Lagrådsremiss

Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 12 juni 2025

Pål Jonson

Samuel Rudvall
(Försvarsdepartementet)

Lagrådsremissens huvudsakliga innehåll

EU antog 2022 ett direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå inom EU, det så kallade NIS 2-direktivet. I syfte att genomföra direktivet i svensk rätt 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 för 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.

Innehållsförteckning

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till

1. cybersäkerhetslag,
2. lag om ändring i lagen (2006:24) om nationella toppdomäner för Sverige på internet,
3. lag om ändring i offentlighets- och sekretesslagen (2009:400),
4. lag om ändring i lagen (2022:482) om elektronisk kommunikation.

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till cybersäkerhetslag

Härigenom föreskrivs[1] följande.

1 kap. Inledande bestämmelser

Syftet med lagen och lagens innehåll

1 § Syftet med denna lag är att uppnå en hög nivå av cybersäkerhet i samhället.

Bestämmelserna i lagen genomför delvis 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), i den ursprungliga lydelsen.

Uttryck i lagen

2 § I denna lag betyder

1. *allmänt elektroniskt kommunikationsnät*: detsamma som i 1 kap. 7 § lagen (2022:482) om elektronisk kommunikation,
2. *allmänt tillgänglig elektronisk kommunikationstjänst*: detsamma som i lagen om elektronisk kommunikation,
3. *anknutet företag*: detsamma som i artikel 3 i bilagan till kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag,
4. *betrodd tjänst*: detsamma som i artikel 3.16 i EU:s förordning om elektronisk identifiering,
5. *betydande cyberhot*: ett cyberhot som, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på en verksamhetsutövares nätverks- och informationssystem eller användarna av verksamhetsutövarens tjänster genom att vålla betydande skada,
6. *betydande incident*: en incident som har orsakat eller kan orsaka allvarlig driftstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller en incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande skada,
7. *cyberhot*: en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare av dessa system och andra personer,

[1] Jfr 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), i den ursprungliga lydelsen.

8. *cybersäkerhet*: all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot,

9. *datacentraltjänst*: en tjänst som omfattar strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av sådan it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och dataöverföringstjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll,

10. *domännamnssystemtjänst (DNS-tjänst)*: en allmän rekursiv tjänst för att lösa domännamnsfrågor till internetslutanvändare, eller en auktoritativ tjänst för att lösa domännamnsfrågor för användning av tredje part, med undantag för rotnamnsservrar,

11. *enskild verksamhetsutövare*: den som uppfyller kraven i någon av 4–7 §§ och som inte är en offentlig verksamhetsutövare,

12. *EU:s förordning om elektronisk identifiering*: 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,

13. *incident*: en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem,

14. *kvalificerad tillhandahållare av betrodda tjänster*: detsamma som i artikel 3.20 i EU:s förordning om elektronisk identifiering,

15. *marknadsplats online*: en tjänst som använder programvara, inbegripet en webbplats, en del av en webbplats eller en applikation, som administreras av en näringsidkare eller för dennas räkning, som ger konsumenterna möjlighet att ingå distansavtal med andra näringsidkare eller konsumenter,

16. *medelstort företag*: ett företag som, utan beaktande av artikel 3.4, räknas som ett medelstort företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag,

17. *molntjänst*: en digital tjänst som möjliggör administration på begäran och bred fjärråtkomst till en skalbar och elastisk pool av gemensamma dataresurser, inbegripet då sådana resurser är distribuerade på flera platser,

18. *nätverk för leverans av innehåll*: ett nätverk av geografiskt spridda servrar vars syfte är att säkerställa hög tillgänglighet för, tillgång till eller snabb leverans av digitalt innehåll och digitala tjänster till internetanvändare för innehålls- och tjänsteleverantörers räkning,

19. *nätverks- och informationssystem*:

a) ett elektroniskt kommunikationsnät enligt 1 kap. 7 § lagen om elektronisk kommunikation,

b) en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter, eller

c) digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av a och b för att de ska kunna användas, skyddas och underhållas,

20. *offentlig verksamhetsutövare*:

a) en statlig myndighet som omfattas av lagen med stöd av 3 § eller uppfyller kraven i någon av 4–7 §§, eller

b) en region, en kommun eller ett kommunalförbund,

21. *partnerföretag*: detsamma som i artikel 3 i bilagan till kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag,

22. *plattform för sociala nätverkstjänster*: en plattform som gör det möjligt för slutanvändare att interagera, dela och upptäcka innehåll, finna andra användare och kommunicera med andra via flera enheter, särskilt genom chattar, inlägg, videor och rekommendationer,

23. *registreringsenhet för toppdomäner*: en verksamhetsutövare som har delegerats en specifik toppdomän och som ansvarar för administrationen av den, dock inte om toppdomänen används endast för registreringsenhetens eget bruk,

24. *sökmotor*: detsamma som i artikel 2.5 i Europaparlamentets och rådets förordning (EU) 2019/1150 av den 20 juni 2019 om främjande av rättvisa villkor och transparens för företagsanvändare av onlinebaserade förmedlingstjänster,

25. *utlokaliserad driftstjänst*: en tjänst som avser installation, förvaltning, drift eller underhåll av IKT-produkter, IKT-nät, IKT-infrastruktur, IKT-tillämpningar eller andra nätverks- och informationssystem, via bistånd eller aktiv administration antingen i kundernas lokaler eller på distans,

26. *utlokaliserad säkerhetstjänst*: en tjänst som tillhandahålls av en leverantör av utlokaliserade driftstjänster och som innebär hantering av eller utgör stöd för hantering av cybersäkerhetsrisker.

Lagens tillämpningsområde

3 § Lagen gäller för en verksamhetsutövare som är

1. en statlig myndighet med befogenhet att fatta beslut som påverkar fysiska eller juridiska personers rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital, och

2. en region, en kommun eller ett kommunalförbund.

De övriga statliga myndigheter som regeringen bestämmer ska också omfattas av lagen.

4 § Lagen gäller också för en verksamhetsutövare som

1. omfattas av bilaga 1 eller 2 till NIS 2-direktivet i den ursprungliga lydelsen, men inte av 5 § 4, 6 § eller 7 § 1–3, eller är en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina,

2. är etablerad i Sverige, och

3. storleksmässigt motsvarar eller är större än ett medelstort företag.

5 § Lagen gäller också för en verksamhetsutövare som uppfyller kraven i 4 § 1 och 2, om

1. verksamhetsutövaren är den enda leverantören av en tjänst i Sverige som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet,

2. en störning av den tjänst som verksamhetsutövaren tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa eller kan medföra betydande systemrisker,

3. verksamhetsutövaren har särskild betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer som är beroende av verksamhetsutövaren, eller

4. verksamhetsutövaren tillhandahåller betrodda tjänster.

6 § Lagen gäller också för en verksamhetsutövare som i Sverige tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster.

7 § Lagen gäller också för en verksamhetsutövare som har huvudsakligt etableringsställe i Sverige eller en företrädare som är etablerad här, om verksamhetsutövaren

1. uppfyller kravet i 4 § 3 eller kraven i någon av 5 § 1–3 och erbjuder molntjänster, datacentraltjänster, nätverk för leverans av innehåll, utlokaliserade driftstjänster, utlokaliserade säkerhetstjänster, marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster,

2. är en registreringsenhet för toppdomäner,

3. erbjuder DNS-tjänster, eller

4. erbjuder domännamnsregistreringstjänster.

8 § Som väsentlig verksamhetsutövare räknas

1. en verksamhetsutövare som är en statlig myndighet,

2. en verksamhetsutövare som är större än ett medelstort företag och som

a) är en kommun eller en region,

b) i övrigt omfattas av bilaga 1 till NIS 2-direktivet i den ursprungliga lydelsen men inte av 7 § 2 eller 3, eller

c) är en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina,

3. en verksamhetsutövare som avses i 6 § och som storleksmässigt motsvarar eller är större än ett medelstort företag,

4. en verksamhetsutövare som avses i 7 § 2 eller 3,

5. en verksamhetsutövare som är en kvalificerad tillhandahållare av betrodda tjänster, och

6. en verksamhetsutövare som räknas som väsentlig enligt föreskrifter som har meddelats med stöd av 14 § andra stycket 2.

