvisning till harmoniserade standarder i *Europeiska unionens officiella tidning* i enlighet med förordning (EU) nr 1025/2012, en period under vilken offentliggörandet i *Europeiska unionens officiella tidning* av hänvisningen till standarden, rättelsen eller ändringen av den förväntas och den bör inte överstiga ett år efter den tidsfrist för utarbetande av en europeisk standard som fastställs i enlighet med förordning (EU) nr 1025/2012.
- (86) För att underlätta bedömningen av överensstämmelse med de väsentliga cybersäkerhetskrav som anges i denna förordning bör det finnas en presumption om överensstämmelse för produkter med digitala element som överensstämmer med de gemensamma specifikationer som antas av kommissionen enligt denna förordning i syfte att formulera detaljerade tekniska specifikationer av dessa krav.
- (87) Tillämpningen av harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering, som antagits enligt förordning (EU) 2019/881 och som ger presumption om överensstämmelse i förhållande till de väsentliga cybersäkerhetskrav som är tillämpliga på produkter med digitala element, kommer att underlätta tillverkarnas bedömning av överensstämmelse. Om tillverkaren väljer att inte tillämpa sådana metoder på vissa krav måste tillverkaren i sin tekniska dokumentation ange hur överensstämmelse i så fall uppnås. Tillämpningen av harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering, som antagits enligt förordning (EU) 2019/881 och som ger presumption om överensstämmelse från tillverkarna, skulle dessutom göra det lättare för marknadskontrollmyndigheterna att kontrollera att produkter med digitala element överensstämmer med kraven. Därför uppmuntras tillverkare av produkter med digitala element att tillämpa sådana harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering.
- (88) Tillverkarna bör utarbeta en EU-försäkrans om överensstämmelse för att tillhandahålla den information som krävs enligt denna förordning vad gäller produkter med digitala elements överensstämmelse med de väsentliga cybersäkerhetskraven i denna förordning och, om tillämpligt, med andra relevanta bestämmelser i unionsharmoniseringslagstiftning som omfattar produkten med digitala element. Tillverkarna kan också åläggas att upprätta en EU-försäkrans om överensstämmelse genom andra unionsrättsakter. För att säkerställa effektiv tillgång till information för marknadskontrolländamål bör en enda EU-försäkrans om överensstämmelse upprättas med avseende på överensstämmelsen med alla berörda unionsrättsakter. För att minska den administrativa bördan för ekonomiska aktörer bör denna enda EU-försäkrans om överensstämmelse kunna utgöras av dokumentation bestående av enskilda relevanta försäkringar om överensstämmelse.
- (89) CE-märkningen visar att en produkt uppfyller kraven och utgör det synliga resultatet av en hel process, som omfattar en bedömning av överensstämmelse i vid bemärkelse. De allmänna principerna för CE-märkning fastställs i Europaparlamentets och rådets förordning (EG) nr 765/2008⁽²⁹⁾. Bestämmelser för hur CE-märkningen ska fästas på produkter med digitala element bör fastställas i den här förordningen. CE-märkningen bör vara den enda märkning som garanterar överensstämmelse med kraven i den här förordningen för produkter med digitala element.
- (90) Det är nödvändigt att föreskriva förfaranden för bedömning av överensstämmelse, för att de ekonomiska aktörerna ska kunna visa överensstämmelse med de väsentliga cybersäkerhetskrav som anges i denna förordning och marknadskontrollmyndigheterna ska kunna säkerställa att de produkter med digitala element som tillhandahålls på marknaden uppfyller dessa krav. Genom Europaparlamentets och rådets beslut nr 768/2008/EG⁽³⁰⁾ fastställs

⁽²⁹⁾ Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30).

⁽³⁰⁾ Europaparlamentets och rådets beslut nr 768/2008/EG av den 9 juli 2008 om en gemensam ram för saluföring av produkter och upphävande av rådets beslut 93/465/EEG (EUT L 218, 13.8.2008, s. 82).

moduler för bedömning av överensstämmelse som står i proportion till risknivån och den säkerhetsnivå som krävs. För att säkerställa enhetlighet mellan olika sektorer och undvika ad hoc-varianter bör förfarandena för bedömning av överensstämmelse för att kontrollera överensstämmelse med de väsentliga cybersäkerhetskraven i denna förordning för produkter med digitala element baseras på dessa moduler. Förfarandena för bedömning av överensstämmelse bör omfatta granskning och kontroll av både produkten och processrelaterade krav som omfattar hela livscykeln för produkter med digitala element, inbegripet planering, utformning, utveckling eller produktion, testning och underhåll av produkten med digitala element.

- (91) Bedömningen av överensstämmelse för produkter med digitala element som inte förtecknas som viktiga eller kritiska produkter med digitala element i denna förordning kan utföras av tillverkaren på eget ansvar i enlighet med förfarandet för intern kontroll baserat på modul A i beslut nr 768/2008/EG i enlighet med denna förordning. Detta är också tillämpligt i fall där en tillverkare väljer att delvis eller inte alls tillämpa en tillämplig harmoniserad standard, gemensam specifikation eller en tillämplig europeisk ordning för cybersäkerhetscertifiering. Tillverkaren har även fortsättningsvis flexibilitet att välja ett striktare förfarande för bedömning av överensstämmelse som involverar tredje part. Inom ramen för det interna kontrollförfarandet för bedömning av överensstämmelse säkerställer och försäkrar tillverkaren på eget ansvar att produkten med digitala element och tillverkarens processer uppfyller de tillämpliga väsentliga cybersäkerhetskrav som fastställs i denna förordning. Om en viktig produkt med digitala element omfattas av klass I bör ytterligare kvalitetssäkring krävas för att visa överensstämmelsen med de väsentliga cybersäkerhetskraven i denna förordning. Tillverkaren bör tillämpa harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering antagna enligt förordning (EU) 2019/881 vilka har identifierats av kommissionen i en genomförandeakt, om den vill utföra bedömningen av överensstämmelse på eget ansvar (modul A). Om tillverkaren inte använder sådana harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering bör tillverkaren genomgå bedömning av överensstämmelse med deltagande av tredje part (baserat på modul B och C eller H). Med beaktande av den administrativa bördan för tillverkare och det faktum att cybersäkerheten har stor betydelse i utformnings- och utvecklingsfaserna för materiella och immateriella produkter med digitala element, har förfaranden för bedömning av överensstämmelse som baseras på modul B och C eller modul H i beslut nr 768/2008/EG valts som mest lämpliga för en proportionell och ändamålsenlig bedömning av överensstämmelse för viktiga produkter med digitala element. Tillverkare som genomför en tredjepartsbedömning av överensstämmelse kan välja det förförande som bäst passar den egna utformnings- och produktionsprocessen. Med tanke på de allt större cybersäkerhetsrisker som är förbundna med användningen av viktiga produkter med digitala element som omfattas av klass II bör bedömningen av överensstämmelse alltid involvera en tredje part, även om produkten helt eller delvis överensstämmer med harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering. Tillverkare av viktiga produkter med digitala element, vilka kategoriseras som programvara med fri och öppen källkod, bör kunna följa förfarandet för intern kontroll baserat på modul A, förutsatt att de gör den tekniska dokumentationen tillgänglig för allmänheten.
- (92) Medan skapandet av materiella produkter med digitala element vanligtvis innebär att tillverkaren måste göra stora ansträngningar under hela utformnings-, utvecklings- och produktionsfaserna, fokuserar skapandet av produkter med digitala element i form av programvara nästan uteslutande på utformning och utveckling, medan produktionsfasen är mindre framträdande. I många fall måste dock programvaruprodukter ändå kompileras, byggas, förpackas, göras tillgängliga för nedladdning eller kopieras till fysiska medier innan de släpps ut på marknaden. Dessa aktiviteter bör anses vara aktiviteter som motsvarar produktion vid tillämpningen av relevanta moduler för bedömning av överensstämmelse för att kontrollera överensstämmelsen med de väsentliga cybersäkerhetskrav som anges i denna förordning under hela utformnings-, utvecklings- och produktionsfaserna för produkter med digitala element.
- (93) När det gäller mikroföretag och små företag bör, för att säkerställa proportionalitet, de administrativa kostnaderna minskas utan att påverka nivån av cybersäkerhetsskydd för produkter med digitala element som omfattas av denna förordnings tillämpningsområde, eller tillverkarnas lika spelregler. Det är därför lämpligt att kommissionen skapar ett förenklat formulär för teknisk dokumentation med inriktning på mikroföretags och små företags behov. Det förenklade formuläret för teknisk dokumentation som antas av kommissionen bör omfatta alla tillämpliga delar av den tekniska dokumentation som anges i denna förordning och specificera hur ett mikroföretag eller ett småföretag kan tillhandahålla de begärda delarna på ett kortfattat sätt, såsom en beskrivning av utformningen, utvecklingen och produktionen av produkten med digitala element. På så sätt skulle formuläret bidra till att minska den administrativa regelbördan genom att ge de berörda företagen rättslig säkerhet om hur omfattande den information som ska lämnas ska vara och vilka uppgifter som ska ingå. Mikroföretag och små företag bör kunna välja att tillhandahålla tillämpliga delar som rör teknisk dokumentation i ett mer omfattande format och att inte använda det förenklade formulär som de har tillgång till.

- (94) För att främja och skydda innovation är det viktigt att särskild hänsyn tas till intressena hos tillverkare som är mikroföretag eller små eller medelstora företag, särskilt mikroföretags och små företags, inbegripet uppstarts företags. För detta ändamål skulle medlemsstaterna kunna utveckla initiativ som riktar sig till tillverkare som är mikroföretag eller små företag, inbegripet om utbildning, medvetandehöjande åtgärder, kommunikation, testning av information och tredjepartsbedömning av överensstämmelse, samt inrättande av sandlådor. Översättningskostnader för obligatorisk dokumentation, såsom den tekniska dokumentationen samt den information och de instruktioner till användaren som krävs enligt denna förordning, och kommunikation med myndigheter, kan innebära en betydande kostnad för tillverkarna, särskilt mindre tillverkare. Medlemsstaterna bör därför kunna anse att ett av de språk som fastställs och godtas av dem för relevant dokumentation från tillverkare och för kommunikation med tillverkare är ett språk som ett så stort antal användare som möjligt huvudsakligen förstår.
- (95) För att tillämpningen av denna förordning ska fungera smidigt bör medlemsstaterna, före den dag då denna förordning börjar tillämpas, sträva efter att säkerställa att tillräckligt många anmälda organ finns tillgängliga för att tredjepartsbedömningar av överensstämmelse ska kunna utföras. Kommissionen bör sträva efter att hjälpa medlemsstaterna och andra berörda parter i detta arbete för att undvika flaskhalsar och hinder för marknadstillträde för tillverkare. Riktad utbildningsverksamhet som leds av medlemsstaterna, inbegripet när så är lämpligt med stöd av kommissionen, kan bidra till tillgången på kvalificerad arbetskraft, och även till att stödja de anmälda organens verksamhet enligt denna förordning. Med tanke på de kostnader som en tredjepartsbedömning av överensstämmelse kan medföra bör dessutom övervägas att finansiera initiativ på unionsnivå och nationell nivå som syftar till att minska sådana kostnader för mikroföretag och små företag.
- (96) För att säkerställa proportionalitet bör organ för bedömning av överensstämmelse, när de fastställer avgifterna för bedömning av överensstämmelse, ta hänsyn till mikroföretags och små och medelstora företags, inbegripet uppstarts företags, särskilda intressen och behov. I synnerhet bör organ för bedömning av överensstämmelse tillämpa det relevanta granskningsförfarande och den testning som föreskrivs i denna förordning endast när så är lämpligt och enligt en riskbaserad metod.
- (97) Syftet med regulatoriska sandlådor bör vara att främja innovation och konkurrenskraft för företag genom att inrätta kontrollerade testmiljöer innan produkter med digitala element släpps ut på marknaden. Regulatoriska sandlådor bör bidra till att förbättra rättssäkerheten för alla aktörer som omfattas av denna förordning och underlätta och påskynda tillträdet till unionsmarknaden för produkter med digitala element, särskilt när de tillhandahålls av mikroföretag och små företag, inbegripet uppstarts företags.
- (98) För genomförandet av tredjepartsbedömningar av överensstämmelse för produkter med digitala element bör organ för bedömning av överensstämmelse anmälas av de nationella anmälade myndigheterna till kommissionen och övriga medlemsstater, under förutsättning att de uppfyller ett antal krav, i synnerhet vad gäller oberoende, kompetens och avsaknad av intressekonflikter.
- (99) För att säkerställa en enhetlig kvalitetsnivå vid bedömning av överensstämmelse för produkter med digitala element måste också krav fastställas för de anmälade myndigheterna och andra organ som är involverade i bedömningen, anmälan och övervakningen av anmälda organ. Det system som fastställs i denna förordning bör kompletteras av ackrediteringssystemet enligt förordning (EG) nr 765/2008. Eftersom ackreditering är ett oundgängligt verktyg för att kontrollera kompetensen hos organen för bedömning av överensstämmelse bör det också användas för anmälningssyften.
- (100) Organ för bedömning av överensstämmelse som har ackrediterats och anmälts enligt unionsrätten och som fastställer krav som liknar dem som fastställs i denna förordning, såsom ett organ för bedömning av överensstämmelse som har anmälts för en europeisk ordning för cybersäkerhetscertifiering vilken antagits enligt förordning (EU) 2019/881 eller som har anmälts enligt delegerad förordning (EU) 2022/30, bör bedömas på nytt och anmälas enligt den här förordningen. Synergier kan dock identifieras av relevanta myndigheter när det gäller överlappande krav för att förhindra en onödigt ekonomisk och administrativ börda och säkerställa en smidig och snabb anmälningssyften.
- (101) De nationella offentliga myndigheterna inom unionen bör betrakta öppen ackreditering som föreskrivs i förordning (EG) nr 765/2008 som det bästa sättet att styrka den tekniska kompetensen hos organen för bedömning av överensstämmelse, för att säkerställa den nödvändiga nivån av förtroendet för intyg om överensstämmelse. Nationella myndigheter kan emellertid anse att de har tillräckliga möjligheter att utföra bedömningen på egen hand. I så fall bör de nationella myndigheterna, för att trygga en rimlig trovärdighetsnivå på bedömningar utförda av andra nationella myndigheter, tillhandahålla den dokumentation som krävs för att visa kommissionen och övriga medlemsstater att de utvärderade organen för bedömning av överensstämmelse uppfyller de relevanta kraven.

EUT L, 20.11.2024

- (102) Organ för bedömning av överensstämmelse lägger ofta ut verksamhet kopplad till bedömningen av överensstämmelse på underentreprenad eller anlitar ett dotterbolag. För att se till att den erforderliga skyddsnivån uppfylls för en produkt med digitala element som ska släppas ut på marknaden är det avgörande att underentreprenörer och dotterbolag uppfyller samma krav som de anmälda organen i fråga om utförandet av bedömning av överensstämmelse.
- (103) Den anmälande myndigheten bör sända anmälan av ett organ för bedömning av överensstämmelse till kommissionen och övriga medlemsstater via databasen Nando. Databasen Nando är det elektroniska anmälningsverktyg som utvecklas och förvaltas av kommissionen och där en förteckning kan hittas över alla anmälda organ.
- (104) Eftersom de anmälda organen får erbjuda sina tjänster i hela unionen är det lämpligt att medlemsstaterna och kommissionen bereds tillfälle att göra invändningar rörande ett anmält organ. Därför är det viktigt att en period fastställs under vilken eventuellt tvivel eller osäkerhet om kompetensen hos organen för bedömning av överensstämmelse kan redas ut innan de börjar fungera som anmälda organ.
- (105) Av konkurrensskäl är det av avgörande betydelse att de anmälda organen tillämpar förfarandena för bedömning av överensstämmelse utan att belasta de ekonomiska aktörerna i onödan. Av samma skäl och för att säkerställa likabehandling av de ekonomiska aktörerna måste en enhetlig teknisk tillämpning av förfarandena för bedömning av överensstämmelse säkerställas. Detta bör bäst uppnås genom lämplig samordning och lämpligt samarbete mellan de anmälda organen.
- (106) Marknadskontroll är ett viktigt verktyg för att säkerställa en korrekt och enhetlig tillämpning av unionsrätten. Det är därför lämpligt att upprätta en rättslig ram för ett ändamålsenligt genomförande av marknadskontroll. De regler om unionens marknadskontroll och kontroll av produkter som förs in på unionsmarknaden som föreskrivs i förordning (EU) 2019/1020 är tillämpliga på produkter med digitala element som omfattas av den här förordningens tillämpningsområde.
- (107) I enlighet med förordning (EU) 2019/1020 genomför en marknadskontrollmyndighet marknadskontroll på den medlemsstats territorium som har utsett den. Den här förordningen bör inte förhindra medlemsstaterna att välja vilka behöriga myndigheter som ska utföra marknadskontroll. Varje medlemsstat bör utse en eller flera marknadskontrollmyndigheter på sitt territorium. Medlemsstaterna bör kunna välja att utse en befintlig eller en ny myndighet till att fungera som marknadskontrollmyndighet, inbegripet behöriga myndigheter utsedda eller inrättade enligt artikel 8 i direktiv (EU) 2022/2555, nationella myndigheter för cybersäkerhetscertifiering utsedda enligt artikel 58 i förordning (EU) 2019/881 eller marknadskontrollmyndigheter utsedda enligt direktiv 2014/53/EU. De ekonomiska aktörerna ska samarbeta fullt ut med marknadskontrollmyndigheterna och andra behöriga myndigheter. Varje medlemsstat bör underrätta kommissionen och övriga medlemsstater om sina marknadskontrollmyndigheter och behörighetsområdena för varje sådan myndighet och bör säkerställa de resurser och kompetenser som dessa behöver för att utföra sina marknadskontrolluppgifter enligt denna förordning. Enligt artikel 10.2 och 10.3 i förordning (EU) 2019/1020 bör varje medlemsstat tillsätta ett centralt samordningskontor som bland annat ska ansvara för att representera en samordnad ståndpunkt från marknadskontrollmyndigheterna och bistå i samarbetet mellan marknadskontrollmyndigheterna i olika medlemsstater.
- (108) En särskild Adco-grupp för cyberresiliens hos produkter med digitala element bör inrättas för en enhetlig tillämpning av denna förordning, enligt artikel 30.2 i förordning (EU) 2019/1020. En Adco-grupp bör bestå av representanter för de nationella marknadskontrollmyndigheterna och, om så är lämpligt, representanter för de centrala samordningskontoren. Kommissionen bör stödja och uppmuntra samarbete mellan marknadskontrollmyndigheter genom unionsnätverket för produktöverensstämmelse, som inrättats enligt artikel 29 i förordning (EU) 2019/1020 och som består av representanter från varje medlemsstat, inbegripet en representant för varje centralt samordningskontor som avses i artikel 10 i den förordningen och en valfri nationell expert, ordförandena för Adco-grupperna och representanter för kommissionen. Kommissionen bör delta i möten i unionsnätverket för produktöverensstämmelse, och i dess undergruppers och Adco-gruppers möten. Den bör också bistå Adco-grupper genom ett verkställande sekretariat som tillhandahåller tekniskt och logistiskt stöd. En Adco-grupp får också bjuda in oberoende experter att delta och samarbeta med andra Adco-grupper, såsom den som inrättats enligt direktiv 2014/53/EU.
- (109) Marknadskontrollmyndigheterna bör, genom Adco-grupper som inrättas enligt denna förordning, ha ett nära samarbete och bör kunna utarbeta vägledningsdokument för att underlätta marknadskontroller på nationell nivå, till exempel genom att utveckla bästa praxis och indikatorer för att effektivt kontrollera att produkter med digitala element överensstämmer med denna förordning.

ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>

- (110) För att säkerställa att proportionella och effektiva åtgärder vidtas i rätt tid när det gäller produkter med digitala element som utgör en betydande cybersäkerhetsrisk bör ett unionsförfarande för skyddsåtgärder som innebär att berörda parter underrättas om åtgärder som är planerade att vidtas för sådana produkter erbjudas. På så sätt bör också marknadskontrollmyndigheterna få möjlighet att, i samarbete med de berörda ekonomiska aktörerna, agera i ett tidigare skede när det är nödvändigt. Om medlemsstaterna och kommissionen är överens om att en medlemsstats åtgärd är berättigad, bör kommissionen inte involveras ytterligare, utom i de fall då den bristande överensstämmelsen kan anses bero på brister i en harmoniserad standard.
- (111) I vissa fall kan en produkt med digitala element som uppfyller kraven i denna förordning ändå utgöra en betydande cybersäkerhetsrisk eller utgöra en risk för människors hälsa eller säkerhet, för uppfyllandet av skyldigheter enligt sådan unionsrätt eller nationell rätt som är avsedd att skydda grundläggande rättigheter, tillgången till och autenticiteten, riktigheten eller konfidentialiteten för tjänster som väsentliga entiteter av den typ som avses i artikel 3.1 i direktiv (EU) 2022/2555 erbjuder med användning av ett elektroniskt informationssystem eller för andra aspekter av skyddet av allmänintresset. Därför är det nödvändigt att fastställa regler som säkerställer att dessa risker minskas. Följaktligen bör marknadskontrollmyndigheterna vidta åtgärder för att lägga den ekonomiska aktören att säkerställa att produkten inte längre utgör en sådan risk, eller att återkalla eller dra tillbaka den, beroende på risken. Så snart en marknadskontrollmyndighet begränsar eller förbjuder den fria rörligheten för en produkt med digitala element på detta sätt bör medlemsstaten utan dröjsmål underrätta kommissionen och övriga medlemsstater om de provisoriska åtgärderna och motivera sitt beslut. Om en marknadskontrollmyndighet antar sådana åtgärder mot produkter med digitala element som utgör en risk bör kommissionen utan dröjsmål inleda samråd med medlemsstaterna och berörda ekonomiska aktörer (en eller flera) samt utvärdera den nationella åtgärden. På grundval av utvärderingsresultaten bör kommissionen fastställa om den nationella åtgärden är motiverad eller inte. Kommissionen bör rikta beslutet till alla medlemsstater och omedelbart delge dem och de berörda ekonomiska aktörerna beslutet. Om åtgärden anses vara berättigad bör kommissionen också överväga att anta förslag om översyn av relevant unionsrätt.
- (112) För produkter med digitala element som utgör en betydande cybersäkerhetsrisk, där det finns skäl att tro att de inte uppfyller kraven i denna förordning, eller för produkter som uppfyller kraven i denna förordning men som utgör andra viktiga risker, exempelvis risker för människors hälsa eller säkerhet, för uppfyllandet av skyldigheter enligt sådan unionsrätt eller nationell rätt som är avsedd att skydda grundläggande rättigheter eller för tillgången till och autenticiteten, riktigheten eller konfidentialiteten för tjänster som väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555 erbjuder med användning av ett elektroniskt informationssystem, bör kommissionen kunna begära att Enisa gör en utvärdering. Baserat på denna utvärdering bör kommissionen genom beförordandeakter kunna vidta korrigerande eller begränsande åtgärder på unionsnivå, inbegripet kräva att de berörda produkterna med digitala element dras tillbaka eller återkallas från marknaden, inom en rimlig tid i förhållande till typen av risk. Kommissionen bör endast kunna tillgripa en sådan åtgärd under exceptionella omständigheter som motiverar ett omedelbart ingripande för att bevara en korrekt fungerande inre marknad och endast när inga verkningfulla åtgärder har vidtagits av marknadskontrollmyndigheterna för att åtgärda situationen. Sådana exceptionella omständigheter kan vara akutsituationer där exempelvis en tillverkare gör en produkt med digitala element som inte uppfyller kraven allmänt tillgänglig i flera medlemsstater och den även används i nyckelsektorer av entiteter som omfattas av direktiv (EU) 2022/2555, och produkten samtidigt innehåller kända sårbarheter som utnyttjas av fientliga aktörer utan att tillverkaren tillhandahåller tillgängliga programfixar. Kommissionen bör vid sådana akutsituationer kunna ingripa endast under den tid som de exceptionella omständigheterna varar och om bristande överensstämmelse med denna förordning eller de betydande riskerna kvarstår.
- (113) Om det finns indikationer på bristande överensstämmelse med denna förordning i flera medlemsstater bör marknadskontrollmyndigheterna kunna genomföra gemensamma åtgärder med andra myndigheter för att kontrollera överensstämmelsen och identifiera cybersäkerhetsrisker för produkter med digitala element.
- (114) Samtidiga samordnade kontrollåtgärder (sweeps) är särskilda kontrollåtgärder som vidtas av marknadskontrollmyndigheterna och som kan förbättra produktsäkerheten ytterligare. Dessa samordnade kontrollåtgärder bör i synnerhet vidtas när det finns marknadstrender, klagomål från konsumenter eller andra indikationer som tyder på att vissa kategorier av produkter med digitala element ofta utgör cybersäkerhetsrisker. När marknadskontrollmyndigheterna fastställer vilka produktkategorier som ska omfattas av sweeps bör de också beakta omständigheter som rör icke-tekniska riskfaktorer. I detta syfte bör marknadskontrollmyndigheterna kunna ta hänsyn till resultaten av de samordnade säkerhetsriskbedömningar av kritiska leveranskedjor på unionsnivå som genomförs i enlighet med artikel 22 i direktiv (EU) 2022/2555, inbegripet omständigheter som rör icke-tekniska riskfaktorer. Enisa bör lämna förslag till marknadskontrollmyndigheterna på kategorier av produkter med digitala element som kan omfattas av samtidiga samordnade kontrollåtgärder, baserat på bland annat de anmälningar om sårbarheter och incidenter som inkommer till Enisa.

- (115) Med tanke på Enisas sakkunskaper och uppdrag bör Enisa kunna stödja processen för genomförande av denna förordning. Enisa bör i synnerhet kunna föreslå gemensamma åtgärder som ska vidtas av marknadskontrollmyndigheter i flera medlemsstater på grundval av indikationer eller information om potentiell bristande överensstämmelse med denna förordning för produkter med digitala element eller identifiera produktkategorier där samtidiga sweeps bör organiseras. Under exceptionella omständigheter bör Enisa, på kommissionens begäran, kunna göra utvärderingar av specifika produkter med digitala element som utgör en betydande cybersäkerhetsrisk, när ett omedelbart ingripande krävs för att bevara en korrekt fungerande inre marknad.
- (116) Genom denna förordning tilldelas Enisa vissa uppgifter som kräver lämpliga resurser i fråga om både sakkunskap och personal för att Enisa ska kunna utföra dessa uppgifter på ett ändamålsenligt sätt. Kommissionen kommer att föreslå nödvändiga budgetmedel för Enisas tjänsteförteckning, i enlighet med förfarandet som anges i artikel 29 i förordning (EU) 2019/881, vid utarbetandet av förslaget till unionens allmänna budget. Under den processen kommer kommissionen att beakta Enisas övergripande resurser för att den ska kunna fullgöra sina uppgifter, inbegripet dem som tilldelats Enisa enligt den här förordningen.
- (117) I syfte att säkerställa att regelverket vid behov kan anpassas bör befogenheten att anta akter i enlighet med artikel 290 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) delegeras till kommissionen med avseende på uppdatering av en bilaga till denna förordning med förteckningen över viktiga produkter med digitala element. Befogenheten att anta akter i enlighet med den artikeln bör delegeras till kommissionen för att identifiera produkter med digitala element som omfattas av andra unionsregler som ger samma skyddsnivå som denna förordning och specificera om det skulle vara nödvändigt med några begränsningar eller uteslutanden från denna förordnings tillämpningsområde samt specificera sådana begränsningars omfattning, i tillämpliga fall. Befogenheten att anta akter i enlighet med den artikeln bör också delegeras till kommissionen med avseende på det potentiella kravet på certifiering enligt en europeisk ordning för cybersäkerhetscertifiering av kritiska produkter med digitala element som anges i en bilaga till denna förordning, liksom för att uppdatera förteckningen över kritiska produkter med digitala element baserat på kritikalitetskriterier som fastställs i denna förordning, samt för att specificera de europeiska ordningarna för cybersäkerhetscertifiering som antagits enligt förordning (EU) 2019/881 och som kan användas för att visa överensstämmelse med de väsentliga cybersäkerhetskrav eller delar av dem som fastställs i en bilaga till den här förordningen. Befogenheten att anta akter bör också delegeras till kommissionen för att specificera minsta tillåtna stödperioder för specifika produktkategorier om marknadskontrolluppgifter tyder på otillräckliga stödperioder, samt för att specificera villkoren för att tillämpa cybersäkerhetsrelaterade skäl när det gäller att skjuta upp spridningen av anmälningar om aktivt utnyttjade sårbarheter. Dessutom bör befogenheten att anta akter delegeras till kommissionen för att inrätta frivilliga program för säkerhetsintyg i syfte att bedöma överensstämmelse för produkter med digitala element som kategoriseras som programvara med fri och öppen källkod, med alla eller vissa väsentliga cybersäkerhetskrav eller andra skyldigheter som fastställs i denna förordning, samt för att specificera minimiinnehåll i EU-försäkrans överensstämmelse och i syfte att komplettera de aspekter som ska ingå i den tekniska dokumentationen. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning⁽¹¹⁾. För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter. Befogenheten att anta delegerade akter i enlighet med denna förordning bör delegeras till kommissionen för en period på fem år från och med den 10 december 2024. Kommissionen bör utarbeta en rapport om delegeringen av befogenhet senast nio månader före utgången av perioden på fem år. Delegeringen av befogenhet bör genom tyst medgivande förlängas med perioder av samma längd, såvida inte Europaparlamentet eller rådet motsätter sig en sådan förlängning senast tre månader före utgången av perioden i fråga.
- (118) För att säkerställa enhetliga villkor för genomförandet av denna förordning bör kommissionen tilldelas genomförandebefogenheter för att specificera den tekniska beskrivning av de kategorier av viktiga produkter med digitala element som anges i en bilaga till denna förordning, specificera formatet för och vad som ska ingå i programvaruförteckningen, ytterligare specificera formatet och förfarandet för de anmälningar om aktivt utnyttjade sårbarheter och allvarliga incidenter som påverkar säkerheten för produkter med digitala element, vilka lämnats in av tillverkarna, fastställa gemensamma specifikationer som omfattar tekniska krav vilka tillhandahåller ett sätt att uppfylla de väsentliga cybersäkerhetskrav som fastställs i en bilaga till denna förordning, fastställa tekniska specifikationer för etiketter, piktogram eller andra märkningar relaterade till säkerheten för produkter med digitala element, deras stödperiod och mekanismer för att främja användningen av sådana och öka allmänhetens medvetenhet om säkerheten för produkter med digitala element, specificera det förenklade formuläret för teknisk dokumentation med inriktning på mikroföretags och små företags behov, samt besluta om korrigerande eller

⁽¹¹⁾ EUT L 123, 12.5.2016, s. 1.

begränsande åtgärder på unionsnivå vid exceptionella omständigheter som motiverar ett omedelbart ingripande för att bevara en korrekt fungerande inre marknad. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011⁽¹²⁾.

- (119) För att säkerställa ett konstruktivt samarbete präglat av förtroende mellan marknadskontrollmyndigheter på unionsnivå och nationell nivå bör alla parter som är involverade i tillämpningen av denna förordning respektera konfidentialiteten för information och data som de erhåller i utförandet av sina uppgifter.
- (120) För att säkerställa en effektiv efterlevnadskontroll av de skyldigheter som fastställs i denna förordning bör varje marknadskontrollmyndighet ha befogenhet att påföra eller begära påförande av administrativa sanktionsavgifter. Det bör därför fastställas maxnivåer för administrativa sanktionsavgifter som kommer att föreskrivas i nationell rätt med avseende på bristande uppfyllande av de skyldigheter som fastställs i denna förordning. När det administrativa sanktionsbeloppet fastställs i varje enskilt fall bör alla relevanta omständigheter i den specifika situationen beaktas och som ett minimum de som uttryckligen fastställs i denna förordning, inbegripet huruvida tillverkaren är ett mikroföretag eller ett småföretag eller medelstort företag, inbegripet ett uppstarts företag, och huruvida samma eller andra marknadskontrollmyndigheter redan har påfört samma ekonomiska aktör administrativa sanktionsavgifter för en liknande överträdelse. Sådana omständigheter skulle kunna vara antingen försvärande, i situationer där samma ekonomiska aktörs överträdelse fortsätter på territoriet för andra medlemsstater än den där den administrativa sanktionsavgiften redan har påförts, eller förmildrande, genom att säkerställa att eventuella administrativa sanktionsavgifter som övervägs av en annan marknadskontrollmyndighet för samma ekonomiska aktör eller samma typ av överträdelse redan bör beakta sanktioner som påförts i andra medlemsstater och storleken på dessa, tillsammans med andra relevanta särskilda omständigheter. I samtliga fall bör den kumulativa administrativa sanktionsavgift som marknadskontrollmyndigheter i flera medlemsstater kan påföra samma ekonomiska aktör för samma typ av överträdelse fastställas med iakttagande av proportionalitetsprincipen. Med tanke på att administrativa sanktionsavgifter inte tillämpas på mikroföretag eller små företag för en underlåtenhet att iaktta tidsfristen på 24 timmar avseende en tidig varning om aktivt utnyttjade sårbarheter eller allvarliga incidenter som påverkar säkerheten för produkten med digitala element, och inte heller på förvaltare av programvara med fri och öppen källkod för någon överträdelse av denna förordning, och med förbehåll för principen om att sanktioner bör vara effektiva, proportionella och avskräckande, bör medlemsstaterna inte lägga dessa enheter andra typer av sanktioner av ekonomisk karaktär.
- (121) Om administrativa sanktionsavgifter påförs en person som inte är ett företag, bör den behöriga myndigheten ta hänsyn till den allmänna inkomstnivån i medlemsstaten och personens ekonomiska situation, när den överväger lämplig sanktionsavgift. Det bör vara upp till medlemsstaterna att fastställa om och i vilken utsträckning myndigheter ska omfattas av administrativa sanktionsavgifter.
- (122) Medlemsstaterna bör, med beaktande av nationella omständigheter, undersöka möjligheten att använda intäkterna från de sanktioner som föreskrivs i denna förordning eller deras ekonomiska motsvarighet till att stödja cybersäkerhetsstrategier och öka cybersäkerhetsnivån i unionen genom att bland annat öka antalet kvalificerade yrkesverksamma inom cybersäkerhet, stärka kapacitetsutbyggnaden för mikroföretag samt små och medelstora företag och förbättra allmänhetens medvetenhet om cyberhot.
- (123) I sina förbindelser med tredjeländer strävar unionen efter att främja internationell handel med reglerade produkter. En mängd olika åtgärder kan vidtas för att främja handel, inbegripet flera rättsliga instrument såsom bilaterala (mellanstatliga) avtal om ömsesidigt erkännande (MRA) av bedömning av överensstämmelse och märkning av reglerade produkter. Avtal om ömsesidigt erkännande upprättas mellan unionen och tredjeländer som är på jämförbar teknisk utvecklingsnivå och har en jämförbar strategi för bedömning av överensstämmelse. Dessa avtal baseras på ett ömsesidigt godtagande av intyg, märkning om överensstämmelse och provningsrapporter som utfärdats av parternas organ för bedömning av överensstämmelse enligt varje parts lagstiftning. I dagsläget finns MRA med flera tredjeländer. Dessa MRA ingås för ett antal specifika sektorer, som kan variera från ett tredjeland till ett annat. För att ytterligare främja handel, och med beaktande av att leveranskedjorna för produkter med digitala element är globala, kan MRA om ömsesidigt erkännande av bedömning av överensstämmelse ingås av unionen i enlighet med artikel 218 i EUF-fördraget för produkter som regleras enligt denna förordning. Samarbete med partner tredjeländer är också viktigt, för att stärka cyberresiliensen globalt, eftersom det långsiktigt kommer att bidra till att stärka cybersäkerhetsramen både inom och utanför unionen.

⁽¹²⁾ Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13, ELI: <http://data.europa.eu/eli/reg/2011/182/oj>).

- (124) Konsumenter bör ha rätt att hävda sina rättigheter med avseende på de skyldigheter som åläggs ekonomiska aktörer enligt denna förordning genom grupptalan enligt Europaparlamentets och rådets direktiv (EU) 2020/1828⁽¹³⁾. För detta ändamål bör det i denna förordning föreskrivas att direktiv (EU) 2020/1828 är tillämpligt på grupptalan om överträdelse av denna förordning som skadar eller kan skada konsumenters kollektiva intressen. Bilaga I till det direktivet bör därför ändras i enlighet med detta. Det åligger medlemsstaterna att säkerställa att dessa ändringar återspeglas i de införlivandeåtgärder som antas enligt det direktivet, även om antagandet av nationella införlivandeåtgärder i det avseendet inte är ett villkor för att det direktivet ska vara tillämpligt på sådan grupptalan. Det direktivets tillämplighet på grupptalan som väcks med avseende på ekonomiska aktörers överträdelse av bestämmelser i denna förordning som skadar eller skulle kunna skada konsumenters kollektiva intressen bör börja tillämpas från och med den 11 december 2027.
- (125) Denna förordning bör med jämna mellanrum utvärderas och ses över av kommissionen i samråd med berörda parter, främst i syfte att avgöra behovet av ändringar mot bakgrund av samhällsutvecklingen, den politiska utvecklingen, den tekniska utvecklingen eller ändrade marknadsvillkor. Denna förordning kommer att underlätta för entiteter som omfattas av förordning (EU) 2022/2554 och direktiv (EU) 2022/2555 och som använder produkter med digitala element att fullgöra skyldigheterna avseende säkerhet i leveranskedjan. Kommissionen bör, som en del av den regelbundna översynen, utvärdera de kombinerade effekterna av unionens cybersäkerhetsram.
- (126) De ekonomiska aktörerna bör ges tillräckligt med tid att anpassa sig till de krav som anges i denna förordning. Förordningen bör tillämpas från och med den 11 december 2027, förutom skyldigheten att rapportera aktivt utnyttjade sårbarheter och allvarliga incidenter som påverkar säkerheten för produkten med digitala element, som bör börja tillämpas från och med den 11 september 2026 och bestämmelserna om anmälan av organ för bedömning av överensstämmelse som bör tillämpas från och med den 11 juni 2026.
- (127) Det är viktigt att ge stöd till mikroföretag samt små och medelstora företag, inbegripet uppstarts företag, vid genomförandet av denna förordning och att begränsa de risker i samband med genomförandet som följer av bristande kunskap och expertis på marknaden, samt att underlätta för tillverkarna att fullgöra sina skyldigheter enligt denna förordning. Programmet för ett digitalt Europa och andra relevanta unionsprogram tillhandahåller ekonomiskt och tekniskt stöd som gör att dessa företag kan bidra till tillväxten i unionens ekonomi och till en stärkt gemensam cybersäkerhetsnivå i unionen. Europeiska kompetenscentrumet för cybersäkerhet och nationella samordningscentrum samt europeiska digitala innovationsknutpunkter som inrättas av kommissionen och medlemsstaterna på unionsnivå eller nationell nivå skulle också kunna stödja företag och organisationer inom den offentliga sektorn och bidra till genomförandet av denna förordning. Inom ramen för sina respektive uppdrag och ansvarsområden skulle de kunna ge tekniskt och vetenskapligt stöd till mikroföretag samt små och medelstora företag, till exempel för testningsverksamhet och tredjepartsbedömningar av överensstämmelse. De skulle också kunna främja användningen av verktyg för att underlätta genomförandet av denna förordning.
- (128) Dessutom bör medlemsstaterna överväga kompletterande åtgärder som syftar till att ge vägledning och stöd till mikroföretag samt små och medelstora företag, såsom att inrätta regulatoriska sandlådor och särskilda kanaler för kommunikation. För att stärka cybersäkerhetsnivån i unionen får medlemsstaterna också överväga att tillhandahålla stöd för att utveckla kapacitet och färdigheter med anknytning till cybersäkerhet för produkter med digitala element, förbättra ekonomiska aktörers cyberresiliens, särskilt för mikroföretag samt små och medelstora företag, och främja allmänhetens medvetenhet om cybersäkerheten för produkter med digitala element.
- (129) Eftersom målet för denna förordning inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.
- (130) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725⁽¹⁴⁾ och avgav ett yttrande den 9 november 2022⁽¹⁵⁾.
- ⁽¹³⁾ Europaparlamentets och rådets direktiv (EU) 2020/1828 av den 25 november 2020 om grupptalan för att skydda konsumenters kollektiva intressen och om upphävande av direktiv 2009/22/EG (EUT L 409, 4.12.2020, s. 1).
- ⁽¹⁴⁾ Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).
- ⁽¹⁵⁾ EUT C 452, 29.11.2022, s. 23.

SV

EUT L, 20.11.2024

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Innehåll

I denna förordning fastställs

- a) regler för tillhandahållande på marknaden av produkter med digitala element, för att säkerställa cybersäkerheten för sådana produkter,
- b) väsentliga cybersäkerhetskrav för utformningen, utvecklingen och tillverkningen av produkter med digitala element, och skyldigheter för ekonomiska aktörer när det gäller cybersäkerheten för dessa produkter,
- c) väsentliga cybersäkerhetskrav för de processer för sårbarhetshantering som tillverkarna inför för att säkerställa cybersäkerheten för produkter med digitala element under den tid som produkterna förväntas vara i bruk samt skyldigheter för ekonomiska aktörer i samband med dessa processer, och
- d) regler om marknadskontroll, inbegripet övervakning, och kontroll av efterlevnaden av de regler och krav som avses i denna artikel.

Artikel 2

Tillämpningsområde

1. Denna förordning är tillämplig på alla produkter med digitala element som tillhandahålls på marknaden och vars avsedda ändamål eller rimligen förutsebara användning omfattar en direkt eller indirekt logisk eller fysisk dataanslutning till en enhet eller ett nät.
2. Förordningen är inte tillämplig på sådana produkter med digitala element som omfattas av följande unionsrättsakter:
 - a) Förordning (EU) 2017/745.
 - b) Förordning (EU) 2017/746.
 - c) Förordning (EU) 2019/2144.
3. Denna förordning ska inte tillämpas på produkter med digitala element som har certifierats i enlighet med förordning (EU) 2018/1139.
4. Denna förordning ska inte tillämpas på utrustning som omfattas av Europaparlamentets och rådets direktiv 2014/90/EU ⁽¹⁶⁾.
5. Denna förordnings tillämpning på produkter med digitala element som omfattas av andra unionsregler där krav fastställs avseende alla eller vissa risker som täcks av de väsentliga cybersäkerhetskraven i bilaga 1 får begränsas eller undantas om
 - a) sådana begränsningar eller undantag är förenliga med den allmänna rättsliga ram som är tillämplig på dessa produkter, och
 - b) sektorsreglerna ger samma eller en högre skyddsnivå än den som föreskrivs i denna förordning.

Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 61 för att komplettera denna förordning genom att specificera om sådana begränsningar eller undantag är nödvändiga, vilka produkter och regler som berörs samt begränsningens omfattning, i förekommande fall.

⁽¹⁶⁾ Europaparlamentets och rådets direktiv 2014/90/EU av den 23 juli 2014 om marin utrustning och om upphävande av rådets direktiv 96/98/EG (EUT L 257, 28.8.2014, s. 146).

6. Denna förordning ska inte tillämpas på reservdelar som tillhandahålls på marknaden för att ersätta identiska komponenter i produkter med digitala element och som tillverkas enligt samma specifikationer som de komponenter som de är avsedda att ersätta.

7. Denna förordning ska inte tillämpas på produkter med digitala element som utvecklats eller ändrats uteslutande för ändamål som rör nationell säkerhet eller försvarsändamål eller på produkter som utformats specifikt för att behandla säkerhetsskyddsklassificerade uppgifter.

8. De skyldigheter som fastställs i denna förordning får inte medföra tillhandahållande av information vars utlämnande skulle strida mot väsentliga intressen i fråga om medlemsstaternas nationella säkerhet, allmänna säkerhet eller försvar.

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

1. *produkt med digitala element*: programvaru- eller hårdvaruprodukt och dess lösningar för fjärrbehandling av data, inbegripet programvaru- eller hårdvarukomponenter som släpps ut på marknaden separat.
2. *fjärrbehandling av data*: databehandling på distans för vilken programvaran utformats och utvecklats av tillverkaren eller under tillverkarens ansvar, och vars avsaknad skulle innebära att produkten med digitala element inte kan utföra en av sina funktioner.
3. *cybersäkerhet*: cybersäkerhet enligt definitionen i artikel 2.1 i förordning (EU) 2019/881.
4. *programvara*: den del av ett elektroniskt informationssystem som utgörs av datorkod.
5. *hårdvara*: ett fysiskt elektroniskt informationssystem, eller delar av ett sådant, som kan behandla, lagra eller överföra digitala data.
6. *komponent*: programvara eller hårdvara som är avsedd att vara integrerad i ett elektroniskt informationssystem.
7. *elektroniskt informationssystem*: ett system, inklusive elektrisk eller elektronisk utrustning, som kan behandla, lagra eller överföra digitala data.
8. *logisk anslutning*: en virtuell representation av en dataförbindelse som genomförs via ett programvarugränssnitt.
9. *fysisk anslutning*: en anslutning mellan elektroniska informationssystem eller komponenter som genomförs med fysiska medel, inbegripet elektriska, optiska eller mekaniska gränssnitt, tråd eller radiovägar.
10. *indirekt anslutning*: en anslutning till en enhet eller ett nät som inte sker direkt utan snarare som en del av ett större system som är direkt anslutningsbart till enheten eller nätet.
11. *slutnod*: enhet som är ansluten till ett nät och som tjänar som ingångspunkt till det nätet.
12. *ekonomisk aktör*: tillverkaren, tillverkarens representant, importören, distributören eller en annan fysisk eller juridisk person som omfattas av skyldigheter avseende tillverkning av produkter med digitala element eller avseende tillhandahållande av produkter med digitala element på marknaden i enlighet med denna förordning.
13. *tillverkare*: en fysisk eller juridisk person som utvecklar eller tillverkar produkter med digitala element, eller som låter utforma, utveckla eller tillverka produkter med digitala element, och saluför dessa under eget namn eller varumärke, vare sig mot betalning, för monetarisering eller kostnadsfritt.
14. *förvaltare av programvara med fri och öppen källkod*: en juridisk person, annan än en tillverkare, som har till syfte eller som mål att systematiskt och varaktigt tillhandahålla stöd för utvecklingen av specifika produkter med digitala element, vilka klassificeras som programvara med fri och öppen källkod och är avsedda för kommersiell verksamhet, och som säkerställer dessa produkters bärkraft.
15. *tillverkarens representant*: en fysisk eller juridisk person som är etablerad i unionen och som enligt skriftlig fullmakt från en tillverkare har rätt att i tillverkarens ställe utföra särskilda uppgifter.