Verksamhetsutövare som inte är väsentliga är viktiga verksamhetsutövare.

Undantag från lagens tillämpningsområde

Krav i andra författningar

9 § Om det i lag eller annan författning finns bestämmelser som innehåller krav på säkerhetsåtgärder eller incidentrapportering ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt 2 kap. 3–10 §§, med beaktande av bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna.

10 § Denna lag gäller inte för verksamhetsutövare som har undantagits enligt artikel 2.4 i 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 (DORA-förordningen).

För en verksamhetsutövare som omfattas av DORA-förordningen gäller inte skyldigheterna enligt 2 kap. 3–10 §§.

Säkerhetskänslig verksamhet och brottsbekämpande verksamhet

11 § Denna lag gäller inte för en statlig myndighet som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585) eller som till övervägande del bedriver brottsbekämpande verksamhet.

Lagen gäller inte heller för en enskild verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen eller som enbart erbjuder tjänster till sådana statliga myndigheter som avses i första stycket.

För andra verksamhetsutövare som till någon del bedriver sådan verksamhet eller erbjuder sådana tjänster som avses i första eller andra stycket gäller inte skyldigheterna i 2 kap. 3–10 §§ för den delen av verksamheten.

Undantagen i första–tredje styckena gäller inte för en verksamhetsutövare som tillhandahåller betrodda tjänster.

12 § Skyldigheterna att lämna uppgifter enligt denna lag gäller inte uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen (2018:585).

Undantag för viss annan offentlig verksamhet

13 § Denna lag gäller inte för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, myndigheter under riksdagen, domstolar och nämnder som utövar rättskipning.

Lagen gäller inte heller för förbundsfullmäktige eller förbundsdirektion i ett kommunalförbund, kommunfullmäktige och regionfullmäktige.

Bemyndigande och beslut om undantag

14 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om

1. vad som utgör huvudsakligt etableringsställe enligt 7 §, och
2. undantag från skyldigheterna enligt denna lag för partnerföretag och anknutna företag som omfattas av lagen med stöd av 4 §.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om

1. vad som utgör en betydande incident enligt 2 § 6, och
2. kriterier för när verksamhetsutövare ska omfattas av lagen enligt 5 § 1–3 och för när sådana verksamhetsutövare ska räknas som väsentliga enligt 8 § första stycket 6.

15 § Regeringen eller den myndighet som regeringen bestämmer får, om det finns särskilda skäl, i enskilda fall besluta om undantag från skyldigheterna enligt denna lag för

1. enskilda utbildningsanordnare som avses i 4 § 1, och
2. partnerföretag och anknutna företag som omfattas av lagen med stöd av 4 §.

Gemensam kontaktpunkt, enhet för hantering av it-säkerhetsincidenter och cyberkrishanteringsmyndighet

16 § Den myndighet som regeringen bestämmer ska vara gemensam kontaktpunkt, enhet för hantering av it-säkerhetsincidenter och cyberkrishanteringsmyndighet enligt artiklarna 8–10 i NIS 2-direktivet, i den ursprungliga lydelsen.

2 kap. Verksamhetsutövares skyldigheter

Skyldighet att utse företrädare

1 § Sådana verksamhetsutövare som avses i 1 kap. 7 § 1–4 och som erbjuder tjänster i Sverige, men saknar etablering inom Europeiska ekonomiska samarbetsområdet (EES), ska utse en företrädare med etablering i Sverige eller i något annat land inom EES där tjänsterna erbjuds.

Anmälningsskyldighet

2 § Verksamhetsutövare ska så snart det kan ske anmäla sig till den myndighet som regeringen bestämmer.

Verksamhetsutövare ska anmäla en förändring avseende i anmälan lämnade uppgifter så snart det kan ske, dock senast 14 dagar efter det att förändringen ägde rum.

Säkerhetsåtgärder

3 § Verksamhetsutövare ska vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och systemens fysiska miljö mot incidenter (säkerhetsåtgärder).

Säkerhetsåtgärderna ska utgå från ett allriskperspektiv och säkerställa en nivå på säkerheten i nätverks- och informationssystemen som är lämplig i förhållande till risken. Säkerhetsåtgärderna ska åtminstone avse

1. strategier för riskanalys och för nätverks- och informationssystemens säkerhet,
2. incidenthantering,
3. kontinuitetshantering och krishantering,
4. säkerhet i leveranskedjan,
5. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem,
6. strategier och förfaranden för att bedöma effektiviteten i säkerhetsåtgärderna,
7. grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,

8. strategier och förfaranden för användning av kryptografi samt, vid behov, kryptering,

9. personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning, och

10. vid behov användning av lösningar för autentisering, säkrade kommunikationer och säkrade nödkommunikationssystem.

Utbildning

4 § Ledningen för en verksamhetsutövare ska genomgå utbildning om säkerhetsåtgärder.

Incidentrapportering och informationsskyldighet

Rapportering av betydande incidenter

5 § Verksamhetsutövare ska upplysa den myndighet som regeringen bestämmer om en betydande incident så snart det kan ske, dock senast 24 timmar efter det att verksamhetsutövaren har fått kännedom om incidenten.

6 § Verksamhetsutövare ska till samma myndighet som avses i 5 § göra en incidentanmälan om den betydande incidenten så snart det kan ske. Verksamhetsutövare som tillhandahåller betrodda tjänster ska göra anmälan senast 24 timmar efter det att verksamhetsutövaren har fått kännedom om incidenten och övriga verksamhetsutövare senast 72 timmar efter sådan kännedom.

7 § På begäran av samma myndighet som avses i 5 § ska verksamhetsutövare lämna en delrapport med relevanta statusuppdateringar för den betydande incidenten.

8 § Senast en månad efter incidentanmälan enligt 6 § ska verksamhetsutövare lämna en slutrapport till samma myndighet. Om den betydande incidenten fortfarande är pågående ska i stället en lägesrapport lämnas vid denna tidpunkt och därefter en slutrapport inom en månad efter det att incidenten har hanterats.

Information vid betydande incidenter och betydande cyberhot

9 § Om det är lämpligt ska verksamhetsutövare så snart det kan ske informera mottagarna av deras tjänster om en betydande incident som sannolikt inverkar negativt på tillhandahållandet av tjänsterna.

10 § Vid ett betydande cyberhot ska verksamhetsutövare så snart det kan ske informera mottagarna av deras tjänster som kan påverkas av hotet om skydds- och motåtgärder som mottagarna kan vidta. Om det är lämpligt ska verksamhetsutövare även informera om själva hotet.

Skyldighet att föra register över domännamn

11 § En verksamhetsutövare som är en registreringsenhet för toppdomäner eller som erbjuder domännamnsregistreringstjänster ska föra ett

register över tilldelade domännamn under toppdomänen och löpande upprätta säkerhetskopior av registeruppgifterna.

Registret ska innehålla

1. domännamnet,
2. namnet på domännamnsinnehavaren och dennes telefonnummer och e-postadress,
3. namnet på den som tekniskt administrerar domännamnet och dennes telefonnummer och e-postadress, och
4. registreringsdatum.

12 § Uppgifterna i registret som avses i 11 § ska kunna hämtas utan avgift via internet. Därutöver ska uppgifter även på begäran lämnas ut skyndsamt och senast 72 timmar från mottagandet av begäran till den som gör en lagligen grundad och motiverad begäran.

Personuppgifter får endast göras tillgängliga på internet om den registrerade har samtyckt till det.

En sådan verksamhetsutövare som avses i 11 § är personuppgiftsansvarig för behandling av personuppgifter i registret.

13 § De skyldigheter som följer av 11 och 12 §§ gäller inte för den som är domänadministratör enligt lagen (2006:24) om nationella toppdomäner för Sverige på internet. För en sådan domänadministratör gäller skyldighet att föra register enligt 6 § den lagen.

Bemyndigande

14 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om utbildning, incidentrapportering, informationsskyldighet och register enligt 4–12 §§.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om säkerhetsåtgärder enligt 3 §.

3 kap. Tillsyn

Tillsynsmyndigheten och tillsynsmyndighetens uppdrag

1 § Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet.

Tillsynsmyndigheten ska utöva tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs. Tillsynsmyndigheten ska också utöva tillsyn över att sådana rättsakter följs som har antagits med stöd av artiklarna 21.5 och 23.11 i NIS 2-direktivet, i den ursprungliga lydelsen.

2 § Tillsynsåtgärder enligt 3, 4, 6 och 7 §§ får när det gäller viktiga verksamhetsutövare vidtas endast när tillsynsmyndigheten har anledning att anta att verksamhetsutövarna inte följer

1. denna lag eller föreskrifter som har meddelats i anslutning till lagen, eller
2. sådana rättsakter som har antagits med stöd av artiklarna 21.5 och 23.11 i NIS 2-direktivet, i den ursprungliga lydelsen.

Tillsynsmyndighetens befogenheter

3 § Den som står under tillsyn ska på begäran tillhandahålla tillsynsmyndigheten de uppgifter eller handlingar som behövs för tillsynen.

4 § Tillsynsmyndigheten har i den omfattning det behövs för tillsynen rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamhet som omfattas av tillsyn.

5 § Tillsynsmyndigheten får utföra regelbundna säkerhetsrevisioner eller låta ett oberoende organ utföra sådana säkerhetsrevisioner av väsentliga verksamhetsutövare.

6 § Tillsynsmyndigheten får om det finns särskilda skäl utföra riktade säkerhetsrevisioner eller låta ett oberoende organ utföra sådana säkerhetsrevisioner av den som står under tillsyn.

7 § Tillsynsmyndigheten får genomföra säkerhetsskanningar hos den som står under tillsyn.

En säkerhetsskanning ska ske i samarbete med verksamhetsutövaren.

8 § Tillsynsmyndigheten får besluta att förelägga den som står under tillsyn att medverka till tillsynsåtgärder enligt 3–7 §§.

Ett föreläggande får förenas med vite. Ett vitesföreläggande får även riktas mot staten.

9 § Tillsynsmyndigheten får begära handräckning av Kronofogdemyndigheten för att genomföra de tillsynsåtgärder som avses i 3 och 4 §§. Vid handräckning gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

Bemyndigande

10 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om säkerhetsrevisioner och säkerhetsskanningar enligt 5–7 §§.

Avgift

11 § Tillsynsmyndigheten får ta ut en handläggningsavgift av en sådan verksamhetsutövare som avses i 1 kap. 6 § och som anmäler verksamhet enligt 2 kap. 2 §. Handläggningsavgiften ska motsvara myndighetens kostnader för handläggningen av ärendet.

Tillsynsmyndigheten ska ta ut en årlig avgift av en sådan verksamhetsutövare som avses i första stycket. De årliga avgifterna ska sammantagna motsvara de kostnader som myndigheten, utöver de kostnader som avses i första stycket, har för sin verksamhet enligt denna lag när det gäller dessa verksamhetsutövare. Avgifterna ska fördelas med skälig andel på var och en av verksamhetsutövarna.

4 kap. Ingripanden

När och hur tillsynsmyndigheten ska ingripa

1 § Tillsynsmyndigheten ska ingripa om en verksamhetsutövare har åsidosatt sina skyldigheter enligt 2 kap. 1–10 §§ eller enligt föreskrifter som har meddelats i anslutning till de paragraferna eller enligt sådana rättsakter som har antagits med stöd av artiklarna 21.5 och 23.11 i NIS 2-direktivet, i den ursprungliga lydelsen.

Ett ingripande sker genom beslut om föreläggande enligt 4 §, ansökan om förbud att inneha ledningsfunktion enligt 6 §, beslut om sanktionsavgift enligt 10 § eller, om det inte finns skäl att ingripa mot en överträdelse på något annat sätt, genom anmärkning.

Tillsynsmyndigheten får avstå från ett ingripande om någon annan tillsynsmyndighet har vidtagit åtgärder mot verksamhetsutövaren med anledning av överträdelsen och dessa åtgärder bedöms tillräckliga.

Omständigheter som ska beaktas vid valet av ingripande

2 § Vid valet av ingripande ska hänsyn tas till hur allvarlig överträdelsen är, hur länge den har pågått och den skada eller risk för skada som uppstått till följd av överträdelsen. Vid bedömningen ska särskilt beaktas

1. om verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse,
2. vad verksamhetsutövaren har gjort för att förhindra eller minska skadan,
3. om överträdelsen har varit uppsåtlig eller berott på oaktsamhet, och
4. den ekonomiska fördel som överträdelsen har inneburit för verksamhetsutövaren.

3 § En överträdelse ska betraktas som allvarlig om verksamhetsutövaren

1. har begått upprepade överträdelser,
2. inte har fullgjort sin skyldighet att rapportera eller informera enligt 2 kap. 5–9 §§,
3. inte har avhjälpt en betydande incident,
4. inte har följt ett föreläggande enligt 4 § första stycket,
5. har hindrat en tillsynsåtgärd enligt 3 kap. 3–7 §§, eller
6. har lämnat falska eller andra grovt oriktiga uppgifter i fråga om säkerhetsåtgärder enligt 2 kap. 3 § eller i samband med incidentrapportering eller fullgörande av informationsskyldighet enligt 2 kap. 5–10 §§.

Förelägganden

4 § Tillsynsmyndigheten får besluta de förelägganden som behövs för att verksamhetsutövare ska fullgöra skyldigheterna som avses i 1 §.

Tillsynsmyndigheten får också förelägga verksamhetsutövare att offentliggöra information om överträdelser av sådana skyldigheter som avses i första stycket.

Ett föreläggande får förenas med vite. Ett vitesföreläggande får även riktas mot staten.

5 § Tillsynsmyndigheten får besluta de förelägganden som behövs för att verksamhetsutövare ska fullgöra skyldigheterna enligt 2 kap. 11 och 12 §§ eller enligt föreskrifter som har meddelats i anslutning till de paragraferna.

Ett föreläggande får förenas med vite. Ett vitesföreläggande får även riktas mot staten.

Förbud att inneha ledningsfunktion

6 § Om ett föreläggande enligt 4 § första stycket inte följs får tillsynsmyndigheten ansöka om förbud att inneha ledningsfunktion för den som är befattningshavare enligt 3 § andra stycket lagen (2014:836) om näringsförbud hos en enskild verksamhetsutövare som är väsentlig.

En ansökan enligt första stycket får göras endast om överträdelsen som ligger till grund för föreläggandet är allvarlig och befattningshavaren uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen.

7 § En ansökan enligt 6 § ska göras till allmän förvaltningsdomstol.

Ansökan ska innehålla uppgifter om den person, befattning och verksamhetsutövare som ansökan avser. Den ska också innehålla uppgift om överträdelsen och de omständigheter som behövs för att kännetecknа den samt de bestämmelser som är tillämpliga på överträdelsen.

Ansökan ska lämnas in till den förvaltningsrätt inom vars domkrets tillsynsmyndigheten är belägen och målet ska prövas skyndsamt av domstolen.

8 § Ett förbud att inneha ledningsfunktion ska gälla lägst ett år och högst tre år.

Tillsynsmyndigheten ska omedelbart begära att förbudet ska upphävas om den bedömer att det inte längre finns förutsättningar för ett förbud enligt 6 §. Den enskilde ska vid ett beslut om förbud upplysas om sin rätt att begära att förbudet ska upphävas enligt 9 §.

9 § Om tillsynsmyndigheten eller den enskilde begär det ska den domstol som avses i 7 § pröva om förbudet ska upphävas. Ett förbud ska upphävas omedelbart om det inte längre finns förutsättningar för det enligt 6 §.

Sanktionsavgift

10 § Tillsynsmyndigheten får besluta att ta ut en sanktionsavgift av en verksamhetsutövare till följd av en överträdelse av de skyldigheter som avses i 1 §.