SV

EUT L, 20.11.2024

16. *importör*: en fysisk eller juridisk person som är etablerad i unionen och som på marknaden släpper ut en produkt med digitala element vilken bär namnet på eller varumärket för en fysisk eller juridisk person som är etablerad utanför unionen.
17. *distributör*: en fysisk eller juridisk person i leveranskedjan, utöver tillverkaren eller importören, som tillhandahåller en produkt med digitala element på unionsmarknaden utan att påverka dess egenskaper.
18. *konsument*: en fysisk person som agerar för ändamål som faller utanför den personens näringsverksamhet, affärsverksamhet, hantverk eller yrke.
19. *mikroföretag, små företag och medelstora företag*: mikroföretag, små företag och medelstora företag enligt definitionen i bilagan till rekommendation 2003/361/EG.
20. *stödperiod*: den period under vilken en tillverkare måste säkerställa att sårbarheter hos en produkt med digitala element hanteras ändamålsenligt och i enlighet med de väsentliga cybersäkerhetskrav som fastställs i bilaga I del II.
21. *utsläppande på marknaden*: tillhandahållande för första gången av en produkt med digitala element på unionsmarknaden.
22. *tillhandahållande på marknaden*: leverans av en produkt med digitala element för distribution eller användning på unionsmarknaden i samband med kommersiell verksamhet, antingen mot betalning eller kostnadsfritt.
23. *avsett ändamål*: den användning för vilken en produkt med digitala element är avsedd av leverantören, inbegripet det specifika sammanhanget och de specifika användningsvillkoren, enligt specifikationerna i de uppgifter som leverantören tillhandahåller i instruktioner till användaren, reklam- eller försäljningsmaterial och uttalanden samt i den tekniska dokumentationen.
24. *rimligen förutsebar användning*: användning som inte nödvändigtvis är det avsedda ändamål som tillverkaren anger i instruktionerna till användaren, reklam- eller försäljningsmaterial och uttalanden eller i den tekniska dokumentationen, men som är den sannolika följden av rimligen förutsebart mänskligt beteende eller tekniska åtgärder eller interaktioner.
25. *rimligen förutsebar felaktig användning*: användning av en produkt med digitala element på ett sätt som inte överensstämmer med dess avsedda ändamål, men som kan vara resultatet av rimligen förutsebart mänskligt beteende eller interaktion med andra system.
26. *anmälade myndighet*: den nationella myndighet som ansvarar för inrättandet och genomförandet av de förfaranden som krävs för bedömning, utseende och anmälan av organ för bedömning av överensstämmelse och för övervakning av dessa.
27. *bedömning av överensstämmelse*: processen där det kontrolleras om de väsentliga cybersäkerhetskraven i bilaga I har uppfyllts.
28. *organ för bedömning av överensstämmelse*: ett organ för bedömning av överensstämmelse enligt definitionen i artikel 2.13 i förordning (EG) nr 765/2008.
29. *anmält organ*: organ för bedömning av överensstämmelse som utsetts i enlighet med artikel 43 och annan relevant unionsharmoniseringslagstiftning.
30. *väsentlig ändring*: en ändring av produkten med digitala element efter dess utsläppande på marknaden, vilken påverkar produktens överensstämmelse med de väsentliga cybersäkerhetskraven i bilaga I del I eller leder till en ändring av det avsedda ändamål för vilket produkten har bedömts.
31. *CE-märkning*: märkning genom vilken en tillverkare anger att en produkt med digitala element och de processer som införts av tillverkaren överensstämmer med de väsentliga cybersäkerhetskraven i bilaga I och annan tillämplig unionsharmoniseringslagstiftning som föreskriver att sådan märkning ska fastas.
32. *unionsharmoniseringslagstiftning*: unionslagstiftning som förtecknas i bilaga I till förordning (EU) 2019/1020 och all annan unionslagstiftning som harmoniserar villkoren för saluföring av produkter som omfattas av den förordningen.
33. *marknadskontrollmyndighet*: en marknadskontrollmyndighet enligt definitionen i artikel 3.4 i förordning (EU) 2019/1020.

EUT L, 20.11.2024

SV

34. *internationell standard*: en internationell standard enligt definitionen i artikel 2.1 a i förordning (EU) nr 1025/2012.
35. *europaisk standard*: en europeisk standard enligt definitionen i artikel 2.1 b i förordning (EU) nr 1025/2012.
36. *harmoniserad standard*: en harmoniserad standard enligt definitionen i artikel 2.1 c i förordning (EU) nr 1025/2012.
37. *cybersäkerhetsrisk*: risk för förlust eller störning orsakad av en incident, som ska uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att incidenten inträffar.
38. *betydande cybersäkerhetsrisk*: en cybersäkerhetsrisk som, baserat på dess tekniska egenskaper, kan antas innebära en hög sannolikhet för en incident som kan medföra allvarliga negativa konsekvenser, inbegripet genom att orsaka betydande materiell eller immateriell förlust eller störning.
39. *programvaruförteckning*: en formell förteckning med närmare uppgifter om och leveranskedjeförhållanden för komponenter som ingår i programvaruelementen i en produkt med digitala element.
40. *sårbarhet*: en svaghet, känslighet eller brist hos en produkt med digitala element som kan utnyttjas genom ett cyberhot.
41. *sårbarhet som kan utnyttjas*: en sårbarhet som kan utnyttjas effektivt av en motståndare under praktiska operativa förhållanden.
42. *aktivt utnyttjad sårbarhet*: en sårbarhet för vilken det finns tillförlitliga bevis på att en fientlig aktör har utnyttjat den i ett system utan tillstånd från systemets ägare.
43. *incident*: en incident enligt definitionen i artikel 6.6 i direktiv (EU) 2022/2555.
44. *incident som påverkar säkerheten för en produkt med digitala element*: en incident som inverkar negativt på eller kan inverka negativt på förmågan hos en produkt med digitala element att skydda tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten för data eller funktioner.
45. *tillbud*: ett tillbud enligt definitionen i artikel 6.5 i direktiv (EU) 2022/2555.
46. *cyberhot*: ett cyberhot enligt definitionen i artikel 2.8 i förordning (EU) 2019/881.
47. *personuppgifter*: personuppgifter enligt definitionen i artikel 4.1 i förordning (EU) 2016/679.
48. *programvara med fri och öppen källkod*: programvara vars källkod delas öppet och som tillhandahålls inom ramen för en licens med fri och öppen källkod som ger alla rättigheter att göra den fritt tillgänglig att användas, modifieras och vidare distribueras.
49. *återkallelse*: återkallelse enligt definitionen i artikel 3.22 i förordning (EU) 2019/1020.
50. *tillbakadragande*: tillbakadragande enligt definitionen i artikel 3.23 i förordning (EU) 2019/1020.
51. *CSIRT-enhet som utsetts till samordnare*: en CSIRT-enhet som utsetts till samordnare enligt artikel 12.1 i direktiv (EU) 2022/2555.

Artikel 4

Fri rörlighet

1. Medlemsstaterna får inte, med hänvisning till aspekter som omfattas av denna förordning, hindra att produkter med digitala element som uppfyller kraven i denna förordning tillhandahålls på marknaden.

SV

EUT L, 20.11.2024

2. Medlemsstaterna får inte förhindra att sådana produkter med digitala element som inte uppfyller kraven i denna förordning visas eller används vid mässor, utställningar och demonstrationer eller liknande evenemang, inbegripet prototyper, förutsatt att produkten visas med en synlig märkning som tydligt anger att den inte uppfyller kraven i denna förordning och att den inte kommer att tillhandahållas på marknaden förrän den gör det.
3. Medlemsstaterna får inte förhindra att ej färdigställd programvara som inte uppfyller kraven i denna förordning tillhandahålls på marknaden, under förutsättning att programvaran tillhandahålls endast under den begränsade tid som krävs för testningsändamål och med en synlig märkning som tydligt anger att den inte uppfyller kraven i denna förordning och att den inte kommer att tillhandahållas på marknaden för andra ändamål än testning.
4. Punkt 3 ska inte tillämpas på säkerhetskomponenter enligt annan unionsharmoniseringslagstiftning än denna förordning.

Artikel 5

Upphandling eller användning av produkter med digitala element

1. Denna förordning ska inte hindra medlemsstaterna från att införa ytterligare cybersäkerhetskrav för produkter med digitala element när det gäller upphandling eller användning av dessa produkter för specifika ändamål, inbegripet när dessa produkter upphandlas eller används för ändamål som rör nationell säkerhet eller försvarsändamål, förutsatt att kraven är förenliga med medlemsstaternas skyldigheter enligt unionsrätten och att de är nödvändiga och proportionella för att uppnå dessa ändamål.
2. Utan att det påverkar tillämpningen av direktiven 2014/24/EU och 2014/25/EU ska medlemsstaterna, när produkter med digitala element som omfattas av denna förordnings tillämpningsområde upphandlas, säkerställa att överensstämmelse med de väsentliga cybersäkerhetskraven i bilaga I till denna förordning, inbegripet tillverkarnas förmåga att ändamålsenligt hantera sårbarheter, beaktas i upphandlingsprocessen.

Artikel 6

Krav för produkter med digitala element

Produkter med digitala element får tillhandahållas på marknaden endast om

- a) de uppfyller de väsentliga cybersäkerhetskraven i bilaga I del I, förutsatt att de är korrekt installerade och underhållna och används för avsett ändamål eller under förhållanden som rimligen kan förutses och, i tillämpliga fall, att de nödvändiga säkerhetsuppdateringarna har installerats, och
- b) de processer som införs av tillverkaren uppfyller de väsentliga cybersäkerhetskrav som fastställs i bilaga I del II.

Artikel 7

Viktiga produkter med digitala element

1. Produkter med digitala element som har kärnfunktionen hos en produktkategori som anges i bilaga III till denna förordning ska anses vara viktiga produkter med digitala element och ska omfattas av de förfaranden för bedömning av överensstämmelse som avses i artikel 32.2 och 32.3. Integreringen av en produkt med digitala element som har kärnfunktionen hos en produktkategori som anges i bilaga III ska inte i sig medföra att den produkt i vilken den är integrerad omfattas av de förfaranden för bedömning av överensstämmelse som avses i artikel 32.2 och 32.3.
2. De kategorier av produkter med digitala element som avses i punkt 1 i denna artikel, indelade i klasserna I och II enligt bilaga III, uppfyller minst ett av följande kriterier:
 - a) Produkten med digitala element utför i första hand funktioner som är kritiska för cybersäkerheten för andra produkter, nät eller tjänster, inbegripet säkerställande av autentisering och åtkomst, intrångsdetektering och intrångsskydd, säkerhet vid slutnoder eller nätskydd.
 - b) Produkten med digitala element utför en funktion som medför en betydande risk för negativa effekter i fråga om dess intensitet och förmåga att störa, kontrollera eller orsaka skada på ett stort antal andra produkter eller på användarnas hälsa, säkerhet eller skydd genom direkt manipulering, såsom en central systemfunktion, inbegripet nätförvaltning, konfigurationsstyrning, virtualisering eller behandling av personuppgifter.

3. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 61 för att ändra bilaga III genom att införa en ny kategori inom varje klass i förteckningen över kategorier av produkter med digitala element och specificera dess definition, flytta en kategori av produkter från en klass till en annan eller stryka en befintlig kategori från förteckningen. När kommissionen bedömer behovet av en ändring av förteckningen i bilaga III ska den ta hänsyn till de cybersäkerhetsrelaterade funktionerna eller funktionen och nivån på den cybersäkerhetsrisk som produkterna med digitala element utgör enligt de kriterier som avses i punkt 2 i den här artikeln.

De delegerade akter som avses i första stycket i denna punkt ska, när så är lämpligt, föreskriva en övergångsperiod på minst tolv månader, särskilt när en ny kategori av viktiga produkter med digitala element läggs till i klass I eller II eller flyttas från klass I till II enligt bilaga III, innan de relevanta förfaranden för bedömning av överensstämmelse som avses i artikel 32.2 och 32.3 börjar tillämpas, såvida inte en kortare övergångsperiod är motiverad av tvingande skyndsamhetsskäl.

4. Senast den 11 december 2025 ska kommissionen anta en genomförandeakt som specificerar den tekniska beskrivningen av kategorierna av produkter med digitala element i klasserna I och II enligt bilaga III och den tekniska beskrivningen av kategorierna av produkter med digitala element enligt bilaga IV. Denna genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 62.2.

Artikel 8

Kritiska produkter med digitala element

1. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 61 med för att komplettera denna förordning för att fastställa vilka produkter med digitala element och med kärnfunktionen hos en produktkategori som anges i bilaga IV till denna förordning som ska erhålla ett europeiskt cybersäkerhetscertifikat på åtminstone assurancesnivån "betydande" enligt en europeisk ordning för cybersäkerhetscertifiering som antagits enligt förordning (EU) 2019/881 för att visa överensstämmelse med de väsentliga cybersäkerhetskraven i bilaga I till den här förordningen eller delar därav, förutsatt att en europeisk ordning för cybersäkerhetscertifiering som omfattar dessa kategorier av produkter med digitala element har antagits i enlighet med förordning (EU) 2019/881 och är tillgänglig för tillverkarna. Dessa delegerade akter ska specificera den assurancesnivå som krävs, vilken ska stå i proportion till den nivå av cybersäkerhetsrisk som är förbunden med produkterna med digitala element och ska ta hänsyn till deras avsedda ändamål, inbegripet det kritiska beroendet av dem av väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555.

Innan kommissionen antar sådana delegerade akter ska den göra en bedömning av de planerade åtgärdernas potentiella marknadseffekter och samråda med berörda parter, inbegripet den europeiska gruppen för cybersäkerhetscertifiering som fastställs genom förordning (EU) 2019/881. Bedömningen ska ta hänsyn till medlemsstaternas beredskap och kapacitetsnivå när det gäller att genomföra den relevanta europeiska ordningen för cybersäkerhetscertifiering. Om inga delegerade akter som avses i första stycket i denna punkt har antagits ska produkter med digitala element och med kärnfunktionen hos en produktkategori som anges i bilaga IV omfattas av de förfaranden för bedömning av överensstämmelse som avses i artikel 32.3.

De delegerade akter som avses i första stycket ska föreskriva en övergångsperiod på minst sex månader, såvida inte en kortare övergångsperiod är motiverad av tvingande skyndsamhetsskäl.

2. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 61 för att ändra bilaga IV genom att lägga till eller stryka kategorier av produkter med digitala element. Vid fastställandet av sådana kategorier av kritiska produkter med digitala element och den assurancesnivå som krävs, i enlighet med punkt 1 i den här artikeln, ska kommissionen beakta de kriterier som avses i artikel 7.2 och säkerställa att kategorierna av produkter med digitala element uppfyller minst ett av följande kriterier:

- a) Väsentliga entiteter som avses i artikel 3 i direktiv (EU) 2022/2555 har ett kritiskt beroende av kategorier av produkter med digitala element.
- b) Incidenter och utnyttjade sårbarheter som rör kategorier av produkter med digitala element kan leda till allvarliga störningar i kritiska leveranskedjor på den inre marknaden.

Innan kommissionen antar sådana delegerade akter ska den göra en bedömning av den typ som avses i punkt 1.

De delegerade akter som avses i första stycket ska föreskriva en övergångsperiod på minst sex månader, såvida inte en kortare övergångsperiod är motiverad av tvingande skyndsamhetsskäl.

Artikel 9

Samråd med berörda parter

1. När kommissionen utarbetar åtgärder för genomförandet av denna förordning ska den samråda med och beakta synpunkter från berörda parter, såsom berörda myndigheter i medlemsstaterna, företag i den privata sektorn, inbegripet mikroföretag och små och medelstora företag, gemenskapen för programvara med fri och öppen källkod, konsumentorganisationer, den akademiska världen och relevanta unionsbyråer och unionsorgan samt expertgrupper som inrättats på unionsnivå. I synnerhet ska kommissionen på ett strukturerat sätt, när så är lämpligt, samråda med och inhämta synpunkter från dessa berörda parter när den

- a) utarbetar den vägledning som avses i artikel 26,
 - b) utarbetar de tekniska beskrivningarna av de produktkategorier som anges i bilaga III i enlighet med artikel 7.4, bedömer behovet av eventuella uppdateringar av förteckningen över produktkategorier i enlighet med artiklarna 7.3 och 8.2 eller genomför den bedömning av potentiella marknadseffekter som avses i artikel 8.1, utan att det påverkar tillämpningen av artikel 61,
 - c) gör förberedande arbete inför utvärderingen och översynen av denna förordning.
2. Kommissionen ska anordna regelbundna samråd och informationsmöten, minst en gång om året, för att inhämta synpunkter från de berörda parter som avses i punkt 1 om genomförandet av denna förordning.

Artikel 10

Förbättra kompetensen i en cyberresilient digital miljö

Vid tillämpningen av denna förordning och för att tillgodose yrkesutövarnas behov, till stöd för genomförandet av denna förordning, ska medlemsstaterna – när så är lämpligt med stöd av kommissionen, Europeiska kompetenscentrumet för cybersäkerhet och Enisa och med full respekt för medlemsstaternas ansvar på utbildningsområdet – främja åtgärder och strategier som syftar till att

- a) utveckla cybersäkerhetskompetensen och skapa organisatoriska och tekniska verktyg för att säkerställa tillräcklig tillgång till kvalificerad arbetskraft för att stödja verksamheten vid marknadskontrollmyndigheterna och organen för bedömning av överensstämmelse,
- b) förbättra samarbetet mellan den privata sektorn, ekonomiska aktörer, bland annat genom omskolning eller kompetenshöjning för tillverkares anställda, konsumenter, utbildningsanordnare och även offentliga förvaltningar, och därmed utöka möjligheterna för unga att få jobb inom cybersäkerhetssektorn.

Artikel 11

Allmän produktsäkerhet

Som avvikelse från artikel 2.1 tredje stycket b i förordning (EU) 2023/988 ska kapitel III avsnitt 1, kapitlen V och VII och kapitlen IX–XI i den förordningen tillämpas på produkter med digitala element med avseende på aspekter och risker eller riskkategorier som inte omfattas av den här förordningen, om dessa produkter inte omfattas av särskilda säkerhetskrav som fastställs i annan av *unionsharmoniseringslagstiftning* enligt definitionen i artikel 3.27 i förordning (EU) 2023/988.

Artikel 12

AI-system med hög risk

1. Utan att det påverkar tillämpningen av kraven på noggrannhet och robusthet som fastställs i artikel 15 i förordning (EU) 2024/1689 ska produkter med digitala element vilka omfattas av denna förordning och klassificeras som AI-system med hög risk enligt artikel 6 i den förordningen anses överensstämma med de cybersäkerhetskrav som fastställs i artikel 15 i den förordningen om

- a) dessa produkter uppfyller de väsentliga cybersäkerhetskrav som fastställs i bilaga I del I,
- b) de processer som tillverkaren infört uppfyller de väsentliga cybersäkerhetskrav som fastställs i bilaga I del II, och

c) uppnåendet av den nivå av cybersäkerhetsskydd som krävs enligt artikel 15 i förordning (EU) 2024/1689 visas genom en EU-försäkran om överensstämmelse som utfärdats enligt denna förordning.

2. För de produkter med digitala element och cybersäkerhetskrav som avses i punkt 1 i denna artikel ska det relevanta förfarande för bedömning av överensstämmelse som föreskrivs i artikel 43 i förordning (EU) 2024/1689 tillämpas. Vid denna bedömning ska anmälda organ som är behöriga att kontrollera överensstämmelsen för AI-system med hög risk inom ramen för förordning (EU) 2024/1689 också vara behöriga att kontrollera överensstämmelsen med kraven i bilaga I till denna förordning för AI-system med hög risk inom ramen för denna förordning, förutsatt att dessa anmälda organs uppfyllande av kraven i artikel 39 i denna förordning har bedömts i samband med anmälningsförfarandet inom ramen för förordning (EU) 2024/1689.

3. Genom avvikelse från punkt 2 i denna artikel ska viktiga produkter med digitala element som förtecknas i bilaga III till denna förordning, vilka omfattas av de förfaranden för bedömning av överensstämmelse som avses i artikel 32.2 a och b och 32.3 i denna förordning, och kritiska produkter med digitala element som förtecknas i bilaga IV till denna förordning, vilka måste få ett europeiskt cybersäkerhetscertifikat enligt artikel 8.1 i denna förordning, eller i avsaknad av det, vilka omfattas av de förfaranden för bedömning av överensstämmelse som avses i artikel 32.3 i denna förordning, och vilka klassificeras som AI-system med hög risk enligt artikel 6 i förordning (EU) 2024/1689 och omfattas av förfarandet för bedömning av överensstämmelse som grundar sig på intern kontroll enligt bilaga VI till förordning (EU) 2024/1689, genomgå de förfaranden för bedömning av överensstämmelse som föreskrivs i den här förordningen i den mån som de väsentliga cybersäkerhetskrav som anges i den här förordningen berörs.

4. Tillverkare av produkter med digitala element som avses i punkt 1 i denna artikel får delta i de regulatoriska sandlådor för AI som avses i artikel 57 i förordning (EU) 2024/1689.

KAPITEL II

EKONOMISKA AKTÖRERS SKYLDIGHETER OCH BESTÄMMELSER OM PROGRAMVARA MED FRI OCH ÖPPEN KÄLLKOD

Artikel 13

Tillverkares skyldigheter

1. När en produkt med digitala element släpps ut på marknaden ska tillverkarna säkerställa att den har utformats, utvecklats och producerats i enlighet med de väsentliga cybersäkerhetskrav som fastställs i bilaga I i del I.

2. För att följa punkt 1 ska tillverkarna göra en bedömning av de cybersäkerhetsrisker som är förbundna med en produkt med digitala element och beakta resultatet av bedömningen under planerings-, utformnings-, utvecklings-, produktions-, leverans- och underhållsfaserna för en produkt med digitala element, för att minimera cybersäkerhetsriskerna, förhindra incidenter och minimera deras konsekvenser, inbegripet vad gäller användarnas hälsa och säkerhet.

3. Bedömningen av cybersäkerhetsrisker ska dokumenteras och uppdateras på lämpligt sätt under en stödperiod som ska fastställas i enlighet med punkt 8 i denna artikel. Bedömningen av cybersäkerhetsrisker ska omfatta åtminstone en analys av cybersäkerhetsriskerna på grundval av det avsedda ändamålet och den rimligen förutsebara användningen samt användningsförhållandena för produkten med digitala element, såsom driftsmiljön eller de tillgångar som ska skyddas, med beaktande av hur länge produkten förväntas vara i bruk. Bedömningen av cybersäkerhetsrisker ska ange huruvida, och i så fall på vilket sätt, de säkerhetskrav som anges i bilaga I del I punkt 2 är tillämpliga på den relevanta produkten med digitala element och hur dessa krav genomförs på grundval av bedömningen av cybersäkerhetsrisker. Det ska också anges hur tillverkaren tillämpar bilaga I del I punkt 1 och de krav på sårbarhetshantering som anges i bilaga I del II.

4. När en produkt med digitala element släpps ut på marknaden ska tillverkaren inkludera den bedömning av cybersäkerhetsrisker som avses i punkt 3 i denna artikel i den tekniska dokumentation som krävs enligt artikel 31 och bilaga VII. För de produkter med digitala element som avses i artikel 12 och som också omfattas av andra unionsrättsakter får bedömningen av cybersäkerhetsriskerna ingå i den riskbedömning som krävs enligt dessa unionsrättsakter. I de fall då vissa väsentliga cybersäkerhetskrav inte är tillämpliga på produkten med digitala element ska tillverkaren inkludera en tydlig motivering till detta i den tekniska dokumentationen.

5. För att uppfylla kraven i punkt 1 ska tillverkarna visa tillbörlig aktsamhet när de integrerar komponenter som kommer från tredje part så att dessa komponenter inte komprometterar cybersäkerheten för produkten med digitala element, inbegripet vid integrering av komponenter i programvara med fri och öppen källkod som inte har tillhandahållits på marknaden i samband med kommersiell verksamhet.

6. Tillverkarna ska när de identifierar en sårbarhet i en komponent, inbegripet en komponent med fri och öppen källkod, som är integrerad i en produkt med digitala element, rapportera sårbarheten till den person eller entitet som tillverkar eller underhåller komponenten och åtgärda och avhjälpa sårbarheten i enlighet med de krav på sårbarhetshandtering som anges i bilaga I del II. Om tillverkarna har utvecklat en programvaru- eller hårdvaruändring för att åtgärda sårbarheten i den komponenten ska de dela den relevanta koden eller dokumentationen med den person eller entitet som tillverkar eller underhåller komponenten, när så är lämpligt, i ett maskinläsbart format.

7. Tillverkarna ska systematiskt och på ett sätt som står i proportion till cybersäkerhetsriskernas art dokumentera relevanta cybersäkerhetsaspekter som rör produkterna med digitala element, inbegripet sårbarheter de får kännedom om och all relevant information som tillhandahålls av tredje part, och ska, i förekommande fall, uppdatera bedömningen av cybersäkerhetsrisker för produkterna.

8. När en produkt med digitala element släpps ut på marknaden, och under stödperioden, ska tillverkarna säkerställa att produktens, inbegripet dess komponenters, sårbarheter hanteras effektivt och i enlighet med de väsentliga cybersäkerhetskrav som fastställs i bilaga I del II.

Tillverkarna ska fastställa stödperioden så att den återspeglar den tidsperiod under vilken produkten förväntas vara i bruk, med särskilt beaktande av rimliga förväntningar från användarna, produktens art, inbegripet dess avsedda ändamål, samt relevant unionsrätt som fastställer livslängden för produkter med digitala element. Vid fastställandet av stödperioden får tillverkarna också beakta stödperioderna för produkter med digitala element som erbjuder en liknande funktion som släppts ut på marknaden av andra tillverkare, tillgången till driftsmiljön, stödperioderna för integrerade komponenter som tillhandahåller kärnfunktioner och kommer från tredje parter samt relevant vägledning från den särskilda administrativa samarbetsgruppen (Adco-gruppen), som inrättats enligt artikel 52.15, och kommissionen. De faktorer som ska beaktas vid fastställandet av den stödperiod som ska beaktas på ett sätt som säkerställer proportionalitet.

Utan att det påverkar tillämpningen av andra stycket ska stödperioden vara minst fem år. Om produkten med digitala element förväntas vara i bruk i mindre än fem år ska stödperioden motsvara den förväntade användningstiden.

Med beaktande av de rekommendationer från Adco-gruppen som avses i artikel 52.16 får kommissionen anta delegerade akter i enlighet med artikel 61 för att komplettera denna förordning genom att specificera den minsta tillåtna stödperioden för specifika produktkategorier om uppgifter från marknadskontrollen tyder på otillräckliga stödperioder.

Tillverkarna ska inkludera den information som har beaktats för att fastställa stödperioden för en produkt med digitala element i den tekniska dokumentationen enligt bilaga VII.

Tillverkarna ska ha lämpliga policyer och förfaranden, inbegripet policyer för samordnad delgivning av information om sårbarheter, enligt bilaga I del II punkt 5, för att behandla och åtgärda de potentiella sårbarheter i produkter med digitala element som rapporterats av interna eller externa källor.

9. Tillverkarna ska säkerställa att varje säkerhetsuppdatering som avses i bilaga I del II punkt 8 och som har gjorts tillgänglig för användare under stödperioden förblir tillgänglig efter det att den har utfärdats i minst tio år eller under återstoden av stödperioden, beroende på vilken period som är längst.

10. Om en tillverkare har släppt ut senare väsentligt ändrade versioner av en programvaruprodukt på marknaden får tillverkaren säkerställa överensstämmelse med det väsentliga cybersäkerhetskrav som anges i bilaga I del II punkt 2 endast för den version som tillverkaren senast släppte ut på marknaden, förutsatt att användarna av de versioner som tidigare släppts ut på marknaden kostnadsfritt har tillgång till den version som senast släpptes ut på marknaden och inte ådrar sig ytterligare kostnader för att anpassa den hårdvaru- och programvarumiljö där de använder den ursprungliga versionen av den produkten.

11. Tillverkarna får upprätthålla offentliga programvaruarkiv som förbättrar användarnas tillgång till äldre versioner. I sådana fall ska användarna på ett lättillgängligt sätt få tydlig information om riskerna med att använda programvara som inte stöds.

12. Innan en produkt med digitala element släpps ut på marknaden ska tillverkarna sammanställa den tekniska dokumentation som avses i artikel 31.

De ska genomföra de valda förfaranden för bedömning av överensstämmelse som avses i artikel 32 eller se till att de genomförs.

När det genom detta förfarande för bedömning av överensstämmelse har visats att produkten med digitala element uppfyller de väsentliga cybersäkerhetskraven i bilaga I del I och att de processer som tillverkaren infört uppfyller de väsentliga cybersäkerhetskraven i bilaga I del II, ska tillverkarna upprätta EU-försäkran om överensstämmelse i enlighet med artikel 28 och fästa CE-märkningarna i enlighet med artikel 30.

13. Tillverkarna ska kunna uppvisa den tekniska dokumentationen och EU-försäkran om överensstämmelse för marknadskontrollmyndigheterna i minst tio år efter det att produkten med digitala element har släppts ut på marknaden, eller under stödperioden, beroende på vilken period som är längst.

14. Tillverkarna ska säkerställa att det finns förfaranden som säkerställer att produkter med digitala element som är en del av serietillverkning fortsätter att överensstämma med kraven i denna förordning. Tillverkarna ska på lämpligt sätt ta hänsyn till förändringar i utvecklings- och tillverkningsprocessen eller i utformningen av eller egenskaperna hos produkten med digitala element samt till ändringar av de harmoniserade standarderna, de europeiska ordningarna för cybersäkerhetscertifiering eller de gemensamma specifikationer som avses i artikel 27 med hänvisning till vilka överensstämmelsen för produkten med digitala element försäkras eller genom vars tillämpning överensstämmelsen kontrolleras.

15. Tillverkarna ska säkerställa att deras produkter med digitala element är försedda med typnummer, partinummer, serienummer eller annan identifieringsmärkning eller, om detta inte är möjligt, säkerställa att den informationen fästas på produktens förpackning eller på ett dokument som åtföljer produkten med digitala element.

16. Tillverkarna ska, på produkten med digitala element, på förpackningen eller i ett dokument som åtföljer produkten med digitala element, ange sitt namn, registrerade firmanamn eller registrerade varumärke samt postadress och e-postadress eller andra digitala kontaktuppgifter och, när så är tillämpligt, webbplatsen där de kan kontaktas. Denna information ska också ingå i den information och de instruktioner till användaren som anges i bilaga II. Kontaktuppgifterna ska vara på ett språk som lätt kan förstås av användarna och marknadskontrollmyndigheterna.

17. Vid tillämpningen av denna förordning ska tillverkarna utse en gemensam kontaktpunkt som gör det möjligt för användarna att kommunicera direkt och snabbt med dem, bland annat för att underlätta rapportering om sårbarheter hos produkten med digitala element.

Tillverkarna ska säkerställa att den gemensamma kontaktpunkten lätt kan identifieras av användarna. De ska också inkludera den gemensamma kontaktpunkten i den information och de instruktioner till användaren som anges i bilaga II.

Den gemensamma kontaktpunkten ska göra det möjligt för användarna att välja det kommunikationsmedel som de föredrar och får inte begränsa sådana medel till automatiserade verktyg.

18. Tillverkarna ska säkerställa att produkter med digitala element åtföljs av information och instruktioner till användaren enligt bilaga II i pappersform eller elektronisk form. Sådan information och sådana instruktioner ska tillhandahållas på ett språk som lätt kan förstås av användarna och marknadskontrollmyndigheterna. De ska vara tydliga, begripliga och läsbara. De ska möjliggöra en säker installation, drift och användning av produkter med digitala element. Tillverkarna ska säkerställa att informationen och instruktionerna till användaren enligt bilaga II förblir tillgängliga för användarna och marknadskontrollmyndigheterna i minst tio år efter det att produkten med digitala element har släppts ut på marknaden, eller under stödperioden, beroende på vilken period som är längst. Om sådan information och sådana instruktioner tillhandahålls online ska tillverkarna säkerställa att de är åtkomliga, användarvänliga och tillgängliga online i minst tio år efter det att produkten med digitala element har släppts ut på marknaden, eller under stödperioden, beroende på vilken period som är längst.

19. Tillverkarna ska säkerställa att slutdatumet för den stödperiod som avses i punkt 8, inbegripet åtminstone månad och år, tydligt och begripligt anges vid tidpunkten för köpet på ett lättillgängligt sätt och, i tillämpliga fall, på produkten med digitala element, dess förpackning eller digitalt.

Om det är tekniskt möjligt mot bakgrund av arten av produkt med digitala element ska tillverkarna visa ett meddelande till användarna om att deras produkt med digitala element har nått slutet av stödperioden.

20. Tillverkarna ska antingen lämna en kopia av EU-försäkran om överensstämmelse eller en förenklad EU-försäkran om överensstämmelse tillsammans med produkten med digitala element. Om en förenklad EU-försäkran om överensstämmelse lämnas ska den innehålla den exakta webbadress där det går att få tillgång till hela texten till EU-försäkran om överensstämmelse.

21. Från och med utsläppandet på marknaden och under stödperioden ska en tillverkare som vet eller har skäl att tro att produkten med digitala element eller de processer som införts av tillverkaren inte överensstämmer med de väsentliga cybersäkerhetskraven i bilaga I omedelbart vidta de korrigerande åtgärder som krävs för att bringa produkten med digitala element eller tillverkarens processer i överensstämmelse eller dra tillbaka eller återkalla produkten, såsom lämpligt.

22. Tillverkarna ska på motiverad begäran av en marknadskontrollmyndighet förse denna med all information och dokumentation som behövs för att visa att produkten med digitala element och de processer som införts av tillverkaren överensstämmer med de väsentliga cybersäkerhetskrav som fastställs i bilaga I, i pappersform eller i elektronisk form och på ett språk som lätt kan förstås av myndigheten. Tillverkarna ska samarbeta med marknadskontrollmyndigheten, på dess begäran, om alla åtgärder som vidtas för att undanröja de cybersäkerhetsrisker som den produkt med digitala element som de har släppt ut på marknaden utgör.

23. En tillverkare som upphör med sin verksamhet och därmed inte kan följa denna förordning ska, innan verksamheten upphör, underrätta de berörda marknadskontrollmyndigheterna om detta och även, i möjligaste mån och på alla tillgängliga sätt, underrätta användarna av de relevanta produkterna med digitala element som släppts ut på marknaden om att verksamheten snart kommer att upphöra.

24. Kommissionen får genom genomförandeakter, med beaktande av europeiska eller internationella standarder och bästa praxis, specificera formatet och de aspekter som ska ingå i den programvaruförteckning som avses i bilaga I del II punkt 1. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 62.2.

25. För att bedöma medlemsstaternas och unionens beroende av programvarukomponenter och i synnerhet av komponenter som klassificeras som programvara med fri och öppen källkod får Adco-gruppen besluta att genomföra en unionsomfattande beroendebedömning för specifika kategorier av produkter med digitala element. För detta ändamål får marknadskontrollmyndigheterna begära att tillverkare av sådana kategorier av produkter med digitala element tillhandahåller den relevanta programvaruförteckning som avses i bilaga I del II punkt 1. På grundval av denna information får marknadskontrollmyndigheterna förse Adco-gruppen med anonymiserad och aggregerad information om programvaruberoenden. Adco-gruppen ska lämna en rapport om resultaten av beroendebedömningen till den samarbetsgrupp som inrättats enligt artikel 14 i direktiv (EU) 2022/2555.

Artikel 14

Tillverkarnas rapporteringsskyldigheter

1. En tillverkare ska till den CSIRT-enhet som utsetts till samordnare i enlighet med punkt 7 i denna artikel och samtidigt till Enisa anmäla alla aktivt utnyttjade sårbarheter i produkten med digitala element som tillverkaren får kännedom om. Tillverkaren ska anmäla den aktivt utnyttjade sårbarheten via den gemensamma rapporteringsplattform som inrättats enligt artikel 16.

2. För den anmälan som avses i punkt 1 ska tillverkaren

a) utan onödigt dröjsmål och under alla omständigheter senast 24 timmar efter att ha fått kännedom om den, lämna in en tidig varning om en aktivt utnyttjad sårbarhet och, i tillämpliga fall, ange de medlemsstater på vars territorium tillverkaren känner till att produkten med digitala element har tillhandahållits,

b) såvida inte relevant information redan har lämnats, utan onödigt dröjsmål och under alla omständigheter senast 72 timmar efter att ha fått kännedom om den aktivt utnyttjade sårbarheten, lämna in en anmälan om sårbarhet, som ska innehålla allmän information, om sådan finns tillgänglig, om den berörda produkten med digitala element, den allmänna karaktären av utnyttjandet och sårbarheten i fråga samt eventuella korrigerande eller riskreducerande åtgärder som vidtagits och korrigerande eller riskreducerande åtgärder som användarna kan vidta, och som också, i tillämpliga fall, ska ange hur känslig tillverkaren anser att den anmälda informationen är,

c) såvida inte relevant information redan har lämnats, senast 14 dagar efter det att en korrigerande eller riskreducerande åtgärd blivit tillgänglig, lämna in en slutrapport, som ska innehålla minst följande:

i) En beskrivning av sårbarheten och dess allvarlighetsgrad och konsekvenser.

ii) I förekommande fall information om en fientlig aktör som har utnyttjat eller som utnyttjar sårbarheten.

iii) Detaljer om säkerhetsuppdateringen eller andra korrigerande åtgärder som har gjorts tillgängliga för att avhjälpa sårbarheten.

EUT L, 20.11.2024

SV

3. En tillverkare ska till den CSIRT-enhet som utsetts till samordnare i enlighet med punkt 7 i denna artikel och samtidigt till Enisa anmäla alla allvarliga incidenter som påverkar säkerheten för produkten med digitala element som tillverkaren får kännedom om. Tillverkaren ska anmäla incidenten via den gemensamma rapporteringsplattform som inrättats enligt artikel 16.

4. För den anmälan som avses i punkt 3 ska tillverkaren

a) lämna in en tidig varning om en allvarlig incident som påverkar säkerheten för produkten med digitala element, utan onödigt dröjsmål och under alla omständigheter senast 24 timmar efter att ha fått kännedom om den, och åtminstone ange om tillverkaren misstänker att incidenten orsakats av olagliga eller fientliga handlingar, och i tillämpliga fall även ange de medlemsstater på vars territorium tillverkaren känner till att produkten med digitala element har tillhandahållits,

b) såvida inte relevant information redan har lämnats, utan onödigt dröjsmål och under alla omständigheter senast 72 timmar efter att ha fått kännedom om incidenten, lämna in en incidentanmälan, som ska innehålla allmän information, om sådan finns tillgänglig, om arten av incident, en första bedömning av incidenten samt eventuella korrigerande eller riskreducerande åtgärder som vidtagits och korrigerande eller riskreducerande åtgärder som användarna kan vidta, och som också, i tillämpliga fall, ska ange hur känslig tillverkaren anser att den anmälda informationen är,

c) såvida inte relevant information redan har lämnats, inom en månad efter inlämningen av den incidentanmälan som avses i led b, lämna in en slutrapport, som ska innehålla minst följande:

i) En detaljerad beskrivning av incidenten, inbegripet dess allvarlighetsgrad och konsekvenser.

ii) Den typ av hot eller grundorsak som sannolikt har utlöst incidenten.

iii) Tillämpade och pågående riskreducerande åtgärder.

5. Vid tillämpning av punkt 3 ska en incident som påverkar säkerheten för produkten med digitala element anses vara allvarlig om

a) den inverkar negativt på eller kan inverka negativt på förmågan hos en produkt med digitala element att skydda tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten för känsliga eller viktiga data eller funktioner, eller

b) den har lett eller kan leda till att en skadlig kod införts eller använts i en produkt med digitala element eller i nätverks- och informationssystemet hos en användare av produkten med digitala element.

6. Vid behov får den CSIRT-enhet som utsetts till samordnare som först tog emot anmälan begära att tillverkarna lämnar en delrapport om relevanta statusuppdateringar om den aktivt utnyttjade sårbarheten eller allvarliga incidenten som påverkar säkerheten för produkten med digitala element.

7. De anmälningar som avses i punkterna 1 och 3 i denna artikel ska lämnas in via den gemensamma rapporteringsplattform som avses i artikel 16 med hjälp av en av de slutpunkter för elektronisk anmälan som avses i artikel 16.1. Anmälan ska lämnas in med hjälp av slutpunkten för elektronisk anmälan hos den CSIRT-enhet som utsetts till samordnare i den medlemsstat där tillverkarna har sitt huvudsakliga verksamhetsställe i unionen och ska samtidigt göras tillgänglig för Enisa.

Vid tillämpning av denna förordning ska en tillverkare anses ha sitt huvudsakliga verksamhetsställe i unionen i den medlemsstat där de cybersäkerhetsrelaterade besluten avseende dess produkter med digitala element i huvudsak fattas. Om en sådan medlemsstat inte kan fastställas ska det huvudsakliga verksamhetsstället anses vara beläget i den medlemsstat där den berörda tillverkaren har det verksamhetsställe som har flest anställda i unionen.

Om en tillverkare inte har något huvudsakligt verksamhetsställe i unionen ska tillverkaren lämna in de anmälningar som avses i punkterna 1 och 3 med hjälp av slutpunkten för elektronisk anmälan hos den CSIRT-enhet som utsetts till samordnare i den medlemsstat som fastställs enligt följande ordning och på grundval av den information som tillverkaren har tillgång till:

a) Den medlemsstat där tillverkarens representant som agerar för tillverkarens räkning för det största antalet produkter med digitala element från den tillverkaren är etablerad.

b) Den medlemsstat där den importör som släpper ut det största antalet produkter med digitala element från den tillverkaren är etablerad.

SV

EUT L, 20.11.2024

c) Den medlemsstat där den distributör som tillhandahåller det största antalet produkter med digitala element från den tillverkaren är etablerad.

d) Den medlemsstat där det största antalet användare av produkter med digitala element från den tillverkaren finns.

När det gäller tredje stycket d får en tillverkare lämna in anmälningar om eventuella efterföljande aktivt utnyttjade sårbarheter eller allvarliga incidenter som påverkar säkerheten för produkten med digitala element till samma CSIRT-enhet som utsetts till samordnare till vilken den först rapporterade.

8. Efter att ha fått kännedom om en aktivt utnyttjad sårbarhet eller en allvarlig incident som påverkar säkerheten för produkten med digitala element, ska tillverkaren underrätta de drabbade användarna av produkten med digitala element, och när så är lämpligt alla användare, om den sårbarheten eller incidenten och, vid behov, om riskreducering och eventuella korrigerande åtgärder som användarna kan vidta för att begränsa konsekvenserna av denna sårbarhet eller incident, om lämpligt i ett strukturerat, maskinläsbart format som är enkelt att automatiskt behandla. Om tillverkaren underlåter att underrätta användarna av produkten med digitala element i tid får de CSIRT-enheter som utsetts till samordnare som mottagit anmälan lämna sådan information till användarna när detta anses vara proportionellt och nödvändigt för att förebygga eller mildra konsekvenserna av sårbarheten eller incidenten.

9. Senast den 11 december 2025 ska kommissionen anta delegerade akter i enlighet med artikel 61 i denna förordning för att komplettera denna förordning genom att specificera villkoren för att tillämpa de cybersäkerhetsrelaterade skälen till att skjuta upp spridningen av anmälningar som avses i artikel 16.2 i denna förordning. Kommissionen ska samarbeta med det CSIRT-nätverk som inrättats enligt artikel 15 i direktiv (EU) 2022/2555 och Enisa vid utarbetandet av utkastet till delegerad akt.

10. Kommissionen får genom genomförandakter ytterligare specificera formatet och förfarandena för de anmälningar som avses i denna artikel samt i artiklarna 15 och 16. Dessa genomförandakter ska antas i enlighet med det granskningsförfarande som avses i artikel 62.2. Kommissionen ska samarbeta med CSIRT-nätverket och Enisa vid utarbetandet av dessa utkast till genomförandakter.

Artikel 15

Frivillig rapportering

1. Tillverkarna och andra fysiska eller juridiska personer får, på frivillig basis, till en CSIRT-enhet som utsetts till samordnare eller till Enisa anmäla eventuella sårbarheter i en produkt med digitala element samt cyberhot som kan påverka riskprofilen för en produkt med digitala element.

2. Tillverkarna och andra fysiska eller juridiska personer får, på frivillig basis, till en CSIRT-enhet som utsetts till samordnare eller till Enisa anmäla eventuella incidenter som påverkar säkerheten för produkten med digitala element och tillbud som hade kunnat leda till en sådan incident.

3. Den CSIRT-enhet som utsetts till samordnare eller Enisa ska behandla de anmälningar som avses i punkterna 1 och 2 i denna artikel i enlighet med det förfarande som anges i artikel 16.

Den CSIRT-enhet som utsetts till samordnare får prioritera behandlingen av obligatoriska anmälningar före behandlingen av frivilliga anmälningar.

4. Om en annan fysisk eller juridisk person än tillverkaren anmäler en aktivt utnyttjad sårbarhet eller en allvarlig incident som påverkar säkerheten för en produkt med digitala element i enlighet med punkt 1 eller 2 ska den CSIRT-enhet som utsetts till samordnare, utan onödigt dröjsmål, informera tillverkaren.

5. Den CSIRT-enhet som utsetts till samordnare och Enisa ska säkerställa konfidentialitet och lämpligt skydd för den information som tillhandahålls av den anmälande fysiska eller juridiska personen. Utan att det påverkar förebyggandet, utredningen, avslöjandet och lagföringen av brott får frivillig rapportering inte leda till att den anmälande fysiska eller juridiska personen åläggs ytterligare skyldigheter som den inte skulle ha blivit föremål för om den inte hade lämnat in anmälan.

Artikel 16

Inrättande av en gemensam rapporteringsplattform

1. För de anmälningar som avses i artikel 14.1 och 14.3 samt artikel 15.1 och 15.2 och för att förenkla tillverkarnas rapporteringsskyldigheter ska Enisa inrätta en gemensam rapporteringsplattform. Den dagliga driften av den gemensamma rapporteringsplattformen ska skötas och upprätthållas av Enisa. Strukturen för den gemensamma rapporteringsplattformen ska göra det möjligt för medlemsstaterna och Enisa att införa sina egna slutpunkter för elektronisk anmälan.

2. Efter att ha mottagit en anmälan ska den CSIRT-enhet som utsetts till samordnare som först tog emot anmälan, utan dröjsmål, sprida anmälan via den gemensamma rapporteringsplattformen till de CSIRT-enheter som utsetts till samordnare på det territorium där tillverkaren har angett att produkten med digitala element har tillhandahållits.

Under exceptionella omständigheter, särskilt på begäran av tillverkaren och mot bakgrund av känslighetsnivån hos den anmälda information som tillverkaren angett i enlighet med artikel 14.2 a i denna förordning, får spridningen av anmälan skjutas upp på grundval av motiverade cybersäkerhetsrelaterade skäl under en tidsperiod som är absolut nödvändig, inbegripet när en sårbarhet är föremål för ett förfarande för samordnad delgivning av information om sårbarheter som avses i artikel 12.1 i direktiv (EU) 2022/2555. Om en CSIRT-enhet beslutar att undanhålla en anmälan ska den omedelbart informera Enisa om beslutet och motivera varför anmälan undanhålls och ange när den kommer att sprida anmälan i enlighet med det spridningsförfarande som fastställs i denna punkt. Enisa får stödja CSIRT-enheten i tillämpningen av cybersäkerhetsrelaterade skäl när det gäller att skjuta upp spridningen av anmälan.

Under särskilt exceptionella omständigheter, om tillverkaren i den anmälan som avses i artikel 14.2 b anger att

- a) den anmälda sårbarheten aktivt har utnyttjats av en fientlig aktör och att den, enligt tillgänglig information, inte har utnyttjats i någon annan medlemsstat än den där den CSIRT-enhet som utsetts till samordnare finns till vilken tillverkaren har anmält sårbarheten,
- b) all omedelbar ytterligare spridning av den anmälda sårbarheten sannolikt skulle leda till tillhandahållande av information vars utlämnande skulle strida mot den medlemsstatens väsentliga intressen, eller
- c) den anmälda sårbarheten utgör en överhängande hög cybersäkerhetsrisk till följd av den fortsatta spridningen,

ska endast information om att tillverkaren har gjort en anmälan, allmän information om produkten, den allmänna karaktären av utnyttjandet och information om att säkerhetsrelaterade skäl angetts göras tillgänglig samtidigt för Enisa till dess att den fullständiga anmälan sprids till de berörda CSIRT-enheterna och Enisa. Om Enisa på grundval av denna information anser att det finns en systemrisk som påverkar säkerheten på den inre marknaden ska Enisa rekommendera den mottagande CSIRT-enheten att sprida den fullständiga anmälan till de andra CSIRT-enheter som utsetts till samordnare och till Enisa själv.

3. Efter att ha mottagit en anmälan om en aktivt utnyttjad sårbarhet i en produkt med digitala element eller om en allvarlig incident som påverkar säkerheten för en produkt med digitala element ska de CSIRT-enheter som utsetts till samordnare förse marknadskontrollmyndigheterna i sina respektive medlemsstater med den anmälda information som behövs för att marknadskontrollmyndigheterna ska kunna fullgöra sina skyldigheter enligt denna förordning.

4. Enisa ska vidta lämpliga och proportionella tekniska, operativa och organisatoriska åtgärder för att hantera säkerhetsriskerna för den gemensamma rapporteringsplattformen och den information som lämnas in eller sprids via den gemensamma rapporteringsplattformen. Enisa ska utan onödigt dröjsmål underrätta CSIRT-nätverket och kommissionen om alla säkerhetsincidenter som påverkar den gemensamma rapporteringsplattformen.

5. Enisa ska, i samarbete med CSIRT-nätverket, tillhandahålla och genomföra specifikationer för de tekniska, operativa och organisatoriska åtgärderna för inrättande, underhåll och säker drift av den gemensamma rapporteringsplattform som avses i punkt 1, inbegripet åtminstone säkerhetsarrangemangen i samband med inrättande, drift och underhåll av den gemensamma rapporteringsplattformen, samt de slutpunkter för elektronisk anmälan som inrättats av de CSIRT-enheter som utsetts till samordnare på nationell nivå och Enisa på unionsnivå, inbegripet förfarandemässiga aspekter för att – i fall där det för en anmäld sårbarhet inte finns några korrigerande eller riskreducerande åtgärder – säkerställa att information om denna sårbarhet delas i enlighet med strikta säkerhetsprotokoll och på grundval av behovsenlig behörighet.

6. Om en CSIRT-enhet som utsetts till samordnare har uppmärksammats på en aktivt utnyttjad sårbarhet, som en del av ett förfarande för samordnad delgivning av information om sårbarheter som avses i artikel 12.1 i direktiv (EU) 2022/2555, får den CSIRT-enhet som utsetts till samordnare som först tog emot anmälan skjuta upp spridningen av den berörda anmälan via den gemensamma rapporteringsplattformen på grundval av motiverade cybersäkerhetsrelaterade skäl under en period som inte är längre än vad som är absolut nödvändigt och till dess att de berörda parterna inom samordnad delgivning av information om sårbarheter har gett sitt samtycke till utlämnande. Detta krav ska inte hindra tillverkarna från att frivilligt anmäla en sådan sårbarhet i enlighet med förfarandet i denna artikel.

Artikel 17

Andra bestämmelser avseende rapportering

1. Enisa får lämna information som anmälts enligt artikel 14.1 och 14.3 samt artikel 15.1 och 15.2 i denna förordning till Europeiska kontaktnätverket för cyberkriser (EU-CyCLONE), som inrättats enligt artikel 16 i direktiv (EU) 2022/2555, om informationen är relevant för den samordnade hanteringen av storskaliga cybersäkerhetsrelaterade skäl under en operativ nivå. För att fastställa sådan relevans får Enisa överväga tekniska analyser som utförs av CSIRT-nätverket, om sådana finns tillgängliga.

2. Om det är nödvändigt att informera allmänheten för att förebygga eller begränsa en allvarlig incident som påverkar säkerheten för produkten med digitala element eller för att hantera en pågående incident, eller om ett avslöjande av incidenten på annat sätt ligger i allmänhetens intresse, får den CSIRT-enhet som utsetts till samordnare för den berörda medlemsstaten, efter samråd med den berörda tillverkaren och, när så är lämpligt, i samarbete med Enisa, informera allmänheten om incidenten eller kräva att tillverkaren gör detta.

3. På grundval av de anmälningar som inkommer enligt artikel 14.1 och 14.3 samt artikel 15.1 och 15.2 i denna förordning ska Enisa vartannat år utarbeta en teknisk rapport om nya trender i fråga om cybersäkerhetsrisker i produkter med digitala element, och lämna den till den samarbetsgrupp som inrättats enligt artikel 14 i direktiv (EU) 2022/2555. Den första av dessa rapporter ska lämnas in inom 24 månader från det att de skyldigheter som fastställs i artikel 14.1 och 14.3 i denna förordning börjar tillämpas. Enisa ska inkludera relevant information från sina tekniska rapporter i sin rapport om cybersäkerhetssituationen i unionen enligt artikel 18 i direktiv (EU) 2022/2555.

4. Själva anmälan i enlighet med artikel 14.1 och 14.3 eller artikel 15.1 och 15.2 ska inte medföra ökat ansvar för den anmälande fysiska eller juridiska personen.

5. Efter det att en säkerhetsuppdatering eller någon annan form av korrigerande eller riskreducerande åtgärd finns tillgänglig ska Enisa, i samförstånd med tillverkaren av den berörda produkten med digitala element, lägga till den allmänt kända sårbarhet som anmälts enligt artikel 14.1 eller 15.1 i denna förordning i den europeiska sårbarhetsdatabas som inrättats enligt artikel 12.2 i direktiv (EU) 2022/2555.

6. De CSIRT-enheter som utsetts till samordnare ska tillhandahålla hjälptjänster i samband med rapporterings-skyldigheterna enligt artikel 14 till tillverkare, särskilt tillverkare som kan betecknas som mikroföretag eller små eller medelstora företag.

Artikel 18

Tillverkarens representanter

1. En tillverkare får genom skriftlig fullmakt utse en tillverkarens representant.

2. Skyldigheterna enligt artikel 13.1–13.11 och artikel 13.12 första stycket samt artikel 13.14 får inte delegeras till tillverkarens representant.

3. Tillverkarens representant ska utföra de uppgifter som anges i fullmakten från tillverkaren. Tillverkarens representant ska på begäran lämna en kopia av fullmakten till marknadskontrollmyndigheterna. Fullmakten ska ge tillverkarens representant rätt att göra minst följande:

- a) Inneha den EU-försäkringen om överensstämmelse som avses i artikel 28 och den tekniska dokumentation som avses i artikel 31 för att kunna uppvisa dem för marknadskontrollmyndigheterna i minst tio år efter det att produkten med digitala element har släppts ut på marknaden, eller under stödperioden, beroende på vilken period som är längst.
- b) På motiverad begäran av en marknadskontrollmyndighet förse denna med all information och dokumentation som behövs för att visa överensstämmelsen för en produkt med digitala element.

- c) På marknadskontrollmyndigheternas begäran samarbeta med dem om åtgärder som vidtas för att undanröja riskerna med en produkt med digitala element som omfattas av fullmakten för tillverkarens representant.

Artikel 19

Importörers skyldigheter

1. Importörer får på marknaden endast släppa ut sådana produkter med digitala element som uppfyller de väsentliga cybersäkerhetskraven i del I i bilaga I och för vilka de processer som införts av tillverkaren uppfyller de väsentliga cybersäkerhetskraven i del II i bilaga I.
2. Innan en produkt med digitala element släpps ut på marknaden ska importörerna säkerställa att
 - a) de tillämpliga förfaranden för bedömning av överensstämmelse som avses i artikel 32 har genomförts av tillverkaren,
 - b) tillverkaren har upprättat den tekniska dokumentationen, och
 - c) produkten med digitala element är försedd med den CE-märkning som avses i artikel 30 och åtföljs av den EU-försäkran om överensstämmelse som avses i artikel 13.20 och den information och de instruktioner till användaren som anges i bilaga II på ett språk som lätt kan förstås av användarna och marknadskontrollmyndigheterna,
 - d) tillverkaren har uppfyllt kraven i artikel 13.15, 13.16 och 13.19.

Vid tillämpningen av denna punkt ska importörerna kunna tillhandahålla nödvändiga dokument som styrker att kraven i denna artikel är uppfyllda.

3. Om en importör anser eller har skäl att tro att en produkt med digitala element eller de processer som införts av tillverkaren inte överensstämmer med denna förordning, får importören inte släppa ut produkten på marknaden förrän produkten eller processerna som införts av tillverkaren har bringats till överensstämmelse med denna förordning. Om en produkt med digitala element utgör en betydande cybersäkerhetsrisk ska importören också underrätta tillverkaren och marknadskontrollmyndigheterna om detta.

Om en importör har skäl att tro att en produkt med digitala element kan utgöra en betydande cybersäkerhetsrisk mot bakgrund av icke-tekniska riskfaktorer, ska importören underrätta marknadskontrollmyndigheterna om detta. Vid mottagandet av sådan information ska marknadskontrollmyndigheterna följa de förfaranden som avses i artikel 54.2.

4. På produkter med digitala element eller på förpackningen eller i ett dokument som åtföljer produkten med digitala element ska importörer ange namn, registrerat firmanamn eller registrerat varumärke, postadress, e-postadress eller annan digital kontaktuppgift samt, i tillämpliga fall, webbplatsen där de kan kontaktas. Kontaktuppgifterna ska vara på ett språk som lätt kan förstås av användarna och marknadskontrollmyndigheterna.

5. Importörer som vet eller har skäl att tro att en produkt med digitala element som de har släppt ut på marknaden inte överensstämmer med denna förordning ska omedelbart vidta de korrigerande åtgärder som krävs för att säkerställa att produkten överensstämmer med denna förordning eller dra tillbaka eller återkalla produkten, om så är lämpligt.

När importörer blir medvetna om en sårbarhet i en produkt med digitala element ska de utan dröjsmål underrätta tillverkaren om denna. Om en produkt med digitala element utgör en betydande cybersäkerhetsrisk ska importörerna dessutom omedelbart underrätta marknadskontrollmyndigheterna i de medlemsstater på vilkas marknad de har tillhandahållit produkten med digitala element, och lämna uppgifter om i synnerhet den bristande överensstämmelsen och de korrigerande åtgärder som vidtagits.

6. Under minst tio år efter det att produkten med digitala element har släppts ut på marknaden eller under stödperioden, beroende på vilken period som är längst, ska importörerna kunna uppvisa en kopia av EU-försäkran om överensstämmelse för marknadskontrollmyndigheterna och säkerställa att dessa myndigheter på begäran kan få tillgång till den tekniska dokumentationen.

7. Importörerna ska på motiverad begäran av en marknadskontrollmyndighet förse denna med all information och dokumentation som behövs för att visa att produkten med digitala element överensstämmer med de väsentliga cybersäkerhetskrav som fastställs i del I i bilaga I och att de processer som införts av tillverkaren överensstämmer med de väsentliga cybersäkerhetskrav som fastställs i del II i bilaga I, i pappersform eller i elektronisk form och på ett språk som lätt

SV

EUT L, 20.11.2024

kan förstås av myndigheten. De ska på begäran samarbeta med den myndigheten om de åtgärder som vidtas för att undanröja de cybersäkerhetsrisker som den produkt med digitala element som de släppt ut på marknaden utgör.

8. När en importör av en produkt med digitala element får kännedom om att produktens tillverkare upphört med sin verksamhet och därmed inte kan uppfylla de skyldigheter som fastställs i denna förordning ska importören underrätta berörda marknadskontrollmyndigheter om detta och även, i möjligaste mån och på alla tillgängliga sätt, underrätta användarna av de produkter med digitala element som släppts ut på marknaden.

Artikel 20

Distributörers skyldigheter

1. När distributörerna tillhandahåller en produkt med digitala element på marknaden ska de agera med vederbörligt iakttagande av kraven i denna förordning.

2. Innan distributörerna tillhandahåller en produkt med digitala element på marknaden ska de kontrollera att

- a) produkten med digitala element är försedd med CE-märkning,
- b) tillverkaren och importören har uppfyllt de krav som anges i artikel 13.15, 13.16, 13.18, 13.19, 13.20 och artikel 19.4, och har försett distributören med alla dokument som krävs.

3. Om en distributör på grundval av information som distributören förfogar över anser eller har skäl att tro att en produkt med digitala element eller de processer som införts av tillverkaren inte överensstämmer med de väsentliga cybersäkerhetskraven i bilaga I, får distributören inte tillhandahålla produkten på marknaden förrän produkten eller processerna som införts av tillverkaren har bringats till överensstämmelse med denna förordning. Om en produkt med digitala element utgör en betydande cybersäkerhetsrisk ska distributören utan onödigt dröjsmål underrätta tillverkaren och marknadskontrollmyndigheterna om detta.

4. Distributörer som på grundval av information som distributörerna förfogar över vet eller har skäl att tro att en produkt med digitala element, som de har tillhandahållit på marknaden, eller de processer som införts av tillverkaren inte överensstämmer med denna förordning ska se till att de korrigerande åtgärder som krävs för att bringa produkten eller tillverkarens processer i överensstämmelse vidtas, eller dra tillbaka eller återkalla produkten, om så är lämpligt.

När importörer blir medvetna om en sårbarhet i en produkt med digitala element ska de utan dröjsmål underrätta tillverkaren om denna. Om en produkt med digitala element utgör en betydande cybersäkerhetsrisk ska distributörerna dessutom omedelbart underrätta marknadskontrollmyndigheterna i de medlemsstater på vilkas marknad de har tillhandahållit produkten med digitala element, och lämna uppgifter om i synnerhet den bristande överensstämmelsen och de korrigerande åtgärder som vidtagits.

5. Distributörerna ska på motiverad begäran av en marknadskontrollmyndighet förse denna med all information och dokumentation som behövs för att visa att produkten med digitala element och de processer som införts av tillverkaren överensstämmer med denna förordning, i pappersform eller i elektronisk form och på ett språk som lätt kan förstås av myndigheten. De ska på begäran samarbeta med marknadskontrollmyndigheten om de åtgärder som vidtas för att undanröja de cybersäkerhetsrisker som den produkt med digitala element som de tillhandahåller på marknaden utgör.

6. När en distributör av en produkt med digitala element på grundval av information som distributören förfogar över får kännedom om att produktens tillverkare upphört med sin verksamhet och därmed inte kan uppfylla de skyldigheter som fastställs i denna förordning ska distributören utan onödigt dröjsmål underrätta berörda marknadskontrollmyndigheter om detta och även, i möjligaste mån och på alla tillgängliga sätt, underrätta användarna av de produkter med digitala element som släppts ut på marknaden.

Artikel 21

Fall där tillverkares skyldigheter gäller för importörer och distributörer

En importör eller distributör ska anses som tillverkare enligt denna förordning och omfattas av artiklarna 13 och 14 om importören eller distributören släpper ut en produkt med digitala element på marknaden i eget namn eller under eget varumärke eller utför en väsentlig ändring av en produkt med digitala element som redan har släppts ut på marknaden.

Artikel 22

Andra fall där tillverkarnas skyldigheter gäller

1. En fysisk eller juridisk person, annan än tillverkaren, importören eller distributören, som utför en väsentlig ändring av en produkt med digitala element och tillhandahåller den produkten på marknaden ska anses som tillverkare vid tillämpningen av denna förordning.
2. Den person som avses i punkt 1 i denna artikel ska omfattas av de skyldigheter som fastställs i artiklarna 13 och 14 när det gäller den del av produkten med digitala element som påverkas av den väsentliga ändringen eller, om den väsentliga ändringen påverkar cybersäkerheten för produkten med digitala element som helhet, för hela produkten.

Artikel 23

Identifiering av ekonomiska aktörer

1. Ekonomiska aktörer ska på begäran förse marknadskontrollmyndigheterna med följande information:
 - a) Namn och adress för ekonomiska aktörer som har levererat en produkt med digitala element till dem.
 - b) Namn och adress för ekonomiska aktörer som de har levererat en produkt med digitala element till, om tillgängligt.
2. De ekonomiska aktörerna ska kunna tillhandahålla den information som avses i punkt 1 i tio år efter det att de har fått en produkt med digitala element levererad och i tio år efter det att de har levererat en produkt med digitala element.

Artikel 24

Skyldigheter för förvaltare av programvara med fri och öppen källkod

1. Förvaltare av programvara med fri och öppen källkod ska på ett verifierbart sätt införa och dokumentera en cybersäkerhetspolicy så att det utvecklas en säker produkt med digitala element och så att utvecklarna av den produkten effektivt hanterar sårbarheter. I denna policy ska också ingå att utvecklarna av den produkten frivilligt rapporterar sårbarheter enligt artikel 15 och att den särskilda karaktären hos förvaltaren av programvara med fri och öppen källkod beaktas liksom de rättsliga och organisatoriska arrangemang som förvaltaren omfattas av. Policyn ska särskilt omfatta aspekter som rör dokumentering, hantering och avhjälpande av sårbarheter och främja utbyte av information om sårbarheter som upptäckts inom nätgemenskapen för öppen källkodsprojekt.
2. Förvaltarna av programvara med fri och öppen källkod ska samarbeta med marknadskontrollmyndigheterna på deras begäran i syfte att minska cybersäkerhetsriskerna med en produkt med digitala element som klassificeras som programvara med fri och öppen källkod.

På motiverad begäran från en marknadskontroll myndighet ska förvaltare av programvara med fri och öppen källkod förse den myndigheten med den dokumentation som avses i punkt 1, på ett språk som lätt kan förstås av den myndigheten, i pappersform eller elektronisk form.
3. De skyldigheter som fastställs i artikel 14.1 ska tillämpas på förvaltare av programvara med fri och öppen källkod i den mån de deltar i utvecklingen av produkter med digitala element. De skyldigheter som fastställs i artikel 14.3 och 14.8 ska tillämpas på förvaltare av programvara med fri och öppen källkod i den mån allvarliga incidenter som påverkar säkerheten för produkter med digitala element påverkar de nätverks- och informationssystem som tillhandahålls av förvaltarna för programvara med fri och öppen källkod för utvecklingen av sådana produkter.

Artikel 25

Säkerhetsintyg för programvara med fri och öppen källkod

I syfte att underlätta den skyldighet att visa tillbörlig aktsamhet som anges i artikel 13.5, särskilt när det gäller tillverkare som införbar komponenter av programvara med fri och öppen källkod i sina produkter med digitala element, ges kommissionen befogenhet att anta delegerade akter i enlighet med artikel 61 för att komplettera denna förordning genom att inrätta frivilliga program för säkerhetsintyg som gör det möjligt för utvecklare eller användare av produkter med digitala element som klassificeras som programvara med fri och öppen källkod samt andra tredje parter att bedöma sådana produkters överensstämmelse med alla eller vissa väsentliga cybersäkerhetskrav eller andra skyldigheter som fastställs i denna förordning.

SV

EUT L, 20.11.2024

Artikel 26

Vägledning

1. För att underlätta genomförandet av denna förordning och säkerställa ett konsekvent genomförande ska kommissionen offentliggöra vägledning som ska vara till hjälp för de ekonomiska aktörerna vid tillämpningen av denna förordning, med särskilt fokus på att underlätta efterlevnaden för mikroföretag samt små och medelstora företag.

2. Om kommissionen avser att tillhandahålla sådan vägledning som avses i punkt 1 ska den ta upp åtminstone följande aspekter:

- a) Denna förordnings tillämpningsområde, med särskilt fokus på lösningar för fjärrbehandling av data och programvara med fri och öppen källkod.
- b) Tillämpningen av stödperioder med avseende på särskilda kategorier av produkter med digitala element.
- c) Vägledning för tillverkare som omfattas av denna förordning och som också omfattas av annan unionsharmoniseringslagstiftning än denna förordning eller av andra relaterade unionsrättsakter.
- d) Begreppet väsentlig ändring.

Kommissionen ska också upprätthålla en lättillgänglig förteckning över de delegerade akter och genomförandeakter som antagits enligt denna förordning.

- 3. Vid utarbetandet av vägledningen enligt denna artikel ska kommissionen samråda med berörda parter.

KAPITEL III

ÖVERENSSTÄMMELSE FÖR PRODUKTEN MED DIGITALA ELEMENT

Artikel 27

Presumtion om överensstämmelse

1. Produkter med digitala element och processer som införts av tillverkaren som överensstämmer med harmoniserade standarder, eller delar av sådana, vilka har offentliggjorts i *Europeiska unionens officiella tidning*, ska förutsättas överensstämma med de väsentliga cybersäkerhetskrav i bilaga I som omfattas av dessa standarder eller delar av dem.

Kommissionen ska i enlighet med artikel 10.1 i förordning (EU) nr 1025/2012 begära att en eller flera europeiska standardiseringsorganisationer utarbetar harmoniserade standarder för de väsentliga cybersäkerhetskraven i bilaga I till den här förordningen. När kommissionen utarbetar begäranden om standardisering för den här förordningen ska den sträva efter att beakta befintliga europeiska och internationella standarder för cybersäkerhet som införts eller håller på att tas fram, i syfte att förenkla utvecklingen av harmoniserade standarder, i enlighet med förordning (EU) nr 1025/2012.

2. Kommissionen får anta genomförandeakter om fastställande av gemensamma specifikationer som omfattar tekniska krav som gör det möjligt att uppfylla de väsentliga cybersäkerhetskraven i bilaga I för produkter med digitala element som omfattas av denna förordnings tillämpningsområde.

Dessa genomförandeakter får endast antas om följande villkor är uppfyllda:

- a) Kommissionen har, enligt artikel 10.1 i förordning (EU) nr 1025/2012, begärt att en eller flera europeiska standardiseringsorganisationer utarbetar en harmoniserad standard för de väsentliga cybersäkerhetskrav som fastställs i bilaga I och
 - i) begäran har inte godtagits,
 - ii) de harmoniserade standarder som avser begäran levereras inte inom den tidsfrist som fastställs i enlighet med artikel 10.1 i förordning (EU) nr 1025/2012 eller
 - iii) de harmoniserade standarderna överensstämmer inte med begäran.

EUT L, 20.11.2024

SV

- b) Ingen hänvisning till harmoniserade standarder som omfattar de relevanta väsentliga cybersäkerhetskraven i bilaga I till denna förordning har offentliggjorts i *Europeiska unionens officiella tidning* i enlighet med förordning (EU) nr 1025/2012, och ingen sådan hänvisning förväntas offentliggöras inom rimlig tid.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 62.2.

3. Innan kommissionen utarbetar det utkast till genomförandeakt som avses i punkt 2 i den här artikeln ska den informera den kommitté som avses i artikel 22 i förordning (EU) nr 1025/2012 om att den anser att villkoren i punkt 2 i den här artikeln är uppfyllda.

4. När kommissionen utarbetar det utkast till genomförandeakt som avses i punkt 2 ska den ta hänsyn till synpunkter från relevanta organ och vederbörligen samråda med alla berörda parter.

5. Produkter med digitala element och processer som har införts av tillverkaren vilka överensstämmer med de gemensamma specifikationer som fastställts i de genomförandeakter som avses i punkt 2 i denna artikel, eller delar av dem, ska förutsättas överensstämma med de väsentliga cybersäkerhetskraven i bilaga I som omfattas av de gemensamma specifikationerna eller delar av dem.

6. Om en harmoniserad standard antas av en europeisk standardiseringsorganisation och föreslås för kommissionen i syfte att offentliggöra hänvisningen till den i *Europeiska unionens officiella tidning*, ska kommissionen bedöma den harmoniserade standarden i enlighet med förordning (EU) nr 1025/2012. När en hänvisning till en harmoniserad standard offentliggörs i *Europeiska unionens officiella tidning* ska kommissionen upphäva de genomförandeakter som avses i punkt 2 i denna artikel, eller delar av dem som omfattar samma väsentliga cybersäkerhetskrav som de som omfattas av denna harmoniserade standard.

7. Om en medlemsstat anser att en gemensam specifikation inte helt uppfyller de väsentliga cybersäkerhetskraven i bilaga I ska den underrätta kommissionen om detta genom att lämna en detaljerad förklaring. Kommissionen ska bedöma denna detaljerade förklaring och får vid behov ändra genomförandeakten om fastställande av den gemensamma specifikationen i fråga.

8. Produkter med digitala element och processer som har införts av tillverkaren för vilka en EU-försäkrans om överensstämmelse eller ett certifikat har utfärdats enligt förordning (EU) 2019/881, ska förutsättas överensstämma med de väsentliga cybersäkerhetskraven i bilaga I i den mån som EU-försäkrans om överensstämmelse eller det europeiska cybersäkerhetscertifikatet, eller delar av dessa, täcker dessa krav.

9. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 61 i denna förordning, för att komplettera denna förordning genom att specificera vilka europeiska ordningar för cybersäkerhetscertifiering inom ramen för förordning (EU) 2019/881 som kan användas för att visa att produkter med digitala element överensstämmer med de väsentliga cybersäkerhetskrav som fastställs i bilaga I till denna förordning, eller delar av dessa. Utfärdandet av ett europeiskt cybersäkerhetscertifikat inom ramen för sådana system, med åtminstone assurancesnivån "betydande", befriar tillverkaren från skyldigheten att utföra en tredjepartsbedömning av överensstämmelse för de motsvarande kraven, i enlighet med artikel 32.2 a och b och 32.3 a och b i den här förordningen.

Artikel 28

EU-försäkrans om överensstämmelse

1. EU-försäkrans om överensstämmelse ska upprättas av tillverkarna i enlighet med artikel 13.12 och ska ange att det har visats att de tillämpliga väsentliga cybersäkerhetskraven i bilaga I uppfylls.
2. EU-försäkrans om överensstämmelse ska utformas i enlighet med mallen i bilaga V och ska innehålla de uppgifter som anges i de relevanta förfaranden för bedömning av överensstämmelse som fastställs i bilaga VIII. En sådan försäkrans ska uppdateras när så är lämpligt. Den ska tillhandahållas på de språk som krävs av den medlemsstat där produkten med digitala element släpps ut på marknaden eller tillhandahålls på marknaden.

Den förenklade EU-försäkrans om överensstämmelse som avses i artikel 13.20 ska utformas i enlighet med mallen i bilaga VI. Den ska tillhandahållas på de språk som krävs av den medlemsstat där produkten med digitala element släpps ut på marknaden eller tillhandahålls på marknaden.

SV

EUT L, 20.11.2024

3. Om en produkt med digitala element omfattas av mer än en unionsrättsakt där det ställs krav på EU-försäkringen om överensstämmelse ska en enda EU-försäkringen om överensstämmelse upprättas med avseende på alla dessa unionsrättsakter. I denna försäkringen ska det anges vilka unionsrättsakter som berörs, inbegripet EUT-hänvisningarna till dem.
4. Genom att EU-försäkringen om överensstämmelse upprättas ska tillverkaren ta ansvar för att produkten överensstämmer med digitala element.
5. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 61 för att komplettera denna förordning genom att lägga till uppgifter till det minimiinnehåll för EU-försäkringen om överensstämmelse som fastställs i bilaga V, för att ta hänsyn till den tekniska utvecklingen.

Artikel 29

Allmänna principer för CE-märkning

CE-märkningen ska omfattas av de allmänna principer som fastställs i artikel 30 i förordning (EG) nr 765/2008.

Artikel 30

Regler och villkor för anbringande av CE-märkning

1. CE-märkningen ska fästas på produkten med digitala element så att den är synlig, läsbar och outplånlig. Om detta inte är möjligt eller inte är lämpligt på grund av produktens art, ska den fästas på förpackningen och på den EU-försäkringen om överensstämmelse enligt artikel 28 som medföljer produkten med digitala element. För produkter med digitala element i form av programvara ska CE-märkningen fästas antingen på EU-försäkringen om överensstämmelse enligt artikel 28 eller på den webbplats som åtföljer programvaruprodukten. I det sistnämnda fallet ska det relevanta avsnittet på webbplatsen kunna nås enkelt och direkt av konsumenterna.
2. På grund av arten av produkt med digitala element får höjden på den CE-märkning som fästas på produkten understiga 5 mm, förutsatt att den förblir synlig och läsbar.
3. CE-märkningen ska fästas innan produkten med digitala element släpps ut på marknaden. Den får åtföljas av ett piktogram eller annan märkning som anger en särskild cybersäkerhetsrisk eller användning som fastställs i de genomförandeakter som avses i punkt 6.
4. CE-märkningen ska följas av det anmälda organets identifikationsnummer, i de fall då det organet är involverat i det förfarande för bedömning av överensstämmelse baserat på fullständig kvalitetssäkring (baserat på modul H) som avses i artikel 32.

Det anmälda organets identifikationsnummer ska fästas av organet självt eller, enligt organets anvisningar, av tillverkaren eller tillverkarens representant.

5. Medlemsstaterna ska utgå från befintliga mekanismer för att säkerställa att bestämmelserna om CE-märkning tillämpas korrekt och vidta lämpliga åtgärder i händelse av otillbörlig användning av märkningen. I de fall då en produkt med digitala element omfattas av annan unionsharmoniseringslagstiftning än denna förordning som också föreskriver CE-märkning ska CE-märkningen visa att produkten även uppfyller kraven som anges i sådan annan unionsharmoniseringslagstiftning.
6. Kommissionen får genom delegerade akter fastställa tekniska specifikationer för etiketter, piktogram eller andra märkningar som rör säkerheten för produkter med digitala element, deras stödperioder och mekanismer för att främja användningen av sådana och öka allmänhetens medvetenhet om säkerheten hos produkter med digitala element. När kommissionen utarbetar utkast till genomförandeakt ska den samråda med berörda parter och, enligt artikel 52.15, med Adco-gruppen om den redan har inrättats. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 62.2.

Artikel 31

Teknisk dokumentation

1. Den tekniska dokumentationen ska omfatta alla relevanta data eller uppgifter om de metoder som tillverkaren använt för att säkerställa att produkter med digitala element och de processer som införts av tillverkaren uppfyller de väsentliga cybersäkerhetskrav som fastställs i bilaga I. Den ska åtminstone omfatta de aspekter som fastställs i bilaga VII.
2. Den tekniska dokumentationen ska upprättas innan produkten med digitala element släpps ut på marknaden och ska uppdateras kontinuerligt, vid behov, under åtminstone stödperioden.
3. För de produkter med digitala element som avses i artikel 12 vilka även omfattas av andra unionsrättsakter som föreskriver teknisk dokumentation ska en enda serie teknisk dokumentation upprättas med den information som avses i bilaga VII och den information som föreskrivs i andra unionsrättsakter.
4. Den tekniska dokumentation och korrespondens som avser förfaranden för bedömning av överensstämmelse ska upprättas på ett officiellt språk i den medlemsstat där det anmälda organet finns eller på ett språk som kan godtas av det organet.
5. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 61 för att komplettera denna förordning genom att lägga till aspekter som ska ingå i den tekniska dokumentationen enligt bilaga VII för att ta hänsyn till den tekniska utvecklingen, samt utveckling som skett under denna förordnings genomförandeprocess. Kommissionen ska därför säkerställa att den administrativa bördan för mikroföretag samt små och medelstora företag är proportionell.

Artikel 32

Förfaranden för bedömning av överensstämmelse för produkter med digitala element

1. Tillverkaren ska genomföra en bedömning av överensstämmelse avseende produkten med digitala element och de processer som införts av tillverkaren, där det ska fastställas om de väsentliga cybersäkerhetskraven i bilaga I uppfylls. Tillverkaren ska visa överensstämmelse med de väsentliga cybersäkerhetskraven genom att använda
 - a) förfarandet för intern kontroll (baserat på modul A) enligt bilaga VIII,
 - b) EU-typkontroll (baserat på modul B) enligt bilaga VIII, följt av förfarandet för överensstämmelse med EU-typ grundat på intern tillverkningskontroll (baserat på modul C) enligt bilaga VIII,
 - c) överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H) enligt bilaga VIII, eller
 - d) en europeisk ordning för cybersäkerhetscertifiering enligt artikel 27.9, om sådan finns och i tillämpliga fall.
2. Vid bedömningen av om en viktig produkt med digitala element som omfattas av klass I som anges i bilaga III och de processer som införts av dess tillverkare överensstämmer med de väsentliga cybersäkerhetskraven i bilaga I gäller att om tillverkaren inte har tillämpat – eller endast delvis har tillämpat – harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering på minst assurancesnivå "betydande" enligt artikel 27, eller om sådana harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering saknas, ska den berörda produkten med digitala element och de processer som införts av tillverkaren genomgå något av följande förfaranden med avseende på något av dessa väsentliga cybersäkerhetskrav:
 - a) EU-typkontroll (baserat på modul B) som anges i bilaga VIII, följt av förfarandet för överensstämmelse med EU-typ grundat på intern tillverkningskontroll (baserat på modul C) enligt bilaga VIII, eller
 - b) bedömning av överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H) enligt bilaga VIII.
3. Om produkten är en viktig produkt med digitala element som omfattas av klass II enligt bilaga III ska tillverkaren visa överensstämmelsen med de väsentliga cybersäkerhetskraven i bilaga I genom att använda något av följande förfaranden:

SV

EUT L, 20.11.2024

- a) EU-typkontroll (baserat på modul B) enligt bilaga VIII, följd av förfarandet för överensstämmelse med EU-typ grundat på intern tillverkningskontroll (baserat på modul C) enligt bilaga VIII,
 - b) överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H) enligt bilaga VIII, eller
 - c) en europeisk ordning för cybersäkerhetscertifiering enligt artikel 27.9 i denna förordning på minst assurancesnivån "betydande" enligt förordning (EU) 2019/881, om sådan finns och i tillämpliga fall.
4. Kritiska produkter med digitala element som förtecknas i bilaga IV ska visa överensstämmelsen med de väsentliga cybersäkerhetskraven i bilaga I genom att använda
- a) en europeisk ordning för cybersäkerhetscertifiering i enlighet med artikel 8.1, eller
 - b) om villkoren i artikel 8.1 inte är uppfyllda, något av de förfaranden som avses i punkt 3 i denna artikel.
5. Tillverkare av produkter med digitala element som klassificeras som programvara med fri och öppen källkod och som omfattas av de kategorier som anges i bilaga III ska kunna visa överensstämmelse med de väsentliga cybersäkerhetskraven i bilaga I genom att använda ett av de förfaranden som avses i punkt 1 i denna artikel, förutsatt att den tekniska dokumentation som avses i artikel 31 görs tillgänglig för allmänheten när dessa produkter släpps ut på marknaden.
6. Mikroföretags och små och medelstora företags, inklusive uppstarts företags, särskilda intressen och behov ska beaktas när avgifterna för bedömning av överensstämmelse fastställs, och dessa avgifter ska minskas i proportion till företagens särskilda intressen och behov.

Artikel 33

Stödåtgärder för mikroföretag och små och medelstora företag, inbegripet uppstarts företag

1. Medlemsstaterna ska, när så är lämpligt, vidta följande åtgärder som är anpassade till mikroföretags och små företags behov:
- a) Anordna särskild informations- och utbildningsverksamhet om tillämpningen av denna förordning.
 - b) Inrätta en särskild kanal för kommunikation med mikroföretag och små företag och, när så är lämpligt, lokala myndigheter för att ge råd och besvara frågor om genomförandet av denna förordning.
 - c) Stödja provning och bedömning av överensstämmelse, när så är lämpligt även med stöd av Europeiska kompetenscentrumet för cybersäkerhet.
2. Medlemsstaterna får, när så är lämpligt, inrätta regulatoriska sandlådor för cyberresiliens. Sådana regulatoriska sandlådor ska tillhandahålla kontrollerade provmiljöer för innovativa produkter med digitala element för att underlätta utvecklingen, utformningen, valideringen och provningen av dem i syfte att uppfylla kraven i denna förordning under en begränsad tidsperiod innan de släpps ut på marknaden. Kommissionen och, när så är lämpligt, Enisa får tillhandahålla tekniskt stöd, rådgivning och verktyg för inrättande och drift av regulatoriska sandlådor. De regulatoriska sandlådorna ska inrättas under marknadskontrollmyndigheternas direkta tillsyn, vägledning och stöd. Medlemsstaterna ska genom Adco-gruppen informera kommissionen och de andra marknadskontrollmyndigheterna om inrättandet av en regulatorisk sandlåda. De regulatoriska sandlådorna ska inte påverka de behöriga myndigheternas tillsynsbefogenheter och korrigerande befogenheter. Medlemsstaterna ska säkerställa öppen, rättvis och transparent tillgång till regulatoriska sandlådor, och i synnerhet underlätta tillgång för mikroföretag och små företag, inbegripet uppstarts företag.
3. I enlighet med artikel 26 ska kommissionen ge mikroföretag och små och medelstora företag vägledning om genomförandet av denna förordning.
4. Kommissionen ska tillkännage att ekonomiskt stöd inom ramen för unionens befintliga program är tillgängligt, särskilt för att minska den ekonomiska bördan för mikroföretag och små företag.

5. Mikroföretag och små företag får tillhandahålla alla delar av den tekniska dokumentation som anges i bilaga VII med användning av ett förenklat formulär. För detta ändamål ska kommissionen genom genomförandeakter specificera det förenklade formuläret för teknisk dokumentation med hänsyn till mikroföretagens och småföretagens behov, inbegripet hur de uppgifter som anges i bilaga VII ska tillhandahållas. Om ett mikroföretag eller ett småföretag väljer att tillhandahålla den information som anges enligt bilaga VII på ett förenklat sätt ska det använda det formulär som avses i denna punkt. Anmälda organ ska godta detta formulär för bedömning av överensstämmelse.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 62.2.

Artikel 34

Avtal om ömsesidigt erkännande

Med beaktande av den tekniska utvecklingsnivån och ett tredjelandets förhållningssätt till bedömning av överensstämmelse får unionen ingå avtal om ömsesidigt erkännande med tredjeländer, i enlighet med artikel 218 i EUF-fördraget, för att främja och underlätta internationell handel.

KAPITEL IV

ANMÄLAN AV ORGAN FÖR BEDÖMNING AV ÖVERENSSTÄMMELSE

Artikel 35

Anmälan

1. Medlemsstaterna ska till kommissionen och övriga medlemsstater anmäla vilka organ som fått i uppdrag att utföra bedömningar av överensstämmelse i enlighet med denna förordning.
2. Medlemsstaterna ska sträva efter att senast den 11 december 2026 säkerställa att det finns ett tillräckligt antal anmälda organ i unionen för att utföra bedömningar av överensstämmelse, i syfte att undvika flaskhalsar och hinder för marknadstillträde.

Artikel 36

Anmälade myndigheter

1. Varje medlemsstat ska utse en anmälade myndighet med ansvar för att inrätta och genomföra de förfaranden som krävs vid bedömning, utseende och anmälan av organ för bedömning av överensstämmelse och vid kontroll, inklusive överensstämmelse med artikel 41.
2. Medlemsstaterna får besluta att den bedömning och övervakning som avses i punkt 1 ska utföras av ett nationellt ackrediteringsorgan i den mening som avses i och i enlighet med förordning (EG) nr 765/2008.
3. Om den anmälade myndigheten delegerar eller på annat sätt överläter den bedömning, anmälan eller övervakning som avses i punkt 1 i denna artikel till ett organ som inte är offentligt, ska detta organ vara en juridisk person och i tillämpliga delar följa artikel 37. Detta organ ska dessutom ha vidtagit åtgärder för att täcka det ansvar som följer av dess verksamhet.
4. Den anmälade myndigheten ska ta fullt ansvar för de uppgifter som utförs av det organ som avses i punkt 3.

Artikel 37

Krav på anmälade myndigheter

1. En anmälade myndighet ska vara inrättad på ett sådant sätt att det inte uppstår någon intressekonflikt med organen för bedömning av överensstämmelse.
2. En anmälade myndighet ska vara organiserad och fungera på ett sådant sätt att dess verksamhet är objektiv och opartisk.
3. En anmälade myndighet ska vara organiserad på ett sådant sätt att alla beslut som rör anmälan av ett organ för bedömning av överensstämmelse fattas av annan behörig personal än den som utförde bedömningen.

SV

EUT L, 20.11.2024

4. En anmälade myndighet får inte erbjuda eller utföra sådan verksamhet som utförs av organ för bedömning av överensstämmelse eller konsulttjänster på kommersiell eller konkurrensmässig grund.
5. En anmälade myndighet ska skydda den konfidentiella information som den mottar.
6. En anmälade myndighet ska ha tillgång till tillräckligt med personal med lämplig kompetens för att korrekt kunna utföra sina uppgifter.

Artikel 38

Anmälade myndigheters informationsskyldighet

1. Medlemsstaterna ska informera kommissionen om sina förfaranden för bedömning och anmälan av organ för bedömning av överensstämmelse och för övervakning av anmälda organ samt om eventuella ändringar.
2. Kommissionen ska offentliggöra den information som avses i punkt 1.

Artikel 39

Krav på anmälda organ

1. För anmälning ska ett organ för bedömning av överensstämmelse uppfylla de krav som anges i punkterna 2–12.
2. Ett organ för bedömning av överensstämmelse ska inrättas i enlighet med nationell rätt och vara juridisk person.
3. Ett organ för bedömning av överensstämmelse ska vara ett tredjepartsorgan som är oberoende av den organisation eller produkt med digitala element som den bedömer.

Detta organ får vara ett tredjepartsorgan som hör till en näringslivsorganisation eller branschorganisation som företräder företag som är involverade i utformning, utveckling, tillverkning, tillhandahållande, montering, användning eller underhåll av de produkter med digitala element som det bedömer, förutsatt att det kan styrkas att organet är oberoende och att intressekonflikter saknas.

4. Ett organ för bedömning av överensstämmelse, dess högsta ledning och den personal som ansvarar för utförandet av bedömningen av överensstämmelse får inte utgöras av den som utformar, utvecklar, tillverkar, levererar, importerar, distribuerar, installerar, köper, äger, använder eller underhåller de produkter med digitala element som bedöms och inte heller av en representant för någon av dessa parter. Detta ska inte hindra att bedömda produkter som är nödvändiga för verksamheten vid organet för bedömning av överensstämmelse används, eller att produkterna används för personligt bruk.

Ett organ för bedömning av överensstämmelse, deras högsta ledning och den personal som ansvarar för utförandet av bedömningen av överensstämmelse får inte vara direkt inblandade i utformningen, utvecklingen, tillverkningen, importen, distributionen, marknadsföringen, installationen, användningen eller underhållet av de produkter med digitala element som de bedömer, och inte heller representera parter som bedriver sådan verksamhet. De får inte delta i någon verksamhet som kan påverka deras objektivitet och integritet i samband med de bedömningar av överensstämmelse för vilka de har anmälts. Detta ska framför allt gälla konsulttjänster.

Organ för bedömning av överensstämmelse ska säkerställa att deras dotterbolags eller underentreprenörers verksamhet inte påverkar konfidentialiteten, objektiviteten eller opartiskheten i organens bedömningar av överensstämmelse.

5. Organ för bedömning av överensstämmelse och deras personal ska utföra bedömningar av överensstämmelse med största möjliga yrkesintegritet, ha erforderlig teknisk kompetens på det specifika området och vara fria från alla påtryckningar och incitament, i synnerhet ekonomiska incitament, som kan påverka deras omdöme eller resultaten av deras bedömningar av överensstämmelse; detta gäller särskilt påtryckningar och incitament från personer eller grupper av personer som berörs av bedömningarnas resultat.

6. Ett organ för bedömning av överensstämmelse ska kunna utföra alla de uppgifter avseende bedömning av överensstämmelse som avses i bilaga VIII och för vilka det har anmälts, oavsett om dessa uppgifter utförs av organet självt eller för dess räkning och under dess ansvar.

Vid alla tidpunkter och vid varje bedömning av överensstämmelse och för varje typ eller kategori av produkt med digitala element för vilka det har anmälts ska organet för bedömning av överensstämmelse ha till sitt förfogande

EUT L, 20.11.2024

SV

- a) personal med teknisk kunskap och tillräcklig och lämplig erfarenhet för att utföra bedömningen av överensstämmelse,
- b) beskrivningar av förfaranden enligt vilka bedömningar av överensstämmelse utförs; dessa beskrivningar ska säkerställa att förfarandena är transparenta och kan reproduceras. Organet ska ha lämpliga rutiner och förfaranden för att skilja mellan de uppgifter som det utför i sin egenskap av anmält organ och annan verksamhet, och
- c) förfaranden som gör det möjligt för organet att utöva sin verksamhet med vederbörlig hänsyn tagen till ett företags storlek, bransch och struktur, den berörda produktteknikens komplexitet och eventuell mass- eller serietillverkning.

Organet för bedömning av överensstämmelse ska ha de nödvändiga medlen för att korrekt kunna utföra de tekniska och administrativa uppgifterna i samband med bedömningen av överensstämmelse och ska ha tillgång till den utrustning och de hjälpmedel som är nödvändiga.

7. Den personal som ansvarar för att utföra bedömningen av överensstämmelse ska ha

- a) fullgod teknisk och yrkesinriktad utbildning som täcker all slags bedömning av överensstämmelse för vilken organet för bedömning av överensstämmelse har anmälts,
- b) tillfredsställande kunskap om kraven för de bedömningar som de utför och befogenhet att utföra dessa bedömningar,
- c) tillräcklig kännedom och insikt om de väsentliga cybersäkerhetskraven i bilaga I, de tillämpliga harmoniserade standarderna och gemensamma specifikationerna och de relevanta bestämmelserna i unionsharmoniseringslagstiftning och genomförandeakter,
- d) förmåga att upprätta intyg, protokoll och rapporter som visar att bedömningarna har utförts.

8. Det ska garanteras att organen för bedömning av överensstämmelse, deras ledning och bedömningspersonal är opartiska.

Ersättningen till organets ledning och bedömningspersonal får inte vara beroende av antalet bedömningar som gjorts eller resultaten av bedömningarna.

9. Organ för bedömning av överensstämmelse ska vara ansvarsförsäkrade, såvida inte ansvaret åligger medlemsstaten enligt nationell rätt eller medlemsstaten själv tar direkt ansvar för bedömningen av överensstämmelse.

10. Personalen vid ett organ för bedömning av överensstämmelse ska iakttä tystnadsplikt beträffande all information som de erhåller vid utförandet av sina uppgifter enligt bilaga VIII eller bestämmelser i nationell rätt som genomför den, utom gentemot marknadskontrollmyndigheterna i den medlemsstat där verksamheten bedrivs. Åganderätten ska vara skyddad. Organet för bedömning av överensstämmelse ska ha dokumenterade förfaranden som säkerställer uppfyllandet av kraven i denna punkt.

11. Organ för bedömning av överensstämmelse ska delta i, eller säkerställa att deras bedömningspersonal känner till, det relevanta standardiseringsarbetet och det arbete som utförs i samordningsgruppen för anmälda organ, som inrättats enligt artikel 51, och de ska som generella riktlinjer tillämpa de administrativa beslut och dokument som är resultatet av gruppens arbete.

12. Organen för bedömning av överensstämmelse ska fungera enligt konsekventa, rättvisa, proportionella och rimliga villkor och bestämmelser, samtidigt som onödiga bördor för de ekonomiska aktörerna undviks, och när det gäller avgifter särskilt beakta mikroföretags samt små och medelstora företags intressen.

Artikel 40

Presumtion om överensstämmelse för anmälda organ

För ett organ för bedömning av överensstämmelse som kan visa att det uppfyller kriterierna i de relevanta harmoniserade standarderna eller delar av dem till vilka hänvisningar har offentliggjorts i *Europeiska unionens officiella tidning* ska en presumtion om överensstämmelse med kraven i artikel 39 gälla, i den mån som dessa krav omfattas av de tillämpliga harmoniserade standarderna.

SV

EUT L, 20.11.2024

Artikel 41

Dotterbolag och underentreprenörer till anmälda organ

1. Om det anmälda organet lägger ut specifika uppgifter med anknytning till bedömningen av överensstämmelse på underentreprenad eller anlitar ett dotterbolag ska det säkerställa att underentreprenören eller dotterbolaget uppfyller kraven som anges i artikel 39 och informera den anmälade myndigheten om detta.
2. De anmälda organen ska ta det fulla ansvaret för underentreprenörernas eller dotterbolagens uppgifter, oavsett var de är etablerade.
3. Verksamhet får läggas ut på underentreprenad eller utföras av ett dotterbolag endast om tillverkaren samtycker till det.
4. De anmälda organen ska se till att den anmälade myndigheten har tillgång till de relevanta dokumenten rörande bedömningen av underentreprenörens eller dotterbolagets kvalifikationer och det arbete som dessa har utfört i enlighet med denna förordning.