11 § Sanktionsavgiften ska bestämmas till lägst 5 000 kronor och högst till

1. det högsta av 2 procent av den totala globala årsomsättningen närmast föregående räkenskapsår eller ett belopp i kronor motsvarande 10 000 000 euro för en enskild verksamhetsutövare som är väsentlig,
2. det högsta av 1,4 procent av den totala globala årsomsättningen närmast föregående räkenskapsår eller ett belopp i kronor motsvarande 7 000 000 euro för en enskild verksamhetsutövare som är viktig, eller

3. 10 000 000 kronor för en offentlig verksamhetsutövare.

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

13 § En sanktionsavgift får beslutas endast om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

14 § En sanktionsavgift ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas i rätt tid, ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

Sanktionsavgiften tillfaller staten.

15 § En sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

5 kap. Överklagande

1 § Tillsynsmyndighetens beslut enligt denna lag får överklagas till allmän förvaltningsdomstol. När ett sådant beslut överklagas är tillsynsmyndigheten motpart i domstolen. Övriga beslut får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

---

1. Denna lag träder i kraft den 15 januari 2026.

2. Genom lagen upphävs lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

3. Den upphävda lagen gäller dock fortfarande för överträdelser som har skett före ikraftträdandet.

2.2 Förslag till lag om ändring i lagen (2006:24) om nationella toppdomäner för Sverige på internet

Härigenom föreskrivs[1] i fråga om lagen (2006:24) om nationella toppdomäner för Sverige på internet[2] att 1, 2 och 4–11 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §	
Denna lag gäller teknisk drift av nationella toppdomäner för Sverige på *Internet* samt tilldelning och registrering av domännamn under dessa toppdomäner.	Denna lag gäller teknisk drift av nationella toppdomäner för Sverige på *internet* samt tilldelning och registrering av domännamn under dessa toppdomäner.
2 §	
I denna lag avses med	
domännamnssystemet: det internationella hierarkiska system som för befordringsändamål på *Internet* används för att tilldela domännamn,	domännamnssystemet: det internationella hierarkiska system som för befordringsändamål på *internet* används för att tilldela domännamn,
domän: nivå i domännamnssystemet och del av domännamn,	
domännamn: unikt namn sammansatt av domäner, där en i domännamnssystemet lägre placerad domän står före en domän som är högre placerad i systemet,	
toppdomän: den domän som återfinns sist i ett domännamn,	
nationell toppdomän: toppdomän som betecknar en nation eller en region,	
administration: teknisk drift av en toppdomän samt tilldelning och registrering av domännamn under denna,	
domänadministratör: den som ansvarar för administration av en nationell toppdomän för Sverige,	
namnserver: dator i ett elektroniskt kommunikationsnät som programmerats så att den lagrar och distribuerar information om domännamn samt tar emot och svarar på frågor om domännamn.	
4 §	
En domänadministratör *skall* anmäla sin verksamhet till den myndighet som regeringen bestämmer (tillsynsmyndigheten). Domän-	En domänadministratör *ska* anmäla sin verksamhet till den myndighet som regeringen bestämmer (tillsynsmyndigheten). Domänadmi-

[1] Jfr 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), i den ursprungliga lydelsen.
[2] Senaste lydelse av lagens rubrik 2019:184.

administratören *skall* också till tillsynsmyndigheten anmäla om administrationen helt eller delvis uppdras åt annan.	nistratören *ska* också till tillsynsmyndigheten anmäla om administrationen helt eller delvis uppdras åt annan.
5 §	
En domänadministratör *skall* bedriva verksamheten på ett säkert och effektivt sätt i allmänhetens intresse. Domänadministratören *skall*	En domänadministratör *ska* bedriva verksamheten på ett säkert och effektivt sätt i allmänhetens intresse. Domänadministratören *ska*
1. lagra tilldelade domännamn och andra uppgifter som är nödvändiga för att stödja den del av domännamnssystemet som toppdomänen omfattar i en databas,	
2. distribuera uppgifterna till namnservrarna för toppdomänen och se till att informationen i dessa är korrekt och lätt tillgänglig,	
3. säkerställa en fungerande trafik mellan namnservrarna och *Internet*,	3. säkerställa en fungerande trafik mellan namnservrarna och *internet*,
4. upprätthålla ett effektivt skydd av uppgifterna i toppdomänen,	
5. ha personal med tillräcklig kompetens och erfarenhet för verksamheten, samt	
6. ha sådana rutiner för verksamheten som uppfyller erkända standarder.	
6 §	
En domänadministratör *skall* föra ett register över tilldelade domännamn under toppdomänen och löpande upprätta säkerhetskopior av registeruppgifterna.	En domänadministratör *ska* föra ett register över tilldelade domännamn under toppdomänen och löpande upprätta säkerhetskopior av registeruppgifterna.
Registret *skall* innehålla	Registret *ska* innehålla
1. domännamnet,	
2. namnet på domännamnsinnehavaren och dennes *postadress,* telefonnummer och *adress för elektronisk post*,	2. namnet på domännamnsinnehavaren och dennes telefonnummer och *e-postadress*,
3. namnet på den som tekniskt administrerar domännamnet och dennes *postadress,* telefonnummer och *adress för elektronisk post*,	3. namnet på den som tekniskt administrerar domännamnet och dennes telefonnummer och *e-postadress*,
4. uppgifter om de namnservrar som är knutna till domännamnet, *samt*	4. uppgifter om de namnservrar som är knutna till domännamnet,
5. övrig teknisk information som behövs för att administrera domännamnet.	5. övrig teknisk information som behövs för att administrera domännamnet*, och*
	6. registreringsdatum.
Uppgifterna i registret *skall* kunna hämtas utan avgift via *Internet*.	Uppgifterna i registret *ska* kunna hämtas utan avgift via *internet. Därutöver ska uppgifter även på begäran lämnas ut skyndsamt och senast 72 timmar efter mottagandet*

	av begäran till den som gör en lagligen grundad och motiverad begäran.
Personuppgifter får dock göras tillgängliga på *detta sätt* endast om den registrerade har samtyckt till det.	Personuppgifter får dock göras tillgängliga på *internet* endast om den registrerade har samtyckt till det.

Domänadministratören är personuppgiftsansvarig för behandling av personuppgifter i registret.

7 §

En domänadministratör *skall* fastställa och ge offentlighet åt sina regler för tilldelning, registrering, avregistrering och överföring av domännamn under toppdomänen. Reglerna *skall* utformas så att förfarandet är öppet och icke-diskriminerande, med särskilt beaktande av	En domänadministratör *ska* fastställa och ge offentlighet åt sina regler för tilldelning, registrering, avregistrering och överföring av domännamn under toppdomänen. Reglerna *ska* utformas så att förfarandet är öppet och icke-diskriminerande, med särskilt beaktande av

1. skyddet för den personliga integriteten,
2. användarnas intressen och andra allmänna intressen, samt

3. utvecklingen inom *Internet-området*.	3. utvecklingen inom *internet-området*.
Domänadministratören *skall* tillhandahålla ett effektivt förfarande för lösning av tvister om tilldelning av domännamn.	Domänadministratören *ska* tillhandahålla ett effektivt förfarande för lösning av tvister om tilldelning av domännamn.

8 §

En domänadministratör *skall* se till att uppgifterna i den databas som anges i 5 § 1 och det register som anges i 6 § överförs till tillsynsmyndigheten.	En domänadministratör *ska* se till att uppgifterna i den databas som anges i 5 § 1 och det register som anges i 6 § överförs till tillsynsmyndigheten.

9 §

Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om

1. på vilket sätt skyldigheter enligt 5 § *skall* fullgöras,	1. på vilket sätt skyldigheter enligt 5 § *ska* fullgöras,

2. register och säkerhetskopior enligt 6 §, samt
3. överföring enligt 8 §.

10 §

Tillsynsmyndigheten *skall* ha tillsyn över efterlevnaden av lagen och av föreskrifter som har meddelats med stöd av lagen.	Tillsynsmyndigheten *ska* ha tillsyn över efterlevnaden av lagen och av föreskrifter som har meddelats med stöd av lagen.

11 §

En domänadministratör *skall* på tillsynsmyndighetens begäran lämna den information och bereda den tillgång till utrustning och annat som behövs för tillsynen.	En domänadministratör *ska* på tillsynsmyndighetens begäran lämna den information och bereda den tillgång till utrustning och annat som behövs för tillsynen.

Tillsynsmyndigheten har rätt att när det behövs för tillsynen få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som omfattas av denna lag bedrivs.

Denna lag träder i kraft den 15 januari 2026.

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

Härigenom föreskrivs[1] i fråga om offentlighets- och sekretesslagen (2009:400)[2]

dels att nuvarande 18 kap. 8 b och 8 c §§ ska betecknas 18 kap. 8 c och 8 d §§,

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

dels att rubrikerna närmast före 18 kap. 8 b och 8 c §§ ska sättas närmast före 18 kap. 8 c respektive 8 d §§,

dels att det ska införas två nya paragrafer, 15 kap. 3 c § och 18 kap. 8 b § av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	15 kap.
	3 c §
	Sekretessen enligt 1 a § hindrar inte att Myndigheten för samhällsskydd och beredskap i egenskap av en sådan gemensam kontaktpunkt, enhet för hantering av it-säkerhetsincidenter eller cyberkrishanteringsmyndighet som avses i 1 kap. 16 § cybersäkerhetslagen (2025:000) lämnar en uppgift till en tillsynsmyndighet enligt samma lag, om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag.
	Sekretessen hindrar inte heller att en sådan tillsynsmyndighet som avses i första stycket lämnar en uppgift till Myndigheten för samhällsskydd och beredskap, om uppgiften behövs för att Myndigheten för samhällsskydd och beredskap ska kunna fullgöra sitt uppdrag som sådan gemensam kontaktpunkt, enhet för hantering av it-säkerhetsincidenter eller cyberkrishanteringsmyndighet som avses i första stycket.

[1] Jfr 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), i den ursprungliga lydelsen.

[2] Senaste lydelse av
18 kap. 8 b § 2019:305
18 kap. 8 c § 2019:305.

En uppgift enligt första eller andra stycket får lämnas endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

18 kap.

8 b §

Sekretess gäller för uppgift i en incidentrapport enligt cybersäkerhetslagen (2025:000) och för uppgift om vilka åtgärder som en verksamhetsutövare har vidtagit till följd av incidenten, om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens framtida verksamhet skadas eller syftet med vidtagen åtgärd motverkas.

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

19 §[3]

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 b*, 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 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

[3] Senaste lydelse 2024:477.

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.

Denna lag träder i kraft den 15 januari 2026.

2.4 Förslag till lag om ändring i lagen (2022:482) om elektronisk kommunikation

Härigenom föreskrivs[1] i fråga om lagen (2022:482) om elektronisk kommunikation[2]

dels att 8 kap. 1–4 §§ ska upphöra att gälla,

dels att rubriken närmast före 8 kap. 1 § ska utgå,

dels att nuvarande 8 kap. 5–9 §§ ska betecknas 8 kap. 1–5 §§,

dels att 1 kap. 7 § och 12 kap. 1 § ska ha följande lydelse,

dels att rubrikerna närmast före 8 kap. 5 och 6 §§ ska sättas närmast före 8 kap. 1 respektive 2 §§,

dels att det ska införas en ny paragraf, 1 kap. 4 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 kap.
	4 a §
	I cybersäkerhetslagen (2025:000) finns det bestämmelser om säkerhetsåtgärder, säkerhetsrevision, incidentrapportering och informationsskyldighet.
	7 §

I lagen avses med

abonnent: den som har ingått avtal med en tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster om tillhandahållande av sådana tjänster,

allmänt elektroniskt kommunikationsnät: ett elektroniskt kommunikationsnät som helt eller huvudsakligen används för att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster och som stöder informationsöverföring mellan nätanslutningspunkter,

användare: den som använder eller efterfrågar en allmänt tillgänglig elektronisk kommunikationstjänst,

Berec: Organet för europeiska regleringsmyndigheter för elektronisk kommunikation,

elektronisk kommunikationstjänst: en tjänst som vanligen tillhandahålls mot ersättning via elektroniska kommunikationsnät och som – med undantag för dels tjänster i form av tillhandahållande av innehåll som överförs med hjälp av elektroniska kommunikationsnät och elektroniska kommunikationstjänster, dels tjänster som innebär utövande av redaktionellt ansvar över sådant innehåll – är en

1. internetanslutningstjänst enligt artikel 2.2 i Europaparlamentets och rådets förordning (EU) 2015/2120 av den 25 november 2015 om åtgärder rörande en öppen internetanslutning och slutkundsavgifter för reglerad

[1] Jfr 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), i den ursprungliga lydelsen.

[2] Senaste lydelse av 8 kap. 5 § 2022:1086.

kommunikation inom EU och om ändring av direktiv 2002/22/EG och förordning (EU) nr 531/2012,

2. interpersonell kommunikationstjänst, eller

3. tjänst som utgörs helt eller huvudsakligen av överföring av signaler, såsom överföringstjänster som används för tillhandahållande av maskin-till-maskin-tjänster eller för rundradio,

elektroniskt kommunikationsnät: ett system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt passiva nätdelar och andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier, oberoende av vilken typ av information som överförs,

elektroniskt meddelande: all information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst, utom information som överförs som del av sändningar av ljudradio- och tv-program som är riktade till allmänheten via ett elektroniskt kommunikationsnät om inte denna information kan sättas i samband med den enskilda abonnenten eller användaren av informationen,

harmoniserat frekvensutrymme: ett frekvensutrymme för vilket harmoniserade villkor för användning har fastställts i en teknisk genomförandeåtgärd i enlighet med artikel 4 i Europaparlamentets och rådets beslut nr 676/ 2002/EG av den 7 mars 2002 om ett regelverk för radiospektrumpolitiken i Europeiska gemenskapen (radiospektrumbeslut),

integritetsincident: en händelse som leder till oavsiktlig eller otillåten utplåning, förlust eller ändring eller otillåtet avslöjande av eller otillåten åtkomst till uppgifter som behandlas i samband med tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster,

internetåtkomst: möjlighet till överföring av ip-paket som ger användaren tillgång till internet,

interpersonell kommunikationstjänst: en tjänst som vanligen tillhandahålls mot ersättning och som möjliggör ett direkt interpersonellt och interaktivt informationsutbyte via elektroniska kommunikationsnät mellan ett begränsat antal personer, varigenom de personer som inleder eller deltar i kommunikationen bestämmer vem eller vilka som ska vara mottagare av denna, dock inte en tjänst som möjliggör interpersonell och interaktiv kommunikation enbart som en extrafunktion av mindre betydelse som är direkt kopplad till en annan tjänst,

lokaliseringsuppgift:

1. en uppgift som behandlas i ett allmänt mobilt elektroniskt kommunikationsnät och som anger den geografiska positionen för en slutanvändares terminalutrustning, eller