Artikel 42

Ansökan om anmälan

1. Ett organ för bedömning av överensstämmelse ska lämna in en ansökan om anmälan till den anmälade myndigheten i den medlemsstat där det är etablerat.
2. Ansökan ska åtföljas av en beskrivning av de bedömningar av överensstämmelse, det eller de förfaranden för bedömning av överensstämmelse och den eller de produkter med digitala element som organet anser sig ha kompetens för samt ett ackrediteringsintyg, om det finns ett sådant, som utfärdats av ett nationellt ackrediteringsorgan och där det intygas att organet för bedömning av överensstämmelse uppfyller kraven i artikel 39.
3. Om organet för bedömning av överensstämmelse inte kan uppvisa något ackrediteringsbevis ska det ge den anmälade myndigheten alla de underlag som krävs för kontroll, erkännande och regelbunden tillsyn av att det uppfyller kraven i artikel 39.

Artikel 43

Anmälningsförfarande

1. De anmälade myndigheterna ska endast anmäla de organ för bedömning av överensstämmelse som har uppfyllt kraven i artikel 39.
2. Den anmälade myndigheten ska underrätta kommissionen och de andra medlemsstaterna via databasen Nando som utvecklats och förvaltas av kommissionen.
3. Anmälan ska innehålla detaljerade uppgifter om bedömningarna av överensstämmelse, modulerna för bedömning av överensstämmelse och de berörda produkterna med digitala element samt ett relevant intyg om kompetens.
4. Om en anmälan inte grundar sig på ett sådant ackrediteringsintyg som avses i artikel 42.2 ska den anmälade myndigheten ge kommissionen och de andra medlemsstaterna de skriftliga underlag som styrker att organet för bedömning av överensstämmelse har erforderlig kompetens och att de system som behövs för att se till att organet övervakas regelbundet och fortsätter att uppfylla kraven i artikel 39 har inrättats.
5. Det berörda organet får bedriva verksamhet som anmält organ endast om kommissionen eller de andra medlemsstaterna inte har rest några invändningar inom två veckor från anmälan, i de fall då ett ackrediteringsintyg används, eller inom två månader från anmälan, i de fall då ingen ackreditering används.

Endast ett sådant organ ska anses vara ett anmält organ vid tillämpning av denna förordning.

6. Kommissionen och övriga medlemsstater ska underrättas om eventuella relevanta senare ändringar av anmälan.

Artikel 44

Identifikationsnummer och förteckningar över anmälda organ

1. Kommissionen ska tilldela varje anmält organ ett identifikationsnummer.

Organet ska tilldelas ett enda sådant nummer även om det anmälts enligt flera unionsrättsakter.

2. Kommissionen ska offentliggöra förteckningen över de organ som anmälts enligt denna förordning, inklusive de identifikationsnummer som de har tilldelats och den verksamhet som de har anmälts för.

Kommissionen ska säkerställa att denna förteckning hålls aktuell.

Artikel 45

Ändringar i anmälan

1. Om en anmälende myndighet har konstaterat eller har informerats om att ett anmält organ inte längre uppfyller de krav som anges i artikel 39 eller att det underlåter att fullgöra sina skyldigheter ska myndigheten i förekommande fall, beroende på hur allvarlig underlåtenheten att uppfylla kraven eller fullgöra skyldigheterna är, begränsa anmälan eller återkalla den tillfälligt eller slutgiltigt. Den ska omedelbart informera kommissionen och de andra medlemsstaterna om detta.

2. I händelse av begränsning eller tillfällig eller slutgiltig återkallelse av anmälan eller om det anmälda organet har upphört med verksamheten ska den anmälende medlemsstaten vidta lämpliga åtgärder för att säkerställa att det anmälda organets ärenden antingen behandlas av ett annat anmält organ eller hålls tillgängliga för de ansvariga anmälende myndigheterna och marknadskontrollmyndigheterna på deras begäran.

Artikel 46

Ifrågasättande av de anmälda organens kompetens

1. Kommissionen ska undersöka alla fall där den hyser tvivel, eller där den upplysts om sådana tvivel, om ett anmält organs kompetens eller ett anmält organs fortsatta uppfyllande av de krav och skyldigheter som det omfattas av.

2. Den anmälende medlemsstaten ska på begäran ge kommissionen all information om grunderna för anmälan eller det berörda organets fortsatta kompetens.

3. Kommissionen ska säkerställa att all känslig information som den erhåller under sina undersökningar behandlas konfidentiellt.

4. Om kommissionen konstaterar att ett anmält organ inte uppfyller eller inte längre uppfyller kraven för anmälan ska den meddela detta till den anmälende medlemsstaten och anmoda medlemsstaten att vidta erforderliga korrigerande åtgärder, t.ex. vid behov återta anmälan.

Artikel 47

De anmälda organens operativa skyldigheter

1. Anmälda organ ska utföra bedömningar av överensstämmelse i enlighet med förfarandena för bedömning av överensstämmelse i artikel 32 och bilaga VIII.

2. Bedömningar av överensstämmelse ska utföras på ett proportionellt sätt så att de inte blir onödigt betungande för de ekonomiska aktörerna. Organ för bedömning av överensstämmelse ska utöva sin verksamhet med vederbörlig hänsyn till företags storlek, särskilt i fråga om mikroföretag och små och medelstora företag, bransch, struktur, komplexitet och cybersäkerhetsrisknivån hos produkterna med digitala element och den berörda tekniken och om produktionsprocessen karaktäriseras som mass- eller serietillverkning.

3. Anmälda organ ska dock iakttä den grad av noggrannhet och den skyddsnivå som krävs för att produkten med digitala element ska överensstämma med denna förordning.

SV

EUT L, 20.11.2024

4. Om ett anmält organ konstaterar att en tillverkare inte uppfyller de krav som anges i bilaga I eller motsvarande harmoniserade standarder eller gemensamma specifikationer som avses i artikel 27, ska det begära att tillverkaren vidtar lämpliga korrigerande åtgärder, och det ska inte utfärda ett intyg om överensstämmelse.

5. Om ett anmält organ vid övervakning av överensstämmelse efter det att ett intyg har utfärdats konstaterar att en produkt med digitala element inte längre uppfyller kraven i denna förordning, ska det kräva att tillverkaren vidtar lämpliga korrigerande åtgärder, och vid behov ska intyget tillfälligt eller slutgiltigt återkallas.

6. Om korrigerande åtgärder inte vidtas eller inte får önskad effekt ska det anmälda organet, beroende på vad som är lämpligt, begränsa eller tillfälligt, alternativt slutgiltigt, återkalla alla intyg.

Artikel 48

Överklagande av de anmälda organens beslut

Medlemsstaterna ska säkerställa att det finns ett förfarande för överklagande av de anmälda organens beslut.

Artikel 49

De anmälda organens informationsskyldighet

1. De anmälda organen ska underrätta den anmälände myndigheten om följande:

- a) Avslag på ansökan om intyg, eller begränsning, tillfälligt tillbakadragande eller återkallelse av ett intyg.
- b) Omständigheter som inverkar på räckvidden och villkoren för anmälan.
- c) Begäran från marknadskontrollmyndigheterna om information om bedömningar av överensstämmelse.
- d) På begäran, bedömningar av överensstämmelse som gjorts inom ramen för anmälan och all annan verksamhet, inklusive gränsöverskridande verksamhet och underentreprenad.

2. De anmälda organen ska ge de andra organ som anmälts enligt denna förordning, och som utför liknande bedömningar av överensstämmelse som täcker samma produkter med digitala element, relevant information om frågor som rör negativa och, på begäran, positiva resultat av bedömningar av överensstämmelse.

Artikel 50

Utbyte av erfarenhet

Kommissionen ska se till att det förekommer utbyte av erfarenhet mellan de myndigheter i medlemsstaterna som ansvarar för riktlinjerna för anmälan.

Artikel 51

Samordning av anmälda organ

1. Kommissionen ska säkerställa att lämplig samordning och samarbete mellan de anmälda organen införs och att samordningen och samarbetet bedrivs på ett tillfredsställande sätt genom en sektorsövergripande grupp av anmälda organ.

2. Medlemsstaterna ska säkerställa att de organ som de har anmält deltar i gruppens arbete direkt eller genom utsedda företrädare.

KAPITEL V

MARKNADSKONTROLL OCH VERKSTÄLLIGHET

Artikel 52

Marknadskontroll och kontroll av produkter med digitala element på unionsmarknaden

1. Förordning (EU) 2019/1020 ska tillämpas på produkter med digitala element som omfattas av den här förordningen.
2. Varje medlemsstat ska utse en eller flera marknadskontrollmyndigheter för att säkerställa ett effektivt genomförande av denna förordning. Medlemsstaterna får utse en befintlig eller en ny myndighet till att fungera som marknadskontrollmyndighet inom ramen för denna förordning.
3. De marknadskontrollmyndigheter som utsetts enligt punkt 2 i denna artikel ska också ansvara för att utföra marknadskontroll rörande de skyldigheter för förvaltare av programvara med fri och öppen källkod som fastställs i artikel 24. Om en marknadskontrollmyndighet konstaterar att en förvaltare av programvara med fri och öppen källkod inte uppfyller de skyldigheter som anges i den artikeln ska den kräva att förvaltaren av programvaran med fri och öppen källkod säkerställer att alla lämpliga korrigerande åtgärder vidtas. Förvaltare av programvara med fri och öppen källkod ska säkerställa att alla lämpliga korrigerande åtgärder vidtas med avseende på deras skyldigheter enligt denna förordning.
4. När så är lämpligt ska marknadskontrollmyndigheterna samarbeta med de nationella myndigheter för cybersäkerhetscertifiering som utsetts enligt artikel 58 i förordning (EU) 2019/881 och regelbundet utbyta information med dessa. När det gäller tillsynen över genomförandet av rapporteringsskyldigheterna enligt artikel 14 i den här förordningen ska de utsedda marknadskontrollmyndigheterna samarbeta och regelbundet utbyta information med de CSIRT-enheter som utsetts till samordnare och Enisa.
5. Marknadskontrollmyndigheterna får be en CSIRT-enhet som utsetts till samordnare eller Enisa att ge tekniska råd i frågor som rör genomförandet och efterlevnaden av denna förordning. Vid genomförandet av en utredning enligt artikel 54 får marknadskontrollmyndigheterna be CSIRT-enheten som utsetts till samordnare eller Enisa att tillhandahålla en analys till stöd för utvärderingar av överensstämmelse för produkter med digitala element.
6. När så är relevant ska marknadskontrollmyndigheterna samarbeta med andra marknadskontrollmyndigheter som utsetts på grundval av annan unionsharmoniseringslagstiftning än denna förordning och regelbundet utbyta information med dessa.
7. Marknadskontrollmyndigheterna ska vid behov samarbeta med de myndigheter som utövar tillsyn över unionens dataskyddsrätt. I detta samarbete ingår att underrätta dessa myndigheter om alla iakttagelser av betydelse för deras fullgörande av sina befogenheter, inbegripet utfärdande av vägledning och råd enligt punkt 10 om vägledningen och råden rör behandling av personuppgifter.

Myndigheter som utövar tillsyn över unionens dataskyddsrätt ska ha befogenhet att begära och få åtkomst till all dokumentation som skapas eller upprätthålls enligt denna förordning när de behöver åtkomst till sådan dokumentation för att utföra sina uppgifter. De ska underrätta de utsedda marknadskontrollmyndigheterna i den berörda medlemsstaten om varje sådan begäran.
8. Medlemsstaterna ska säkerställa att de utsedda marknadskontrollmyndigheterna har tillräckliga ekonomiska och tekniska resurser, inbegripet vid behov verktyg för automatisk databehandling samt personalresurser med nödvändig cybersäkerhetskompetens för att kunna fullgöra sina uppgifter enligt denna förordning.
9. Kommissionen ska uppmuntra och underlätta utbytet av erfarenhet mellan utsedda marknadskontrollmyndigheter.
10. Marknadskontrollmyndigheterna får ge ekonomiska aktörer vägledning och råd om genomförandet av denna förordning, med stöd av kommissionen och CSIRT-enheter och Enisa när så är lämpligt.
11. Marknadskontrollmyndigheterna ska informera konsumenterna om var klagomål som kan indikera bristande överensstämmelse med denna förordning, i enlighet med artikel 11 i förordning (EU) 2019/1020 lämnas in, och ska informera konsumenterna om var och hur de kan få tillgång till mekanismer för att underlätta rapportering av sårbarheter, incidenter och cyberhot som kan påverka produkter med digitala element.

12. Marknadskontrollmyndigheterna ska när så är lämpligt underlätta samarbetet med berörda parter, inbegripet vetenskapliga organisationer samt forsknings- och konsumentorganisationer.

13. Marknadskontrollmyndigheterna ska årligen rapportera resultaten av relevant marknadskontroll till kommissionen. De utsedda marknadskontrollmyndigheterna ska utan dröjsmål rapportera till kommissionen och berörda nationella konkurrensmyndigheter om all information som framkommit i samband med marknadskontrollen och som kan vara av potentiellt intresse för tillämpningen av unionens konkurrensrätt.

14. För produkter med digitala element som omfattas av denna förordning och som klassificeras som AI-system med hög risk enligt artikel 6 i förordning (EU) 2024/1689 ska de marknadskontrollmyndigheter som utsetts enligt den förordningen vara de myndigheter som ansvarar för den marknadskontroll som föreskrivs i den här förordningen. De marknadskontrollmyndigheter som utsetts enligt förordning (EU) 2024/1689 ska vid behov samarbeta med de marknadskontrollmyndigheter som utsetts i enlighet med den här förordningen och, när det gäller tillsyn över genomförandet av rapporteringsskyldigheten enligt artikel 14 i den här förordningen, med de CSIRT-enheter som utsetts till samordnare och Enisa. De marknadskontrollmyndigheter som utsetts enligt förordning (EU) 2024/1689 ska i synnerhet underrätta de marknadskontrollmyndigheter som utsetts enligt den här förordningen om alla iakttagelser av betydelse för fullgörandet av deras uppgifter förbundna med genomförandet av den här förordningen.

15. En Adco-grupp ska inrättas för en enhetlig tillämpning av denna förordning, enligt artikel 30.2 i förordning (EU) 2019/1020. Adco-gruppen ska bestå av företrädare för de utsedda marknadskontrollmyndigheterna och, om så är lämpligt, företrädare för de centrala samordningskontoren. Adco-gruppen ska också behandla särskilda frågor som rör marknadskontroll rörande de skyldigheter som åläggs förvaltare av programvara med fri och öppen källkod.

16. Marknadskontrollmyndigheterna ska övervaka hur tillverkarna har tillämpat de kriterier som avses i artikel 13.8 när de fastställer stödperioden för sina produkter med digitala element.

Adco-gruppen ska i en allmänt tillgänglig och användarvänlig form offentliggöra relevant statistik om kategorier av produkter med digitala element, inbegripet genomsnittliga stödperioder, vilka fastställs av tillverkaren enligt artikel 13.8, samt tillhandahålla vägledning som inbegriper vägledande stödperioder för kategorier av produkter med digitala element.

Om uppgifterna tyder på otillräckliga stödperioder för specifika kategorier av produkter med digitala element får Adco-gruppen utfärda rekommendationer till marknadskontrollmyndigheterna om att inrikta sin verksamhet på sådana kategorier av produkter med digitala element.

Artikel 53

Tillgång till data och dokumentation

När det behövs för att bedöma överensstämmelsen med de väsentliga cybersäkerhetskraven i bilaga I för produkter med digitala element och de processer som införts av tillverkarna ska marknadskontrollmyndigheterna på motiverad begäran beviljas tillgång, på ett språk som lätt kan förstås av dem, till de data som behövs för att bedöma utformningen, utvecklingen, produktionen och sårbarhetshanteringen av sådana produkter, inbegripet tillhörande intern dokumentation hos den berörda ekonomiska aktören.

Artikel 54

Förfarande på nationell nivå för produkter med digitala element som utgör en betydande cybersäkerhetsrisk

1. Om marknadskontrollmyndigheten i en medlemsstat har tillräckliga skäl att anse att en produkt med digitala element, inbegripet dess sårbarhetshantering, utgör en betydande cybersäkerhetsrisk, ska den, utan onödigt dröjsmål och om lämpligt i samarbete med den berörda CSIRT-enheten, göra en utvärdering av den berörda produkten med digitala element med avseende på dess uppfyllande av alla krav som fastställs i denna förordning. De berörda ekonomiska aktörerna ska när så krävs samarbeta med marknadskontrollmyndigheten.

Om marknadskontrollmyndigheten vid utvärderingen konstaterar att en produkt med digitala element inte uppfyller kraven i denna förordning ska den utan dröjsmål ålägga den berörda ekonomiska aktören att vidta alla lämpliga korrigerande åtgärder för att se till att produkten med digitala element uppfyller dessa krav eller dra tillbaka produkten från marknaden eller återkalla den inom en rimlig tid som marknadskontrollmyndigheten fastställer i förhållande till typen av cybersäkerhetsrisk.

Marknadskontrollmyndigheten ska informera det berörda anmälde organet om detta. Artikel 18 i förordning (EU) 2019/1020 ska tillämpas på de korrigerande åtgärderna.

2. När marknadskontrollmyndigheterna fastställer betydelsen av en cybersäkerhetsrisk som avses i punkt 1 i denna artikel ska de också beakta icke-tekniska riskfaktorer, särskilt de som fastställts till följd av samordnade säkerhetsriskbedömningar av kritiska leveranskedjor på unionsnivå som genomförs i enlighet med artikel 22 i direktiv (EU) 2022/2555. Om en marknadskontrollmyndighet har tillräckliga skäl att anse att en produkt med digitala element utgör en betydande cybersäkerhetsrisk mot bakgrund av icke-tekniska riskfaktorer ska den informera de behöriga myndigheter som utsetts eller inrättats enligt artikel 8 i direktiv (EU) 2022/2555 och när så krävs samarbeta med dessa myndigheter.

3. Om marknadskontrollmyndigheten anser att den bristande överensstämmelsen inte bara gäller det nationella territoriet, ska den informera kommissionen och de andra medlemsstaterna om utvärderingsresultaten och om de åtgärder som den har ålagt den ekonomiska aktören att vidta.

4. Den ekonomiska aktören ska säkerställa att alla lämpliga korrigerande åtgärder vidtas i fråga om alla berörda produkter med digitala element som den har tillhandahållit på unionsmarknaden.

5. Om den ekonomiska aktören inte vidtar lämpliga korrigerande åtgärder inom den period som avses i punkt 1 andra stycket, ska marknadskontrollmyndigheten vidta alla lämpliga provisoriska åtgärder för att förbjuda eller begränsa tillhandahållandet av produkten med digitala element på sin nationella marknad, dra tillbaka produkten från den marknaden eller återkalla den.

Myndigheten ska utan dröjsmål anmäla dessa åtgärder till kommissionen och de andra medlemsstaterna.

6. I den information som avses i punkt 5 ska alla tillgängliga uppgifter ingå, särskilt de uppgifter som krävs för att kunna identifiera den produkt med digitala element som inte uppfyller kraven, dess ursprung, vilken typ av bristande överensstämmelse som görs gällande och den risk produkten utgör, vilken typ av nationell åtgärd som vidtagits och åtgärdens varaktighet samt den berörda ekonomiska aktörens synpunkter. Marknadskontrollmyndigheten ska särskilt ange om den bristande överensstämmelsen beror på en eller flera av följande orsaker:

- a) Produkten med digitala element eller de processer som införts av tillverkaren uppfyller inte de väsentliga cybersäkerhetskraven i bilaga I.
- b) Det finns brister i de harmoniserade standarder, de europeiska ordningar för cybersäkerhetscertifiering eller de gemensamma specifikationer som avses i artikel 27.

7. Marknadskontrollmyndigheterna i andra medlemsstater än den som inledde förfarandet ska utan dröjsmål informera kommissionen och de andra medlemsstaterna om alla vidtagna åtgärder och eventuella kompletterande uppgifter som de har tillgång till med avseende på bristande överensstämmelse hos den berörda produkten med digitala element samt eventuella invändningar mot den anmälda nationella åtgärden.

8. Åtgärden ska anses vara berättigad om ingen medlemsstat eller kommissionen har gjort invändningar inom tre månader efter mottagandet av den anmälan som avses i punkt 5 i denna artikel mot en provisorisk åtgärd som vidtagits av en medlemsstat. Detta påverkar inte den ekonomiska aktörens processuella rättigheter i enlighet med artikel 18 i förordning (EU) 2019/1020.

9. Marknadskontrollmyndigheterna i alla medlemsstater ska säkerställa att lämpliga begränsande åtgärder vidtas utan dröjsmål med avseende på den berörda produkten med digitala element, till exempel att produkten dras tillbaka från marknaden.

Artikel 55

Unionens förfarande i fråga om skyddsåtgärder

1. Om en medlemsstat inom tre månader efter mottagandet av den anmälan som avses i artikel 54.5 har gjort invändningar mot en åtgärd som vidtagits av en annan medlemsstat, eller om kommissionen anser att åtgärden strider mot unionsrätten, ska kommissionen utan dröjsmål inleda samråd med den berörda medlemsstaten och den eller de ekonomiska aktörerna och ska utvärdera den nationella åtgärden. På grundval av utvärderingsresultaten ska kommissionen besluta om den nationella åtgärden är berättigad eller inte inom nio månader från den anmälan som avses i artikel 54.5 och meddela beslutet till den berörda medlemsstaten.

SV

EUT L, 20.11.2024

2. Om den nationella åtgärden anses vara berättigad, ska alla medlemsstater vidta de åtgärder som krävs för att säkerställa att den produkt med digitala element som inte uppfyller kraven dras tillbaka från deras marknader och underrätta kommissionen om detta. Om den nationella åtgärden inte anses vara berättigad ska den berörda medlemsstaten upphäva åtgärden.
3. Om den nationella åtgärden anses vara berättigad och produktens bristande överensstämmelse kan tillskrivas brister i de harmoniserade standarderna ska kommissionen tillämpa det förfarande som föreskrivs i artikel 11 i förordning (EU) nr 1025/2012.
4. Om den nationella åtgärden anses vara berättigad och produktens bristande överensstämmelse kan tillskrivas brister i en europeisk ordning för cybersäkerhetscertifiering som avses i artikel 27, ska kommissionen överväga att ändra eller upphäva eventuella delegerade akter som antagits enligt artikel 27.9 som specificerar presumptionen om överensstämmelse för det certifieringssystemet.
5. Om den nationella åtgärden anses vara berättigad och produktens bristande överensstämmelse kan tillskrivas i de gemensamma specifikationer som avses i artikel 27, ska kommissionen överväga att ändra eller upphäva eventuella genomförandeakter som antagits enligt artikel 27.2 som fastställer dessa gemensamma specifikationer.

Artikel 56

Förfarande på unionsnivå för produkter med digitala element som utgör en betydande cybersäkerhetsrisk

1. Om kommissionen har tillräckliga skäl, inbegripet baserat på information från Enisa, att anse att en produkt med digitala element som utgör en betydande cybersäkerhetsrisk inte uppfyller kraven enligt denna förordning ska den informera de berörda marknadskontrollmyndigheterna. Om marknadskontrollmyndigheterna gör en utvärdering av produkten med digitala element som kan utgöra en betydande cybersäkerhetsrisk med avseende på dess överensstämmelse med kraven i denna förordning ska de förfaranden som avses i artiklarna 54 och 55 tillämpas.
2. Om kommissionen har tillräckliga skäl att anse att en produkt med digitala element utgör en betydande cybersäkerhetsrisk mot bakgrund av icke-tekniska riskfaktorer ska den informera de berörda marknadskontrollmyndigheterna och, om så är lämpligt, de behöriga myndigheter som utsetts eller inrättats enligt artikel 8 i direktiv (EU) 2022/2555 och när så krävs samarbeta med dessa myndigheter. Kommissionen ska också beakta relevansen hos de identifierade riskerna för produkten med digitala element med tanke på sina uppgifter avseende de samordnade säkerhetsriskbedömningar av kritiska leveranskedjor på unionsnivå som föreskrivs i artikel 22 i direktiv (EU) 2022/2555, och vid behov samråda med den samarbetsgrupp som inrättats enligt artikel 14 i direktiv (EU) 2022/2555 och Enisa.
3. Vid omständigheter som motiverar ett omedelbart ingripande för att bevara en välfungerande inre marknad, och där kommissionen har tillräckliga skäl att anse att den produkt med digitala element som avses i punkt 1 fortfarande inte uppfyller kraven enligt denna förordning och inga effektiva åtgärder har vidtagits av de berörda marknadskontrollmyndigheterna, ska kommissionen göra en utvärdering av överensstämmelsen och får begära att Enisa tillhandahåller en analys för att stödja den. Kommissionen ska underrätta de berörda marknadskontrollmyndigheterna om detta. De berörda ekonomiska aktörerna ska när så krävs samarbeta med Enisa.
4. Baserat på den utvärdering som avses i punkt 3 får kommissionen besluta att en korrigerande eller begränsande åtgärd krävs på unionsnivå. Därför ska kommissionen utan dröjsmål samråda med de berörda medlemsstaterna och berörda ekonomiska aktörer (en eller flera).
5. Baserat på det samråd som avses i punkt 4 i denna artikel får kommissionen anta genomförandeakter för att föreskriva korrigerande eller begränsande åtgärder på unionsnivå, inbegripet krav på att de berörda produkterna med digitala element ska dras tillbaka från marknaden eller återkallas, inom en rimlig tid i förhållande till typen av risk. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 62.2.
6. Kommissionen ska omedelbart delge berörda ekonomiska aktörer de genomförandeakter som avses i punkt 5. Medlemsstaterna ska genomföra dessa genomförandeakter utan dröjsmål och underrätta kommissionen om detta.
7. Punkterna 3–6 ska vara tillämpliga under den tid som den exceptionella situation som motiverade kommissionens ingripande varar, under förutsättning att den berörda produkten med digitala element inte bringas till överensstämmelse med denna förordning.

Artikel 57

Produkter med digitala element som överensstämmer med kraven men utgör en betydande cybersäkerhetsrisk

1. Marknadskontrollmyndigheten i en medlemsstat ska kräva att en ekonomisk aktör vidtar alla lämpliga åtgärder om den, efter att ha gjort en utvärdering enligt artikel 54, konstaterar att en produkt med digitala element och de processer som införts av tillverkaren överensstämmer med denna förordning, men att de utgör en betydande cybersäkerhetsrisk och en risk för

- a) människors hälsa eller säkerhet,
- b) efterlevnad av skyldigheter enligt unionsrätt eller nationell rätt avsedda att skydda de grundläggande rättigheterna,
- c) tillgången till och autenticiteten, riktigheten eller konfidentialiteten för tjänster som de väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555 erbjuder med användning av ett elektroniskt informationssystem, eller
- d) andra aspekter av skyddet av allmänintresset.

De åtgärder som avses i första stycket får omfatta åtgärder för att säkerställa att den berörda produkten med digitala element och de processer som införts av tillverkaren inte längre utgör de berörda riskerna när den tillhandahålls på marknaden, tillbakadragande från marknaden av den berörda produkten med digitala element eller återkallande av den, och ska stå i proportion till typen av risker.

2. Tillverkaren eller andra berörda ekonomiska aktörer ska säkerställa att korrigerande åtgärder vidtas i fråga om berörda produkter med digitala element som de har tillhandahållit på marknaden i unionen inom den tidsfrist som fastställs av den marknadskontrollmyndighet i medlemsstaten som avses i punkt 1.

3. Medlemsstaten ska omedelbart underrätta kommissionen och de andra medlemsstaterna om de åtgärder som vidtagits enligt punkt 1. Informationen ska innehålla alla tillgängliga uppgifter, särskilt de uppgifter som krävs för att kunna identifiera den berörda produkten med digitala element, dess ursprung och leveranskedja, vilken typ av risk som produkten utgör samt vilken typ av nationella åtgärder som vidtagits och deras varaktighet.

4. Kommissionen ska utan dröjsmål inleda samråd med medlemsstaterna och den berörda ekonomiska aktören samt utvärdera de nationella åtgärder som vidtagits. På grundval av utvärderingsresultaten ska kommissionen besluta om åtgärden är berättigad eller inte, och vid behov föreslå lämpliga åtgärder.

5. Kommissionen ska rikta det beslut som avses i punkt 4 till medlemsstaterna.

6. Om kommissionen har tillräckliga skäl, däribland baserat på information från Enisa, att anse att en produkt med digitala element som uppfyller kraven i denna förordning ändå utgör de risker som avses i punkt 1 i denna artikel, ska den informera och begära att berörda marknadskontrollmyndigheter (en eller flera) gör en utvärdering och följer de förfaranden som avses i artikel 54 och i punkterna 1, 2 och 3 i denna artikel.

7. Vid omständigheter som motiverar ett omedelbart ingripande för att bevara en välfungerande inre marknad, och där kommissionen har tillräckliga skäl att anse att den produkt med digitala element som avses i punkt 6 fortsätter att utgöra de risker som avses i punkt 1 och att inga effektiva åtgärder har vidtagits av de berörda nationella marknadskontrollmyndigheterna, ska kommissionen göra en utvärdering av de risker som produkten med digitala element utgör och får begära att Enisa tillhandahåller en analys för att stödja denna utvärdering och ska underrätta de berörda marknadskontrollmyndigheterna om detta. De berörda ekonomiska aktörerna ska när så krävs samarbeta med Enisa.

8. Baserat på den utvärdering som avses i punkt 7 får kommissionen besluta att en korrigerande eller begränsande åtgärd krävs på unionsnivå. Därför ska kommissionen utan dröjsmål samråda med de berörda medlemsstaterna och berörda ekonomiska aktörer (en eller flera).

9. Baserat på det samråd som avses i punkt 8 i denna artikel får kommissionen anta genomförandeakter för att besluta om korrigerande eller begränsande åtgärder på unionsnivå, inbegripet krav på att de berörda produkterna med digitala element ska dras tillbaka från marknaden eller återkallas, inom en rimlig tid i förhållande till typen av risk. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 62.2.

10. Kommissionen ska omedelbart delge berörda ekonomiska aktörer de genomförandeakter som avses i punkt 9. Medlemsstaterna ska genomföra dessa genomförandeakter utan dröjsmål och underrätta kommissionen om detta.

SV

EUT L, 20.11.2024

11. Punkterna 6–10 ska tillämpas under den tid som den exceptionella situation som motiverade kommissionens ingripande varar och så länge som den berörda produkten med digitala element fortsätter att utgöra de risker som avses i punkt 1.

Artikel 58

Formell bristande överensstämmelse

1. Om marknadskontrollmyndigheten i en medlemsstat konstaterar något av följande ska den lägga den berörda tillverkaren att åtgärda den bristande överensstämmelsen:

- a) CE-märkningen har fästs i strid med artiklarna 29 och 30.
- b) CE-märkning saknas.
- c) Det har inte upprättats någon EU-försäkrans om överensstämmelse.
- d) EU-försäkrans om överensstämmelse har inte upprättats på ett korrekt sätt.
- e) Identifikationsnumret för det anmälda organ som deltar i förfarandet för bedömning av överensstämmelse saknas i tillämpliga fall.
- f) Den tekniska dokumentationen är antingen inte tillgänglig eller inte komplett.

2. Om sådan bristande överensstämmelse som avses i punkt 1 kvarstår ska den berörda medlemsstaten vidta lämpliga åtgärder för att begränsa eller förbjuda tillhandahållandet av produkten med digitala element på marknaden eller säkerställa att den återkallas eller dras tillbaka från marknaden.

Artikel 59

Marknadskontrollmyndigheternas gemensamma aktiviteter

1. Marknadskontrollmyndigheter får komma överens med andra berörda myndigheter om att genomföra gemensamma aktiviteter för att säkerställa cybersäkerheten och skyddet av konsumenter med avseende på specifika produkter med digitala element som släpps ut på marknaden eller tillhandahålls på marknaden, i synnerhet produkter med digitala element som ofta finns utgöra cybersäkerhetsrisker.

2. Kommissionen eller Enisa ska föreslå gemensamma aktiviteter för att kontrollera överensstämmelsen med denna förordning vilka ska genomföras av marknadskontrollmyndigheter baserat på indikationer eller information om potentiell bristande överensstämmelse i flera medlemsstater med kraven i denna förordning när det gäller produkter med digitala element som fastställs i denna förordning.

3. Marknadskontrollmyndigheterna och i tillämpliga fall kommissionen ska säkerställa att överenskommelsen om att genomföra gemensamma aktiviteter inte leder till illojal konkurrens mellan ekonomiska aktörer och inte har någon negativ påverkan på objektiviteten, oberoendet och opartiskheten för parterna i överenskommelsen.

4. En marknadskontrollmyndighet får använda all information som erhållits genom genomförda gemensamma aktiviteter som ett led i utredningar som den gör.

5. Den berörda marknadskontrollmyndigheten och i tillämpliga fall kommissionen ska göra överenskommelsen om gemensamma aktiviteter, inbegripet namnen på de berörda parterna, tillgänglig för allmänheten.

Artikel 60

Samordnade tillsynsåtgärder

1. Marknadskontrollmyndigheterna ska genomföra samtidiga samordnade tillsynsåtgärder (sweeps) för specifika produkter med digitala element eller kategorier av sådana produkter för att kontrollera överensstämmelsen med eller upptäcka överträdelser av denna förordning. Dessa samordnade tillsynsåtgärder får omfatta inspektioner av produkter med digitala element som förvärvat under fingerad identitet.

2. Om inte annat överenskomits mellan de berörda marknadskontrollmyndigheterna ska samordnade tillsynsåtgärder samordnas av kommissionen. Samordnaren av den samordnade tillsynsåtgärden ska, när så är lämpligt, offentliggöra de sammanställda resultaten.

L, 20.11.2024

SV

3. Om Enisa vid utförandet av sina uppgifter, däribland baserat på de anmälningar som inkommit enligt artikel 14.1 och 14.3, identifierar kategorier av produkter med digitala element som får omfattas av samordnade tillsynsåtgärder ska Enisa lämna in ett förslag till en samordnad tillsynsåtgärd till den samordnare som avses i punkt 2 i den här artikeln för att övervägas av marknadskontrollmyndigheterna.
4. I samband med samordnade tillsynsåtgärder får marknadskontrollmyndigheterna utnyttja de utredningsbefogenheter som fastställs i artiklarna 52–58 och andra befogenheter som tilldelats dem enligt nationell rätt.
5. Marknadskontrollmyndigheterna får bjuda in kommissionens tjänstemän och andra medföljande personer som bemyndigats av kommissionen att delta i samordnade tillsynsåtgärder.

KAPITEL VI

DELEGERADE BEFOGENHETER OCH KOMMITTÉFÖRFARANDE

Artikel 61

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.
2. Den befogenhet att anta delegerade akter som avses i artiklarna 2.5 andra stycket, 7.3, 8.1 och 8.2, 13.8 fjärde stycket, 14.9, 25, 27.9, 28.5 och 31.5 ska ges till kommissionen för en period på fem år från och med den 10 december 2024. Kommissionen ska utarbeta en rapport om delegeringen av befogenhet senast nio månader före utgången av perioden på fem år. Delegeringen av befogenhet ska genom tyst medgivande förlängas med perioder av samma längd, såvida inte Europaparlamentet eller rådet motsätter sig en sådan förlängning senast tre månader före utgången av perioden i fråga.
3. Den delegering av befogenhet som avses i artiklarna 2.5 andra stycket, 7.3, 8.1 och 8.2, 13.8 fjärde stycket, 14.9, 25, 27.9, 28.5 och 31.5 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.
4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.
5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.
6. En delegerad akt som antas enligt artiklarna 2.5 andra stycket, 7.3, 8.1 eller 8.2, 13.8 fjärde stycket, 14.9, 25, 27.9, 28.5 eller 31.5 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 62

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.
2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.
3. Om kommitténs yttrande ska inhämtas genom skriftligt förfarande, ska det förfarandet avslutas utan resultat om kommitténs ordförande, inom tidsfristen för att avge yttrandet, så beslutar eller en kommittéledamot så begär.

KAPITEL VII
KONFIDENTIALITET OCH SANKTIONER

Artikel 63

Konfidentialitet

1. Alla parter som deltar i tillämpningen av denna förordning ska respektera konfidentialiteten för den information och de data som de erhåller när de utför sina uppgifter och sin verksamhet på ett sådant sätt att de skyddar följande:
 - a) Immateriella rättigheter och en fysisk eller juridisk persons konfidentiella affärsinformation eller företagshemligheter, inbegripet källkod, utom i de fall som avses i artikel 5 i Europaparlamentets och rådets direktiv (EU) 2016/943⁽¹⁷⁾.
 - b) Ett ändamålsenligt genomförande av denna förordning, särskilt med avseende på inspektioner, utredningar eller revisioner.
 - c) Intressen som rör allmän och nationell säkerhet.
 - d) Integriteten i straffrättsliga eller administrativa förfaranden.
2. Utan att det påverkar tillämpningen av punkt 1 får information som utbyts på konfidentiell basis mellan marknadskontrollmyndigheterna och mellan marknadskontrollmyndigheter och kommissionen inte lämnas ut utan föregående samtycke från den marknadskontrollmyndighet som ursprungligen lämnat informationen.
3. Punkterna 1 och 2 påverkar inte kommissionens, medlemsstaternas och de anmälda organens rättigheter och skyldigheter när det gäller att utbyta information och utfärda varningar och inte heller de berörda personernas skyldighet att lämna information enligt medlemsstaternas straffrätt.
4. Kommissionen och medlemsstaterna får vid behov utbyta känslig information med berörda myndigheter i tredjeländer med vilka de har slutit bilaterala eller multilaterala avtal om konfidentialitet som garanterar en tillräcklig skyddsnivå.

Artikel 64

Sanktioner

1. Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av bestämmelserna i denna förordning och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder utan dröjsmål samt utan dröjsmål eventuella ändringar som berör dem.
2. Bristande efterlevnad av de väsentliga cybersäkerhetskrav som anges i bilaga I och de skyldigheter som fastställs i artiklarna 13 och 14 ska medföra administrativa sanktionsavgifter på upp till 15 000 000 EUR eller, om överträdelsen begås av ett företag, upp till 2,5 % av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst.
3. Bristande efterlevnad av de skyldigheter som anges i artiklarna 18–23, 28, 30.1–30.4, 31.1–31.4, 32.1, 32.2 och 32.3. Artiklarna 33.5, 39, 41, 47, 49 och 53 ska bli föremål för administrativa sanktionsavgifter på upp till 10 000 000 EUR eller, om överträdelsen begås av ett företag, upp till 2 % av dess totala globala årsomsättning för det föregående räkenskapsåret, beroende på vilket som är högst.
4. Tillhandahållande av oriktig, ofullständig eller vilseledande information till anmälda organ och marknadskontrollmyndigheter som svar på en begäran ska medföra administrativa sanktionsavgifter på upp till 5 000 000 EUR eller, om överträdelsen begås av ett företag, upp till 1 % av dess totala globala årsomsättning för det föregående räkenskapsåret, beroende på vilket som är högst.

⁽¹⁷⁾ Europaparlamentets och rådets direktiv (EU) 2016/943 av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs (EUT L 157, 15.6.2016, s. 1).

EUT L, 20.11.2024

SV

5. Vid beslut om storleken på den administrativa sanktionsavgiften i varje enskilt fall ska alla relevanta omständigheter i den specifika situationen beaktas och vederbörlig hänsyn ska tas till
- a) överträdelsens art, allvarlighetsgrad och varaktighet samt dess konsekvenser,
- b) huruvida administrativa sanktionsavgifter redan har påförts av samma eller andra marknadskontrollmyndigheter på samma ekonomiska aktör för en liknande överträdelse,
- c) storleken på, särskilt när det gäller mikroföretag, små och medelstora företag, inbegripet uppstarts företag, och marknadsandelen för den ekonomiska aktör som begått överträdelsen.
6. Marknadskontrollmyndigheter som påför administrativa sanktionsavgifter ska meddela marknadskontrollmyndigheterna i andra medlemsstater detta via det informations- och kommunikationssystem som avses i artikel 34 i förordning (EU) 2019/1020.
7. Varje medlemsstat ska fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter och offentliga organ som är inrättade i medlemsstaten.
8. Beroende på medlemsstatens rättssystem kan reglerna om administrativa sanktionsavgifter tillämpas på ett sådant sätt att sanktionsavgifterna utdöms av behöriga nationella domstolar eller andra organ, i enlighet med befogenheter som fastställs på nationell nivå i dessa medlemsstater. Tillämpningen av sådana regler i dessa medlemsstater ska ha motsvarande verkan.
9. Administrativa sanktionsavgifter får, beroende på omständigheterna i det enskilda fallet, påföras utöver eventuella andra korrigerande eller begränsande åtgärder som marknadskontrollmyndigheterna tillämpar på samma överträdelse.
10. Genom undantag från punkterna 3–9 ska de administrativa sanktionsavgifter som avses i dessa punkter inte tillämpas på följande:
- a) Tillverkare som klassificeras som mikroföretag eller små företag när det gäller underlåtenhet att iaktta den tidsfrist som avses i artikel 14.2 a eller 14.4 a.
- b) Alla överträdelser av denna förordning som begås av förvaltare av programvara med fri och öppen källkod.

Artikel 65

Grupptalan

Direktiv (EU) 2020/1828 ska tillämpas på grupptalan om ekonomiska aktörers överträdelser av bestämmelserna i denna förordning som skadar eller kan skada konsumenternas kollektiva intressen.

KAPITEL VIII

ÖVERGÅNGS- OCH SLUTBESTÄMMELSER

Artikel 66

Ändring av förordning (EU) 2019/1020

I bilaga I till förordning (EU) 2019/1020 ska följande punkt läggas till:

"72. Europaparlamentets och rådets förordning (EU) 2024/2847 (*).

(*) Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen) (EUT L, 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>)."

Artikel 67

Ändring av direktiv (EU) 2020/1828

I bilaga I till direktiv (EU) 2020/1828 ska följande punkt läggas till:

"69. Europaparlamentets och rådets förordning (EU) 2024/2847 (*).

(*) Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen) (EUT L, 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>."

Artikel 68

Ändringar av förordning (EU) nr 168/2013

I del C1, i tabellen i bilaga II till Europaparlamentets och rådets förordning (EU) nr 168/2013 ⁽³⁸⁾ ska följande post läggas till:

"

16	18	Skydd av fordon mot cybe- rattacker		x	x	x	x	x	x	x	x	x	x	x	x	x	x

"

Artikel 69

Övergångsbestämmelser

- EU-typkontrollintyg och beslut om godkännande som utfärdats avseende cybersäkerhetskrav för produkter med digitala element som omfattas av annan unionsharmoniseringslagstiftning än denna förordning ska fortsätta att gälla till och med den 11 juni 2028, såvida de inte löper ut före den dagen, eller något annat anges i sådan annan unionsharmoniseringslagstiftning, i vilket fall de förblir giltiga enligt den lagstiftningen.
- Produkter med digitala element som har släppts ut på marknaden före den 11 december 2027 ska omfattas av kraven som anges i denna förordning endast om de, från och med den dagen, är föremål för en väsentlig ändring.
- Som avvikelse från punkt 2 i denna artikel ska de skyldigheter som fastställs i artikel 14 tillämpas på alla produkter med digitala element som omfattas av denna förordnings tillämpningsområde och som har släppts ut på marknaden före den 11 december 2027.

Artikel 70

Utvärdering och översyn

- Kommissionen ska senast den 11 december 2030 och därefter vart fjärde år, överlämna en rapport om utvärderingen och översynen av denna förordning till Europaparlamentet och rådet. Dessa rapporter ska offentliggöras.
- Senast den 11 september 2028 ska kommissionen, efter samråd med Enisa och CSIRT-nätverket, lägga fram en rapport för Europaparlamentet och rådet med en bedömning av ändamålsenligheten hos den gemensamma rapporteringsplattform som anges i artikel 16 samt effekterna av tillämpningen av de cybersäkerhetsrelaterade skäl som avses i artikel 16.2 av de CSIRT-enheter som utsetts till samordnare för den gemensamma rapporteringsplattformens ändamålsenlighet när det gäller att snabbt sprida mottagna anmälningar till andra relevanta CSIRT-enheter.

Artikel 71

Ikraftträdande och tillämpning

- Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

⁽³⁸⁾ Europaparlamentets och rådets förordning (EU) nr 168/2013 av den 15 januari 2013 om godkännande av och marknadskontroll för två- och trehjuliga fordon och fyrhjulingar (EUT L 60, 2.3.2013, s. 52).

EUT L, 20.11.2024

SV

2. Denna förordning ska tillämpas från och med den 11 december 2027.
Artikel 14 ska dock tillämpas från och med den 11 september 2026 och kapitel IV (artiklarna 35–51) ska tillämpas från och med den 11 juni 2026.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Strasbourg den 23 oktober 2024.

På Europaparlamentets vägnar
R. METSOLA
Ordförande

På rådets vägnar
ZSIGMOND B. P.
Ordförande

BILAGA I

VÄSENTLIGA CYBERSÄKERHETSKRAV

Del I Cybersäkerhetskrav avseende egenskaper hos produkter med digitala element

1. Produkter med digitala element ska utformas, utvecklas och produceras på ett sådant sätt att de säkerställer en lämplig cybersäkerhetsnivå baserat på riskerna.
2. På grundval av den bedömning av cybersäkerhetsrisker som avses i artikel 13.2, och i tillämpliga fall, ska produkter med digitala element
 - a) tillhandahållas på marknaden utan kända sårbarheter som kan utnyttjas,
 - b) tillhandahållas på marknaden med en säker standardkonfiguration, såvida inte tillverkaren och företagsanvändaren kommit överens om något annat med avseende på en skräddarsydd produkt med digitala element, inbegripet möjlighet att återställa produkten till dess ursprungliga skick,
 - c) säkerställa att sårbarheter kan åtgärdas genom säkerhetsuppdateringar, inbegripet, i tillämpliga fall, genom automatiska säkerhetsuppdateringar som installeras inom en lämplig tidsram som möjliggörs som standardinställning, med en tydlig och lättanvänd undantagsmekanism, genom att meddela användarna tillgängliga uppdateringar, och möjligheten att tillfälligt skjuta upp dem,
 - d) säkerställa skydd mot obehörig åtkomst genom lämpliga kontrollmekanismer, inbegripet men inte begränsat till system för autentisering, identitet eller åtkomsthantering, samt rapportera om eventuell obehörig åtkomst,
 - e) skydda konfidentialiteten för lagrade, överförda eller på annat sätt behandlade uppgifter, personuppgifter eller andra uppgifter, t.ex. genom kryptering av relevanta data i vila eller i transit med hjälp av de senaste metoderna, och med användning av andra tekniska lösningar,
 - f) skydda riktigheten hos lagrade, överförda eller på annat sätt behandlade uppgifter, personuppgifter eller andra uppgifter, kommandon, program och konfigurationer mot manipulation eller ändringar som inte godkänts av användaren, samt rapportera om datadistorsion,
 - g) endast behandla personuppgifter eller andra uppgifter som är adekvata, relevanta och begränsade till vad som är nödvändigt i förhållande till det avsedda syftet med produkten med digitala element ("uppgiftsminimering"),
 - h) skydda tillgången till väsentliga och grundläggande funktioner, även efter en incident, inbegripet genom resiliens- och begränsningsåtgärder mot överbelastningsattacker,
 - i) minimera de negativa effekterna av produkterna i sig eller av tillhörande tjänster på tillgången till tjänster som tillhandahålls av andra enheter eller nätverk,
 - j) utformas, utvecklas och produceras för att begränsa attackytor, inbegripet externa gränssnitt,
 - k) utformas, utvecklas och produceras för att minska effekterna av en incident med hjälp av lämpliga mekanismer och tekniker för att begränsa utnyttjandet,
 - l) tillhandahålla säkerhetsrelaterad information genom att registrera och övervaka relevant intern verksamhet, inbegripet tillgång till eller ändring av data, tjänster eller funktioner, med en undantagsmekanism för användaren,
 - m) ge användarna möjlighet att på ett säkert och enkelt sätt permanent ta bort alla data och inställningar och, om sådana data kan överföras till andra produkter eller system, säkerställa att detta görs på ett säkert sätt.

Del II Krav på sårbarhetshantering

Tillverkare av produkter med digitala element ska

1. identifiera och dokumentera sårbarheter och komponenter i produkter med digitala element, bland annat genom att upprätta en programvaruförteckning för material i ett allmänt använt och maskinläsbart format som åtminstone täcker produktens viktigaste (top-level) beroenden,

2. när det gäller riskerna för produkter med digitala element, utan dröjsmål åtgärda och avhjälpa sårbarheter, bland annat genom att tillhandahålla säkerhetsuppdateringar; om det är tekniskt möjligt ska nya säkerhetsuppdateringar tillhandahållas separat från funktionsuppdateringar,
3. tillämpa effektiva och regelbundna provningar och granskningar av säkerheten hos produkten med digitala element,
4. när en uppdatering av säkerheten har gjorts tillgänglig, dela och offentligt redovisa information om åtgärdade sårbarheter, inbegripet en beskrivning av sårbarheterna, information som gör det möjligt för användarna att identifiera den produkt med digitala element som påverkas, sårbarheternas konsekvenser, deras allvarlighetsgrad och tydlig och tillgänglig information som underlättar för användarna att avhjälpa sårbarheterna; i vederbörligen motiverade fall, om tillverkarna anser att säkerhetsriskerna med offentliggörande är större än säkerhetsfördelarna, får de skjuta upp offentliggörandet av information om en åtgärdad sårbarhet till dess att användarna har fått möjlighet att använda den relevanta programfixen,
5. införa och verkställa en policy för samordnad delgivning av information om sårbarheter,
6. vidta åtgärder för att underlätta utbyte av information om potentiella sårbarheter i sin produkt med digitala element och i tredjepartskomponenter som ingår i produkten, inbegripet genom att tillhandahålla en kontaktadress för rapportering av de sårbarheter som upptäckts i produkten med digitala element,
7. tillhandahålla mekanismer för säker distribution av uppdateringar av produkter med digitala element för att säkerställa att sårbarheter åtgärdas eller begränsas i tid och, i tillämpliga fall för säkerhetsuppdateringar, på ett automatiskt sätt,
8. säkerställa att säkerhetsuppdateringar, i de fall då de finns tillgängliga för att hantera identifierade säkerhetsproblem, sprids utan dröjsmål och, såvida inte tillverkaren och företagsanvändaren kommit överens om något annat med avseende på en skräddarsydd produkt med digitala element, kostnadsfritt, åtföljs av rådgivande meddelanden som ger användarna relevant information, inbegripet om eventuella åtgärder som ska vidtas.

BILAGA II

INFORMATION OCH INSTRUKTIONER TILL ANVÄNDAREN

Produkten med digitala element ska åtminstone åtföljas av

1. tillverkarens namn, registrerade firmanamn eller registrerade varumärke samt den postadress, den e-postadress eller andra digitala kontaktpunkter och, om tillgänglig, den webbplats där tillverkaren kan kontaktas,
2. den gemensamma kontaktpunkt där information om sårbarheter hos produkten med digitala element kan rapporteras och tas emot och där tillverkarens policy för samordnad delgivning av information om sårbarheter kan hittas,
3. namn och typ samt eventuell ytterligare information som möjliggör unik identifiering av produkten med digitala element,
4. det avsedda syftet med produkten med digitala element, inbegripet den säkerhetsmiljö som tillhandahålls av tillverkaren, samt produktens väsentliga funktioner och information om säkerhetsegenskaperna,
5. varje känd eller förutsebar omständighet, som har samband med användningen av produkten med digitala element i enlighet med dess avsedda ändamål eller under förhållanden där det kan förekomma rimligen förutsebar felaktig användning, som kan leda till betydande cybersäkerhetsrisker,
6. i tillämpliga fall, den internetadress där EU-försäkrans om överensstämmelse finns tillgänglig,
7. den typ av tekniskt säkerhetsstöd som erbjuds av tillverkaren och slutdatumet för den stödperiod under vilken användarna kan förvänta sig att sårbarheter ska hanteras och få säkerhetsuppdateringar,
8. detaljerade instruktioner eller en internetadress som hänvisar till sådana detaljerade instruktioner och information om
 - a) nödvändiga åtgärder under den inledande idrifttagningen och under hela livslängden för produkten med digitala element för att säkerställa en säker användning,
 - b) hur ändringar av produkten med digitala element kan påverka datasäkerheten,
 - c) hur säkerhetsrelevanta uppdateringar kan installeras,
 - d) säker avveckling av produkten med digitala element, inbegripet information om hur användardata kan avlägsnas på ett säkert sätt,
 - e) hur standardinställningen som möjliggör automatisk installation av säkerhetsuppdateringar i enlighet med kravet i del I led 2.c i bilaga I kan stängas av,
 - f) om produkten med digitala element är avsedd att integreras i andra produkter med digitala element, den information som krävs för att integratorn ska kunna uppfylla de väsentliga cybersäkerhetskrav som anges i bilaga I och dokumentationskraven i bilaga VII,
9. Om tillverkaren beslutar att göra programvaruförteckningen tillgänglig för användaren, information om var programvaruförteckningen kan nås.

BILAGA III

VIKTIGA PRODUKTER MED DIGITALA ELEMENT

Klass I

1. Identitetshanteringssystem och programvara och hårdvara för hantering av privilegierad åtkomst, inbegripet läsare för autentisering och åtkomstkontroll, inbegripet biometrisk läsare.
2. Fristående och inbyggda webbläsare.
3. Lösenordshanterare.
4. Programvara som söker efter och avlägsnar skadlig programvara eller sätter den i karantän.
5. Produkter med digitala element som fungerar som virtuella privata nätverk (VPN).
6. System för nätverksförvaltning.
7. System för säkerhetsinformation och händelsehantering (SIEM).
8. Starthanterare.
9. Infrastruktur för kryptering med öppen nyckel (PKI) och programvara för utfärdande av digitala certifikat.
10. Fysiska och virtuella nätverksgränssnitt.
11. Operativsystem.
12. Routrar, modem avsedda för anslutning till internet och dataväxlar.
13. Mikroprocessorer med säkerhetsrelaterade funktioner.
14. Mikrokontroller med säkerhetsrelaterade funktioner.
15. Applikationsspecifika integrerade kretsar (ASIC) och fältprogrammerbara grindmatriser (FPGA) med säkerhetsrelaterade funktioner.
16. Smarta virtuella assistenter för allmänna ändamål.
17. Smarta hemprodukter med säkerhetsfunktioner, inbegripet smarta dörrlås, säkerhetskameror, babyövervakningssystem och larmsystem.
18. Internetanslutna leksaker som omfattas av Europaparlamentets och rådets direktiv 2009/48/EG⁽¹⁾ och som har sociala interaktiva funktioner (t.ex. tal eller filmning) eller som har positionsspåringsfunktioner.
19. Personliga kroppsburna produkter som ska bäras eller placeras på en människokropp och som har ett hälsoövervakningssyfte (t.ex. spårning) och som inte omfattas av förordning (EU) 2017/745 eller (EU) 2017/746, eller personliga kroppsburna produkter som är avsedda att användas av och för barn.

Klass II

1. Hypervisorer och system för körning av programbehållare som stöder virtualiserad exekvering av operativsystem och liknande miljöer.
2. Brandväggar, intrångsdetekterings- och intrångsskyddssystem.
3. Manipulationssäkra mikroprocessorer.
4. Manipulationssäkra mikrokontroller.

⁽¹⁾ Europaparlamentets och rådets direktiv 2009/48/EG av den 18 juni 2009 om leksakers säkerhet (EUT L 170, 30.6.2009, s. 1).

SV

EUT L, 20.11.2024

BILAGA IV

KRITISKA PRODUKTER MED DIGITALA ELEMENT

1. Hårdvaruenheter med säkerhetsboxar.
2. Smarta mätarportar inom smarta mätersystem enligt definitionen i artikel 2.23 i Europaparlamentets och rådets direktiv (EU) 2019/944⁽¹⁾ och andra enheter för avancerade säkerhetsändamål, inbegripet för säker kryptobehandling.
3. Smartkort eller liknande enheter, inbegripet säkra element.

⁽¹⁾ Europaparlamentets och rådets direktiv (EU) 2019/944 av den 5 juni 2019 om gemensamma regler för den inre marknaden för el och om ändring av direktiv 2012/27/EU (EUT L 158, 14.6.2019, s. 125).

BILAGA V

EU-FÖRSÄKRAN OM ÖVERENSSTÄMMELSE

Den EU-försäkrans om överensstämmelse som avses i artikel 28 ska innehålla samtliga uppgifter som anges nedan:

1. Namn och typ samt eventuell ytterligare information som möjliggör unik identifiering av produkten med digitala element.
2. Namn och adress till tillverkaren eller tillverkarens representant.
3. En förklaring om att EU-försäkrans om överensstämmelse utfärdas på leverantörens eget ansvar.
4. Föremål för försäkrans (identifiering av produkten med digitala element så att den kan spåras, vilket vid behov kan innebära ett fotografi).
5. En förklaring om att det föremål för försäkrans som beskrivs ovan överensstämmer med den relevanta unionsharmoniseringslagstiftningen.
6. Hänvisningar till relevanta harmoniserade standarder som använts eller andra gemensamma specifikationer eller system för cybersäkerhetscertifiering enligt vilka överensstämmelsen försäkras.
7. I tillämpliga fall, det anmälda organets namn och nummer, en beskrivning av det använda förfarandet för bedömning av överensstämmelse och uppgifter om det utfärdade intyget.
8. Ytterligare information:
Undertecknad för:
(ort och datum):
(namn, befattning) (namnteckning):

SV

EUT L, 20.11.2024

BILAGA VI

FÖRENKLAD EU-FÖRSÄKRAN OM ÖVERENSSTÄMMELSE

Den förenklade EU-försäkran om överensstämmelse som avses i artikel 13.20 ska utfärdas enligt följande:

Härmed försäkras ...[tillverkarens namn] att produkten med digitala element ...[beteckning för typ av produkt med digitalt element] uppfyller kraven i (EU) 2024/2847 ⁽¹⁾.

Den fullständiga texten till EU-försäkran om överensstämmelse finns på följande internetadress: ...

⁽¹⁾ EUT L, 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>.

BILAGA VII

DEN TEKNISKA DOKUMENTATIONENS INNEHÅLL

Den tekniska dokumentation som avses i artikel 31 ska åtminstone innehålla följande information, beroende på vad som är tillämpligt för den relevanta produkten med digitala element:

1. En allmän beskrivning av produkten med digitala element, inbegripet
 - a) dess avsedda ändamål,
 - b) versioner av programvara som påverkar överensstämmelsen med de väsentliga cybersäkerhetskraven,
 - c) om produkten med digitala element är en hårdvaruprodukt, fotografier eller illustrationer som visar yttre egenskaper, märkning och inre layout,
 - d) användarinformation och bruksanvisning enligt bilaga II.
2. En beskrivning av utformningen, utvecklingen och produktionen av produkten med digitala element samt processer för sårbarhetshantering, inbegripet
 - a) nödvändig information om utformning och utveckling av produkten med digitala element, i tillämpliga fall inbegripet ritningar och scheman och/eller en beskrivning av systemarkitekturen som förklarar hur programvarukomponenter byggs på eller matas in i varandra och integreras i den övergripande behandlingen,
 - b) nödvändig information om och specifikationer av de processer för sårbarhetshantering som tillverkaren infört, inbegripet programvaruförteckningen, policyn för samordnad delgivning av information om sårbarheter, bevis på tillhandahållandet av en kontaktadress för rapportering av sårbarheter och en beskrivning av de tekniska lösningar som valts för säker distribution av uppdateringar,
 - c) nödvändig information om och specifikationer av produktions- och övervakningsprocesser för produkten med digitala element och validering av dessa processer.
3. En bedömning av de cybersäkerhetsrisker mot vilka produkten med digitala element utformas, utvecklas, produceras, levereras och underhålls som fastställs enligt artikel 13, inbegripet hur de väsentliga cybersäkerhetskraven i del I i bilaga I är tillämpliga.
4. Relevant information som beaktades för att fastställa stödperioden enligt artikel 13.8 för produkten med digitala element.
5. En förteckning över de harmoniserade standarder som helt eller delvis har följts och till vilka hänvisningar har offentliggjorts i *Europeiska unionens officiella tidning*, gemensamma specifikationer enligt artikel 27 i denna förordning eller europeiska ordningar för cybersäkerhetscertifiering som antagits enligt förordning (EU) 2019/881 enligt artikel 27.8 i denna förordning, och, om dessa harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering inte har tillämpats, beskrivningar av de lösningar som valts för att uppfylla de väsentliga cybersäkerhetskraven i delarna I och II i bilaga I, inbegripet en förteckning över andra relevanta tekniska specifikationer som tillämpats. När det gäller delvis tillämpade harmoniserade standarder, gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering ska det i den tekniska dokumentationen specificeras vilka delar som har tillämpats.
6. Rapporter om de provningar som utförts för att kontrollera att produkten med digitala element och processerna för sårbarhetshantering överensstämmer med de tillämpliga väsentliga cybersäkerhetskraven i delarna I och II i bilaga I.
7. Kopia av EU-försäkran om överensstämmelse.
8. I tillämpliga fall, programvaruförteckningen, efter en motiverad begäran från en marknadskontrollmyndighet, förutsatt att det är nödvändigt för att denna myndighet ska kunna kontrollera överensstämmelsen med de väsentliga cybersäkerhetskraven i bilaga I.

BILAGA VIII

FÖRFARANDE FÖR BEDÖMNING AV ÖVERENSSTÄMMELSE

Del I Förfarande för bedömning av överensstämmelse som grundar sig på intern kontroll (baserat på modul A)

1. Intern kontroll är det förfarande för bedömning av överensstämmelse genom vilket tillverkaren fullgör skyldigheterna som anges i punkterna 2, 3 och 4 i denna del samt säkerställer och försäkrar på eget ansvar att produkter med digitala element uppfyller alla de väsentliga cybersäkerhetskraven i del I i bilaga I och att tillverkaren uppfyller de väsentliga cybersäkerhetskraven i del II i bilaga I.
2. Tillverkaren ska upprätta den tekniska dokumentation som beskrivs i bilaga VII.
3. Utformning, utveckling, produktion och sårbarhetshantering av produkter med digitala element

Tillverkaren ska vidta alla åtgärder som krävs för att säkerställa att utformningen, utvecklingen, produktionen samt processerna för sårbarhetshantering och övervakningen av dessa ska leda till att de tillverkade eller utvecklade produkterna med digitala element och de processer som tillverkaren infört överensstämmer med de väsentliga cybersäkerhetskraven i delarna I och II i bilaga I.

4. Märkning om överensstämmelse och försäkringen om överensstämmelse

4.1 Tillverkaren ska fästa CE-märkningen på varje enskild produkt med digitala element som uppfyller de tillämpliga kraven som anges i denna förordning.

4.2 Tillverkaren ska upprätta en skriftlig EU-försäkringen om överensstämmelse för varje produkt med digitala element i enlighet med artikel 28 och ska kunna uppvisa den tillsammans med den tekniska dokumentationen för de nationella myndigheterna under en period på 10 år efter det att produkten med digitala element har släppts ut på marknaden eller under stödperioden, beroende på vilken period som är längst. I EU-försäkringen om överensstämmelse ska det anges för vilken produkt med digitala element den har upprättats. En kopia av EU-försäkringen om överensstämmelse ska på begäran göras tillgänglig för de relevanta myndigheterna.

5. Tillverkarens representanter

Tillverkarens representant får fullgöra tillverkarens skyldigheter enligt punkt 4 för dennes räkning och på dennes ansvar, förutsatt att de relevanta skyldigheterna specificeras i fullmakten.

Del II EU-typkontroll (baserat på modul B)

1. EU-typkontroll är den del av ett förfarande för bedömning av överensstämmelse genom vilken ett anmält organ undersöker den tekniska utformningen och utvecklingen hos produkten med digitala element och de processer för sårbarhetshantering som tillverkaren infört och intygar att en produkt med digitala element uppfyller de väsentliga cybersäkerhetskraven i del I i bilaga I och att tillverkaren uppfyller de väsentliga cybersäkerhetskraven i del II i bilaga I.
2. EU-typkontroll ska göras genom bedömning av lämpligheten hos den tekniska utformningen och utvecklingen av produkten med digitala element genom granskningen av den tekniska dokumentationen och de underlag som avses i punkt 3 samt undersökningen av provexemplar av en eller flera kritiska delar av produkten (kombination av produktionstyp och utformningstyp).
3. Tillverkaren ska lämna in ansökan om EU-typkontroll till ett valfritt anmält organ.

Ansökan ska innehålla följande:

- 3.1 Tillverkarens namn och adress och, om ansökan lämnas in av tillverkarens representant, även namn och adress för den tillverkarens representant.
- 3.2 En skriftlig försäkringen om att samma ansökan inte har lämnats in till något annat anmält organ.
- 3.3 Den tekniska dokumentationen, vilken ska göra det möjligt att bedöma överensstämmelsen hos produkten med digitala element med de tillämpliga väsentliga cybersäkerhetskraven i del I i bilaga I och tillverkarens processer för sårbarhetshantering enligt del II i bilaga I, och ska innehålla en tillfredsställande analys och bedömning av riskerna. Den tekniska dokumentationen ska innehålla de tillämpliga kraven och, i den mån det krävs för bedömningen, även en beskrivning av utformningen, tillverkningen och funktionen avseende produkten med digitala element. Den tekniska dokumentationen ska, i tillämpliga fall, innehålla minst de uppgifter som anges i bilaga VII.

- 3.4 Underlag som visar att de lösningarna för teknisk utformning och utveckling samt processerna för sårbarhetshandling är lämpliga. I underlaget ska anges alla dokument som har använts, särskilt när de relevanta harmoniserade standarderna och/eller de tekniska specifikationerna inte har tillämpats fullt ut. Underlaget ska vid behov innehålla resultaten av provningar som utförts i tillverkarens därtill ägnade laboratorium eller i något annat provningslaboratorium för dennes räkning och under dennes ansvar.
4. Det anmälda organet ska göra följande:
- 4.1 Granska den tekniska dokumentationen och underlaget för att bedöma om den tekniska utformningen och utvecklingen av produkten med digitala element uppfyller de väsentliga cybersäkerhetskraven i del I i bilaga I och om de processer för sårbarhetshandling som tillverkaren infört uppfyller de väsentliga cybersäkerhetskraven i del II i bilaga I.
- 4.2 Kontrollera att provexemplaren har utvecklats eller tillverkats i enlighet med den tekniska dokumentationen och identifiera de delar som har utformats och utvecklats i enlighet med de tillämpliga bestämmelserna i de relevanta harmoniserade standarderna eller de tekniska specifikationerna, liksom de delar som har utformats och utvecklats utan att de tillämpliga bestämmelserna i dessa standarder har följts.
- 4.3 Utföra eller låta utföra lämpliga undersökningar och provningar för att, i de fall där tillverkaren har valt att tillämpa lösningarna i de relevanta harmoniserade standarderna eller de tekniska specifikationerna för de krav som anges i bilaga I, kontrollera att de lösningarna har tillämpats på rätt sätt.
- 4.4 Utföra eller låta utföra lämpliga undersökningar och provningar för att, i de fall där lösningarna i relevanta harmoniserade standarder eller tekniska specifikationer för de krav som anges i bilaga I inte har tillämpats, kontrollera om de lösningar som tillverkaren använt uppfyller de väsentliga cybersäkerhetskraven.
- 4.5 Komma överens med tillverkaren om var undersökningarna och provningarna ska utföras.
5. Det anmälda organet ska utarbeta en bedömningsrapport i vilken de åtgärder som utförts i enlighet med punkt 4 och resultatet av dem redovisas. Utan att det påverkar det anmälda organets skyldigheter gentemot de anmälade myndigheterna får organet endast offentliggöra hela eller delar av innehållet i rapporten med tillverkarens samtycke.
6. Om typen och processerna för sårbarhetshandling uppfyller de väsentliga cybersäkerhetskraven i bilaga I ska det anmälda organet utfärda ett EU-typintyg till tillverkaren. Intyget ska innehålla tillverkarens namn och adress, slutsatserna av undersökningen, eventuella giltighetsvillkor och de uppgifter som krävs för identifiering av den godkända typen och processerna för sårbarhetshandling. Intyget kan ha en eller flera bilagor.
- Intyget och bilagorna ska innehålla all information som behövs för att bedöma om de tillverkade eller utvecklade produkterna med digitala element överensstämmer med den undersökta typen och processerna för sårbarhetshandling och för att kontrollera produkter i bruk.
- Om typen och processerna för sårbarhetshandling inte uppfyller de tillämpliga väsentliga cybersäkerhetskraven i bilaga I ska det anmälda organet avslå ansökan om EU-typintyg och informera sökanden om detta samt utförligt motivera avslaget.
7. Det anmälda organet ska följa med i den tekniska utvecklingen, och om denna tyder på att den godkända typen och processerna för sårbarhetshandling inte längre uppfyller de tillämpliga väsentliga cybersäkerhetskraven i bilaga I ska organet fastställa om det krävs ytterligare undersökningar. Om så är fallet ska det anmälda organet underrätta tillverkaren om detta.
- Tillverkaren ska underrätta det anmälda organ som innehar den tekniska dokumentationen för EU-typintyget om alla ändringar av den godkända typen och processerna för sårbarhetshandling som kan påverka överensstämmelsen med de väsentliga cybersäkerhetskraven i bilaga I eller villkoren för intygets giltighet. För sådana ändringar krävs ytterligare godkännande i form av ett tillägg till det ursprungliga EU-typintyget.
8. Det anmälda organet ska regelbundet genomföra revisioner för att säkerställa att processerna för sårbarhetshandling enligt del II i bilaga I genomförs på ett tillfredsställande sätt.

SV

EUT L, 20.11.2024

9. Varje anmält organ ska underrätta sina anmälade myndigheter om de EU-typintyg och tillägg till dessa som det har utfärdat eller återkallat, och det ska periodiskt återkommande eller på begäran ge de anmälade myndigheterna tillgång till förteckningen över de intyg och eventuella tillägg till dessa som det har avslagit, tillfälligt återkallat eller på annat sätt belagt med restriktioner.

Varje anmält organ ska underrätta de övriga anmälda organen om de EU-typintyg och eventuella tillägg till dessa som det har vägrat utfärda, slutgiltigt eller tillfälligt återkallat eller på annat sätt belagt med restriktioner och, på begäran, om de intyg och tillägg till dessa som det har utfärdat.

Kommissionen, medlemsstaterna och de övriga anmälda organen har rätt att på begäran få en kopia av EU-typkontrollintyget och alla tillägg till det. Kommissionen och medlemsstaterna har rätt att på begäran få en kopia av den tekniska dokumentationen och av resultaten från de undersökningar som utförts av det anmälda organet. Det anmälda organet ska spara en kopia av EU-typintyget med bilagor och tillägg samt av den tekniska dokumentationen, inklusive dokumentation från tillverkaren, så länge som intyget är giltigt.

10. Tillverkaren ska för de nationella myndigheterna kunna uppvisa en kopia av EU-typintyget med bilagor och tillägg tillsammans med den tekniska dokumentationen under tio år efter det att produkten med digitala element släpptes ut på marknaden eller under stödperioden, beroende på vilken period som är längst.

11. Tillverkarens representant får lämna in den ansökan som avses i punkt 3 och fullgöra skyldigheterna enligt punkterna 7 och 10, förutsatt att de relevanta skyldigheterna specificeras i fullmakten.

Del III Överensstämmelse med typ som grundar sig på intern tillverkningskontroll (baserat på modul C)

1. Överensstämmelse med typ som grundar sig på intern tillverkningskontroll är den del av ett förfarande för bedömning av överensstämmelse genom vilken tillverkaren fullgör skyldigheterna som anges i punkterna 2 och 3 i denna del samt säkerställer och försäkrar att de berörda produkterna med digitala element överensstämmer med typen enligt beskrivningen i EU-typintyget och uppfyller de väsentliga cybersäkerhetskraven i del I i bilaga I och att tillverkaren uppfyller de väsentliga cybersäkerhetskraven i del II i bilaga I.

2. Produktion

Tillverkaren ska vidta alla nödvändiga åtgärder för att produktionen och övervakningen av den ska leda till att de tillverkade produkterna med digitala element överensstämmer med den godkända typen enligt beskrivningen i EU-typintyget och med de väsentliga cybersäkerhetskraven i del I i bilaga I och säkerställer att tillverkaren uppfyller de väsentliga cybersäkerhetskraven i del II i bilaga I.

3. Märkning om överensstämmelse och försäkrar om överensstämmelse

- 3.1 Tillverkaren ska fästa CE-märkningen på varje enskild produkt med digitala element som överensstämmer med typen enligt beskrivningen i EU-typintyget och uppfyller de tillämpliga kraven som anges i denna förordning.

- 3.2 Tillverkaren ska upprätta en skriftlig försäkrar om överensstämmelse för en produktmodell och kunna uppvisa den för de nationella myndigheterna under en period på tio år efter det att produkten med digitala element har släppts ut på marknaden eller under stödperioden, beroende på vilken period som är längst. I försäkrar om överensstämmelse ska det anges för vilken produktmodell den har upprättats. En kopia av försäkrar om överensstämmelse ska på begäran göras tillgänglig för de behöriga myndigheterna.

4. Tillverkarens representant

Tillverkarens representant får fullgöra tillverkarens skyldigheter enligt punkt 3 för dennes räkning och på dennes ansvar, förutsatt att de relevanta skyldigheterna specificeras i fullmakten.

Del IV Överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H)

1. Överensstämmelse som grundar sig på fullständig kvalitetssäkring är det förfarande för bedömning av överensstämmelse genom vilket tillverkaren fullgör skyldigheterna som anges i punkterna 2 och 5 i denna del samt säkerställer och försäkrar på eget ansvar att de berörda produkterna med digitala element eller produktkategorierna uppfyller de väsentliga cybersäkerhetskraven i del I i bilaga I och att de processer för sårbarhetshantering som tillverkaren infört uppfyller kraven i del II i bilaga I.

EUT L, 20.11.2024

SV

2. Utformning, utveckling, produktion och sårbarhetshantering av produkter med digitala element

Tillverkaren ska tillämpa ett godkänt kvalitetssystem enligt punkt 3 för utformning, utveckling, slutlig produktkontroll och provning av de berörda produkterna med digitala element och för hantering av sårbarheter, upprätthålla dess effektivitet under hela stödperioden och ska stå under övervakning i enlighet med punkt 4.

3. Kvalitetssystem

3.1 Tillverkaren ska hos ett valfritt anmält organ ansöka om att få sitt kvalitetssystem för de berörda produkterna med digitala element bedömt.

Ansökan ska innehålla följande:

- a) Tillverkarens namn och adress och, om ansökan lämnas in av tillverkarens representant, namn och adress för den tillverkarens representant.
- b) Den tekniska dokumentationen för en modell av varje kategori av produkter med digitala element som är tänkt att tillverkas eller utvecklas. Den tekniska dokumentationen ska, i tillämpliga fall, innehålla de uppgifter som anges i bilaga VII.
- c) Dokumentation av kvalitetssystemet.
- d) En skriftlig försäkras om att samma ansökan inte har lämnats till något annat anmält organ.

3.2 Kvalitetssystemet ska säkerställa att produkterna med digitala element uppfyller de väsentliga cybersäkerhetskraven i del I i bilaga I och att de processer för sårbarhetshantering som tillverkaren infört uppfyller kraven i del II i bilaga I.

Alla de faktorer, krav och bestämmelser som tillverkaren tagit hänsyn till ska dokumenteras på ett systematiskt och överskådligt sätt i form av skriftliga riktlinjer, förfaranden och anvisningar. Denna dokumentation av kvalitetssystemet ska möjliggöra en enhetlig tolkning av rutiner och kvalitetsåtgärder, såsom program, planer, manualer och protokoll.

Den ska framför allt innehålla en fullgod beskrivning av

- a) kvalitetsmålen och organisationsstruktur samt ledningens ansvar och befogenheter när det gäller utformning, utveckling, produktkvalitet och sårbarhetshantering,
- b) de tekniska specifikationer för utformning och utveckling, inbegripet standarder, som ska tillämpas och, när de relevanta harmoniserade standarderna eller de tekniska föreskrifterna inte tillämpas fullt ut, de medel som används för att säkerställa att de väsentliga cybersäkerhetskraven i del I i bilaga I som är tillämpliga för produkterna med digitala element uppfylls,
- c) de tekniska specifikationer för förfaranden, inklusive standarder, som ska tillämpas och, när de relevanta harmoniserade standarderna eller de tekniska föreskrifterna inte tillämpas fullt ut, de medel som används för att säkerställa att de väsentliga cybersäkerhetskraven i del II i bilaga I som är tillämpliga för tillverkaren uppfylls,
- d) kontrollen av utformning och utveckling, samt de metoder, processer och systematiska förfaranden för verifikation av utformning och utveckling som ska användas vid utformning och utveckling av produkter med digitala element inom den berörda kategorin,
- e) de motsvarande metoder, processer och systematiska åtgärder för produktion, kvalitetskontroll och kvalitets-säkring som ska användas,
- f) de undersökningar och provningar som kommer att utföras före, under och efter produktionen, och hur ofta de kommer att utföras,

SV

EUT L, 20.11.2024

g) kvalitetsdokumenten, t.ex. kontrollrapporter, provningsresultat, kalibreringsresultat och redogörelser för den berörda personalens kvalifikationer.

h) metoderna för övervakning av att den erforderliga utformnings- och produktkvaliteten uppnås och att kvalitetssystemet fungerar effektivt.

3.3 Det anmälda organet ska bedöma kvalitetssystemet för att avgöra det uppfyller kraven i punkt 3.2.

Det ska förutsättas att kraven är uppfyllda i fråga om de delar av kvalitetssäkringssystemet som uppfyller motsvarande specifikationer i den nationella standard genom vilken den relevanta harmoniserade standarden eller de tekniska specifikationerna genomförs.

Utöver erfarenhet av kvalitetsledningssystem ska minst en av revisionsgruppens deltagare ha erfarenhet av bedömning av det aktuella produktområdet och den berörda produkttekniken, och känna till de tillämpliga kraven som anges i denna förordning. Revisionen ska även omfatta ett bedömningsbesök i tillverkarens anläggning, om en sådan anläggning finns. Revisionsgruppen ska granska den tekniska dokumentation som avses i punkt 3.1 b för att kontrollera att tillverkaren känner till de tillämpliga kraven som anges i denna förordning och kan utföra de undersökningar som krävs för att säkerställa att produkten med digitala element överensstämmer med kraven.

Tillverkaren eller tillverkarens representant ska meddela beslutet.

Meddelandet ska innehålla slutsatserna från revisionen och det motiverade bedömningsbeslutet.

3.4 Tillverkaren ska åta sig att fullgöra de skyldigheter som är förenade med det godkända kvalitetssystemet och att upprätthålla det så att det förblir ändamålsenligt och effektivt.

3.5 Tillverkaren ska informera det anmälda organ som har godkänt kvalitetssystemet om alla planerade ändringar av systemet.

Det anmälda organet ska bedöma de föreslagna ändringarna och avgöra om ett ändrat kvalitetssystem fortfarande uppfyller de krav som avses i punkt 3.2 eller om en ny bedömning är nödvändig.

Det ska meddela tillverkaren sitt beslut. Meddelandet ska innehålla slutsatserna från undersökningen och det motiverade bedömningsbeslutet.

4. Övervakning under det anmälda organets ansvar

4.1 Syftet med övervakningen är att säkerställa att tillverkaren fullgör de skyldigheter som är förenade med det godkända kvalitetssystemet.

4.2 För att möjliggöra en bedömning ska tillverkaren ge det anmälda organet tillträde till lokaler för utformning, utveckling, produktion, kontroll, provning och lagring och tillhandahålla all nödvändig information, särskilt i fråga om

a) dokumentationen av kvalitetssystemet,

b) de dokument som anges i kvalitetssystemets utformningsdel, t.ex. resultat från analyser, beräkningar och provningar,

c) de dokument som anges i kvalitetssystemets tillverkningsdel, t.ex. kontrollrapporter, provningsresultat, kalibreringsresultat och redogörelser för den berörda personalens kvalifikationer.

4.3 Det anmälda organet ska regelbundet genomföra revisioner för att säkerställa att tillverkaren vidmakthåller och tillämpar kvalitetssystemet, samt överlämna en revisionsrapport till tillverkaren.

5. Märkning om överensstämmelse och försäkras om överensstämmelse

5.1 Tillverkaren ska fästa CE-märkningen och, under ansvar av det anmälda organ som avses i punkt 3.1, organets identifikationsnummer på varje enskild produkt med digitala element som uppfyller kraven i del I i bilaga I.

EUT L, 20.11.2024

SV

- 5.2 Tillverkaren ska upprätta en skriftlig försäkran om överensstämmelse för en produktmodell och kunna uppvisa den för de nationella myndigheterna under en period på tio år efter det att produkten med digitala element har släppts ut på marknaden eller under stödperioden, beroende på vilken period som är längst. I försäkran om överensstämmelse ska det anges för vilken produktmodell den har upprättats.

En kopia av försäkran om överensstämmelse ska på begäran göras tillgänglig för de behöriga myndigheterna.

6. Tillverkaren ska under en period på minst tio år efter det att produkten med digitala element har släppts ut på marknaden eller under stödperioden, beroende på vilken period som är längst, kunna uppvisa följande för de nationella myndigheterna:
- a) Den tekniska dokumentation som avses i punkt 3.1.
 - b) Sådan dokumentation av kvalitetssystemet som avses i punkt 3.1.
 - c) Godkända ändringar som avses i punkt 3.5.
 - d) De beslut och rapporter från det anmälda organet som avses i punkterna 3.5 och 4.3.

7. Varje anmält organ ska underrätta sina anmälade myndigheter om de godkännanden av kvalitetssystem som det har utfärdat eller återkallat och ska regelbundet eller på begäran ge de anmälade myndigheterna tillgång till förteckningen över godkännanden som det har vägrat att utfärda, tillfälligt återkallat eller på annat sätt belagt med restriktioner.

Varje anmält organ ska underrätta de övriga anmälda organen om de godkännanden av kvalitetssystem som det har vägrat utfärda eller tillfälligt eller slutgiltigt återkallat och, på begäran, om de godkännanden av kvalitetssystem som det har utfärdat.

8. Tillverkarens representant

Tillverkarens skyldigheter enligt punkterna 3.1, 3.5, 5 och 6 får fullgöras, för dennes räkning och på dennes ansvar, av tillverkarens representant, förutsatt att de relevanta skyldigheterna specificeras i fullmakten.

Ett uttalande har gjorts om denna akt och återges i EUT C, 2024/6786, 20.11.2024, ELI: <http://data.europa.eu/eli/C/2024/6786/oj>.



Europeiska unionens
officiella tidning

SV
L-serien

2025/90555

2.7.2025

Rättelse till Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen)

(Europeiska unionens officiella tidning L, 2024/2847, 20 november 2024)

Sidan 65, artikel 64.10, inledningsfrasen

- I stället för:* "Genom undantag från punkterna 3–9 ska de administrativa sanktionsavgifter som avses i dessa punkter inte tillämpas på följande:"
- ska det stå:* "Genom undantag från punkterna 2–9 ska de administrativa sanktionsavgifter som avses i dessa punkter inte tillämpas på följande:"



Europeiska unionens
officiella tidning

SV
L-serien

2025/90828

17.10.2025

Rättelse till Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen)

(Europeiska unionens officiella tidning L, 2024/2847, 20 november 2024)

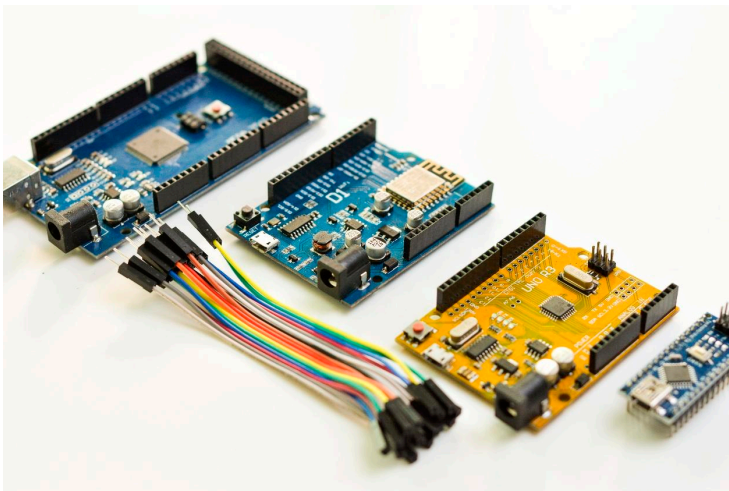
Sidan 66, artikel 67

I stället för: "69. Europaparlamentets och rådets förordning (EU) 2024/2847 (*)."

ska det stå: "72. Europaparlamentets och rådets förordning (EU) 2024/2847 (*)."

Konsekvenser avseende krav i EU:s cyberresiliensförordning 2024/2847

Analys på uppdrag av
Cyberresiliensutredningen (Fi 2024:07)



2025-09-30
Svante Eriksson och Johan Werkström



Innehållsförteckning

Sammanfattning 3

Summary 9

1. Inledning 14

1.1. BAKGRUND 14

1.2. SYFTE OCH MÅL 14

1.3. UPPDRAGETS FRÅGESTÄLLNINGAR 15

1.4. FÖRUTSÄTTNINGAR FÖR ANALYSEN OCH AVGRÄNSNINGAR 16

1.5. GENOMFÖRANDE OCH DISPOSITION 17

2. Påverkan på svenska tillverkare, importörer och distributörer 19

2.1. CRA OMFATTAR PRODUKTER FRÅN MÅNGA OMRÅDEN 19

2.2. PRODUKTKATEGORIER OCH TILLVERKARENS KONTROLLANSVAR 20

2.3. SVENSKA TILLVERKARE AV PRODUKTER INOM CRA:S OMRÅDE 23

2.4. KOSTNADER FÖR BERÖRDA TILLVERKARE 28

2.5. FÖRVALTARE AV PROGRAMVARA MED FRI OCH ÖPPEN KÄLLKOD 33

2.6. SVENSKA IMPORTÖRER OCH DISTRIBUTÖRER AV PRODUKTER MED DIGITALA ELEMENT 35

2.7. PÅVERKAN PÅ SMÅ- OCH MEDELSTORA FÖRETAG 38

3. Tillgång till organ för bedömning av överensstämmelse 40

3.1. ROLLEN SOM ORGAN FÖR BEDÖMNING AV ÖVERENSSTÄMMELSE I CRA 40

3.2. BEHOV AV ORGAN FÖR BEDÖMNING AV ÖVERENSSTÄMMELSE NÄR CRA TRÄDER I KRAFT 40

3.3. UTBUD AV SVENSKA ORGAN FÖR BEDÖMNING AV ÖVERENSSTÄMMELSE NU OCH PÅ SIKT 41

3.4. KONSEKVENSER AV EN POTENTIELL BRIST PÅ SVENSKA ORGAN FÖR BEDÖMNING AV ÖVERENSSTÄMMELSE 43

4. Marknadskontrollmyndighetens resursbehov 45

4.1. MARKNADSKONTROLLEN I DAG 45

4.2. UPPBYGGNADSFASEN FÖR DEN NYA MARKNADSKONTROLLUPPGIFTEN 48

4.3. LÖPANDE VERKSAMHET I DEN NYA MARKNADSKONTROLLUPPGIFTEN 49

4.4. SUMMERING 53

Referenser 55



Sammanfattning

På uppdrag av Cyberresiliensutredningen (Fi 2024:07) har Governo analyserat vissa frågor kopplade till EU:s cyberresiliensförordning (CRA) och framtagandet av kompletterande svenska regler. Uppdraget har berört följande frågor och aktörer:

- + Hur många **svenska ekonomiska aktörer** (tillverkare, importörer och distributörer) kommer att omfattas av regelverket och hur påverkas de av regleringen?
- + Vilken tillgång finns på svenska **kontrollorgan** (organ för bedömning av överensstämmelse) som kan genomföra bedömning av överensstämmelse enligt CRA?
- + Hur stora resurser behöver tillföras till den myndighet som i Sverige ska ges rollen som **marknadskontrollmyndighet** enligt CRA?

Uppdraget har genomförts under augusti–september 2025. Analysen är baserad på tillgängligt skriftligt material samt kontakter med Cyberresiliensutredningen och några externa branschföreträdare och experter.

Väsentliga förutsättningar för analysen

I dagsläget finns ett flertal osäkerheter och utestående frågor om hur CRA i praktiken kommer att fungera. Förordningen är visserligen antagen – den trädde i kraft den 10 december 2024 och börjar tillämpas fullt ut den 11 december 2027. Men det pågår ett arbete i de olika medlemsstaterna med att utreda hur reglerna ska anpassas och tillämpas på nationell nivå. Vissa viktiga delar av det tänkta systemet är heller inte på plats än, bland annat saknas ännu de harmoniserade standarder som aktörerna ska kunna hänvisa till vid bedömning av överensstämmelse.

De osäkerheter som föreligger har påverkat våra möjligheter att göra precisa uppskattningar kring de frågor uppdraget omfattar. Vissa av de delfrågor som ställs i uppdraget har vi endast kunnat besvara partiellt eller mer översiktligt.

Samtidigt finns det också faktorer som minskar osäkerheterna om hur CRA ska fungera i praktiken. En sådan är att förordningen bygger på den grundstruktur som sedan länge finns etablerad kring hanteringen av produkters säkerhet och fria rörlighet inom EU. Enligt denna grundstruktur är det som huvudregel tillverkarens ansvar att en produkt uppfyller gällande krav och för uppfyllandet av kraven kan tillverkaren i hög grad hänvisa till tillämpning av gemensamma standarder. Vidare krävs det inte någon förhandskontroll av produkten från myndighetshåll innan den släpps ut på marknaden, utan i stället används marknadskontroll för att säkerställa att produkter på marknaden överensstämmer med gällande krav.

Vidare omfattas många av de produkter som träffas av CRA:s krav redan av säkerhetskrav och marknadskontroll utifrån andra EU-regler. Bland många berörda aktörer och myndigheter finns det därför sedan tidigare en förståelse för de grundläggande tankesätten och systemets tänkta funktion. Detta bör underlätta aktörernas möjligheter att leva upp till kraven, även om cyberresilienskrav i sig kan vara något nytt för somliga aktörer och att deras kompetens kring sådana frågor kan vara mindre väl utvecklad.



Påverkan på svenska ekonomiska aktörer

I uppdraget har ingått att uppskatta antalet svenska ekonomiska aktörer (tillverkare, importörer och distributörer) som omfattas av CRA och ekonomiska konsekvenser för dessa aktörer. Uppskattningen av antalet svenska ekonomiska aktörer har baserats på EU-kommissionens Impact Assessment Report och statistik från SCB:s företagsregister. Vår bedömning är att mellan 24 000 och 38 000 svenska tillverkare omfattas av förordningen. En stor majoritet av dessa (90% eller mer) är verksamma inom kategorin "övriga produkter", medan uppskattningsvis 8% tillverkar "viktiga produkter" och 2% tillverkar "kritiska produkter".

CRA innebär betydande kostnader för svenska aktörer. För tillverkare av "övriga produkter" uppskattas engångskostnader för att uppfylla förordningens krav till ca 588 000 kronor per tillverkare, och årligen återkommande kostnader till mellan 160 000 och 220 000 kronor. För tillverkare av viktiga och kritiska produkter uppskattas engångskostnader till 779 500 kronor per aktör, och årligen återkommande kostnader varierar mellan 242 000 och 302 000 kronor.

Antalet förvaltare av programvara med fri och öppen källkod på den svenska marknaden, som omfattas av särskilda delar av CRA, uppskattas till cirka 300. För dessa aktörer beräknas engångskostnaderna uppgå till omkring 85 000 kronor, medan de årligen återkommande kostnaderna uppskattas till cirka 12 000 kronor.

Utifrån samma metod som tillämpades för att identifiera antalet tillverkare uppskattar vi för Sveriges del antalet importörer till mellan 10 000 och 15 000 och antalet distributörer likaså till mellan 10 000 och 15 000. Den främsta kostnaden för dessa företag är relaterad till orientering kring de nya skyldigheterna, det vill säga anpassningskostnader för att sätta sig in i de nya rättsliga kraven och etablering av systematiska processer för efterlevnad av regelverket. Detta arbete antar vi rymms inom företagets redan pågående satsningar på kompetens- och processutveckling.

Sammanfattningsvis innebär CRA en betydande ekonomisk belastning för både tillverkare, importörer och distributörer av digitala produkter. För små och medelstora tillverkare, som uppskattas utgöra den betydande majoriteten av det totala antalet tillverkare, blir CRA:s påverkan särskilt omfattande då dessa aktörer generellt saknar kompetens och processer för att säkerställa cybersäkerhet i dagsläget. Detsamma gäller för små importörer av produkter från tillverkare utanför EU, som bär ett direkt ansvar för att dessa uppfyller kraven i förordningen, även om de själva inte har insyn i tillverkarens processer eller tekniska kapacitet. Detta innebär att de måste utveckla rutiner för att granska dokumentation, säkerställa CE-märkning och vid behov inhämta försäkringar om att sårbarheter hanteras, trots att de i praktiken kan ha begränsad möjlighet att bedöma detta.

Utmaningar avseende nationell tillgång på organ för bedömning av överensstämmelse

Även om CRA utgår från modellen att det är tillverkarens ansvar att en produkt uppfyller gällande krav, så krävs i vissa situationer att tillverkaren för bedömningen av överensstämmelse med kraven anlitar oberoende organ för att säkerställa att pro-



dukter på marknaden överensstämmer med gällande krav. Organen ska vara s.k. anmälda organ, vilket innebär att medlemslandet som de arbetar i ska anmäla organisationen som godkänts till EU-kommissionen – för svenska organ ansvarar Swedac för denna anmälan. Enligt CRA ska medlemsländerna sträva efter att senast den 11 december 2026 ha ett tillräckligt antal anmälda organ för bedömning av överensstämmelse tillgängliga för att undvika flaskhalsar och marknadshinder.

När CRA träder i kraft kommer det initialt att finnas ett omfattande behov av organens tjänster. Det stora initiala trycket på existerande organ för bedömning av överensstämmelse kan medföra flaskhalsproblem. Dessa riskerar dessutom att förvärras om de harmoniserade standarder som aktörerna ska kunna hänvisa till vid bedömning av överensstämmelse inte hinner tas fram i tid, eftersom en sådan situation leder till ett ökat behov för tillverkarna att anlita organ för bedömning av överensstämmelse.

Experter som vi talat med bedömer att Sverige ligger förhållandevis väl till när det gäller tillgång på relevanta organ för bedömning av överensstämmelse. Inom området cybersäkerhet finns i dagsläget tre organ som av Swedac ackrediterats som certifieringsorgan och organ för bedömning av överensstämmelse för cybersäkerhetsprodukter och -tjänster enligt EU:s ramverk. Dessa torde vara väl lämpade att också bli anmälda organ enligt CRA – den bild vi fått i utredningen är dock att endast två av de tre i praktiken är intresserade av en sådan roll. Även andra aktörer – som i dag arbetar med likartade kontrolluppgifter inom andra områden eller har annan relevant kompetens – kan dock antas vilja vara intresserade av att bli anmälda som organ för bedömning av överensstämmelse enligt CRA. För det talar bland annat att det med största sannolikhet kommer att finnas en efterfrågan på kontrolltjänster från både svenska tillverkare och företag från andra EU-länder. Det bör rimligtvis utgöra ett starkt incitament för dessa aktörer. I dagsläget påverkas dock företagets marknadsanalyser av att marknaden inväntar utvecklingen av harmoniserade standarder på området. Att investera i att bygga upp kompetens, system och processer innan standarderna är på plats kan upplevas som ett visst risktagande, eftersom standarder kan innebära behov av omfattande justeringar.