2. en uppgift i ett allmänt fast elektroniskt kommunikationsnät om nätanslutningspunktens fysiska adress,

meddelandehantering: utbyte eller överföring av ett elektroniskt meddelande som inte är ett samtal och inte heller är information som överförs som en del av sändningar av ljudradio- eller tv-program,

mikroföretag: ett företag som, i enlighet med avdelning I i bilagan till kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag, sysselsätter färre än 10 personer och vars omsättning eller balansomslutning inte överstiger 2 miljoner euro per år,

misslyckad uppringning: en uppringning som kopplas fram utan att nå en mottagare,

nummerbaserad interpersonell kommunikationstjänst: en interpersonell kommunikationstjänst som etablerar en förbindelse till nummer i nationella eller internationella nummerplaner eller som möjliggör kommunikation med sådana nummer,

nummeroberoende interpersonell kommunikationstjänst: en interpersonell kommunikationstjänst som varken etablerar en förbindelse till nummer i nationella eller internationella nummerplaner eller möjliggör kommunikation med sådana nummer,

nätanslutningspunkt: en fysisk punkt vid vilken en slutanvändare ansluts till ett allmänt elektroniskt kommunikationsnät,

nät med mycket hög kapacitet: ett elektroniskt kommunikationsnät som helt består av fiberoptik åtminstone fram till slutanvändarnas lokaler eller en basstation eller ett elektroniskt kommunikationsnät som kan erbjuda liknande nätprestanda under normala högtrafikförhållanden,

nödkommunikation: kommunikation med samhällets alarmeringstjänst genom en interpersonell kommunikationstjänst,

operatör: den som tillhandahåller eller avser att tillhandahålla ett allmänt elektroniskt kommunikationsnät eller en tillhörande facilitet,

operatörslås: sådana begränsningar när det gäller användningen av terminalutrustning som en tillhandahållare har infört eller låtit införa för att hindra att utrustningen används för nyttjande av andra tillhandahållares elektroniska kommunikationstjänster,

radioanläggning: en anordning som möjliggör radiokommunikation eller bestämning av position, hastighet eller andra kännetecken hos ett föremål genom sändning av radiovågor (radiosändare) eller mottagning av radiovågor (radiomottagare),

radiokommunikation: överföring, utsändning eller mottagning av tecken, signaler, skrift, bilder, ljud eller meddelanden av varje slag med hjälp av radiovågor,

radiovågor: elektromagnetiska vågor med frekvenser från 9 kilohertz till 3 000 gigahertz som breder ut sig utan särskilt anordnad ledare,

rent grossistföretag: ett företag som inte bedriver verksamhet på någon slutkundsmarknad, inte är närstående till eller genom ägarintressen kontrollerar ett företag som bedriver verksamhet på någon slutkundsmarknad och inte genom avtal är bundet att exklusivt handla med ett enskilt företag som verkar på någon slutkundsmarknad,

samtal: en förbindelse genom en allmänt tillgänglig interpersonell kommunikationstjänst som möjliggör talkommunikation i båda riktningarna,

samtrafik: fysisk och logisk sammankoppling av allmänna elektroniska kommunikationsnät för att göra det möjligt för användare att kommunicera med varandra eller få tillgång till tjänster som tillhandahålls i näten,

skadlig störning: en störning som äventyrar funktionen hos en radionavigationstjänst eller någon annan säkerhetstjänst eller som på något annat sätt allvarligt försämrar, hindrar eller upprepat avbryter en radiokommunikationstjänst som fungerar i enlighet med gällande bestämmelser, inbegripet störning av befintliga eller planerade tjänster på nationellt tilldelade frekvenser,

slutanvändare: en användare som inte tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst,

små företag: företag som, i enlighet med avdelning I i bilagan till kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag, sysselsätter färre än 50 personer och vars omsättning eller balansomslutning inte överstiger 10 miljoner euro per år,

säkerhet i nät och tjänster: elektroniska kommunikationsnäts och elektroniska kommunikationstjänsters förmåga att vid en viss tillförlitlighetsnivå motstå händelser som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos näten eller tjänsterna, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller elektroniska kommunikationstjänster,

säkerhetsincident: en händelse med en faktisk negativ inverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller elektroniska kommunikationstjänster, eller på förmågan att motstå sådana händelser,

talkommunikationstjänst: en allmänt tillgänglig elektronisk kommunikationstjänst som gör det möjligt att ringa och ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan,

telefonitjänst: en elektronisk kommunikationstjänst som innebär en möjlighet att ringa eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan,

tillhörande facilitet: en anordning, funktion eller något annat som har samband med ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och som möjliggör, stöder eller kan stödja tillhandahållande av tjänster via det nätet eller den tjänsten,

trafikuppgift: en uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande,

trådlösa accesspunkter med kort räckvidd: små trådlösa nätanslutningsutrustningar med låg effekt och kort räckvidd som kan vara utrustade med en eller flera antenner med låg visuell inverkan och som gör det möjligt för användare att få trådlös tillgång till elektroniska kommunikationsnät oberoende av om den underliggande nättopologin är mobil eller fast,

trådlösa lokala nät: trådlösa kommunikationssystem med låg effekt och kort räckvidd som på icke-exklusiv grund använder ett harmoniserat frekvensutrymme och som har låg risk för störningar på andra sådana system som utnyttjas av andra användare i omedelbar närhet av systemet,

vertikalt integrerad operatör: en operatör som tillhandahåller tjänster till företag som den konkurrerar med på marknader i efterföljande handelsled.

12 kap.

1 §[3]

Tillsynsmyndigheten ska besluta att ta ut en sanktionsavgift av den som

1. inte tillhandahåller en sammanfattning av avtalet i enlighet med 7 kap. 1 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 102.3 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,

2. inte tillämpar villkor om bindningstid eller uppsägningstid i enlighet med 7 kap. 8, 13 eller 14 §,

3. inte uppfyller kraven på nummerportabilitet i enlighet med 7 kap. 19 och 20 §§ eller föreskrifter om nummerportabilitet som har meddelats med stöd av 7 kap. 21 § första stycket,

4. inte vidtar åtgärder för att hantera risker som hotar säkerheten i nät och tjänster i enlighet med 8 kap. 1 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,

5. inte rapporterar om säkerhetsincidenter i enlighet med 8 kap. 3 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,

6. inte informerar om hot om säkerhetsincidenter i enlighet med 8 kap. 4 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter

[3] Senaste lydelse 2022:1086.

som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,

7. inte vidtar skyddsåtgärder i enlighet med 8 kap. 5 § eller föreskrifter som har meddelats med stöd av den paragrafen,

8. inte vidtar åtgärder för att säkerställa skydd av uppgifter som behandlas i samband med tillhandahållandet av en tjänst i enlighet med 8 kap. 6 § eller föreskrifter som har meddelats med stöd av den paragrafen,

9. inte informerar abonnenten om särskilda risker för bristande skydd av behandlade uppgifter i enlighet med 8 kap. 7 §,

10. inte underrättar om integritetsincidenter i enlighet med 8 kap. 8 § eller 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,

11. inte behandlar uppgifter i ett elektroniskt meddelande eller trafikuppgifter som hör till detta meddelande i enlighet med 9 kap. 27 §,

12. inte bedriver sin verksamhet så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs i enlighet med 9 kap. 29 § första stycket eller föreskrifter som har meddelats i anslutning till det stycket,

13. inte ordnar uppgifter och gör dem tillgängliga i ett format som gör att de enkelt kan tas om hand i enlighet med 9 kap. 29 b § andra stycket eller föreskrifter som har meddelats i anslutning till det stycket,

4. inte vidtar skyddsåtgärder i enlighet med 8 kap. *1 §* eller föreskrifter som har meddelats med stöd av den paragrafen,

5. inte vidtar åtgärder för att säkerställa skydd av uppgifter som behandlas i samband med tillhandahållandet av en tjänst i enlighet med 8 kap. *2 §* eller föreskrifter som har meddelats med stöd av den paragrafen,

6. inte informerar abonnenten om särskilda risker för bristande skydd av behandlade uppgifter i enlighet med 8 kap. *3 §*,

7. inte underrättar om integritetsincidenter i enlighet med 8 kap. *4 §* eller 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,

8. inte behandlar uppgifter i ett elektroniskt meddelande eller trafikuppgifter som hör till detta meddelande i enlighet med 9 kap. 27 §,

9. inte bedriver sin verksamhet så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs i enlighet med 9 kap. 29 § första stycket eller föreskrifter som har meddelats i anslutning till det stycket,

10. inte ordnar uppgifter och gör dem tillgängliga i ett format som gör att de enkelt kan tas om hand i enlighet med 9 kap. 29 b § andra stycket eller föreskrifter som har meddelats i anslutning till det stycket,

14. inte överför signaler till samverkanspunkter i enlighet med 9 kap. 30 § eller föreskrifter som har meddelats med stöd av den paragrafen, eller	*11*. inte överför signaler till samverkanspunkter i enlighet med 9 kap. 30 § eller föreskrifter som har meddelats med stöd av den paragrafen, eller
15. inte lämnar ut en uppgift i enlighet med 9 kap. 33 §.	*12*. inte lämnar ut en uppgift i enlighet med 9 kap. 33 §.

En sanktionsavgift enligt första stycket 2 ska, när det är fråga om ett paket enligt 7 kap. 26 §, tas ut endast om överträdelsen avser en allmänt tillgänglig elektronisk kommunikationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst eller en överföringstjänst som används för tillhandahållande av maskin-till-maskintjänster.

---

1. Denna lag träder i kraft den 15 januari 2026.
2. Äldre bestämmelser gäller fortfarande för överträdelser som skett före ikraftträdandet.

3 Ärendet och dess beredning

Europaparlamentet och rådet antog den 14 december 2022 direktiv (EU) 2022/2555 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), se *bilaga 1*. Samma dag antogs Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, i det följande benämnt CER-direktivet. Medlemsstaterna ska senast den 17 oktober 2024 ha antagit de nationella bestämmelser som krävs för att genomföra direktiven.

Regeringen beslutade den 23 februari 2023 att ge en särskild utredare i uppdrag att föreslå hur de två direktiven ska genomföras i svensk rätt (dir. 2023:30). Utredningen antog namnet Utredningen om genomförande av NIS2- och CER-direktiven (Fö 2023:01). I mars 2024 överlämnade utredningen sitt delbetänkande Nya regler om cybersäkerhet (SOU 2024:18) som behandlar genomförandet av NIS 2-direktivet. En sammanfattning av delbetänkandet finns i *bilaga 2* och delbetänkandets lagförslag finns i *bilaga 3*. Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 4*. Remissvaren finns tillgängliga på regeringens webbplats (regeringen.se) och i lagstiftningsärendet (Fö2024/00496).

Utredningen överlämnade i september 2024 sitt slutbetänkande Motståndskraft i samhällsviktiga tjänster (SOU 2024:64) som behandlar genomförandet av CER-direktivet samt vissa frågor om samordningen mellan kraven i direktiven. I slutbetänkandet föreslås bland annat ändringar i offentlighets- och sekretesslagen (2009:400) kopplat till genomförandet av NIS 2-direktivet. En sammanfattning av slutbetänkandet finns i *bilaga 5* och slutbetänkandets lagförslag i aktuella delar finns i *bilaga 6*. Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 7*. Remissvaren finns tillgängliga på regeringens webbplats (regeringen.se) och i lagstiftningsärendet (Fö2024/01550).

I denna lagrådsremiss behandlas utredningens lagförslag i delbetänkandet och utredningens förslag i slutbetänkandet om ändringar i offentlighets- och sekretesslagen kopplat till genomförandet av NIS 2-direktivet. Utredningens övriga förslag avseende bland annat genomförandet av CER-direktivet bereds vidare inom Regeringskansliet.

4 NIS 2-direktivets bakgrund, syfte och huvudsakliga innehåll

4.1 NIS-direktivet

Det så kallade NIS-direktivet, det vill säga Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen, upphörde att gälla den 18 oktober 2024. NIS-direktivet har ersatts av NIS 2-direktivet, det vill säga 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).

Syftet med NIS-direktivet var att förbättra den inre marknadens funktion genom att bland annat fastställa åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverks- och informationssystem inom unionen. Direktivet innebar bland annat att vissa leverantörer av samhällsviktiga respektive digitala tjänster skulle vidta säkerhetsåtgärder för att hantera risker och förebygga incidenter i nätverks- och informationssystem som de använder för att kunna tillhandahålla tjänsterna. Leverantörerna skulle också rapportera incidenter som hade en betydande respektive avsevärd inverkan på kontinuiteten i tjänsterna.

NIS-direktivet gällde för leverantörer av samhällsviktiga tjänster inom sju särskilt utpekade sektorer: energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. Därutöver gällde direktivet för leverantörer av digitala tjänster. Medlemsstaterna var enligt direktivet skyldiga att dels upprätta en förteckning över de tjänster som är samhällsviktiga, dels identifiera de leverantörer på deras territorium som tillhandahåller sådana tjänster. De leverantörer av digitala tjänster som omfattades av direktivet var sådana som tillhandahåller internetbaserade marknadsplatser, internetbaserade sökmotorer eller molntjänster.

Medlemsstaterna skulle enligt NIS-direktivet utse myndigheter med särskilda uppgifter, till exempel tillsynsmyndigheter, nationella kontaktpunkter och enheter för hantering av incidenter, så kallade CSIRT-enheter (Computer Security Incident Response Team). Medlemsstaterna skulle också säkerställa att tillsynsmyndigheterna hade befogenheter och medel för att kontrollera att berörda leverantörer uppfyllde sina skyldigheter enligt direktivet och fastställa regler om sanktioner för överträdelse av de nationella bestämmelser som hade antagits. NIS-direktivet innehöll vidare en skyldighet för varje medlemsstat att anta en nationell strategi för säkerhet i nätverks- och informationssystem.

När det gällde leverantörer av samhällsviktiga tjänster fick medlemsstaterna anta eller behålla bestämmelser som syftade till att uppnå en högre nivå på säkerheten i nätverks- och informationssystem än vad som angavs i direktivet. För leverantörer av digitala tjänster fick medlemsstaterna emellertid inte införa ytterligare säkerhets- eller rapporteringskrav.

NIS-direktivet genomfördes i svensk rätt genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen) och den tillhörande förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-förordningen).

4.2 NIS 2-direktivet

I NIS 2-direktivet anges att en översyn av NIS-direktivet har visat inneboende brister som hindrar det sistnämnda direktivet från att effektivt hantera befintliga och framväxande utmaningar på cybersäkerhetsområdet (skäl 2). Vidare anges att översynen har visat på stora skillnader i med-

lemsstaternas genomförande av NIS-direktivet som har medfört en fragmentering av den inre marknaden och som kan ha en skadlig inverkan på dess funktion. Det anges också att NIS 2-direktivets mål är att undanröja skillnaderna mellan medlemsstaterna (skäl 4 och 5). Mot denna bakgrund upphävdes NIS-direktivet och ersattes av NIS 2-direktivet.

Syftet med NIS 2-direktivet är att förbättra den inre marknadens funktion genom att fastställa åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen (artikel 1.1). NIS 2-direktivet innebär skärpta krav på berörda aktörer jämfört med NIS-direktivet och omfattar betydligt fler aktörer.

NIS 2-direktivet är tillämpligt på offentliga eller privata entiteter av den typ som avses i direktivets bilaga 1 eller 2, som uppfyller ett visst storleks-krav och som tillhandahåller sina tjänster eller bedriver sin verksamhet i unionen (artikel 2.1). Med uttrycket entitet avses enligt artikel 6.38 en fysisk eller juridisk person som bildats och erkänts som sådan enligt nationell rätt där den etablerats och som i eget namn får utöva rättigheter och ha skyldigheter. Direktivet är även tillämpligt på vissa entiteter oavsett storlek (artikel 2.2–2.4). I bilaga 1 och 2 till direktivet anges de 18 sektorer, uppdelade i högkritiska och andra kritiska sektorer, som omfattas av direktivet:

- energi
- transporter
- bankverksamhet
- finansmarknadsinfrastruktur
- hälso- och sjukvårdssektorn
- dricksvatten
- avloppsvatten
- digital infrastruktur
- förvaltning av IKT-tjänster (mellan företag)
- offentlig förvaltning
- rymden
- post- och budtjänster
- avfallshantering
- tillverkning, produktion och distribution av kemikalier
- produktion, bearbetning och distribution av livsmedel
- tillverkning
- digitala leverantörer
- forskning

Entiteter som omfattas av direktivet ska antingen anses vara väsentliga eller viktiga beroende på bland annat vilken sorts entitet det är fråga om och entitetens storlek (artikel 3). Denna indelning påverkar bland annat vilka tillsynsåtgärder som kan komma i fråga. Medlemsstaterna ska senast den 17 april 2025 upprätta en förteckning över väsentliga och viktiga entiteter och regelbundet uppdatera den (artikel 3.3).