Samtidigt kan det inte uteslutas att det svenska utbudet på kontrolltjänster inte kommer att kunna täcka upp alla svenska tillverkares efterfrågan vid CRA:s – åtminstone inte från start. Initialt kan därför svenska tillverkare komma att vända sig till anmälda organ i andra EU-länder. Rent principiellt bör detta inte innebära några särskilda konsekvenser då kontrollen är tänkt att vara en standardiserad process inom EU. Däremot kan en brist på svenska organ för bedömning av överensstämmelse innebära en ökad tröskel för svenska företag, som sannolikt skulle föredra att vända sig till svenska organ.

Risken för ett initialt underskott på svenska organ för bedömning av överensstämmelse talar för att det inför CRA:s start kan behövas statliga insatser för att stimulera fler aktörer att bli sådana organ, till exempel statligt stöd eller utbildningsinsatser.



Marknadskontrollmyndighetens resursbehov

I uppdraget har ingått att analysera vilka resurser den myndighet som i Sverige utses till marknadskontrollmyndighet enligt CRA behöver tillföras för uppgiften. Vi har utgått från att Post- och telestyrelsen, PTS, ska tilldelas denna uppgift, eftersom Cyberresiliensutredningen enligt uppgift avser att föreslå detta.

PTS arbetar sedan länge med marknadskontroll, bland annat avseende de svenska aktörer som omfattas av det s.k. radioutrustningsdirektivet. Härmed har myndigheten god kunskap om vad marknadskontroll innebär och erfarenhet av de aktiviteter som ingår, inklusive samverkan med andra myndigheter m.fl. Det bör därför finnas goda möjligheter att utvinna synergier till befintlig verksamhet när PTS ska bygga upp och driva den nya funktionen för marknadskontroll enligt CRA.

Marknadskontrollen enligt CRA förväntas dock komma att innehålla fler moment än den marknadskontroll som i dag vanligen sker inom olika produktområden. Befintlig marknadskontroll begränsas i normalfallet till kontroll av produkter som tillhandahålls på marknaden. Kontroller i konstruktions- eller produktionsskedet liksom regelbunden kontroll eller besiktning för att kontrollera om en produkt som används fortfarande uppfyller gällande krav omfattas i de allra flesta fall inte. Beträffande CRA kommer dock tillverkarna att behöva tillhandahålla säkerhetsuppdateringar under produktens hela livscykel. Behovet av marknadskontroll kommer då också att föreligga under hela denna hela stödperiod, det vill säga det behöver ske en viss övervakning efter utsläppandet på marknaden. Av bland annat detta skäl kan marknadskontrollen enligt CRA antas bli mer omfattande än den marknadskontroll PTS i dag bedriver avseende radioutrustning.

Arbetet med att starta upp marknadskontrollverksamheten avseende CRA kommer att medföra två typer av kostnader för PTS. Dels kostnader för PTS interna insatser för att bygga upp och etablera den nya funktionen för marknadskontroll. Hit hör exempelvis kostnader för kompetensuppbyggnad, för eventuella nyrekryteringar, för praktiska frågor (till exempel anskaffning av lokaler och datorer) med mera. Dels kostnader för att etablera den nya marknadskontrollfunktionen i en extern kontext. Hit hör till exempel kostnader för att informera berörda aktörer om den nya rollen, för att bygga upp nödvändig samverkan med andra myndigheter med mera. Vi bedömer att kostnaderna för uppbyggnadsfasen för den nya marknadskontrolluppgiften sammantaget kommer att uppgå till mellan 4 och 8 miljoner kronor.

I den löpande verksamheten avseende den nya marknadskontrolluppgiften kommer PTS att bland annat ha kostnader för personal, lokaler, teknisk utrustning, genomförande av undersökningar och tester, samverkan m.m.

För att uppskatta hur stora de löpande kostnaderna kan bli har vi laborerat med tre alternativ. Först har vi beräknat ett "nollalternativ", det vill säga en realistisk minsta nivå för hur stora resurser den löpande verksamheten kan tänkas kräva. Denna nivå har vi sedan ställt mot två – i varierande grad – mer expansiva alternativ ("Midi-alternativet" och "Maxi-alternativet"). Nedan sammanfattas de resursbehov som skulle uppstå med respektive alternativ. Vi har förutsatt att den angivna resursåtgången för respektive



alternativ täcker samtliga de arbetsuppgifter som ingår i PTS ansvar som marknads-kontrollmyndighet avseende CRA.

Nollalternativet

I dagsläget bedöms resursåtgången i PTS marknadskontroll avseende radioutrustning uppgå till cirka 3,5 till 4,5 årsarbetskrafter och cirka 6,5 miljoner kronor per år. För beräkningen av nollalternativet har vi tagit denna nivå som utgångspunkt.

Marknadskontrollen enligt CRA bedöms omfatta cirka tre gånger så många aktörer som PTS befintliga radioutrustningskontroll. Flera skäl talar dock för att omfattningen på marknadskontrollen enligt CRA inte bör beräknas rakt av som en proportionerlig uppskalning jämfört med dagens radioutrustningskontroll. Detta bland annat då PTS bör kunna utvinna synergier mellan sin nuvarande marknadskontrollverksamhet och den nyttillkommande CRA-kontrollen. Därtill finns en viss överlappning mellan CRA och radioutrustningslagen vad gäller berörda företag, samtidigt som också en stor andel av de produkter som berörs av CRA hör hemma i kategorin "övriga", det vill säga produkter som torde medföra en relativt sett lägre risk än viktiga och kritiska produkter och därför rimligen lär kunna prioriteras förhållandevis lågt i marknadskontrollen.

Mot denna bakgrund har vi antagit att 50 procent större resursåtgång för den nya marknadskontrollfunktionen jämfört med dagens radioutrustningskontroll ger en realistisk minsta nivå för hur stora resurser den nya marknadskontrollfunktionens löpande verksamhet kan tänkas kräva. Som nollalternativ i analysen har vi därmed antagit att den nya marknadskontrollfunktionen för CRA kommer att kräva 6 årsarbetskrafter och ha löpande kostnader på totalt ca 9–10 miljoner kronor per år.

Midi-alternativet

Som framgått förväntas marknadskontrollen enligt CRA komma att innehålla fler arbetsmoment än den marknadskontroll som i dag vanligen sker inom olika produktområden, inklusive PTS radioutrustningskontroll. Framför allt tillkommer det i CRA mer av löpande kontroll under berörda produkters hela livslängd. Möjligen kommer kontrollen enligt CRA därtill att kräva mer samverkan med andra myndigheter m.fl. än den traditionella marknadskontrollen.

Mot denna bakgrund kan antas att kostnaden för den nya marknadskontrollfunktionens löpande verksamhet kommer att bli relativt sett högre än i den befintliga marknads-kontrollen. I Midi-alternativet antar vi att denna merkostnad kommer att bli 50 procent högre än i nollalternativet. Med detta antagande skulle den nya marknadskontroll-funktionen vid PTS komma att kräva ca 9 årsarbetskrafter och ha löpande kostnader på totalt ca 13,5–15 miljoner kronor per år.

Maxi-alternativet

I detta alternativ görs motsvarande justering som i Midi-alternativet, men vi antar att merkostnaden blir 100 procent högre än i nollalternativet (inklusive en dubblering av personalbehovet). Med detta antagande skulle den nya marknadskontrollfunktionen



vid PTS komma att kräva ca 12 årsarbetskrafter och ha löpande kostnader på totalt ca 18–20 miljoner kronor per år.

Summering

Utifrån nuvarande kunskapsläge och de antaganden vi kunnat göra om rimliga utfall, uppskattar Governo att PTS resursbehov för den nya uppgiften att bedriva marknadskontroll enligt CRA sammantaget kommer att uppgå till:

- + mellan 4 och 8 miljoner kronor för att starta upp verksamheten, och
- + mellan 10 och 20 miljoner kronor per år för marknadskontrollfunktionens löpande verksamhet.



Summary

On behalf of the Cyber Resilience Inquiry (Fi 2024:07), Governo has analyzed certain issues related to the EU Cyber Resilience Act (CRA) and the development of complementary Swedish regulations. The assignment has addressed the following questions and stakeholders:

- ✦ How many Swedish economic actors (manufacturers, importers, and distributors) will be covered by the regulation and how will they be affected by it?
- ✦ What is the availability of Swedish conformity assessment bodies that can carry out conformity assessments according to CRA?
- ✦ What resources need to be allocated to the authority in Sweden that will be assigned the role of market surveillance authority under CRA?

The assignment was carried out during August–September 2025. The analysis is based on available written materials as well as contacts with the Cyber Resilience Inquiry and some external industry representatives and experts.

Key Assumptions for the Analysis

At present, there are several uncertainties and outstanding questions about how CRA will function in practice. The regulation has been adopted – coming into force on December 10, 2024, and being fully implemented on December 11, 2027. However, work is ongoing in the member states to investigate how the rules will be adapted and applied at the national level. Some key components of the intended system are also not yet in place, including the harmonized standards that actors should refer to when assessing compliance.

The uncertainties present have affected our ability to make precise estimates about the issues addressed in the assignment. Some of the sub-questions posed in the assignment could only be partially or broadly answered.

At the same time, there are factors that reduce the uncertainties about how CRA will work in practice. One such factor is that the regulation is based on a fundamental structure that has long been established regarding product safety and the free movement of goods within the EU. According to this structure, the manufacturer is generally responsible for ensuring that a product meets the relevant requirements, and the manufacturer can largely refer to the application of common standards in fulfilling these requirements. Furthermore, there is no pre-market control of the product by authorities; instead, market surveillance is used to ensure that products on the market comply with applicable requirements.

Moreover, many of the products covered by CRA's requirements are already subject to safety requirements and market surveillance under other EU regulations. Among many affected actors and authorities, there is already an understanding of the basic concepts and the intended functioning of the system. This should facilitate the actors'



ability to meet the requirements, even though cyber resilience requirements may be new for some actors and their competence in such matters may be less developed.

Impact on Swedish Economic Actors

The assignment included estimating the number of Swedish economic actors (manufacturers, importers, and distributors) covered by CRA and the economic impact on these actors. The estimate of the number of Swedish economic actors was based on the European Commission's Impact Assessment Report and statistics from Statistics Sweden's business register. Our assessment is that between 24,000 and 38,000 Swedish manufacturers will be covered by the regulation. The vast majority of these (over 90%) operate in the "other products" category, while approximately 8% manufacture "important products" and 2% manufacture "critical products."

CRA entails significant costs for Swedish actors. For manufacturers of "other products," one-time costs to comply with the regulation are estimated at about 588,000 SEK per manufacturer, with recurring annual costs between 160 000 and 220 000 SEK. For manufacturers of important and critical products, one-time costs are estimated at 779 500 SEK per actor, with recurring annual costs ranging from 240,000 to 302,000 SEK.

The number of open-source software stewards on the Swedish market, who are covered by specific parts of CRA, is estimated at about 300. For these actors, one-time costs are estimated at 85,000 SEK, with recurring annual costs estimated at 12,000 SEK.

Using the same method applied to estimate the number of manufacturers, we estimate the number of Swedish importers at between 10,000 and 15,000 and the number of Swedish distributors at the same range. The primary cost for these companies is related to orientation around the new obligations, i.e., adjustment costs to familiarize themselves with the new legal requirements and establish systematic processes for compliance with the regulation. We assume this work falls within the companies' ongoing investments in competence and process development.

In summary, CRA represents a significant financial burden for manufacturers, importers, and distributors of digital products. For small and medium-sized manufacturers, who are estimated to make up the majority of the total number of manufacturers, the impact of CRA is particularly extensive since these actors generally lack the competence and processes to ensure cybersecurity at present. The same applies to small importers of products from manufacturers outside the EU, who bear direct responsibility for ensuring that these meet the regulation's requirements, even though they may have no insight into the manufacturer's processes or technical capacity. This means they must develop procedures to review documentation, ensure CE marking, and, if necessary, obtain assurances that vulnerabilities are addressed, even though they may have limited ability to assess this in practice.

Challenges Regarding National Availability of Notified Bodies

Although CRA is based on the model that it is the manufacturer's responsibility to ensure a product complies with applicable requirements, certain situations require the



manufacturer to engage independent conformity assessment bodies to ensure that products on the market comply with the relevant requirements. These bodies must be "notified bodies," meaning that the member state in which they operate must notify the organization as approved to the European Commission – Swedac is responsible for this notification in Sweden. According to CRA, member states are to aim to have a sufficient number of notified control bodies available by December 11, 2026, to avoid bottlenecks and market barriers.

When CRA comes into force, there will initially be a significant demand for the services of control bodies. The large initial pressure on existing control bodies could cause bottlenecks, which may be exacerbated if the harmonized standards that actors should refer to when assessing compliance are not developed in time, as this would lead to an increased need for manufacturers to hire control bodies.

Experts we have spoken with assess that Sweden is relatively well-positioned regarding access to relevant control bodies. Within the area of cybersecurity, there are currently three bodies that Swedac has accredited as certification bodies and bodies for conformity assessment for cybersecurity products and services under the EU framework. These should be well-suited to also become notified bodies under CRA – however, the impression we have gotten in the investigation is that only two of the three are practically interested in such a role. Other actors – such as those currently working with similar control tasks in other areas or with other relevant expertise – are likely to be interested in becoming notified as control bodies under CRA. This is further supported by the fact that there is likely to be demand for control services from both Swedish manufacturers and companies from other EU countries. This should provide a strong incentive for these actors. However, businesses' market analyses are currently affected by the fact that the market is awaiting the development of harmonized standards in the area. Investing in building competence, systems, and processes before the standards are in place may be seen as a certain risk, as standards could lead to the need for extensive adjustments.

At the same time, it cannot be ruled out that the Swedish supply of control services will not be able to meet all Swedish manufacturers' demand at the outset of CRA – at least not initially. Swedish manufacturers may therefore have to turn to notified control bodies in other EU countries. In principle, this should not result in any particular consequences, as the control is intended to be a standardized process within the EU. However, a lack of Swedish control bodies could raise the threshold for Swedish companies, who are likely to prefer to turn to Swedish control bodies.

The risk of an initial shortage of Swedish control bodies suggests that state interventions may be needed before the start of CRA to stimulate more actors to become control bodies, such as government support or training initiatives.

Resource Needs for the Market Surveillance Authority

The assignment also involved analyzing what resources the authority assigned as the market surveillance authority under CRA in Sweden will need to perform the task. We



have assumed that the Swedish Post and Telecom Authority (PTS) will be tasked with this, as the Cyber Resilience Inquiry is reportedly planning to propose this.

PTS has long been involved in market surveillance, including for Swedish actors covered by the Radio Equipment Directive. The authority therefore has good knowledge of what market surveillance entails and experience with the activities involved, including collaboration with other authorities, etc. Thus, there should be good opportunities to leverage synergies with existing activities when PTS builds and operates the new market surveillance function under CRA.

However, market surveillance under CRA is expected to involve more steps than the market surveillance typically conducted today within various product areas. Existing market surveillance is usually limited to checking products available on the market. Controls in the construction or production phase, as well as regular checks or inspections to verify whether a product in use still meets the relevant requirements, are not usually covered. However, under CRA, manufacturers will need to provide security updates throughout the product's entire lifecycle. Therefore, there will be a need for market surveillance during this entire support period, meaning that monitoring after market release will also be necessary. For these reasons, market surveillance under CRA is expected to be more comprehensive than the market surveillance PTS currently conducts for radio equipment.

Starting the market surveillance activities related to CRA will involve two types of costs for PTS. First, costs for PTS's internal efforts to establish and build the new market surveillance function. This includes costs for competence building, potential new hires, practical matters (e.g., acquiring premises and equipment), and more. Second, costs for establishing the new market surveillance function in an external context. This includes costs for informing affected actors about the new role, building necessary collaboration with other authorities, and more. We estimate that the startup costs for the new market surveillance task will range between 4 and 8 million SEK.

In the ongoing operations of the new market surveillance function, PTS will incur costs for personnel, premises, technical equipment, conducting investigations and tests, collaboration, etc. To estimate the ongoing costs, we considered three options: a "zero option," representing the minimum realistic level of resources required, and two more expansive options (the "Midi option" and the "Maxi option").

Zero Option

The current resource use for PTS's market surveillance of radio equipment is estimated to require approximately 3.5 to 4.5 full-time equivalents and 6.5 million SEK per year. For the zero option, we have assumed that the new market surveillance function for CRA will require 6 full-time equivalents and annual operating costs of approximately 9-10 million SEK.

**Midi Option**

Given that market surveillance under CRA is expected to involve more steps, including ongoing checks throughout the product lifecycle, we assume that ongoing costs will be higher than for current market surveillance. Under the Midi option, we estimate a 50% increase in costs compared to the zero option, requiring about 9 full-time equivalents and 13.5-15 million SEK per year.

Maxi Option

Under the Maxi option, we assume that costs will be double those of the zero option, including a doubling of personnel. This would result in about 12 full-time equivalents and 18-20 SEK million per year.

Summary

Based on current knowledge and reasonable assumptions about likely outcomes, Governo estimates that PTS's resource needs for the new market surveillance task under CRA will be:

- ✦ Between 4 and 8 million SEK for startup costs, and
- ✦ Between 10 and 20 million SEK per year for ongoing operations.



1. Inledning

1.1. Bakgrund

EU:s cyberresiliensförordning (eller CRA efter det engelska namnet Cyber Resilience Act) ställer cybersäkerhetskrav på produkter med digitala element, det vill säga hård- och mjukvara, som tillhandhålls på den inre marknaden. Förordningen trädde i kraft den 10 december 2024 och börjar tillämpas fullt ut den 11 december 2027. Vissa bestämmelser träder dock i kraft tidigare.

Med produkter med digitala element avses enligt CRA maskinvaru- eller programvaru-produkter inklusive dess fjärrdatabehandlingslösningar. Därmed omfattas inte bara själva den fysiska eller digitala produkten, utan även tillhörande digitala tjänster som produkten är beroende av för att fungera korrekt. Enligt förordningen avses med fjärrdatabehandling av data databehandling på distans som utvecklats av (eller på uppdrag av) tillverkaren och vars avsaknad skulle hindra produkten från att utföra en av sina funktioner. Sådana integrerade fjärrtjänster (relaterade digitala tjänster), betraktas i dessa fall som en del av produkten och måste uppfylla cybersäkerhetskraven i förordningen. Ekonomiska aktörer som tillverkare, importörer och distributörer av berörda produkter måste uppfylla de uppställda kraven i förordningen för att få tillhandahålla produkterna på den inre marknaden.

EU:s cyberresiliensförordning ställer krav på att nationella förberedelser och åtgärder vidtas för att regleringen ska få avsedd effekt. I november 2024 tillsatte regeringen därför en särskild utredare med uppdrag att analysera behovet av och föreslå åtgärder och kompletterande författningsbestämmelser som behövs i syfte att anpassa svensk rätt till EU:s cyberresiliensförordning. Cyberresiliensutredningen (Fi 2024:07) ska redovisa sitt arbete senast den 15 december 2025.

För att Cyberresiliensutredningen ska kunna bedöma effekterna och konsekvenserna av EU:s cyberresiliensförordning och den kompletterande lagen som utredningen kan komma att föreslå behövs ett underlag som belyser utmaningar och behov för berörda aktörer i Sverige. Governo har därför fått i uppdrag att utreda och analysera aktuella förutsättningar och eventuella utmaningar kopplade till genomförandet av den angivna lagstiftningen, med fokus på följande aktörer:

- + Ekonomiska aktörer – svenska tillverkare, importörer och distributörer som omfattas av de nya kraven.
- + Organ för bedömning av överensstämmelse (kontrollorgan).
- + Marknadskontrollmyndigheten.

1.2. Syfte och mål

Syftet med Governos uppdrag är att kartlägga och analysera eventuella utmaningar och resursbehov som följer av regleringens genomförande. Analysen ska ge en bild av Sveriges utgångsläge inför att förordningens olika bestämmelser träder i kraft, samt ge



underlag för beslut om eventuella åtgärder som behövs för att säkerställa ett effektivt genomförande.

Målet är att ta fram ett underlag som även beskriver konsekvenserna för näringsliv och berörda myndigheter, och att lämna rekommendationer på hur identifierade problem kan adresseras.

1.3. Uppdragets frågeställningar

Governo ska genomföra en fördjupad undersökning, inkluderande att beskriva, analysera samt lämna rekommendationer och förslag inom ramen för nedan angivna frågeställningar. I uppdraget ingår även att analysera förutsättningar och bedöma eventuella konsekvenser.

1.3.1. Påverkan på svenska tillverkare, importörer och distributörer

Governo ska beskriva och analysera hur många svenska ekonomiska aktörer enligt förordningen som kan komma att omfattas av regelverket samt vilka ekonomiska och andra konsekvenser som regleringen medför för dessa aktörer. Beskrivningen och analysen ska bland annat innefatta att

- + identifiera vilka branscher, företagstyper och företag (tillverkare) i Sverige som omfattas,
- + bedöma hur många företag som verkar som importörer eller distributörer enligt förordningen samt analysera hur regelverket påverkar företagen ekonomiskt och på andra sätt,
- + analysera kostnader och investeringar som företagen kan behöva göra för att uppfylla kraven i förordningen med fokus på små och medelstora företag (SME), och
- + identifiera andra konsekvenser för berörda aktörer, bland annat om dessa hinner anpassa sina processer/produkter i anslutning till att de olika bestämmelserna i CRA börjar tillämpas.

I uppdraget ingår även att utifrån de analyser som görs lämna rekommendationer och förslag på åtgärder för att hantera identifierade utmaningar. Beträffande påverkan på svenska tillverkare, importörer och distributörer ska vi därvid särskilt diskutera åtgärder för att underlätta företagens regelefterlevnad, särskilt för små och medelstora aktörer, till exempel utveckling av vägledning, utbildningsinsatser eller ekonomiska incitament.

1.3.2. Tillgång till organ för bedömning av överensstämmelse

Governo ska utreda och beskriva det nuvarande läget och de utmaningar som finns vad avser nationell tillgång på kontrollorgan som kan genomföra bedömning av överensstämmelse enligt EU:s cyberresiliensförordning. Detta ska även omfatta:

- + En bedömning av hur många och vilka typer av kontrollorgan som kan behövas i Sverige för att möta kraven i CRA. Förordningen kräver att medlemsländerna "strävar efter" att senast den 11 december 2026 ha ett tillräckligt antal anmälda organ tillgängliga för att undvika flaskhalsar och marknadshinder.



- ✦ En analys av om det finns brist på kompetens nationellt för att bedriva verksamhet som anmält kontrollorgan inom förordningens tillämpningsområde, och om en eventuell brist medför att svenska tillverkare kan behöva vända sig till utländska kontrollorgan och konsekvenserna av detta.
- ✦ En beskrivning och analys av om det kan behövas statliga insatser för att stimulera fler aktörer att bli kontrollorgan, till exempel statligt stöd eller utbildningsinsatser.
- ✦ En sammanfattande analys av Sveriges förutsättningar att möta kraven i kapitel IV i EU:s cyberresiliensförordning när det gäller förekomsten av ett tillräckligt antal anmälda kontrollorgan för att undvika flaskhalsar och marknadshinder.

Vad gäller rekommendationer och förslag på åtgärder nämns i uppdraget att vi – om en brist på kontrollorgan konstateras – särskilt ska överväga hur antalet kontrollorgan kan öka eller deras kapacitet stärkas.

Det bör noteras att den funktion som i uppdragstexten benämns kontrollorgan snarare i detta sammanhang vanligen bör benämnas "organ för bedömning av överensstämmelse", varför vi i allmänhet använder det begreppet i rapporten.

1.3.3. Marknadskontrollmyndighetens resursbehov

Governo ska med utgångspunkt i förslaget om marknadskontrollmyndighet beskriva och analysera vilka resurser den utsedda myndigheten behöver tillföras. Beskrivningen och analysen ska bland annat innehålla bedömningar av

- ✦ vad det kostar att starta upp marknadskontrollverksamhet,
- ✦ hur många produkter med digitala element marknadskontrollmyndigheten rimligtvis bör kontrollera, det vill säga i form av slumpmässiga kontroller respektive risk-baserade kontroller (mot bakgrund av antalet produkter som omfattas av CRA), och
- ✦ den genomsnittliga kostnaden för ett marknadskontrollärende (kontroll av administrativa och tekniska krav).

Beträffande rekommendationer och förslag på åtgärder ska vi enligt uppdraget särskilt överväga hur marknadskontrollmyndigheten kan organiseras och resursställas.

1.4. Förutsättningar för analysen och avgränsningar

Vissa väsentliga förutsättningar och avgränsningar har påverkat vår analys, bland annat att det för närvarande finns flera osäkerheter kring hur CRA i praktiken kommer att fungera. Även om förordningen är antagen så pågår ett arbete i de olika medlemsstaterna med att utreda hur reglerna ska anpassas och tillämpas på nationell nivå – i detta skiljer sig inte Sverige från övriga EU. Därtill är vissa viktiga delar av det tänkta systemet inte helt på plats, bland annat saknas ännu de harmoniserade standarder som aktörerna ska kunna hänvisa till vid bedömning av överensstämmelse (enligt plan ska dessa levereras först sommaren/hösten 2026 och hösten 2027). Det faktum att det alltför handlar om en pågående process – med ett delvis osäkert kunskapsläge – har påverkat våra möjligheter att göra precisa uppskattningar kring de frågor uppdraget omfattar. Vissa av de delfrågor som ställs i uppdraget har vi endast kunnat besvara partiellt eller mer översiktligt.



Samtidigt finns det också faktorer som minskar osäkerheterna om hur CRA ska fungera i praktiken. En väsentlig sådan faktor är att förordningen bygger på den grundstruktur som sedan länge finns etablerad kring hanteringen av produkters säkerhet och fria rörlighet inom EU. Principen om fri rörlighet för varor på den inre marknaden är grundläggande för EU-samarbetet. För att uppnå fri rörlighet för varor har EU bland annat antagit ett stort antal gemensamma regler med produktkrav som gäller i alla medlemsstater. Reglerna bygger oftast på tillämpning av gemensamma standarder. Det är som huvudregel tillverkarens ansvar att en produkt uppfyller gällande krav och det krävs inte någon förhandskontroll av produkten från myndighetshåll innan den släpps ut på marknaden. För att säkerställa att produkter på marknaden överensstämmer med gällande krav används i stället marknadskontroll.¹

Många av de produkter som träffas av cyberresiliensförordningen omfattas redan av säkerhetskrav och marknadskontroll utifrån andra EU-regler. Bland många berörda aktörer och myndigheter finns det därför sedan tidigare en förståelse för de grundläggande tankesätten och systemets tänkta funktion. En stor del av de berörda företagen torde också ha uppbyggda rutiner för internkontroll av produktsäkerhet, rapportering av problem, CE-märkning, vid behov anlita av oberoende organ för bedömning av överensstämmelse, etc. Detta bör ha stor betydelse för aktörernas kostnader för att leva upp till kraven, avseende till exempel administrativa kostnader. Låt vara att cyberresilienskrav i sig kan vara något nytt för somliga aktörer och att deras kompetens kring sådana frågor kan vara mindre väl utvecklad.

Startpunkten i vårt arbete har varit att försöka uppskatta antal produkter och aktörer som för svensk del omfattas av CRA. Som kommer att framgå närmare av kapitel 2 har vi sökt identifiera berörda produktgrupper och gruppera dem dels i viktiga (klass 1 och 2), kritiska och övriga produkter, dels utifrån branscher. Dessa uppskattningar har sedan varit en utgångspunkt även för vår analys avseende tillgång till organ för bedömning av överensstämmelse och marknadskontrollmyndighetens resursbehov.

När vi har beskrivit de konsekvenser och effekter (nyttor och kostnader) som förväntas uppstå, så har ambitionen varit att så långt möjligt kvantifiera förväntade konsekvenser och effekter. I vissa fall har vi dock inte haft tillgång till relevanta data från berörda aktörer av sådan art att en mer detaljerad kvantifiering av nyttor och kostnader har varit möjlig att göra. Vi har då tvingats stanna vid en mer övergripande beskrivning. Där så är relevant har vi också så långt möjligt sökt beakta påverkan på sådant som de ekonomiska aktörernas regelbörda och på innovation/konkurrenskraft.

1.5. Genomförande och disposition

Uppdraget har genomförts under augusti och september 2025. Analysen baseras på tillgängligt skriftligt material (se referenslista), diskussioner med Cyberresiliensutredningen

¹ SOU 2020:49 Enhetlig och effektiv marknadskontroll. Betänkande av 2019 års marknadskontrollutredning, s. 177.



samt intervjuer med externa branschföreträdare och experter – i form av kontrollorganet Atsec, Post- och telestyrelsen (PTS) och Försvarets materielverk (FMV).

Under projektets genomförande har Governo och Cyberresiliensutredningen haft flera avstämningmöten där vi kunnat diskutera det framtagna materialet och de preliminära resultaten och gemensamt stämt av vad som är en rimlig detaljnivå i analysen.

Beställaren gavs möjlighet att faktagranska en utkastversion av denna rapport innan slutversionen överlämnades den 30 september 2025.

Den fortsatta framställningen har disponerats på följande sätt:

- + I kapitel 2 behandlar vi frågor om cyberresiliensförordningens påverkan på svenska tillverkare, importörer och distributörer.
- + Kapitel 3 tar upp frågor om tillgång till organ för bedömning av överensstämmelse.
- + Kapitel 4 behandlar marknadskontrollmyndighetens resursbehov



2. Påverkan på svenska tillverkare, importörer och distributörer

I vårt uppdrag ingår att analysera vissa frågor kring påverkan på svenska tillverkare, importörer och distributörer. Som framgått av kapitel 1 ska vi beskriva och analysera hur många svenska ekonomiska aktörer enligt förordningen som kan komma att omfattas av regelverket samt vilka ekonomiska och andra konsekvenser som regleringen medför för dessa aktörer. I uppdraget ingår även att utifrån de analyser som görs lämna rekommendationer och förslag på åtgärder för att hantera identifierade utmaningar.

2.1. CRA omfattar produkter från många områden

Cyberresiliensförordningen är tillämplig på alla produkter med digitala element som tillhandahålls på EU:s marknad och vars avsedda ändamål eller rimligen förutsebara användning omfattar en direkt eller indirekt logisk eller fysisk dataanslutning till en enhet eller ett nät. Detta inkluderar både hårdvara och mjukvara som är uppkopplade eller kan ansluta till nätverk, såsom smartphones, datorer, IoT-enheter², nätverkskomponenter och programvara för säkerhet. Även digitala tjänster ingår, exempelvis databehandling som produkten är beroende av för sin funktion.

CRA gäller i princip för alla produkter som har en digital funktion och är kopplade till ett nätverk. Produkter från många områden berörs därmed av CRA. Det handlar exempelvis om produkter för industriell automation och IT-säkerhetslösningar, men också om produkter som konsumenterna använder i vardagen, till exempel uppkopplade produkter såsom smarta TV-apparater, hushållsapparater, datorer, telefoner, spel och andra leksaker m.m.

Vissa produkter med digitala element ligger dock utanför tillämpningsområdet för CRA, eftersom det finns andra regler för dem. Se faktarutan nedan.

Faktaruta 1. Produktområden som inte omfattas av CRA

- + Produkter med digitala element som omfattas av följande unionsakter:
 - Förordning (EU) 2017/745 och (EU) 2017/746 om medicintekniska produkter
 - Förordning (EU) 2019/2144 om motorfordon.
- + Produkter med digitala element som har certifierats i enlighet med förordning (EU) 2018/1139 (civil luftfart).
- + Utrustning som omfattas av Europaparlamentets och rådets direktiv 2015/90/EU om marin utrustning.

² IoT-enheter (av Internet of Things) avser fysiska föremål utrustade med sensorer, programvara och andra teknologier som gör att de kan ansluta till och kommunicera med varandra och centrala system via internet. Dessa enheter samlar in och utbyter data, vilket möjliggör automatisering, fjärrstyrning och övervakning av olika processer. Exempel inkluderar smarta klockor, termostater och smarta kylskåp.



- + Produkter med digitala element som omfattas av andra unionsregler där krav fastställs avseende alla eller vissa risker som täcks av de väsentliga cybersäkerhetskraven i bilaga I får begränsas eller undantas om sådana begränsningar eller undantag är förenliga med den allmänna rättsliga ram som är tillämplig på dessa produkter, och sektorsreglerna ger samma eller en högre skyddsnivå än den som föreskrivs i CRA.
- + Reservdelar som tillhandahålls på marknaden för att ersätta identiska komponenter i produkter med digitala element och som tillverkas enligt samma specifikationer som de komponenter som de är avsedda att ersätta.
- + Produkter med digitala element som utvecklats eller ändrats uteslutande för ändamål som rör nationell säkerhet eller försvarsändamål eller på produkter som utformats specifikt för att behandla säkerhetsskyddsklassificerade uppgifter.
- + Molntjänster och programvara med fri och öppen källkod.

2.2. Produktkategorier och tillverkarens kontrollansvar

Kraven enligt CRA gäller för alla produkter inom berörda varuslag. De risker olika produkter medför i ett cyberresiliensperspektiv varierar dock. CRA skiljer därför mellan **viktiga produkter** och **kritiska produkter**, vilket gör det möjligt att tillämpa regler och kontrollåtgärder på ett sätt som reflekterar deras olika nivåer av säkerhetsrisk och samhällspåverkan. Ungefär 10% av samtliga produkter som omfattas av CRA faller under kategorierna viktiga och kritiska produkter. Kategoriseringen av olika produkter hjälper till att säkerställa att produkter som är avgörande för säkerheten och funktionen av samhällsviktiga system genomgår striktare reglering än produkter som har lägre riskprofil.

Liksom allmänt gäller beträffande EU:s regelverk för den fria rörligheten för varor inom EU, bygger CRA på att det är tillverkarens ansvar att göra en riskanalys och se till att produkterna uppfyller berörda krav innan de släpps ut på EU-marknaden. Vilka insatser som krävs i denna bedömning av överensstämmelse varierar beroende på produktens risknivåer. För många produkter kan tillverkaren utföra en egenkontroll (intern dokumentation och försäkran om överensstämmelse), i andra fall kan man behöva anlita externa organ för granskningen.³ Vilken nivå kontrollen ska ha anges i EU-systemet med olika bedömningsmoduler, allt från Modul A som i princip handlar om intern tillverkningskontroll från tillverkarens sida, till Modul H som innebär fullständig kvalitetssäkring där ett anmält organ granskar tillverkarens kvalitetssystem för att säkerställa att produkten uppfyller tillämpliga krav. Se tabellen nedan.

³ I de kontakter vi haft i utredningen har framförts att Sveriges position är att dessa organ ska vara ackrediterade för att bevisa sin kompetens.



Tabell 1. Produktkategorier och bedömningsmoduler

Produktkategorier	Exempel	Bedömningsmoduler
Alla produkter som omfattas av CRA (med undantag för nedanstående produkt-kategorier)	Hushållsapparater, hem-elektronik, enklare IoT, övriga produkter som omfattas av CRA	Modul A
Viktiga produkter (klass 2 enligt bilaga III)	Brandväggar, manipula-tionssäkra mikroprocesser och - kontroller	Modul B + C + ev. H
Kritiska produkter (enligt bilaga IV)	Hårdvaruenheter med säker-hetsboxar, smarta elmätare och andra enheter för avan-cerade säkerhetsmål	Modul B + C + ev. H

Utöver ovanstående föreskriver CRA även att certifiering enligt europeiska cybersäkerhetsakten (CSA) kan användas som ett verktyg för att visa överensstämmelse med de väsentliga kraven enligt CRA. Det möjliggör flexibilitet och att dubbelreglering och dubbla kontroller kan undvikas. Enligt artikel 32 är det dock endast för produkter som klassas som kritiska enligt bilaga IV som CSA-certifiering är obligatorisk. För övriga produktkategorier kan CSA-certifiering tillämpas frivilligt eller användas som ett sätt att styrka uppfyllelse. I de kontakter vi haft i utredningen har dock påtalats att det för närvarande finns osäkerheter om hur denna ordning kommer att fungera i praktiken. Detta då en delegerad akt behöver tas fram för varje produktkategori, och under framtagningen av delegerade akter ska det utredas i vilken utsträckning kraven i CSA möter de väsentliga kraven i CRA.

De olika modulerna enligt CRA beskrivs mer i detalj nedan. Framställningen utgår från Cyberresiliensutredningens beskrivningar av dessa förfaranden, som vi fått ta del av.

2.2.1. Intern kontroll baserad på modul A

Intern kontroll baserad på modul A är ett förfarande för bedömning av överensstämmelse genom vilket tillverkaren säkerställer och försäkrar på eget ansvar att produkter med digitala element uppfyller alla de väsentliga cybersäkerhetskraven. Tillverkaren ska upprätta en skriftlig EU-försäkran om överensstämmelse för varje produkt med digitala element i. Tillsammans med den tekniska dokumentationen ska denna kunna uppvisas för de berörda nationella myndigheterna under en period på 10 år efter det att produkten med digitala element har släppts ut på marknaden eller under stödperioden, beroende på vilken period som är längst.

2.2.2. EU-typkontroll baserad på modul B

I bedömningen av överensstämmelse innebär EU-typkontroll baserad på modul B att ett anmält organ undersöker den tekniska utformningen och utvecklingen hos en produkt



med digitala element och de processer för sårbarhetshantering som tillverkaren infört, och intygar att produkten uppfyller de väsentliga cybersäkerhetskraven. Tillverkaren ska lämna in en ansökan om EU-typkontroll, vilket får ske till valfritt anmält organ.

Tillverkaren ska sedan underrätta det anmälda organ som innehar den tekniska dokumentationen för EU-typintyget om alla ändringar av den godkända typen och processerna för sårbarhetshantering som kan påverka överensstämmelsen med de väsentliga cybersäkerhetskraven eller villkoren för intygets giltighet. För sådana ändringar krävs ytterligare godkännande i form av ett tillägg till det ursprungliga EU-typintyget.

2.2.3. Intern tillverkningskontroll baserad på modul C

Här bedömer tillverkaren överensstämmelse med typ grundat på intern tillverkningskontroll enligt modul C. Det innebär att tillverkaren fullgör föreskrivna skyldigheter i denna del samt säkerställer och försäkrar att de berörda produkterna med digitala element överensstämmer med typen enligt beskrivningen i EU-typintyget och uppfyller de väsentliga cybersäkerhetskraven.

Tillverkaren ska i detta fall vidta alla nödvändiga åtgärder för att produktionen och övervakningen av den ska leda till att de berörda produkterna överensstämmer med den godkända typen enligt beskrivningen i EU-typintyget, med de väsentliga cybersäkerhetskraven. Tillverkaren ska även i dessa fall fästa CE-märkningen på varje enskild produkt med digitala element som överensstämmer med typen enligt beskrivningen i EU-typintyget och uppfyller de tillämpliga kraven som anges i lagstiftningsinstrumentet. Tillverkaren ska även upprätta en skriftlig försäkran om överensstämmelse för en produktmodell och kunna uppvisa den för de nationella myndigheterna under en period på tio år efter det att produkten med digitala element har släppts ut på marknaden eller under stödperioden, beroende på vilken period som är längst.

2.2.4. Fullständig kvalitetssäkring baserad på modul H

I detta fall kräver bedömningen av överensstämmelse att tillverkaren hos ett valfritt anmält organ ansöker om att få sitt kvalitetssystem för de berörda produkterna med digitala element bedömt. Det anmälda organet ska bedöma kvalitetssystemet för att avgöra om det uppfyller kraven och ska förutsätta att kraven är uppfyllda i fråga om de delar av kvalitetssäkringssystemet som uppfyller motsvarande specifikationer i sammanhanget relevanta standarder.

2.2.5. Sårbarhets- och incidentrapportering

Enligt artikel 14.1 och 14.3 i CRA har tillverkare en skyldighet att rapportera alla aktivt utnyttjade sårbarheter i och allvarliga incidenter som påverkar säkerheten för produkten som tillverkaren får kännedom om till den nationella CSIRT-enheten⁴ och till Europeiska unionens cybersäkerhetsbyrå (ENISA). Tillverkaren ska utan onödigt dröjsmål och under alla omständigheter senast 24 timmar efter kännedom lämna in en tidig varning och, i

⁴ Computer Security Incident Response Team.



tillämpliga fall, ange de medlemsstater på vars territorium tillverkaren känner till att produkten med digitala element har tillhandahållits. Inom 72 timmar från kännedom ska tillverkaren lämna ytterligare information, om denna information inte redan har lämnats. Senast 14 dagar efter det att en korrigerande eller riskreducerande åtgärd blivit tillgänglig ska tillverkaren lämna in en slutrapport, om informationen inte redan har lämnats. Den ska åtminstone innehålla en beskrivning av sårbarheten och dess allvarighetsgrad och konsekvenser, i förekommande fall information om en fientlig aktör som har utnyttjat eller som utnyttjar sårbarheten samt detaljer om säkerhetsuppdateringen eller andra korrigerande åtgärder som har gjorts tillgängliga för att avhjälpa sårbarheten. Artikel 14.8 i CRA anger att tillverkaren även ska underrätta drabbade användare av produkten med digitala element.

2.3. Svenska tillverkare av produkter inom CRA:s område

I uppdraget ingår att vi ska bedöma hur många och vilka typer av ekonomiska aktörer i Sverige som omfattas av CRA. I detta avsnitt behandlar vi tillverkare, och tar sedan upp importörer och distributörer i kommande avsnitt.

2.3.1. Metod som använts för uppskattningen

För att skatta hur många svenska aktörer som omfattas av CRA har vi utgått från den metod som EU-kommissionen tidigare har använt för att uppskatta antal berörda aktörer inom hela EU (EU-kommissionens *Impact assessment report*⁵) och sedan gjort motsvarande beräkningar för den svenska marknaden med hjälp av statistik från SCB:s företagsregister⁶.

Vi menar att det finns en styrka i att tillämpa samma metod för Sverige som tidigare använts för EU, eftersom det ger en konsekvent och likvärdig behandling av material. Samtidigt bör sägas att metoden kräver en del teoretiska förenklingar jämfört med de komplexa produktområden som CRA i praktiken innebär. För förståelsens skull vill vi här nämna följande:

- ✦ SCB:s statistik delar in företagen efter deras *huvudsakliga verksamhet*, vilket innebär att om ett företag både tillverkar, importerar och distribuerar produkter klassificeras företaget endast efter ett av dessa affärsområden.
- ✦ CRA:s indelning i viktiga och kritiska produkter omfattar endast digitala produkter som uttryckligen definieras i bilaga tre och fyra i förordningen, medan kommissionens rapport utgår från en bredare grupp av produkter med digitala element som inte nödvändigtvis faller inom dess tillämpningsområde.
- ✦ Kommissionens uppskattningar baseras på antagandet att en tillverkare tillverkar en produkt⁷. Detta är givetvis ett förenklande antagande, men å andra sidan torde det till viss del kompensera för den överskattning som uppstår p.g.a. det bredare under-

⁵ https://eur-lex.europa.eu/resource.html?uri=cellar:af2401a4-34e9-11e9-9c68-01aa75ed71a1.0001.02/DOC_2&format=PDF (s. 48)

⁶ https://www.foretagsregistret.scb.se/Rakna?RakneTyp=RAKNA_FORETAG

⁷ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022SC0282>



laget av produkter med digitala element enligt föregående punkt. I utredningen har vi inte haft möjlighet att mer i detalj uppskatta antalet produkter på den svenska marknaden som omfattas av CRA.

2.3.2. Antal svenska tillverkare av produkter med digitala element

I EU-kommissionens *Impact assessment report* uppskattas antalet tillverkare av produkter med digitala element på EU:s marknad till **615 272**. Författarna av rapporten kombinerar branschdata över antalet tillverkare av mjukvara med uppskattningar av hur många hårdvarutillverkare som använder digitala komponenter i produktionen.

Svenska företag utgör 3,9% av det totala antalet företag inom EU⁸. Om vi antar att detta motsvarar Sveriges andel av det totala antalet företag enligt *Impact assessment report*, skulle det finnas 23 996 svenska tillverkare av produkter med digitala element, och lika många produkter – med de antaganden som används för uppskattningen.

Vi menar att denna siffra kan vara en bra utgångspunkt för att bedöma antalet svenska tillverkare som omfattas av CRA. Det krävs dock en del modifieringar för att komma fram till en mer realistisk uppskattning. Det handlar bland annat om att separata beräkningar bör göras för mjuk- respektive hårdvarutillverkare och att vissa produkter som därvid kommer med behövs subtraheras från totalen (av skäl och utifrån antaganden som anges nedan).

Svenska mjukvarutillverkare

I kommissionens rapport utgår beräkningarna från s.k. NACE-koder, det vill säga en EU-gemensam näringsgrensstandard för att klassificera företag och arbetsställen efter deras ekonomiska aktiviteter. Rapporten utgår alltså inte från vilka specifika produkter företagen tillverkar. Den svenska versionen av den europeiska näringsgrensstandarden NACE utgörs av standarden för svensk näringsgrensindelning, SNI.

Genom att utifrån NACE-koder göra utdrag ur SCB:s företagsregister kan vi göra en mer systematisk uppskattning av antalet svenska tillverkare. Detta förfarande beskrivs mer utförligt nedan.

I nedanstående tabell har NACE-koder använts för att hämta statistik över svenska tillverkare av mjukvara från SCB:s företagsregister⁹.

⁸ https://www.ekonomifakta.se/sakomraden/foretagande/naringslivet/foretagens-storlek_1212719.html

⁹ <https://www.foretagsregistret.scb.se/>



Tabell 2. Svenska tillverkare av mjukvara som omfattas av CRA

Benämning	Antal företag
Förlag	
Utgivare av dataspel	1 738
Utgivare av annan programvara	4 379
Programvaruproducenter, datakonsulter o.d.	
Programvaruproducenter	35 370
Informationstjänstföretag	
Datasevicebyråer, hostingföretag o.d.	3 376
Total	44 863

Av den framräknade siffran 44 863 utgörs 35 370 av programvaruproducenter (ca 79%). I ovanstående statistik inkluderas dock tillverkare av molntjänster, men som framgått av faktaruta 1 omfattas inte molntjänster av CRA. Det innebär att färre programvaruproducenter omfattas av CRA än de som ingår i summeringen ovan.

Vi saknar uppgift om hur många av programvaruproducenterna som av detta skäl bör subtraheras från uppskattningen av hur många svenska företag som omfattas av CRA. Vi vet däremot att den svenska marknaden för molntjänster har växt kraftigt under senare år, och förväntas växa även framåt¹⁰. För resonemangets skull antar vi över- siktligt att varannan programvaruproducent faller bort, det vill säga att antalet programvaruproducenter som omfattas av CRA är 50%. Därmed blir den nya siffran över antal svenska tillverkare av mjukvara som omfattas av CRA **27 178**.

Svenska hårdvarutillverkare

Uppskattningen av antalet tillverkare av hårdvaruprodukter som omfattas av CRA är mer komplicerad. Till att börja med har kommissionen i sin rapport räknat fram antalet företag i två steg. Först redovisas ett slags bruttolista där alla produkter som tillverkas i vissa utvalda branscher antas vara digitala eller innehålla digitala komponenter (detta kriterium kallas i rapporten **ICT-EXC**, ICT manufacturing sector – extended classification). Men eftersom många företag inom berörda branscher även producerar produkter som inte är digitala så räknar kommissionen sedan fram en nettolista baserad på en justerad indikator (**ICT-EXT adjusted**).

I det följande har vi gjort motsvarande beräkningar genom att använda samma koder för att hämta statistik över svenska tillverkare av hårdvara från SCB:s företagsregister.

En ytterligare komplikation är att EU-kommissionens *Impact assessment report* uppskattar det totala antalet tillverkare av produkter med digitala element på EU:s marknad, medan vissa branscher är exkluderade från CRA eftersom de täcks av

¹⁰ <https://techtidningen.se/ny-rapportsvenska-foretagens-investeringar-i-molntjanster-har-fordubblats/>



motsvarande krav i andra regelverk (se faktaruta 1). I sammanställningen har vi därför räknat bort de företag som hör hemma i branscherna skeppsvarv, flygplansindustrin, industri för medicinska och dentala tillbehör.

Tabell 3. Svenska hårdvarutillverkare påverkade av CRA (med ICT-EXC, icke-justerad)

Benämning	Antal företag
Industri för datorer, elektronikvaror och optik	
Industri för elektroniska komponenter	311
Industri för datorer och kringutrustning	198
Industri för kommunikationsutrustning	268
Industri för hemelektroteknik	272
Industri för instrument och apparater för mätning, provning och navigering	518
Industri för magnetiska och optiska medier	17
Industri för optiska instrument och fotoutrustning	95
Industri för elapparatur	
Industri för elmotorer, generatorer och transformatorer	115
Industri för eldistributions- och elkontrollapparater	282
Batteri- och ackumulationsindustri	109
Industri för belysningsarmatur	318
Industri för hushållsmaskiner och hushållsapparater	78
Industri för annan elapparatur	244
Övrig maskinindustri	
Industri för maskiner för allmänt ändamål	503
Industri för jord- och skogsbruksmaskiner	289
Industri för verktygsmaskiner och metallbearbetning	194
Industri för övriga specialmaskiner	751
Annan industri	
Industri för smycken och andra guld- och silversmedvaror	1688
Musikinstrumentindustri	468
Sportvaruindustrin	621
Industri för spel och leksaker	535
Diverse övrig tillverkningsindustri	2692
Reparationsverkstäder och installationsföretag för maskiner och apparater	
Reparationsverkstäder för metallvaror	492
Reparationsverkstäder för maskiner	9126
Installationsföretag för industrimaskiner och -utrustning	1250
Total	21 434



Som nämndes ovan riskerar dock ovanstående att ge en skev och överdriven bild då många företag inom dessa branscher även tillverkar produkter som inte är digitala. När man i kommissionens rapport justerar detta med indikatorn ICT-EXT adjusted multipliers branschens totala antal aktörer med en viktcoefficient som visar hur stor andel av företagen i branschen som använder digitala processer i sin produktion. Även om det ger en mer realistisk uppskattning så är inte heller detta en metod utan brister, eftersom koefficienten mäter graden av digitalisering i själva produktionen och inte andelen av produkterna som är digitala. I nedanstående tabell har samma metodik använts för att justera antalet svenska tillverkare av hårdvara som omfattas av CRA.

Tabell 4. Svenska hårdvarutillverkare påverkade av CRA (med ICT-EXC adjusted, justerad)

Gruppering	Antal företag	Andel företag med digitala processer (2019)	Antal företag (justerad)
Industri för datorer, elektronikvaror och optik	1 679	100%	1679
Industri för elapparatur	1 146	63%	722
Övrig maskinindustri	1 737	60%	1042
Annan industri	6 004	40%	2402
Reparationsverkstäder och installationsföretag för maskiner och apparater	10 868	40%	4347
Total			10 192

Summering av svenska mjuk- och hårdvarutillverkare som omfattas av CRA

Tillsammans med antalet tillverkare av mjukvara (27 178) blir det totala antalet tillverkare som omfattas av CRA **37 370**.

Det kan jämföras med, som nämndes tidigare, att antalet svenska företag utifrån företagsstruktur jämfört med kommissionens angivna antal skulle bli **23 996**. En anledning till den högre siffran som är baserad på SNI-koder kan vara Sveriges tredjeplacering bland EU-länder gällande digital intensitet i företagsverksamhet (2024)¹¹.

Som framgått finns stora osäkerheter i beräkningarna. Men rimligen bör kunna antas att antalet svenska tillverkare som omfattas av CRA ligger någonstans mellan ovanstående siffror, dvs. inom spannet ca 24 000 till ca 38 000 företag.

2.3.3. Tillverkare av produkter efter produktkategori i CRA

För vår analys av hur aktörerna påverkas är det också intressant att uppskatta hur antalet tillverkare enligt ovan fördelar sig utifrån CRA:s indelning efter viktiga, kritiska och övriga produkter.

¹¹ <https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2025>



EU-kommissionen har bedömt att 90% av den totala mängden digitala produkter på EU:s marknad tillhör kategorin "övriga produkter"¹²¹³, vilket bör ge en rimlig utgångspunkt för att uppskatta hur många svenska tillverkare som finns inom respektive kategori. Hur resterande 10% fördelar sig mellan viktiga och kritiska produkter framgår inte av kommissionens underlag. Rimligen är det dock en mindre del som avser kritiska produkter – för våra beräkningar har vi antagit en 80/20 fördelning mellan viktiga och kritiska produkter.

Givet dessa beräkningsförutsättningar anges i tabellen nedan fördelningen mellan respektive kategori utifrån den ovan angivna siffran 37 370 berörda svenska tillverkare.

Tabell 5. Summering av svenska tillverkare/produkter per produktkategori i CRA

Kategori	Uppskattad andel	Antal tillverkare
Viktiga klass I och II	8%	2 990
Kritiska	2 %	747
Övriga	90%	33 633
Totalt	100%	37 370

Som kommentar till tabellen bör sägas att det baserat på produktkategorierna i CRA finns anledning att tro att andelen av berörda tillverkare som tillverkar produkter under kategorin "övrigt" är större än 90%, då det finns få tillverkare av vissa av produktkategorierna som beskrivs i bilaga III och IV i CRA. I utredningen har vi dock inte haft möjlighet att närmare kartlägga andelen tillverkare inom respektive produktkategori. Vidare bör nämnas att EU-kommissionens beräkningsmetod även i detta fall innehåller en del förenklingar. Framför allt kan antas att många företag tillverkar produkter som faller inom flera kategorier.

2.4. Kostnader för berörda tillverkare

Även för uppskattning av kostnader och investeringar som svenska tillverkare kommer behöva göra för att uppfylla kraven i CRA har vi metodologiskt utgått från EU-kommissionens *Impact assesment report*, kompletterat med vissa andra källor och egna antaganden.

I kommissionens rapport antas att kostnaden för att tillverka en produkt med digitala element uppgår till i genomsnitt 140 000 euro¹⁴. Kommissionens rapport uppskattar även att 50% av tillverkare av produkter med digitala element arbetar systematiskt med säker produktutveckling. Uppskattningen baseras på tidigare genomförda studier av tillverkare i USA (2010), Norge (2015) och Finland (2021).

¹² https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI%282022%29739259_EN.pdf

¹³ Bygger på antagandet om att en tillverkare tillverkar en produkt som kommissionen tillämpar i sin rapport.

¹⁴ https://eur-lex.europa.eu/resource.html?uri=cellar:af2401a4-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC_2&format=PDF (s. 56).



Givet produkternas karaktär bör dock enligt vår mening kunna förutsättas att betydligt fler än hälften av tillverkarna av viktiga och kritiska produkter redan arbetar systematiskt med säkerhet i produktionsprocessen. Kostnader för bland annat bedömningar av anmälda organ ökar däremot med komplexiteten i produkten, vilket innebär en ökad kostnad för tillverkare av dessa produkter.

Omvandlingen från euro till svenska kronor i summeringen av kostnader för berörda aktörer har utgått från en växelkurs på 10,95 kronor per euro, vilket motsvarar den gällande växelkursen 2025-09-14.

2.4.1. Bedömning av överensstämmelse för produkter med digitala element som inte förtecknas som viktiga eller kritiska produkter

Bedömningen av överensstämmelse för produkter med digitala element som inte förtecknas som viktiga eller kritiska produkter med digitala element i CRA, dvs. de vi valt att kalla "övriga", kan utföras av tillverkaren på eget ansvar i enlighet med modul A. I den svenska kontexten innebär det, givet vår skattning av antal berörda, 33 633¹⁵ tillverkare.

Kommissionen har gjort följande uppskattning av engångskostnader och återkommande kostnader för att upprätta teknisk dokumentation, CE-märkning, riskanalys och informationsbeskrivningar för användare:

- ✦ Engångskostnad: 6 615 euro per tillverkare/produkt
- ✦ Återkommande kostnader: 945 euro (årligen)¹⁶.

Tillverkare av produkter som faller under kategorin "övrigt" är även skyldiga att rapportera till marknadskontrollmyndigheten när en produkt utgör en risk för cybersäkerheten och att rapportera utnyttjade sårbarheter och incidenter till ENISA (EU:s cybersäkerhetsbyrå). Kommissionen har uppskattat dessa kostnader till:

- ✦ Engångskostnad: 4 410 euro
- ✦ Återkommande kostnader: 630 euro (årligen)¹⁷

I samma rapport har kostnaden för att integrera cybersäkerhet i produktionsprocessen uppskattats till 30,5%¹⁸ av den totala produktionskostnaden.

- ✦ Engångskostnad: 42 700 euro¹⁹

¹⁵ Uppskattning av antal svenska tillverkare av produkter med digitala element inom kategorin "övrigt" (se avsnitt 2.3.2).

¹⁶ _Impact_assessment_Cyber_Resilience_Act_oFz3rACXW0RU8B0TrCo22ErI6Y_89545%20(6).pdf (s. 82;84).

¹⁷ _Impact_assessment_Cyber_Resilience_Act_oFz3rACXW0RU8B0TrCo22ErI6Y_89545%20(6).pdf (s. 84)

¹⁸ De finns en betydande osäkerhet i denna uppskattning. Siffran baseras på en studie från 2021 som utgick från att det inte fanns processer eller åtgärder för säkerhet på plats hos tillverkaren. Troligen är situationen en annan idag, men vi har inte haft möjlighet att göra mer precisa uppskattningar.

¹⁹ https://eur-lex.europa.eu/resource.html?uri=cellar:af2401a4-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC_2&format=PDF (s. 56).



I kostnadsuppskattningen av åtgärder för att säkerställa produktsäkerhet ingår säker kodning, verifiering och testning, men det saknas indirekta organisatoriska kostnader. Tillverkare kommer behöva investera resurser för att stärka kompetensen i de krav som ställs genom CRA. Detta kan ske på olika sätt, exempelvis genom att fördela en del av befintlig personals tid till cybersäkerhetsarbete, genom konsult hjälp eller (för vissa större aktörer) genom att anställa en CISO (Chief Information Security Officer). Många mindre företag lär dock välja en betydligt mindre omfattande och kostsam lösning, medan de flesta stora företag redan har relevant personal och processer på plats.

För mindre företag, som enligt EU-kommissionens *Impact assessment report*²⁰ utgör en betydande majoritet av det totala antalet tillverkare som omfattas av CRA, kan det räcka att använda en delmängd av den befintliga personalens tid för att uppfylla de grundläggande säkerhetskraven i CRA. I dessa fall kan en intern resurs, såsom en IT-ansvarig eller systemadministratör, tilldelas ansvaret för upprättandet av säkerhetspolicies, att riskbedömningar genomförs och incidenter hanteras. Vid behov kan företaget även behöva anlita externa konsulter för delar av arbetet. För resonemangets skull antar vi att en intern resurs förväntas lägga 20 h per månad på uppgifter för att uppfylla skyldigheterna, vilket innebär en kostnad på cirka 128 000 kronor per år om vi uppskattar arbetskraftskostnaden för en anställd till 535 kr/h²¹. Behovet av konsult hjälp vid specifika uppgifter kan uppskattas till 10–50 h per år, vilket skulle medföra en kostnad på 15 000 – 75 000 kronor per år om vi antar ett timarvode på 1500 kr. Sammanlagt ger detta ett kostnadsintervall för personella resurser på 143 000–203 000 kronor, eller 13 059–18 539 euro.

Tabell 6. Summering av kostnader för tillverkare av produkter med digitala element som inte förtecknas som viktiga eller kritiska produkter ("övriga")²²

Kategori	Engångskostnad	Återkommande kostnad (årligen)
Upprättande av teknisk dokumentation, CE-märkning och dylikt	6 616 euro	945 euro
Rapporteringskyldighet	4 410 euro	630 euro
Cybersäkerhet i produktionen	42 700 euro	-
Personella resurser	-	13 059 – 18 539 euro
Total (Euro)	53 726	14 634 – 20 114
Total (Kronor)	588 300	160 242 – 220 248

²⁰ Se avsnitt 2.7.1.

²¹ Baserat på en genomsnittlig månadslön på 56 000 för IT-arkitekter, systemutvecklare och testledare m.fl. enligt SCB:s lönestatistik, samt ett personalomkostnadspåslag om 40%: <https://www.scb.se/hitta-statistik/statistik-efter-amne/arbetsmarknad/loner-och-arbetskostnader/lonestrukturstatistik-privat-sektor-slp/pong/tabell-och-diagram/tjansteman-2016/genomsnittlig-manadslon-efter-yrke-2024/>

²² Uppskattningen baseras på kommissionens rapport. Det bör dock noteras att vi i utredningen mött synpunkter om att den återkommande kostnaden både för upprättande av teknisk dokumentation, CE-märkning o.d. och för rapporteringskyldighet möjligen är väl lågt satt.



2.4.2. Bedömning av överensstämmelse för viktig produkt med digitala element (klass I och II)

I avsnitt 2.3.3 uppskattades antal tillverkare av viktiga produkter med digitala element (klass I och II) till 2 990. För de produkter som klassas som viktiga (klass I) kan tillverkaren göra en egen bedömning på eget ansvar (modul A), så länge de tillämpar:

- ✦ harmoniserade cybersäkerhetsstandarder, eller
- ✦ en europeisk ordning för cybersäkerhetscertifiering enligt artikel 27.9 i CRA, på minst assurancesnivån "betydande", om sådan finns och i tillämpliga fall.

I de fall då dessa standarder och certifieringssystem är på plats blir kostnaden identisk med de kostnader som beskrevs i avsnitt 2.4.1. I de fall standarder eller system inte finns för den aktuella produkten, eller om tillverkaren inte har tillämpat dessa, blir förfarandet detsamma som för tillverkare av viktiga produkter som faller inom klass II. I dessa fall ska tillverkaren visa överensstämmelse med de väsentliga cybersäkerhetskraven genom att använda något av följande förfaranden:

- ✦ EU-typkontroll (baserat på modul B), följd av förfarandet för överensstämmelse med EU-typ grundat på intern tillverkningskontroll (baserat på modul C)
- ✦ överensstämmelse som grundar sig på fullständig kvalitetssäkring (baserat på modul H), eller
- ✦ en europeisk ordning för cybersäkerhetscertifiering enligt artikel 27.9 i CRA, på minst assurancesnivån "betydande", om sådan finns och i tillämpliga fall.

Kommissionen har uppskattat kostnaden för att låta ett anmält organ undersöka den tekniska utformningen och utvecklingen hos en produkt enligt modul B och C till:

- ✦ Engångskostnad: 17 500 euro
- ✦ Återkommande kostnad: 7 500 euro²³ (årligen)

I nedanstående tabell adderas kostnaden för certifiering av ett anmält organ till tidigare kostnader.

²³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022SC0282#footnote178>



Tabell 7. Summering av kostnader för tillverkare av viktiga produkter med digitala element (klass I och II)

Kategori	Engångskostnad	Återkommande kostnad (årligen)
Upprättande av teknisk dokumentation, CE-märkning och dylikt	6615 euro	945 euro
Rapporteringskyldighet	4410 euro	630 euro
Cybersäkerhet i produktionen	42 700 euro	-
Personella resurser	-	13 059 – 18 539 euro
Certifiering av anmält organ	17 500 euro	7 500 euro
Total (Euro)	71 225	22 134 – 27 614
Total (Kronor)	779 500	242 367 – 302 373

2.4.3. Bedömning av överensstämmelse för kritiska produkter med digitala element

I avsnitt 2.3.3 uppskattades antal tillverkare av kritiska produkter med digitala element till 747. Kritiska produkter med digitala element som förtecknas i bilaga IV ska visa överensstämmelsen med de väsentliga cybersäkerhetskraven i bilaga I genom:

- + en europeisk ordning för cybersäkerhetscertifiering i enlighet med artikel 8.1 i CRA
- + om villkoren i artikel 8.1 inte är uppfyllda, något av de förfaranden som beskrevs för viktiga produkter (klass II) i avsnitt 2.4.2.

I de fall tillverkaren inte kan visa överensstämmelsen genom en europeisk ordning för cybersäkerhetscertifiering kan kostnaden därmed likställas de uppskattade kostnaderna som presenterades i avsnitt 2.4.2.



Tabell 8. Summering av kostnader för tillverkare av kritiska produkter med digitala element

Kategori	Engångskostnad	Återkommande kostnad (årligen)
Upprättande av teknisk dokumentation, CE-märkning och dylikt	6615 euro	945 euro
Rapporteringskyldighet	4410 euro	630 euro
Cybersäkerhet i produktionen	42 700 euro	-
Personella resurser	-	13 059 – 18 539 euro
Certifiering av anmält organ	17 500 euro	7 500 euro
Total (Euro)	71 225	22 134 – 27 614
Total (Kronor)	779 500	242 367 – 302 373

Tabell 9. Summering av kostnader för svenska tillverkare per produktkategori i CRA

Kategori	Antal tillverkare	Engångskostnad	Återkommande kostnad (årligen)
Tillverkare av övriga produkter	33 633	588 300 kronor	160 242 – 220 248 kronor
Tillverkare av viktiga produkter (klass I och II)	2 990	779 500 kronor	242 367 – 302 373 kronor
Tillverkare av kritiska produkter	747	779 500 kronor	242 367 – 302 373 kronor

2.5. Förvaltare av programvara med fri och öppen källkod

Förvaltare av programvara med fri och öppen källkod särskiljs från övriga berörda aktörer i CRA och omfattas av ett förenklat och anpassat regelverk. Förvaltaren är en juridisk person, annan än en tillverkare, som har till syfte eller som mål att systematiskt och varaktigt tillhandahålla stöd för utvecklingen av specifika produkter med digitala element, vilka klassificeras som programvara med fri och öppen källkod och är avsedda för kommersiell verksamhet, och som säkerställer dessa produkters bärkraft.

Dessa aktörer ska på ett verifierbart sätt införa och dokumentera en cybersäkerhetspolicy så att det utvecklas en säker produkt med digitala element och så att utvecklarna av den produkten effektivt hanterar sårbarheter. Policyn ska särskilt omfatta aspekter som rör dokumentering, hantering och avhjälpande av sårbarheter och främja utbyte av information om sårbarheter som upptäckts inom nätgemenskapen för öppna källkodsprojekt. Förvaltare ska även samarbeta med marknads-kontrollmyndigheten och på begäran förse myndigheten med cybersäkerhetspolicyn.



De skyldigheter som fastställs i artikel 14.1 om tillverkarens rapporteringsskyldigheter ska tillämpas på förvaltare av programvara med fri och öppen källkod i den mån de deltar i utvecklingen av produkter med digitala element. De skyldigheter som fastställs i artikel 14.3 (anmälan av allvarliga incidenter) och 14.8 (underrätta drabbade användare om utnyttjande av sårbarheter och allvarliga incidenter) ska tillämpas på förvaltare av programvara med fri och öppen källkod i den mån allvarliga incidenter som påverkar säkerheten för produkter med digitala element påverkar de nätverks- och informationssystem som tillhandahålls av förvaltarna för programvara med fri och öppen källkod för utvecklingen av sådana produkter.

2.5.1. Antal svenska förvaltare av programvara med fri och öppen källkod

Att uppskatta antalet svenska förvaltare av programvara med fri och öppen källkod är en komplex uppgift. Användningen och utvecklingen av öppen källkod är ofta decentraliserad och informell, vilket innebär att många projekt inte är officiellt registrerade eller strukturerade på samma sätt som kommersiella mjukvaruföretag. Ett sätt att ge en preliminär uppskattning av antalet förvaltare av programvara med fri och öppen källkod är att räkna antalet medlemmar i nätverk på området. NOSAD (Network Open Source and Data) är ett svenskt nätverk som syftar till att främja samverkan och kunskapsutbyte för att förenkla digital utveckling. Nätverket består idag av över **300 organisationer** (från både offentlig sektor, civilsamhället och näringslivet) som delar vägledningar, goda exempel och öppen programvara²⁴.

2.5.2. Kostnader för berörda förvaltare

Framtagandet av cybersäkerhetspolicyn kan jämföras med skyldigheten att upprätta teknisk dokumentation, CE-märkning, riskanalys och informationsbeskrivningar för användare som presenterades i avsnitt 2.4.1. Att ta fram en policy är däremot i huvudsak en administrativ och organisatorisk åtgärd. Den kan kräva konsultstöd, juridisk kompetens och expertis inom cybersäkerhet, men arbetet är främst text- och processbaserat. Kostnaderna uppstår framför allt i form av arbetstid (intern eller extern). Här uppskattar vi att kostnaderna för upprättandet av en cybersäkerhetspolicy till höften av kostnaderna för att upprätta teknisk dokumentation:

- ✦ Engångskostnad: 3 308²⁵ euro per tillverkare/produkt
- ✦ Återkommande kostnader: 473²⁶ euro (årligen)²⁷.

Kostnaden för att rapportera till marknadskontrollmyndigheten när en produkt utgör en risk för cybersäkerheten och att rapportera utnyttjade sårbarheter och incidenter till ENISA (EU:s cybersäkerhetsbyrå) uppskattades i avsnitt 2.4.1 till:

- ✦ Engångskostnad: 4 410 euro

²⁴ <https://nosad.se/om-nosad>

²⁵ 6 615/2, se tabell 6 i avsnitt 2.4.1.

²⁶ 945/2, se tabell 6 i avsnitt 2.4.1.

²⁷ [_Impact_assessment_Cyber_Resilience_Act_oFz3rACXW0R8B0TrCo22ErI6Y_89545%20\(6\).pdf](#) (s. 82;84).



✦ Återkommande kostnader: 630 euro (årligen)²⁸

Tabell 10: Summering av kostnader för förvaltare av programvara med fri och öppen källkod

Kategori	Engångskostnad	Återkommande kostnad (årligen)
Upprättande cybersäkerhetspolicy	3 308 euro	473 euro
Rapporteringskyldighet	4 410 euro	630 euro
Total (Euro)	7 718	1 103
Total (kronor)	84 512	12 078

2.6. Svenska importörer och distributörer av produkter med digitala element

CRA omfattar alla aktörer i försörjningskedjan för produkter med digitala element, men deras ansvar skiljer sig åt. Tillverkare omfattas av flera delar av CRA jämfört med distributörer och importörer. Importörer och distributörer har inte en skyldighet att aktivt söka efter tekniska sårbarheter i produkterna, men de måste försäkra sig om att tillverkaren har uppfyllt sina skyldigheter och att de har processer för att snabbt kunna agera vid misstanke om att produkten utgör en cybersäkerhetsrisk. Sanktionerna i artikel 64 gör ingen skillnad mellan tillverkare, distributörer eller importörer.

I följande avsnitt beskriver vi importörens och distributörens roller i CRA mer i detalj, uppskattar ur många distributörer och importörer av produkter med digitala element som finns på den svenska marknaden och vilka typer av kostnader och investeringar som är nödvändiga för att efterleva kraven i CRA.

2.6.1. Svenska importörer av produkter med digitala element

Importörer på marknaden får endast släppa ut sådana produkter med digitala element som uppfyller de väsentliga cybersäkerhetskraven. Importören gör detta genom att kontrollera att tillverkaren har utfört överensstämmelsebedömning enligt produktens klassificering, och att produkten har en CE-märkning och EU-försäkran om överensstämmelse. Importören måste även ha tillgång till den tekniska dokumentationen och kunna visa den på begäran av marknadskontrollmyndigheten.

Om importören anser eller har skäl att tro att en produkt med digitala element inte överensstämmer med CRA:s bestämmelser får importören inte släppa ut produkten på marknaden förrän produkten eller tillverkarens processer har bringats till överensstämmelse med förordningen. Om importören vet eller har skäl att tro att en digital produkt som har släppts ut på marknaden inte överensstämmer med förordningens

²⁸ _Impact_assessment_Cyber_Resilience_Act_ofZ3rACXW0RU8B0TrCo22ErI6Y_89545%20(6).pdf (s. 84)



bestämmelser ska importörerna dessutom omedelbart underrätta marknadskontrollmyndigheten. Om importören av en produkt med digitala element får kännedom om att produktens tillverkare har upphört med sin verksamhet och därmed inte kan uppfylla de skyldigheter som fastställts i CRA ska importören underrätta marknadskontrollmyndigheten om detta och även underrätta användare av produkterna.

I nedanstående tabell har SNI-koder använts för att hämta statistik över svenska importörer av produkter med digitala element från SCB:s företagsregister²⁹.

Tabell 11. Svenska importörer av produkter med digitala element

Benämning	Antal företag
Partihandel med datorer och kringutrustning samt programvara	2123
Partihandel med ljud- och bildanläggningar samt videoutrustning	670
Partihandel med elartiklar	629
Partihandel med fotografiska och optiska produkter	226
Partihandel med jordbruksmaskiner och -utrustning	1027
Partihandel med gruv- bygg- och anläggningsmaskiner	1128
Partihandel med mät- och precisionsinstrument	507
Partihandel med datoriserad materialhanteringsutrustning	117
Partihandel med sport- och fritidsartiklar	2025
Partihandel med VVS-varor	949
Partihandel med verktygsmaskiner	651
Partihandel med elektronikkomponenter	1453
Partihandel med teleprodukter	433
Partihandel med elektriska hushållsmaskiner och apparater	780
Total	12 718

Den främsta kostnaden för dessa företag är relaterad till orientering kring de nya skyldigheterna, det vill säga anpassningskostnader för att sätta sig in i de nya rättsliga kraven och etablering av systematiska processer för efterlevnad av regelverket. Här förutsätter vi att detta arbete ryms inom företagets redan pågående satsningar på kompetens- och processutveckling. Förutsättningar och konsekvenser för små och medelstora importörer diskuteras vidare i avsnitt 2.7.2.

2.6.2. Svenska distributörer av produkter med digitala element

På liknande sätt som importörer får distributörer av produkter endast tillhandahålla produkter med digitala element som uppfyller de väsentliga cybersäkerhetskraven. Distributören gör detta genom att kontrollera att produkten är försedd med CE-

²⁹ <https://www.foretagsregistret.scb.se/>



märkning, åtföljs av den information som krävs och att tillverkaren och importören har fullgjort sina skyldigheter enligt CRA.

Om distributören anser eller har skäl att tro att en produkt med digitala element inte överensstämmer med CRA:s bestämmelser får produkten inte tillhandahållas på marknaden förrän överensstämmelse har säkerställts. Om distributören vet eller har skäl att tro att en digital produkt som redan tillhandahålls inte uppfyller förordningens krav, ska distributören omedelbart underrätta marknadskontrollmyndigheten. Distributören är dessutom skyldig att samarbeta med marknadskontrollmyndigheterna och på begäran tillhandahålla all information och dokumentation som behövs för att visa att produkten efterlever kraven i CRA.

I nedanstående tabell har SNI-koder använts för att hämta statistik över svenska distributörer av produkter med digitala element från SCB:s företagsregister³⁰.

Tabell 12. Svenska distributörer av produkter med digitala element

Benämning	Antal företag
Datorbutiker; data- och tv-spelsbutiker	932
Telebutiker	480
Radio och TV-affärer	811
Leksaksaffärer	530
Butiker för vitvaror och andra elektriska hushållsmaskiner- och apparater	710
Butiker med belysningsartiklar	317
Sportaffärer	2728
Postorderhandel och detaljhandel på internet med datorer och annan elektronisk utrustning	1162
Postorderhandel och detaljhandel på internet med sport- och fritidsutrustning	1707
Total	10 467

Utöver ovanstående finns även vissa allmänt inriktade butiker som kan ha produkter med digitala element i sitt sortiment, till exempel stora livsmedelsbutiker. Sannolikt tillkommer därmed något/några hundratal butiker utöver de som anges i tabellen.

Den främsta kostnaden för dessa företag är, i likhet med importörer, relaterad till orientering kring de nya skyldigheterna, det vill säga anpassningskostnader för att sätta sig in i de nya rättsliga kraven och etablering av systematiska processer för efterlevnad av regelverket. Här förutsätter vi att detta arbete rymms inom företagens redan pågående satsningar på kompetens- och processutveckling. Förutsättningar och konsekvenser för små och medelstora distributörer diskuteras vidare i avsnitt 2.7.2.

³⁰ <https://www.foretagsregistret.scb.se/>



Fall där tillverkares skyldigheter gäller för importörer och distributörer

En central del i CRA är att importörer och distributörer anses som tillverkare enligt CRA och omfattas av tillverkarens skyldigheter (se avsnitt 2.3–2.4) om importören eller distributören släpper ut en produkt med digitala element på marknaden *i eget namn, under eget varumärke eller utför en väsentlig ändring* av en produkt med digitala element som redan har släppts ut på marknaden.

2.7. Påverkan på små- och medelstora företag

2.7.1. Små och medelstora tillverkare av produkter med digitala element

I kommissionens *Impact assessment report* framgår att 99,58% av de 615 272 tillverkarna av produkter med digitala element på EU:s marknad utgörs av små och medelstora företag (SME)³¹. I en svensk kontext innebär detta att 37 213³² tillverkare är små och medelstora företag.

Dessa aktörer riskerar att relativt sett påverkas i större utsträckning än större företag. Stora företag kommer ha större möjligheter att fördela engångskostnader för att sätta sig in i nya regleringar. Brist på medvetenhet och kompetens inom cybersäkerhetsområdet kan medföra att mindre aktörer i hög grad behöver anlita konsulter. De mindre företagens begränsade laboratoriekapacitet, både vad gäller resurser och kompetens, kan potentiellt innebära att de måste använda externa testlaboratorier eller organ för bedömning av överensstämmelse för att säkerställa efterlevnad för produkter som faller under de lägre riskklasserna i CRA.

I kommissionens rapport framgår att 61% av tillfrågade små och medelstora företag upplever hinder för att säkerställa sin cybersäkerhet. 12,3 % av företagen anger att deras informationssäkerhetsarbete ligger "under" eller "klart under" branschstandard, jämfört med 2,1% för större företag³³. För de företag som tidigare inte arbetat strukturerat med cybersäkerhet kan kostnaderna bli särskilt betungande, då de både måste stärka sin utvecklingskapacitet och avsätta resurser för löpande uppföljning och rapportering. Samtidigt kan en utebliven anpassning innebära att de inte längre får tillträde till EU:s inre marknad, vilket gör att efterlevnaden av CRA blir en strategiskt avgörande fråga även för de minsta aktörerna.

2.7.2. Små och medelstora importörer och distributörer av produkter med digitala element

Små och medelstora importörer kan komma att påverkas särskilt av CRA, inte minst eftersom de ofta saknar omfattande resurser och expertis inom cybersäkerhet och

³¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022SC0282#footnote67>. Med medelstora företag avses företag med färre än 250 anställda och en årsomsättning som inte överstiger 50 miljoner EUR eller en balansomslutning som inte överstiger 43 miljoner EUR. Med små företag avses företag med färre än 50 anställda och en årsomsättning eller balansomslutning som inte överstiger 10 miljoner EUR.

³² 99,58% av 37 370 (se avsnitt 2.3.1).

³³ <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment>



regelefterlevnad. Importörer som tar in produkter från tillverkare utanför EU bär ett direkt ansvar för att dessa uppfyller kraven i förordningen, även om de själva inte har insyn i tillverkarens processer eller tekniska kapacitet. Detta innebär att de måste utveckla rutiner för att granska dokumentation, säkerställa CE-märkning och vid behov inhämta försäkringar om att sårbarheter hanteras, trots att de i praktiken kan ha begränsad möjlighet att bedöma detta. Bristen på resurser och systematiska processer gör att kostnaderna för utbildning, administrativa kontroller och eventuell förstärkning av personalstyrkan kan väga tungt i förhållande till företagets storlek.

För dessa aktörer kan CRA därför innebära både en organisatorisk och ekonomisk utmaning, där riskerna främst ligger i att inte upptäcka brister i importerade produkter och därmed själva hållas ansvariga.



3. Tillgång till organ för bedömning av överensstämmelse

I Governos uppdrag ingår att analysera vissa frågor kring det nuvarande läget och de utmaningar som finns vad avser nationell tillgång på organ för bedömning av överensstämmelse. Som framgått av kapitel 1 ska vi beskriva och analysera vilka typer av organ för bedömning av överensstämmelse som kan behövas i Sverige för att möta kommande behov, vad en eventuell brist på organ skulle innebära för svenska tillverkare och om det finns ett behov av statliga insatser för att stimulera fler aktörer att bli organ för bedömning av överensstämmelse.

3.1. Rollen som organ för bedömning av överensstämmelse i CRA

I CRA spelar organ för bedömning av överensstämmelse en avgörande roll i att säkerställa att produkter (främst viktiga produkter i klass två och kritiska produkter) och tjänster uppfyller de cybersäkerhetskrav som ställs enligt lagstiftningen. Syftet med organens roll är att produkter på EU:s marknad både är säkra vid lansering och att de kan hantera säkerhetsrisker på längre sikt.

Organen är oberoende juridiska personer som ansvarar för att bedöma att tillverkare följer reglerna för cybersäkerhet, inklusive riskhantering, sårbarhetsbedömning och säkerhetsåtgärder. För att kunna bedriva verksamhet som organ för bedömning av överensstämmelse måste företagen bland annat ha personal med tillräcklig teknisk kunskap och kännedom om de väsentliga cybersäkerhetskraven och tillämpliga harmoniserade standarder på området.

3.2. Behov av organ för bedömning av överensstämmelse när CRA träder i kraft

Övergångsperioden är densamma för alla tillverkare vars produkter omfattas av CRA. Det betyder att många aktörer ungefär samtidigt kommer att behöva genomföra bedömning av överensstämmelse, i vissa fall med behov att anlita oberoende organ. Efterfrågan på organ för bedömning av överensstämmelse kommer därför att vara stor inledningsvis. Detta leder sannolikt till flaskhalsar och längre väntetider, huvudsakligen för produkter som klassas i de högre riskkategorierna (viktiga produkter i klass 2 och kritiska produkter) och därmed kräver en mer omfattande prövning.

I syfte att undvika onödiga administrativa bördor medger CRA att det inte ska finnas en skyldighet för tillverkare att genomföra en tredjepartsbedömning av överensstämmelse enligt CRA om ett europeiskt cybersäkerhetscertifikat har utfärdats enligt sådana europeiska ordningar för cybersäkerhetscertifiering, på åtminstone assurancesnivån betydande i de fall produktkategorin har pekats ut i en delegerad akt. Detta kan möjligen minska behovet av organ för bedömning av överensstämmelse på mark-



naden på sikt. Detsamma gäller för tillverkare som tillämpar harmoniserade cybersäkerhetsstandarder. I avsnitt 2.4.2 konstaterades att en avsaknad av standarder medför att tillverkare, som annars endast hade behövt genomföra en bedömning av överensstämmelse enligt modul A, i detta fall måste tillämpa andra moduler på samma sätt som viktiga produkter i klass II. Tidpunkten för när harmoniserande standarder är på plats blir därmed avgörande för behovet av organ för bedömning av överensstämmelse när CRA träder i kraft.

I sammanhanget bör även nämnas hur CRA förhåller sig till EU:s förordning 2024/1689 om harmoniserade regler för artificiell intelligens. Anmällda organ som är behöriga att kontrollera överensstämmelsen för AI-system med hög risk inom ramen för CRA kommer även vara behöriga att kontrollera överensstämmelser under CRA, givet att de uppfyller ett flertal angivna krav. Detta borde rimligtvis minska behovet av organ för bedömning av överensstämmelse enligt CRA, även om tillgången till sådana organ enligt förordning 2024/1689 är under utveckling.

3.3. Utbud av svenska organ för bedömning av överensstämmelse nu och på sikt

3.3.1. Organ för bedömning av överensstämmelse på den svenska marknaden

I dagsläget finns det tre svenska ackrediterade organ för bedömning av överensstämmelse med kompetens inom cybersäkerhet: Intertek, Atsec och Combitech. Av vår dialog med FMV framgick dock att ett av dessa företag sannolikt inte kommer att vara intresserade av rollen som kontrollorgan på området framåt. Att ändå fortsatt ha två ackrediterade organ med kompetens inom cybersäkerhet sägs enligt FMV ge Sverige en god utgångspunkt för anpassning till CRA.

I vårt arbete har vi noterat indikationer på att fler svenska företag kan antas vara intresserade av att ta sig an uppgiften att vara organ för bedömning av överensstämmelse enligt cyberresiliensförordningen framöver. Ett tydligt exempel är RISE, som i sitt remissyttrande avseende EU:s cybersäkerhetsakt bedömde att man kan spela en central roll när olika certifieringsordningar ska implementeras. RISE såg då en möjlighet att agera som organ för bedömning av överensstämmelse på både lägre och högsta assurancesnivå och som utvärderare/granskare genom tillgången till institutets testlaboratorier³⁴. RISE är även en ackrediterat organ inom ramen för EU:s radioutrustningsdirektiv (2014/53/EU) och kan antas vara intresserade av att bibehålla rollen även framåt. Sammantaget förefaller det inte osannolikt att RISE kan vara intresserade av rollen som organ för bedömning av överensstämmelse i enlighet med CRA. Men det finns även andra svenska företag inom IKT-området med tillräckliga resurser och testkapacitet för att kunna antas vara intresserade av rollen inom ramen för CRA.

³⁴ <https://www.regeringen.se/contentassets/26576869594a49b88e4e1cfa4df94104/rise-research-institutes-of-sweden-ab.pdf>



3.3.2. Ökat utbud av svenska organ för bedömning av överensstämmelse på sikt

Utbudet av organ för bedömning av överensstämmelse enligt CRA kan också antas öka på längre sikt eftersom det med största sannolikhet kommer finnas en efterfrågan på deras tjänster. Ett flertal företag som idag har kompetens inom cybersäkerhet (eller inom närliggande områden) kommer rimligtvis vara intresserade av att utveckla sin verksamhet för att kunna genomföra tester enligt EU:s modulförfaranden. Det finns exempelvis idag sju ackrediterade svenska organ inom området "Ledningssystem för informationssäkerhet", vilket visar på en kompetens inom närliggande områden. Det är däremot viktigt att notera att ackreditering inom detta område inte direkt innebär att dessa organ är kvalificerade för att genomföra tester enligt CRA:s modulförfaranden, då det krävs en ny kontrollform och ett specifikt tekniskt kunnande.

Även redan existerande organ på marknaden som har väletablerade processer för modulförfaranden liknande de som krävs inom ramen för CRA, kan potentiellt vara intresserade av att utveckla en kompetens inom cybersäkerhet. Detta skulle kunna vara ett strategiskt steg för att möta den ökande efterfrågan som förväntas i samband med den nya lagstiftningen. Genom att bygga på sina befintliga styrkor och anpassa sig till de nya krav som ställs kan dessa organ positionera sig för att bättra tillgodose marknadens behov i framtiden. Ett exempel är förfarandet för testning och riskklassificering av medicintekniska produkter enligt MDR (Medical Device Regulation, 2016/745), som i likhet med CRA använder modulbaserad konformitetsbedömning utifrån riskklassificering av produkter. I Sverige finns idag fem ackrediterade organ inom området "Ledningssystem för medicintekniska produkter".

Det är komplicerat att uppskatta i vilken utsträckning företag kommer anpassa sin verksamhet för att potentiellt ta en roll som organ för bedömning av överensstämmelse. Med största sannolikhet kommer det att finnas en efterfrågan på kontrolltjänster från både svenska tillverkare och företag från andra EU-länder, vilket rimligtvis bör utgöra ett starkt incitament för dessa aktörer. Men att bygga upp kompetens, system och processer är dock både resurskrävande och innebär ett risktagande. Och våra kontakter i utredningen visar att många företag i dagsläget är osäkra på hur marknaden ska utvecklas – bland annat i avvaktan på att harmoniserade standarder ska tas fram på området – och därför avvaktar med sina investeringsbeslut. De aktörer som redan har eller förbereder sig för att implementera interna processer baserat på befintliga standarder som till exempel ISO/IEC 27001 (informationssäkerhet) och IEC 62443 (säkerhet för industriella automationssystem) bör vara väl förberedda inför att specifika standarder för cyberresiliensförfordningen blir tillgängliga.

Om staten ser behov av att öka tillgången på svenska organ för bedömning av överensstämmelse så skulle en tänkbar åtgärd för att komplettera marknadens utbud möjligen kunna vara att etablera ett organ för bedömning av överensstämmelse hos en svensk myndighet, t.ex. FMV eller PTS. Vi har inte närmare undersökt vilka förutsättningar som finns för det. Men vi uppfattade i våra kontakter med FMV att man där är tveksamma till om det vore en lämplig lösning.

I sammanhanget kan noteras att risken för att det ska uppstå en flaskhalsproblematik också kan påverkas av om Swedac momentant har tillräcklig kapacitet för att



ackreditera och anmäla de organ som kan krävas för att tillgodose svenska tillverkares behov. Den tid det tar för ett företag att bli ackrediterat spelar också en central roll. Avsaknaden av etablerad praxis och standarder för ackreditering inom nya områden innebär en tidskrävande bedömningsprocess, vilket sannolikt kan fördröja ett växande utbud av organ för bedömning av överensstämmelse på den svenska marknaden.

3.4. Konsekvenser av en potentiell brist på svenska organ för bedömning av överensstämmelse

När CRA träder i kraft kommer det initialt finnas ett omfattande behov av organens tjänster. Det stora initiala trycket på existerande organ kan innebära att organen tvingas prioritera vissa produktgrupper, att tillverkare riskerar förseningar i marknads-tillträde och att mindre aktörer hamnar i underläge om de inte är ute i god tid.

En möjlig konsekvens av ett initialt stort behov av organ för bedömning av överensstämmelse är att svenska tillverkare kommer att vända sig till organ i andra EU-länder. Rent principiellt bör detta inte innebära några särskilda konsekvenser då kontrollen är tänkt att vara en standardiserad process inom EU. En brist på tillgång till svenska organ kan däremot innebära en ökad tröskel för svenska företag, som sannolikt skulle föredra att vända sig till svenska organ. Att svenska tillverkare vänder sig till organ för bedömning av överensstämmelse utomlands innebär även ett bortfall av intäkter för svenskt näringsliv och förlorade arbetstillfällen.

3.4.1. Tidigare erfarenheter från MDR (2017/745) och RED (2014/53)

Det går att hämta vissa lärdomar från andra håll om vilka problem som potentiellt kan uppstå om det finns ett underskott på organ för bedömning av överensstämmelse när en ny förordning träder i kraft.

Ett sådant fall är situationen när EU:s Medicintekniska förordning (MDR) trädde i kraft i maj 2021. Målsättningen med regelverket var att få en likriktad implementering av krav inom hela EU och en anpassning av krav till den teknikutveckling som skett inom det medicintekniska området. Kraven syftade även till att säkerställa att endast säkra och ändamålsenliga produkter släpps ut på marknaden. Läkemedelsverket konstaterade vid årsskiftet 2023/2024 att tillgången till CE-märkta produkter inom medicinteknik riskerar att störas under kommande år. Delar av branschen konstaterades ha svårt att anpassa verksamheten till regelverket, bland annat på grund av en brist på den kapaciteten hos anmälda organ. I Sverige riskerar detta att leda till brist på framtida CE-märkta medicintekniska produkter, och att medicintekniska företag i Sverige behöver prioritera sina produktportföljer³⁵.

Ett fall som ligger närmare CRA:s tillämpningsområde är nya cybersäkerhetskrav i radio-trustningsdirektivet (2014/53) som trädde i kraft i augusti 2025, och som innefattar

³⁵

https://www.lakemedelsverket.se/globalassets/dokument/regeringsuppdrag/slutrapport_regeringsuppdrag_sprida-kunskap-om-eu-forordningar-medicintekniska-produkter.pdf



väsentliga krav för produkter som bedöms kunna ha potentiella risker kopplade till cybersäkerhet. I anslutning till bestämmelsernas ikraftträdande skulle tre vägledande standarder tas fram³⁶, men dessa blev försenade. Fördröjningen mellan publiceringen av standarderna och deras tillämpning innebär att tillverkare har haft begränsad tid att anpassa sina produkter för att uppfylla de nya cybersäkerhetskraven innan de blir obligatoriska. Inom ramen för CRA har kommissionen utfärdat ett standardiseringsuppdrag som omfattar utvecklingen av totalt 41 harmoniserade standarder som ska stödja implementeringen av CRA³⁷. Om framtagandet av dessa standarder försenas så lär det rimligen medföra omfattande konsekvenser för både tillverkare och marknadsaktörer som kan behöva anpassa verksamheten till nya regler med kort varsel.

3.4.2. Behov av statliga informations- och utbildningsinsatser

Vi har tidigare konstaterat att det är sannolikt att det vid CRA:s ikraftträdande kommer finnas ett underskott av organ för bedömning av överensstämmelse på den svenska marknaden. Det lär därför komma att behövas informationsinsatser från statliga aktörer för att stimulera fler aktörer att bli organ för bedömning av överensstämmelse.

Även här kan en jämförelse göras med EU:s Medicintekniska förordning (MDR) som beskrevs i föregående avsnitt. Läkemedelsverket har konstaterat att när MDR trädde i kraft så fanns det initialt ett omfattande behov av informationsinsatser då det fanns stora brister i regulatorisk kunskap bland berörda aktörer. Givet den höga innovations-takten inom både medicinteknik och de produktområden som omfattas av CRA finns det anledning att tro att en liknande situation kan uppstå när CRA träder i kraft.

Även om staten sannolikt kommer att behöva genomföra informations- och utbildningsinsatser när CRA införs, så bör nämnas att även näringslivsorganisationer m.fl. lär komma att bedriva ett motsvarande arbete. Sådana informationsinsatser förekommer för övrigt redan i dag.³⁸

³⁶ https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=OJ:L_202500138

³⁷ [https://ec.europa.eu/transparency/documents-register/detail?ref=C\(2025\)618&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=C(2025)618&lang=en)

³⁸ Se t.ex. Svenskt Näringsliv, Cyberresiliensförordningen – nya krav för uppkopplade produkter och tjänster.



4. Marknadskontrollmyndighetens resursbehov

I uppdraget ingår att analysera vissa frågor om marknadskontrollmyndighetens resursbehov. Som framgått av kapitel 1 ska vi beskriva och analysera vilka resurser den utsedda marknadskontrollmyndigheten behöver tillföras. I det ingår att bland annat analysera hur myndigheten kan organiseras och resurssättas, kostnaden för att starta upp marknadskontrollverksamhet, hur många produkter med digitala element kontrollen bör omfatta samt sannolik genomsnittlig kostnad för ett marknadskontrollärende.

Enligt uppdraget ska vår analys göras med utgångspunkt i Cyberresiliensutredningens förslag avseende marknadskontrollmyndighet. Något slutgiltigt sådant förslag föreligger inte vid tiden för vårt uppdrag. Men våra kontakter med utredningen talar för att Post- och telestyrelsen, PTS, är huvudkandidat för uppgiften, varför vi utgått från det.

Eftersom två av de frågor vi ska behandla berör marknadskontrollmyndighetens uppbyggnadsfas och två av frågorna dess mer löpande verksamhet har vi valt att dela in analysen i dessa två faser. Först ges dock en översiktlig beskrivning av dagens marknadskontroll och hur den förhåller sig till cyberresiliensförordningen.

Inledningsvis bör upprepas, som nämndes i avsnitt 1.4, att det osäkra kunskapsläge som för närvarande delvis råder kring hur CRA i praktiken kommer att fungera, innebär att vi beträffande vissa av de delfrågor som ställs i uppdraget endast har kunnat redovisa partiella eller mer översiktliga svar.

4.1. Marknadskontrollen i dag

4.1.1. Vad är marknadskontroll?³⁹

Som nämndes i kapitel 1 bygger den grundstruktur som sedan länge finns etablerad kring hantering av produkters säkerhet och fria rörlighet inom EU på att det som huvudregel är tillverkarens ansvar att en produkt uppfyller gällande krav och det krävs inte någon förhandskontroll av produkten från myndighetshåll innan den släpps ut på marknaden. För att säkerställa att produkter på marknaden överensstämmer med gällande krav används i stället marknadskontroll.

Marknadskontroll syftar till att säkerställa säkerhet, hälsa och konsumentskydd och att motverka snedvridning av konkurrens mellan företag.

Marknadskontroll innebär att ansvarig myndighet kontrollerar att produkter som finns på marknaden uppfyller gällande lagstiftning och att de är märkta och kontrollerade på föreskrivet sätt. Myndigheten ska vidta åtgärder mot de ekonomiska aktörer vars

³⁹ Om inget annat anges är uppgifterna i avsnittet hämtade från Marknadskontrollrådets hemsida; <https://marknadskontroll.se/for-myndigheter/vad-ar-marknadskontroll/>, hämtad 2025-08-16.



produkter inte uppfyller ställda krav. Åtgärder som kan bli aktuella är till exempel försäljningsförbud, tillbakadragande av produkter från marknaden eller återkallande av produkter från slutanvändare.

Marknadskontroll sker i form av informationsinsatser, planerade kontroller hos tillverkare, importörer eller återförsäljare eller reaktioner på rapporterade olyckor, klagomål från allmänheten eller varningar från myndigheter i andra länder. Marknadskontroll omfattar inte förhandskontroll eller kontroller av produkter i bruk.

Hur marknadskontroll bedrivs och är organiserad kan variera från land till land. I Sverige är den uppdelad mellan ett stort antal myndigheter, som alla kontrollerar sina respektive ansvarsområden.⁴⁰ Swedac är ansvarig myndighet för samordning av den svenska marknadskontrollen. Samordningen sker bland annat i Marknadskontrollrådet, där representanter från berörda myndigheter ingår. Swedac är även centralt samordningskontor för marknadskontroll och representerar Sverige i EU:s nätverk för produktöverensstämmelse.

4.1.2. Omfattning på dagens marknadskontroll

Vi saknar en heltäckande, aktuell bild av storleken på dagens svenska marknadskontroll. Vissa indikationer ges dock av olika källor.

I betänkandet från 2019 års marknadskontrollutredning redovisades en översiktlig kartläggning som utredningen genomfört.⁴¹ Utredningen erhöll inte uppgifter från samtliga marknadskontrollmyndigheter, men de som svarade angav att de 2019 hade haft de ärendemängder i sin marknadskontroll som framgår av tabell 13 nedan. Utöver vad som redovisas hade flera myndigheter också haft vissa ärenden i samarbete med Tullverket.

I syfte att hitta mer aktuella siffror har vi i uppdraget studerat hur arbetet med marknadskontroll beskrivs i berörda myndigheters årsredovisningar för 2024. Uppgifter om antal ärenden framgår dock endast i cirka hälften av myndigheternas årsredovisningar.

De ärendemängder som framgår av 2019 års marknadskontrollutredning respektive av årsredovisningarna för 2024 visas i tabellen nedan. (iu. betyder ingen uppgift.)

⁴⁰ Arbetsmiljöverket, Boverket, Elsäkerhetsverket, Folkhälsomyndigheten, Inspektionen för vård och omsorg, Kemikalieinspektionen, Konsumentverket, Läkemedelsverket, Myndigheten för samhällsskydd och beredskap, Naturvårdsverket, Post- och telestyrelsen, Statens energimyndighet, Strålsäkerhetsmyndigheten, Styrelsen för ackreditering och teknisk kontroll och Transportstyrelsen. I Marknadskontrollrådet ingår även Kommerskollegium och Tullverket.

⁴¹ SOU 2020:49 Enhetlig och effektiv marknadskontroll. Betänkande av 2019 års marknadskontrollutredning, s. 211.



Tabell 13. Marknadskontrollmyndigheternas antal ärenden, 2019 och 2024

Myndighet	Antal marknadskontrollärenden	
	2019	2024
Arbetsmiljöverket	250	232
Boverket	100	iu.
Elsäkerhetsverket	435	374
Folkhälsomyndigheten	1	51
Inspektionen för vård och omsorg	iu.	iu.
Kemikalieinspektionen	730	847
Konsumentverket	300	189
Läkemedelsverket	iu.	iu.
Myndigheten för samhällsskydd och beredskap	44	31
Naturvårdsverket	iu.	iu.
Post- och telestyrelsen	14	23
Statens energimyndighet	70	iu.
Strålsäkerhetsmyndigheten	iu.	iu.
Swedac	iu.	iu.
Transportstyrelsen	540	iu.

Tabellen tyder på att antalet marknadskontrollärenden hos berörda myndigheter kan variera över tid. I de flesta fall tycks det dock inte ha handlat om några kraftiga trendbrott under den aktuella tidsperioden – möjligen med undantag för Folkhälso-myndigheten.

År 2022 uppskattades den totala budgeten för svensk marknadskontroll avseende de 14 myndigheter som ingår i den nationella strategin för marknadskontroll uppgå till cirka 130 miljoner kronor per år och vad gäller personella resurser till totalt 80 årsarbets-krafter.⁴² I genomsnitt per myndighet motsvarar det 9,3 miljoner kronor per år och 5,7 årsarbetskrafter.

4.1.3. Dagens marknadskontroll i relation till CRA

Vi har tidigare konstaterat att många av de produkter med digitala element som omfattas av kraven i EU:s cyberresiliensförordning redan omfattas av krav på produkt-säkerhet och liknande enligt andra EU-regler. Därmed är dessa produkter också sedan tidigare föremål för marknadskontroll, och dessutom inte sällan av flera myndigheter utifrån olika regelverk.

⁴² Utrikesdepartementet (2022) Nationell strategi för marknadskontroll Sverige 2022–2025, s. 13. De 14 myndig-heter som omfattas av strategin är de som framgår i tabell 13, exklusive Inspektionen för vård och omsorg och Strålsäkerhetsmyndigheten, men med tillägg av Tullverket.



Några exempel på detta inom berörda branscher är att avseende såväl dataprodukter som hemelektronik bedriver Elsäkerhetsverket, Energimyndigheten och Post- och telestyrelsen marknadskontroll utifrån olika aspekter. PTS utför också marknadskontroll inom branschen för mobiltelefoni och både Elsäkerhetsverket och Energimyndigheten avseende vitvaror och hushållsapparater. Avseende leksaker och barnprodukter är såväl Elsäkerhetsverket, Kemikalieinspektionen som Konsumentverket ansvariga för marknadskontroll utifrån olika aspekter.

I sammanhanget bör dock sägas att marknadskontrollen enligt CRA förväntas komma att innehålla fler moment än den marknadskontroll som i dag vanligen sker inom olika produktområden. Befintlig marknadskontroll begränsas i normalfallet till kontroll av produkter som tillhandahålls på marknaden. Kontroller i konstruktions- eller produktions-skedet liksom regelbunden kontroll eller besiktning för att kontrollera om en produkt som används fortfarande uppfyller gällande krav omfattas i de allra flesta fall inte.⁴³

I detta hänseende skiljer sig kraven enligt CRA till en del. Det är väsentligt att säkerställa att produkter med digitala element är säkra både när de släpps ut på marknaden och under den tid som produkten med digitala element förväntas vara i bruk. Tillverkarna ska därför säkerställa att deras produkter uppfyller ett antal väsentliga cybersäkerhetskrav under hela deras livslängd, eller stödperiod (minst fem år, såvida inte produktens livslängd är kortare). Tillverkaren kommer därmed att behöva tillhandahålla säkerhetsuppdateringar under produktens hela livscykel. Behovet av marknadskontroll kommer då också att föreligga under hela denna hela stödperiod, det vill säga det behöver ske en viss övervakning efter utsläppandet på marknaden.

4.2. Uppbyggnadsfasen för den nya marknadskontrolluppgiften

Arbetet med att starta upp marknadskontrollverksamheten avseende CRA kommer – med en grov kategorisering – att medföra två typer av kostnader för den myndighet som utses som ansvarig (PTS):

- ✦ Kostnader för PTS interna insatser för att bygga upp och etablera den nya funktionen för marknadskontroll. Hit hör exempelvis kostnader för kompetensuppbyggnad, för eventuella nyrekryteringar, för praktiska frågor (till exempel anskaffning av lokaler och datorer) med mera.
- ✦ Kostnader för att etablera den nya marknadskontrollfunktionen i en extern kontext – i syfte att den löpande verksamheten sedan ska kunna fungera som tänkt. Hit hör till exempel kostnader för att informera berörda aktörer om den nya rollen, för att bygga upp nödvändig samverkan med andra myndigheter med mera.

Hur stora ovanstående kostnader kommer att bli i praktiken är svårt att bedöma exakt. Men beträffande den första kategorin kan viss vägledning ges av andra myndighetsverksamheter som startats eller planerats att starta på senare år. Ett exempel är den utredning som föregick bildandet av Myndigheten för totalförsvarsanalys i vilken

⁴³ SOU 2020:49 Enhetlig och effektiv marknadskontroll. Betänkande av 2019 års marknadskontrollutredning, s. 202.



bedömdes att kostnaderna för att starta upp myndigheten skulle bli cirka 0,5 miljoner kronor per årsarbetskraft.⁴⁴ Ett annat exempel är att Governo i ett uppdrag åt utredningen om ungdomskriminalitetsnämnder bedömde att uppstartskostnaden för den av utredningen föreslagna Myndigheten mot ungdomskriminalitet skulle ligga på cirka 0,25 miljoner kronor per årsarbetskraft.⁴⁵

Båda de nämnda exemplen avsåg helt nya myndigheter som föreslogs få klart fler årsarbetskrafter (mellan cirka 40 och 70) än vad den nya marknadskontrollfunktionen vid PTS kan antas få – som kommer att framgå av avsnitt 4.3 antar vi att denna kommer att omfatta mellan sex och tolv årsarbetskrafter. Allt annat lika torde det innebära att uppstartskostnaden per årsarbetskraft skulle bli något större avseende den nya marknadskontrollfunktionen än i de två de nämnda exemplen.

Samtidigt får förutsättas att PTS kommer att organisera den nya marknadskontrollfunktionen som en del av sin befintliga marknadskontroll. Det faktum att PTS redan bedriver marknadskontroll – inte sällan riktad mot samma aktörer som kommer att omfattas av kontroll enligt CRA – bör rimligen innebära att synergier kan utvinnas gentemot den befintliga funktionen både i uppbyggnadskedet och senare i den löpande verksamheten. Synergier avseende exempelvis kompetens, lokaler och IT och som alltså berör både de interna och de externa förhållandena som nämns i punkterna ovan.

Sammantaget antar vi att den större uppstartskostnaden per årsarbetskraft till följd av verksamhetens mindre storlek kompenseras av de förväntade synergier, och att de två nämnda SOU:erna därför kan användas som förlaga för beräkningen i detta fall. Om den nya marknadskontrollfunktionen skulle komma att omfatta cirka mellan sex och tolv årsarbetskrafter, antar vi därmed att kostnaderna för PTS interna insatser för att bygga upp och etablera den nya funktionen skulle uppgå till mellan ca tre och sex miljoner kronor.

Till detta ska då också läggas kostnaderna för att etablera den nya marknadskontrollfunktionen i en extern kontext. Med en grov uppskattning antar vi att kostnaderna för dessa insatser (information m.m.) kan komma att uppgå till cirka en till två miljoner kronor.

Sammantaget antar vi därmed att kostnaderna för uppbyggnadsfasen för den nya marknadskontrolluppgiften kommer att uppgå till mellan 4 och 8 miljoner kronor.

4.3. Löpande verksamhet i den nya marknadskontrolluppgiften

4.3.1. Tillvägagångssätt

Enligt uppdraget ska vi – som grund för att kunna bedöma marknadskontrollmyndighetens resursbehov – analysera hur många produkter med digitala element

⁴⁴ SOU 2021:103 Totalförsvarsanalys – en oberoende myndighet för uppföljning och utvärdering. Betänkande av Utredningen om totalförsvarsanalys.

⁴⁵ SOU 2024:30 En statlig ordning med brottsförebyggande åtgärder för barn och unga. Betänkande av Utredningen om ungdomskriminalitetsnämnder.



kontrollen bör omfatta och sannolik genomsnittlig kostnad för ett marknadskontroll-
ärende.

Den genomsnittliga kostnaden för ett marknadskontrollärende beror givetvis på hur
många kontroller som görs. Med nuvarande kunskapsläge har vi dock svårt att närmare
bedöma hur många produkter som bör kontrolleras och hur många kontroller som bör
göras. Något givet svar finns heller inte på detta, utan det finns ett visst tolknings-
utrymme när det gäller att bestämma kontrollens omfattning och frekvens. Var bedöm-
ningen i slutändan kommer att landa beror på flera omständigheter som ännu inte är
helt kända, till exempel vilka politiska prioriteringar som görs, hur CRA:s regler fortsatt
anpassas och tillämpas på nationell nivå, vilken riskbedömning som görs avseende
produktsammansättningen på marknaden och hur stora resurser marknadskontroll-
myndigheten tilldelas.

Mot denna bakgrund har vi valt en annan – mer top down-betonad – ansats för att
försöka bedöma storleken på de kostnader som kommer att uppstå i den löpande
verksamheten avseende den nya marknadskontrolluppgiften. Dessa kostnader handlar
bland annat om kostnader för personal, lokaler, teknisk utrustning, genomförande av
undersökningar och tester, samverkan m.m.

Vår ansats har varit att först ange ett "nollalternativ", det vill säga en realistisk minsta
nivå för hur stora resurser den nya marknadskontrollfunktionens löpande verksamhet
kan tänkas kräva. Denna nivå har vi sedan ställt mot två – i varierande grad – mer
expansiva alternativ ("Midi-alternativet" och "Maxi-alternativet"). I samtliga alternativ
antas att de beräknade summorna inkluderar samtliga de arbetsuppgifter som ingår i
PTS ansvar som marknadskontrollmyndighet enligt CRA. Övriga förutsättningar,
antaganden och nivåer för de olika alternativen redovisas nedan.

4.3.2. Beräkning av nollalternativet

PTS bedriver i dag marknadskontroll enligt EU:s radioutrustningsdirektiv, som genomförs
genom radioutrustningslagen. Radioutrustningsdirektivet reglerar tekniska och admini-
strativa krav för radioutrustning. Radioutrustning är enkelt uttryckt elektriska eller elektro-
niska produkter som avsiktligt avger eller mottar radiovågor för radiokommunikation
eller radiobestämning. Radioutrustningen kan också vara hushållsutrustning med in-
byggda radiokomponenter för trådlös anslutning. Radiokomponenter finns i till exempel
trådlösa hörlurar, radiostyrda leksaker, kommunikationsradio, inbrottslarm och trygghets-
larm.

Vi saknar aktuella uppgifter om hur många svenska aktörer som omfattas av reglerna i
radioutrustningslagen och PTS marknadskontroll. Inför att radioutrustningslagen skulle
införas 2016 tog dock PTS fram föreskrifter om radioutrustning. I förslaget till dessa
föreskrifter redovisade myndigheten en konsekvensutredning. I denna bedömdes att



1 421 tillverkare, 500 importörer och 14 507 distributörer skulle vara berörda av radioutrustningsdirektivet i Sverige.⁴⁶

Beträffande resursåtgång tyder vår intervju med PTS på att personalåtgången i myndighetens radioutrustningskontroll i dagsläget uppgår till cirka 3,5 till 4,5 årsarbetskrafter. Om man antar att PTS samlade resursåtgång är proportionerlig till de genomsnittsvärden som i avsnitt 4.1.2 redovisades för samtliga Sveriges marknadskontrollmyndigheter, så skulle PTS totala kostnad för radioutrustningskontrollen därmed uppgå till cirka 6,5 miljoner kronor per år. Vi har förutsatt att den angivna resursåtgången täcker samtliga de arbetsuppgifter som ingår i PTS ansvar som marknadskontrollmyndighet avseende radioutrustningslagen.

En stor del av de företag som omfattas av radioutrustningslagen omfattas även av CRA, men somliga gör det inte. Det finns också många företag från andra branscher som omfattas av CRA, men som inte omfattas av radioutrustningslagen. Även med de överlappningar som finns kan konstateras att marknadskontrollen enligt CRA kommer att omfatta klart fler företag än den radioutrustningskontroll som PTS bedriver i dag. I kapitel 2 uppskattade vi ju att CRA kommer att omfatta ca 24–38 000 tillverkare, ca 10–15 000 importörer och ca 10–15 000 distributörer.

Det finns dock skäl att anta att omfattningen på marknadskontrollen enligt CRA inte bör beräknas rakt av som en proportionerlig uppskalning jämfört med dagens radioutrustningskontroll. För det talar bland annat att, som framgått av kapitel 2, en stor andel av berörda produkter är sådana som inte förtecknas som viktiga eller kritiska produkter enligt CRA ("övriga produkter" med vår benämning). Såvitt vi kan förstå torde dessa produkter medföra en relativt sett lägre risk än viktiga och kritiska produkter och lär därför kunna prioriteras förhållandevis lågt i marknadskontrollen. Andra skäl för att en proportionerlig uppskalning inte är lämplig är att det finns en viss överlappning mellan CRA och radioutrustningslagen vad gäller berörda företag samt att PTS bör kunna utvinna flera olika typer av synergier mellan sin nuvarande marknadskontrollverksamhet och den nytiltkommande CRA-kontrollen.

Vid en samlad bedömning antar vi att en 50 procent större resursåtgång för den nya marknadskontrollfunktionen jämfört med dagens radioutrustningskontroll ger en realistisk minsta nivå för hur stora resurser den nya marknadskontrollfunktionens löpande verksamhet kan tänkas kräva.

För analysen antar vi således som nollalternativ för den nya marknadskontrollfunktionen att den kommer att kräva sex årsarbetskrafter och ha löpande kostnader på totalt ca 9–10 miljoner kronor per år.

4.3.3. Beräkning av Midi-alternativet

Som vi beskrev i avsnitt 4.1.3 förväntas marknadskontrollen enligt CRA komma att innehålla fler arbetsmoment än den marknadskontroll som i dag vanligen sker inom olika

⁴⁶ Post- och telestyrelsen (2016) Konsekvensutredning om inför Post- och telestyrelsens förslag till föreskrifter om radioutrustning (PTSFS 2016:5).



produktområden, inklusive PTS radioutrustningskontroll. Framför allt tillkommer det i cyberresiliensförordningen mer av löpande kontroll under berörda produkters hela livslängd. Möjligen kommer kontrollen enligt CRA därtill att kräva mer samverkan med andra myndigheter m.fl. än den traditionella marknadskontrollen. Det kan därför antas att kostnaden för den nya marknadskontrollfunktionens löpande verksamhet kommer att bli relativt sett högre än i den befintliga marknadskontrollen.

I Midi-alternativet antar vi att denna merkostnad kommer att bli 50 procent högre än i nollalternativet. Med detta antagande skulle den nya marknadskontrollfunktionen vid PTS komma att kräva ca 9 årsarbetskrafter och ha löpande kostnader på totalt ca 13,5–15 miljoner kronor per år.

4.3.4. Beräkning av Maxi-alternativet

I detta alternativ görs motsvarande justering som i Midi-alternativet, men vi antar att merkostnaden blir 100 procent högre än i nollalternativet (inklusive en dubbling av personalbehovet). Med detta antagande skulle den nya marknadskontrollfunktionen vid PTS komma att kräva ca 12 årsarbetskrafter och ha löpande kostnader på totalt ca 18–20 miljoner kronor per år.

En jämförelse kan göras med nationella myndigheten för cybersäkerhetscertifiering

För ett test på rimligheten i Maxi-alternativets nivå kan en jämförelse göras med beräkningar som gjordes inför att Försvarets materielverk (FMV) utsågs som nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt.

Cybersäkerhetsakten, som började tillämpas sommaren 2021, har till huvudsakligt syfte att uppnå en hög nivå i fråga om cybersäkerhet, cyberresiliens och förtroende inom unionen och säkerställa en väl fungerande inre marknad. Cybersäkerhetsakten ställer krav på att medlemsstaterna ska utse en eller flera nationella myndigheter för cybersäkerhetscertifiering. FMV är i Sverige utsedd som nationell myndighet för cybersäkerhetscertifiering. Myndigheten ska därmed fullgöra de uppgifter som följer av det europeiska ramverket för cybersäkerhetscertifiering. I uppgifterna ingår omvärldsbvakning av området för cybersäkerhet, samverkan med nationella och internationella aktörer, ansvar för cybersäkerhetscertifiering på den högsta assurancesnivån samt ansvar för tillsyn över regelsystemets efterlevnad.

I den utredning som föreslog att FMV skulle utses till nationell myndighet för cybersäkerhetscertifiering gjordes en uppskattning av hur stora resurser den nya uppgiften skulle kräva.⁴⁷ Utredningen bedömde att FMV inledningsvis skulle behöva en resursförstärkning för uppgiften, främst i form av personalförstärkning. Till utredningen uppgav FMV att tillkommande uppgifter och ansvarsområden som nationell myndighet för cybersäkerhetscertifiering skulle medföra ett ökat personalbehov som initialt beräknades uppgå till 10–12 heltidsanställda, främst för administrativa, juridiska och tekniska

⁴⁷ SOU 2020:58 EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering. Delbetänkande av Cybersäkerhetsutredningen.



uppgifter. Vidare pekade myndigheten på ett behov av lokaler och administrativt stöd för denna verksamhet, men utan att ange någon kostnadsberäkning för det angivna resursbehovet. Såvitt Governo kan förstå torde de angivna resursbehoven, inklusive personalkostnader, motsvara totalt cirka 15 miljoner kronor i årliga kostnader.

Den tillsynsuppgift som ingår i rollen som nationell myndighet för cybersäkerhetscertifiering har likheter med marknadskontroll. Således ingår i tillsynsuppgiften bland annat att FMV ska behandla klagomål som rör en utfärdad EU-försäkran om överensstämmelse eller ett europeiskt cybersäkerhetscertifikat. Vidare ska FMV kontrollera att tillverkare eller leverantörer som genomför självbedömning av överensstämmelse av IKT-produkter, IKT-tjänster och IKT-processer, dvs. när en EU-försäkran om överensstämmelse utfärdas, fullgör sina skyldigheter och att ett europeiskt cybersäkerhetscertifikat som utfärdas överensstämmer med kraven i den aktuella europeiska ordningen för cybersäkerhetscertifiering. Myndigheten ska även bistå det nationella ackrediteringsorganet med övervakning och kontroll av verksamhet som bedrivs av organen för bedömning av överensstämmelse i enlighet med cybersäkerhetsaktens bestämmelser.

Vi saknar uppgift om hur stor del av det samlade resursbehovet för rollen som nationell myndighet för cybersäkerhetscertifiering som åtgår för tillsynsuppgiften. En indikation ges dock av FMV:s årsredovisning för 2024. Enligt denna åtgick detta år nio årsarbetskrafter för "nationell tillsyn cybersäkerhet", vilket var en ökning från sju årsarbetskrafter 2023 och tre årsarbetskrafter 2022.⁴⁸

Vi förutsätter att posten "nationell tillsyn cybersäkerhet" i årsredovisningen huvudsakligen avser FMV:s tillsyn i rollen som nationell myndighet för cybersäkerhetscertifiering. Vi antar därmed att denna tillsyn kräver ca 8–9 årsarbetskrafter och ca 11–12 miljoner kronor i årliga kostnader.

Denna uppskattning kan ge en indikation på hur stora resurser som kommer att krävas för marknadskontrollen enligt CRA. Den bild vi har fått är visserligen att tillsynen över efterlevnaden av regelsystemet enligt cybersäkerhetsakten torde vara mindre än den marknadskontroll som ska bedrivas enligt CRA. Om man därför överslagsmässigt antar att marknadskontrollen enligt CRA kommer att kräva 50 procent mer resurser än FMV:s tillsyn, så överensstämmer totalen tämligen väl med vad som ovan angavs som nivå för Maxi-alternativet.

4.4. Summering

Ovanstående resonemang ska tolkas med försiktighet. Som nämnts finns många osäkerhetsfaktorer, både avseende hur cyberresiliensförordningens regler slutligt kommer att tillämpas på nationell nivå och avseende de synergier som PTS rimligtvis bör kunna utvinna om/när den nya marknadskontrollfunktionen på lämpligt sätt inlemmas i PTS organisation för myndighetens befintliga marknadskontroll. Med hänsyn till att de olika osäkerheterna kan slå åt olika håll, så menar vi ändå att ovanstående resone-

⁴⁸ Försvarets materielverk (2025) Årsredovisning 2024.



mang kan antas utgöra en rimlig, övergripande skattning av marknadskontrollmyndighetens resursbehov.

Utifrån nuvarande kunskapsläge och de antaganden vi kunnat göra om rimliga utfall, är Governos bedömning att marknadskontrollmyndighetens (PTS) resursbehov för den nya uppgiften att bedriva marknadskontroll enligt CRA sammantaget kommer att uppgå till:

- ✦ mellan 4 och 8 miljoner kronor för att starta upp verksamheten, och
- ✦ mellan ca 10 och 20 miljoner kronor per år för marknadskontrollfunktionens löpande verksamhet.



Referenser

Intervjuade organisationer

Atsec
Försvarets materielverk
Post- och telestyrelsen

Rapporter, regelverk, med mera

EU Commission implementing decision on a standardization request to the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU) 2024/2847 (Cyber Resilience Act)

EU Commission (2021) Study on the need of Cybersecurity requirements for ICT products – No. 2020-0715. Final Study Report.

EU-Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

Europaparlamentets och rådets förordning (EU) 2023/988 av den 10 maj 2023 om allmän produkt säkerhet, ändring av Europaparlamentets och rådets förordning (EU) nr 1025/2012 och Europaparlamentets och rådets direktiv (EU) 2020/1828 och om upphävande av Europaparlamentets och rådets direktiv 2001/95/EG och rådets direktiv 87/357/EEG.

Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen).

Försvarets materielverk (2025) Årsredovisning 2024.

Kommissionens genomförandebeslut (EU) 2025/138 av den 28 januari 2025 om ändring av genomförandebeslut (EU) 2022/2191 vad gäller harmoniserade standarder till stöd för de väsentliga krav i Europaparlamentets och rådets direktiv 2014/53/EU som rör



cybersäkerhet, för de kategorier och klasser av radioutrustning som anges i delegerad förordning (EU) 2022/30

Kommittédirektiv 2024:119 Kompletterande bestämmelser till EU:s cyberresiliensförordning.

Läkemedelsverket (2023), Sprida kunskap om EU-förordningar om medicintekniska produkter samt analysera hur deras införande påverkar tillgången till sådana produkter.

Post- och telestyrelsen (2016) Konsekvensutredning om inför Post- och telestyrelsens förslag till föreskrifter om radioutrustning (PTSFS 2016:5).

Prop. 2022/23:42 Genomförande av tillgänglighetsdirektivet.

RISE (2021), Remissyttrande från RISE avseende EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering, SOU 2020:58.

SOU 2020:58 EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering. Delbetänkande av Cybersäkerhetsutredningen.

SOU 2021:44 Tillgänglighetsdirektivet. Betänkande av Utredningen om genomförandet av tillgänglighetsdirektivet.

SOU 2020:49 Enhetlig och effektiv marknadskontroll. Betänkande av 2019 års marknadskontrollutredning.

SOU 2021:103 Totalförsvarsanalys – en oberoende myndighet för uppföljning och utvärdering. Betänkande av Utredningen om totalförsvarsanalys.

SOU 2024:30 En statlig ordning med brottsförebyggande åtgärder för barn och unga. Betänkande av Utredningen om ungdomskriminalitetsnämnder.

SOU 2025:68 Nya samverkansformer, modern byggnads- och reparationsberedskap – för ökad försörjningsberedskap. Slutbetänkande av Utredningen om näringslivets försörjningsberedskap.

SOU 2025:79 Samlade förmågor för ökad cybersäkerhet. Betänkande av Utredningen om ett stärkt nationellt cybersäkerhetscenter.

Svenskt Näringsliv, Cyberresiliensförordningen – nya krav för uppkopplade produkter och tjänster.

Utrikesdepartementet (2022) Nationell strategi för marknadskontroll Sverige 2022–2025.

Hemsidor

Ekonomifakta – Företagens storlek,
https://www.ekonomifakta.se/sakomraden/foretagande/naringslivet/foretagens-storlek_1212719.html

Eurostat – Business demography statistics, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Business_demography_statistics



Eurostat – Digitalisation in Europe – 2025 edition,
<https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2025>

Marknadskontrollrådet, <https://marknadskontroll.se>

Nosad (Network Open Source and Data), <https://nosad.se/om-nosad>

Post- och telestyrelsen, <https://pts.se/digital-inkludering/lagen-om-vissa-produkters-och-tjansters-tillganglighet/pts-marknadskontroll/>

Statistiska centralbyråns företagsregister, <https://www.foretagsregistret.scb.se/>

Statistiska centralbyråns lönestrukturstatistik, <https://www.scb.se/hitta-statistik/statistik-efter-amne/arbetsmarknad/loner-och-arbetskostnader/lonestrukturstatistik-privat-sektor-slp/pong/tabell-och-diagram/tjansteman-2016/genomsnittlig-manadslon-efter-yrke-2024/>

Swedac, <https://www.swedac.se/>

Techtidningen, <https://techtidningen.se/ny-rapportsvenska-foretagens-investeringar-i-molntjanster-har-fordubblats/>

Statens offentliga utredningar 2025

Kronologisk förteckning

1. Skärpta krav för svenskt medborgarskap. Ju.
2. Några frågor om grundläggande fri- och rättigheter. Ju.
3. Skatteincitament för forskning och utveckling. En översyn av FoU-avdraget och expertskatte-reglerna. Fi.
4. Moderna och enklare skatteregler för arbetslivet. Fi.
5. Avgift för områdessamverkan – och andra åtgärder för trygghet i byggd miljö. LI.
6. Plikten kallar! En modern personalförsörjning av det civila försvaret. Fö.
7. Ny kärnkraft i Sverige – effektivare tillståndsprövning och ändamålsenliga avgifter. KN.
8. Bättre förutsättningar för trygghet och studiero i skolan. U.
9. På språklig grund. U.
10. En förändrad abortlag – för en god, säker och tillgänglig abortvård. S.
11. Straffbarhetsåldern. Ju.
12. AI-kommissionens Färdplan för Sverige. Fi.
13. En effektivare organisering av mindre myndigheter – analys och förslag. Fi.
14. En skärpt miljöstraffrätt och ett effektivt sanktionssystem. KN.
15. Stärkta drivkrafter och möjligheter för biståndsmottagare. Volym 1 och 2. S.
16. Ett nytt regelverk för uppsikt och förvar. Ju.
17. Anpassning av svensk rätt till EU:s avskogningsförordning. LI.
18. Ett likvärdigt betygssystem. Volym 1 och 2. U.
19. Kunskap för alla – nya läroplaner med fokus på undervisning och lärande. U.
20. Kommunal anslutning till Utbetalningsmyndighetens verksamhet. Fi.
21. Miljömålsberedningens förslag om en strategi för hur Sverige ska leva upp till EU:s åtaganden inom biologisk mångfald respektive nettoupptag av växthusgaser från markanvändningssektorn (LULUCF). KN.
22. Förbättrad konkurrens i offentlig och privat verksamhet. KN.
23. Ersättningsregler med brottsoffret i fokus. Ju.
24. Publiken i fokus – reformer för ett starkare filmland. Ku.
25. Arbetslivskriminalitet – upplägg, verktyg och åtgärder, fortsatt arbete. A.
26. Tid för undervisningsuppdraget – åtgärder för god undervisning och läraryrkenas attraktivitet. U.
27. En socionomutbildning i tiden. U.
28. Frihet från våld, förtryck och utnyttjande. En jämställdhetspolitisk strategi mot våld och en stärkt styrning av centrala myndigheter. A.
29. Ökad kvalitet hos Samhall och fler vägar till skyddat arbete. A.
30. Enklare mervärdesskatteregler vid försäljning av begagnade varor och donation av livsmedel. Fi.
31. Utmönstring av permanent uppehållstillstånd och vissa anpassningar till miniminivån enligt EU:s migrations- och asylpakt. Ju.
32. Vissa förändringar av jaktlagstiftningen. LI.
33. Skärpta och tydligare krav på vandel för uppehållstillstånd. Ju.
34. Ett modernare konsumentskydd vid distansavtal. Ju.
35. Etableringsboendelagen – ett nytt system för bosättning för vissa nyanlända. A.

36. Skydd för biologisk mångfald i havsområden utanför nationell jurisdiktion. UD.
37. Skärpta villkor för friskolesektorn. U.
38. Att omhänderta barn och unga. S.
39. Digital teknik på lika villkor.
En reglering för socialtjänsten och verksamhet enligt LSS. S.
40. Säkrare tivoli. Ju.
41. Pensionsnivåer och pensionsavgiften – analyser på hundra års sikt. S.
42. Säkerhetsskyddslagen – ytterligare kompletteringar. Ju.
43. Säkerställ tillgången till läkemedel – förordnande och utlämnande i bristsituationer. S.
44. Förbättrat stöd i skolan. U.
45. Ökat informationsutbyte mellan myndigheter – några anslutande frågor. Ju.
46. Tryggare idrottsarrangemang. Ju.
47. Spänning i tillvaron – hur säkrar vi vår framtida elförsörjning? KN.
48. Stärkt pandemiberedskap. S.
49. Säkerhetspolisens behandling av personuppgifter. Ju.
50. En ny nationell myndighet för viltförvaltning. LI.
51. Bättre förutsättningar för klimatanpassning. KN.
52. Ökad insyn i politiska processer. Ju.
53. Kvalificering till socialförsäkring och ekonomiskt bistånd för vissa grupper. S.
54. Ett skärpt regelverk om utvisning på grund av brott. Ju.
55. En reformerad samhällsorientering för bättre integration. A.
56. Stärkt skydd för domstolarnas och domarnas oberoende. Ju.
57. Polisiär beredskap i fred, kris och krig. Ju.
58. En stärkt hästnäring – för företagande, jämställdhet, jämlikhet och folkhälsa. LI.
59. Stärkt lagstiftning mot hedersrelaterat våld och förtryck. Ju.
60. En starkare fondmarknad. Fi.
61. Sveriges internationella adoptionsverksamhet – lärdomar och vägen framåt. Volym 1 och 2. S.
62. Ansvar för hälso- och sjukvården. Volym 1 Bedömningar och förslag. Volym 2 Underlagsrapporter. S.
63. Stärkt patientsäkerhet genom rätt kompetens – utifrån hälso- och sjukvårdens och tandvårdens behov. S.
64. En ny kontrollorganisation i livsmedelskedjan – för ökad effektivitet, likvärdighet och konkurrenskraft. LI.
65. En mer flexibel hyresmarknad. Ju.
66. En straffreform. Volym 1, 2, 3 och 4. Ju.
67. Arlanda – en viktig port för det svenska välbefindandet. Åtgärder som stärker konkurrenskraften för Arlanda flygplats. LI.
68. Nya samverkansformer, modern byggnads- och reparationsberedskap – för ökad försörjningsberedskap. KN.
69. Effektivare samverkan för djur- och folkhälsa. LI.
70. Längre liv, längre arbetsliv – förlängd rätt att kvarstå i anställningen. A.
71. Fortsatt utveckling av en nationell läkemedelslista – en del i en ny nationell infrastruktur för datadelning. Del 1 och 2. S.
72. Verktyg för en mer likvärdig resursfördelning till skolan. U.
73. En arbetsmiljöstrategi för ett förändrat arbetsliv. A.
74. Ny reglering för den arbetsmarknadspolitiska verksamheten. A.
75. Folkbokföringsverksamhet, biometri och brottsbekämpning. Fi.
76. Det handlar om oss – så bryter vi utanförskapet och bygger en starkare gemenskap. A.
77. En översyn av den statliga lönegarantin. A.
78. En reformerad underrättelseverksamhet. Fö.
79. Samlade förmågor för ökad cybersäkerhet. Fö.

80. Koordinatbestämda fastighetsgränser. Ju.
81. En ny organisation av ekobrottsbekämpningen. Ju.
82. Sysselsättning och boende på landsbygden – Juridiska personers förvärv av jordbruksmark och en effektiv tillämpning av glesbygdsbestämmelserna. LI.
83. Ett nationellt förbud mot tiggeri. Ju.
84. Hem för barn och unga. För en trygg, säker och meningsfull vård. S.
85. Ökad tydlighet, stärkt samverkan – förutsättningar för framtidens utvecklingspolitik. LI.
86. Redo! En utredning om personalförsörjningen av det militära försvaret. Fö.
87. Straffrättsliga åtgärder mot korruption och tjänstefel. Ju.
88. Tidigt besked om lämplig användning av mark och vatten. KN.
89. En moderniserad fiskelagstiftning. Volym 1 och 2. LI.
90. Förmedling av post till personer med skydd i folkbokföringen. Fi.
91. Nya regler om arv och testamente – bland annat ett testamentsregister i offentlig regi och ett stärkt skydd för efterlevande sambor. Ju.
92. En kulturkanon för Sverige. Ku.
93. En robust skogspolitik för aktivt skogsbruk. Del 1 och 2. LI.
94. En säkrare utrikesförvaltning. UD.
95. Skärpta villkor för anhörginvandring. Ju.
96. Fler möjligheter till ökat välbästand. Fi.
97. Krishantering och ändrade rörelse regler för försäkringsföretag. Volym I, II, III & IV. Fi.
98. En bättre organisering av fastighetsbildningsverksamheten. LI.
99. Ändring av permanent uppehållstillstånd för vissa utlänningar. Ju.
100. Åtgärder mot illegal ip-tv. Ku.
101. Anpassningar till AI-förordningen – säker användning, effektiv kontroll och stöd för innovation. Fi.
102. Bättre ansvarsfördelning. Ju.
103. En ny produktansvarslag. Ju.
104. Ny kärnkraft i Sverige – ett samlat system för omhändertagande av radioaktivt avfall. KN.
105. Om överföring av Första AP-fondens verksamhet och tillgångar till Tredje och Fjärde AP-fonderna. Fi.
106. Om överföring av Sjätte AP-fondens verksamhet och tillgångar till Andra AP-fonden. Fi.
107. Sveriges nationella klimatmål – uppdaterat etappmål till 2030. KN.
108. Ett datalyft mot fel, fusk och frånvaro. S.
109. Särskilda provocativa åtgärder. Ju.
110. Snabbare bredband i hela landet – åtgärder för effektivare utbyggnad av gigabitinfrastruktur. Fi.
111. Rättssäkerhetens pris. Ju.
112. Verktyg för skydd av EU-medel. Rättsliga förutsättningar för svenska myndigheter att använda Arachne och Edes. Fi.
113. En förbättrad elevhälsa. U.
114. Skärpningar i lagen om särskild kontroll av vissa utlänningar och utlänningslagen. Volym 1 och 2. Ju.
115. Kompletterande bestämmelser till EU:s cyberresiliensförordning. Fi.

Statens offentliga utredningar 2025

Systematisk förteckning

Arbetsmarknadsdepartementet

- Arbetslivskriminalitet – upplägg, verktyg och åtgärder, fortsatt arbete. [25]
- Frihet från våld, förtryck och utnyttjande. En jämställdhetspolitisk strategi mot våld och en stärkt styrning av centrala myndigheter. [28]
- Ökad kvalitet hos Samhall och fler vägar till skyddat arbete. [29]
- Etableringsboendelagen – ett nytt system för bosättning för vissa nyanlända. [35]
- En reformerad samhällsorientering för bättre integration. [55]
- Längre liv, längre arbetsliv – förlängd rätt att kvarstå i anställningen. [70]
- En arbetsmiljöstrategi för ett förändrat arbetsliv. [73]
- Ny reglering för den arbetsmarknads-politiska verksamheten. [74]
- Det handlar om oss
– så bryter vi utanförskapet
och bygger en starkare gemenskap. [76]
- En översyn av den statliga löne-garantin. [77]

Finansdepartementet

- Skatteincitament för forskning och utveckling. En översyn av FoU-avdraget och expertskatte-reglerna. [3]
- Moderna och enklare skatteregler för arbetslivet. [4]
- AI-kommissionens Färdplan för Sverige. [12]
- En effektivare organisering av mindre myndigheter – analys och förslag. [13]
- Kommunal anslutning till Utbetalnings-myndighetens verksamhet. [20]
- Enklare mervärdesskatte regler vid försäljning av begagnade varor och donation av livsmedel. [30]
- En starkare fondmarknad. [60]

- Folkbokföringsverksamhet, biometri och brottsbekämpning. [75]
- Förmedling av post till personer med skydd i folkbokföringen. [90]
- Fler möjligheter till ökat välbstånd. [96]
- Krishantering och ändrade rörelser regler för försäkringsföretag. Volym I, II, III & IV. [97]
- Anpassningar till AI-förordningen – säker användning, effektiv kontroll och stöd för innovation. [101]
- Om överföring av Första AP-fondens verksamhet och tillgångar till Tredje och Fjärde AP-fonderna. [105]
- Om överföring av Sjätte AP-fondens verksamhet och tillgångar till Andra AP-fonden. [106]
- Snabbare bredband i hela landet
– åtgärder för effektivare utbyggnad av gigabitinfrastruktur. [110]
- Verktyg för skydd av EU-medel. Rättsliga förutsättningar för svenska myndig-heter att använda Arachne och Edes. [112]
- Kompletterande bestämmelser till EU:s cyberresiliensförordning. [115]

Försvarsdepartementet

- Plikten kallar! En modern personal-försörjning av det civila försvaret. [6]
- En reformerad underrättelse-verksamhet. [78]
- Samlade förmågor för ökad cybersäkerhet. [79]
- Redo! En utredning om personalförsörj-ningen av det militära försvaret. [86]

Justitiedepartementet

Skärpta krav för svenskt medborgarskap. [1]

Några frågor om grundläggande fri- och rättigheter. [2]

Straffbarhetsåldern. [11]

Ett nytt regelverk för uppsikt och förvar. [16]

Ersättningsregler med brottsoffret i fokus. [23]

Utmönstring av permanent uppehållstillstånd och vissa anpassningar till miniminivån enligt EU:s migrations- och asylpakt. [31]

Skärpta och tydligare krav på vandel för uppehållstillstånd. [33]

Ett modernare konsumentskydd vid distansavtal. [34]

Säkrare tivoli. [40]

Säkerhetsskyddslagen – ytterligare kompletteringar. [42]

Ökat informationsutbyte mellan myndigheter – några anslutande frågor. [45]

Tryggare idrottsarrangemang. [46]

Säkerhetspolisens behandling av personuppgifter. [49]

Ökad insyn i politiska processer. [52]

Ett skärpt regelverk om utvisning på grund av brott. [54]

Stärkt skydd för domstolarnas och domarnas oberoende. [56]

Polisiär beredskap i fred, kris och krig. [57]

Stärkt lagstiftning mot hedersrelaterat våld och förtryck. [59]

En mer flexibel hyresmarknad. [65]

En straffreform. Volym 1, 2, 3 och 4. [66]

Koordinatbestämda fastighetsgränser. [80]

En ny organisation av ekobrottsbekämpningen. [81]

Ett nationellt förbud mot tiggeri. [83]

Straffrättsliga åtgärder mot korruption och tjänstefel. [87]

Nya regler om arv och testamente

– bland annat ett testamentsregister i offentlig regi och ett stärkt skydd för efterlevande sambor. [91]

Skärpta villkor för anhöriginvandring. [95]

Ändring av permanent uppehållstillstånd för vissa utlänningar. [99]

Bättre ansvarsfördelning. [102]

En ny produktansvarslag. [103]

Särskilda provokativa åtgärder. [109]

Rättssäkerhetens pris. [111]

Skärpningar i lagen om särskild kontroll av vissa utlänningar och utlänningslagen. Volym 1 och 2. [114]

Klimat- och näringslivsdepartementet

Ny kärnkraft i Sverige – effektivare tillståndsprövning och ändamålsenliga avgifter. [7]

En skärpt miljöstraffrätt och ett effektivt sanktionssystem. [14]

Miljömålsberedningens förslag om en strategi för hur Sverige ska leva upp till EU:s åtaganden inom biologisk mångfald respektive nettoupptag av växthusgaser från markanvändningssektorn (LULUCF). [21]

Förbättrad konkurrens i offentlig och privat verksamhet. [22]

Spänning i tillvaron – hur säkrar vi vår framtida elförsörjning? [47]

Bättre förutsättningar för klimatanpassning. [51]

Nya samverkansformer, modern byggnads- och reparationsberedskap – för ökad försörjningsberedskap. [68]

Tidigt besked om lämplig användning av mark och vatten. [88]

Ny kärnkraft i Sverige – ett samlat system för omhändertagande av radioaktivt avfall. [104]

Sveriges nationella klimatmål – uppdaterat etappmål till 2030. [107]

Kulturdepartementet

Publiken i fokus – reformer för ett starkare filmland. [24]

En kulturkanon för Sverige. [92]

Åtgärder mot illegal ip-tv. [100]

Landsbygds- och infrastrukturdepartementet

Avgift för områdessamverkan – och andra åtgärder för trygghet i byggd miljö. [5]

Anpassning av svensk rätt till EU:s avskogningsförordning. [17]

Vissa förändringar av jaktlagstiftningen. [32]

En ny nationell myndighet för viltförvaltning. [50]

En stärkt hästnäring – för företagande, jämställdhet, jämlikhet och folkhälsa. [58]

En ny kontrollorganisation i livsmedelskedjan – för ökad effektivitet, likvärdighet och konkurrenskraft. [64]

Arlanda – en viktig port för det svenska väståndet. Åtgärder som stärker konkurrenskraften för Arlanda flygplats. [67]

Effektivare samverkan för djur- och folkhälsa. [69]

Sysselsättning och boende på landsbygden – Juridiska personers förvärv av jordbruksmark och en effektiv tillämpning av glesbygdsbestämmelserna. [82]

Ökad tydlighet, stärkt samverkan – förutsättningar för framtidens utvecklingspolitik. [85]

En moderniserad fiskelagstiftning. Volym 1 och 2. [89]

En robust skogspolitik för aktivt skogsbruk. Del 1 och 2. [93]

En bättre organisering av fastighetsbildningsverksamheten. [98]

Socialdepartementet

En förändrad abortlag – för en god, säker och tillgänglig abortvård. [10]

Stärkta drivkrafter och möjligheter för biståndsmottagare Volym 1 och 2. [15]

Att omhänderta barn och unga. [38]

Digital teknik på lika villkor.

En reglering för socialtjänsten och verksamhet enligt LSS. [39]

Pensionsnivåer och pensionsavgiften – analyser på hundra års sikt. [41]

Säkerställ tillgången till läkemedel – förordnande och utlämnande i bristsituationer. [43]

Stärkt pandemiberedskap. [48]

Kvalificering till socialförsäkring och ekonomiskt bistånd för vissa grupper. [53]

Sveriges internationella adoptionsverksamhet – lärdomar och vägen framåt. Volym 1 och 2. [61]

Ansvar för hälso- och sjukvården. Volym 1 Bedömningar och förslag. Volym 2 Underlagsrapporter. [62]

Stärkt patientsäkerhet genom rätt kompetens – utifrån hälso- och sjukvårdens och tandvårdens behov. [63]

Fortsatt utveckling av en nationell läkemedelslista – en del i en ny nationell infrastruktur för datadelning. Del 1 och 2. [71]

Hem för barn och unga. För en trygg, säker och meningsfull vård. [84]

Ett datalyft mot fel, fusk och frånvaro. [108]

Utbildningsdepartementet

Bättre förutsättningar för trygghet och studiero i skolan. [8]

På språklig grund. [9]

Ett likvärdigt betygssystem Volym 1 och 2. [18]

Kunskap för alla – nya läroplaner med fokus på undervisning och lärande. [19]

Tid för undervisningsuppdraget – åtgärder för god undervisning och lärarkraftens attraktivitet. [26]

En socionomutbildning i tiden. [27]

Skärpta villkor för friskolesektorn. [37]

Förbättrat stöd i skolan. [44]

Verktyg för en mer likvärdig
resursfördelning till skolan. [72]
En förbättrad elevhälsa. [113]

Utrikesdepartementet

Skydd för biologisk mångfald i
havsområden utanför nationell
jurisdiktion. [36]
En säkrare utrikesförvaltning. [94]