Genom NIS 2-direktivet har kraven skärpts på vilka åtgärder berörda aktörer ska vidta för att bland annat hantera risker och förhindra incidenter kopplade till nätverks- och informationssystem som de använder (artikel 21). Dessutom har mer precisa rapporteringsskyldigheter införts,

bland annat avseende skyldigheten att på visst sätt rapportera alla betydande incidenter till en utpekad myndighet (artikel 23). I syfte att harmonisera sanktionssystemen i medlemsstaterna innehåller NIS 2-direktivet även bestämmelser om tillsyns- och efterlevnadskontrollåtgärder samt sanktioner (artiklarna 32–36).

I likhet med vad som gällde enligt NIS-direktivet ska medlemsstaterna utse en eller flera behöriga myndigheter och en nationell gemensam kontaktpunkt (artikel 8). De behöriga myndigheterna ska utöva tillsyn och övervaka tillämpningen av direktivet på nationell nivå (artiklarna 31–33). Den nationella gemensamma kontaktpunkten ska ha en sambandsfunktion som säkerställer gränsöverskridande samarbete mellan medlemsstatens myndigheter och relevanta myndigheter i andra medlemsstater samt ett sektorsövergripande samarbete mellan de nationella behöriga myndigheterna i medlemsstaten. NIS 2-direktivet föreskriver, i likhet med vad som gällde enligt NIS-direktivet, att det ska finnas en eller flera enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter) med vissa närmare angivna uppgifter (artiklarna 10–15). Vidare ska medlemsstaterna utse en eller flera behöriga myndigheter, så kallade cyberkrishanteringsmyndigheter, som ska ansvara för hanteringen av storskaliga cybersäkerhetsincidenter och cyberkriser (artikel 9).

NIS 2-direktivet ställer upp strängare krav på strategiskt och operativt samarbete mellan medlemsstaterna än NIS-direktivet. Genom NIS-direktivet inrättades bland annat en samarbetsgrupp för att stödja och underlätta strategiskt samarbete och utbyte av information mellan medlemsstaterna samt ett nätverk för nationella CSIRT-enheter. I och med NIS 2-direktivet stärks det befintliga samarbetet inom samarbetsgruppen och såväl denna samarbetsgrupp som CSIRT-nätverket får delvis nya uppgifter (artiklarna 14 och 15).

Genom NIS 2-direktivet inrättas även nya forum för samarbete mellan medlemsstaterna. Ett av dessa är det europeiska kontaktnätverket för cyberkriser, EU-CyCLONe (artikel 16). Nätverket, som ska verka stödjande vid samordning och hantering av storskaliga incidenter och cyberkriser, får genom direktivet en tydlig rättslig grund. I likhet med NIS-direktivet föreskriver NIS 2-direktivet också en skyldighet för medlemsstaterna att anta en nationell strategi för cybersäkerhet (artikel 7).

NIS 2-direktivet är ett så kallat minimidirektiv, vilket innebär att medlemsstaterna får anta eller behålla bestämmelser som säkerställer en högre cybersäkerhetsnivå, förutsatt att sådana bestämmelser står i överensstämmelse med medlemsstaternas förpliktelser enligt unionsrätten (artikel 5). Medlemsstaterna ska enligt NIS 2-direktivet anta och offentliggöra de bestämmelser som är nödvändiga för att följa direktivet senast den 17 oktober 2024 och tillämpa bestämmelserna från och med den 18 oktober samma år.

5 En ny cybersäkerhetslag

5.1 Direktivet ska genomföras genom en ny lag

Regeringens förslag: NIS 2-direktivet ska i huvudsak genomföras genom en ny cybersäkerhetslag.

Syftet med den nya lagen ska vara att uppnå en hög nivå av cybersäkerhet i samhället.

Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster ska upphävas.

Utredningens förslag överensstämmer i allt väsentligt med regeringens. Utredningen föreslår att syftet med lagen ska vara att uppnå en hög cybersäkerhetsnivå och att lagen ska benämnas lag om cybersäkerhet.

Remissinstanserna: Majoriteten av remissinstanserna tillstyrker förslaget om att införa en ny cybersäkerhetslag, exempelvis *Myndigheten för digital förvaltning*, *Post- och telestyrelsen* och ett antal kommuner och regioner.

Bland andra *Malmö kommun* och *Netnod AB*, anser att lagens föreslagna rubrik är missvisande. Ett flertal remissinstanser, däribland *Certezza AB* och *Tech Sverige* anser att lagens syfte bör förtydligas. Ett antal remissinstanser, däribland *Svenskt Näringsliv* och Tech Sverige, framhåller behovet av att värna företagen i utformningen av lagstiftningen och att införa en reglering som är proportionerlig och lämplig utifrån en jämförelse med övriga EU-länder.

Skälen för regeringens förslag

En ny lag bör införas

NIS-direktivet genomfördes i huvudsak i svensk rätt genom NIS-lagen. I samband med genomförandet gjordes överväganden kring huruvida direktivet skulle genomföras genom ett samlat regelverk, det vill säga i huvudsak genom en ny lag med anslutande förordning, eller genom flera olika sektorsspecifika regelverk. Regeringen bedömer i likhet med utredningen att NIS 2-direktivet bör genomföras på motsvarande sätt som NIS-direktivet, det vill säga i ett samlat regelverk.

NIS 2-direktivet skiljer sig från NIS-direktivet på flera sätt, bland annat genom att regleringen omfattar betydligt fler aktörer och ställer tydligare krav på det som i direktivet benämns som riskhanteringsåtgärder. Syftet med NIS 2-direktivet är också formulerat på ett annat sätt än i NIS-direktivet. Det skulle krävas mycket omfattande ändringar av NIS-lagen för att anpassa lagen till det nya direktivet. Regeringen bedömer därför, som utredningen, att det är lämpligast att NIS 2-direktivet genomförs i en ny lag och att NIS-lagen upphävs.

Lagens syfte och namn

I artikel 1 i NIS 2-direktivet anges att direktivet fastställer åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen, i syfte att förbättra den inre marknadens funktion.

Uttrycket cybersäkerhet definieras i NIS 2-direktivet genom hänvisning till artikel 2.1 i EU:s cybersäkerhetsakt, det vill säga 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 526/2103 (cybersäkerhetsakten). Cybersäkerhet definieras därmed som all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot.

Även uttrycket cyberhot definieras i NIS 2-direktivet genom en hänvisning till artikel 2.8 i EU:s cybersäkerhetsakt. Cyberhot definieras därmed som en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare av dessa system och andra personer.

Utredningen föreslår att den nya lagen ska innehålla en inledande bestämmelse om lagens syfte och att syftet ska vara att uppnå en hög cybersäkerhetsnivå. Ett flertal remissinstanser efterfrågar ett förtydligande av vad det sistnämnda innebär. *Tech Sverige* anser exempelvis att det krävs ett förtydligande i fråga om lagen syftar till att främja den inre marknaden.

Regeringen anser, i likhet med *Certezza AB*, att lagens syfte bör vara att uppnå en hög nivå av cybersäkerhet i samhället. Sveriges cybersäkerhet påverkas av ett antal sårbarheter som kan ha olika ursprung och manifestera sig inom ett antal områden. Dessa sårbarheter kan samlat eller var för sig utgöra strategiska sårbarheter i ett digitaliserat samhälles cybersäkerhetslandskap och riskera att påverka samhällsviktig verksamhet och ytterst Sveriges säkerhet. Den lag som genomför NIS 2-direktivet i Sverige måste ta sin utgångspunkt i denna hotbild och dessa utmaningar. Även om regelverket som genomför NIS 2-direktivet delvis tar sin utgångspunkt i nationella behov kommer det i förlängningen också att bidra till att främja den inre marknaden.

Bland andra *Svenskt Näringsliv* och Tech Sverige framhåller behovet av att införa en reglering som är proportionerlig och lämplig utifrån en jämförelse med övriga EU-länder. Det finns inte utrymme för att inom ramen för denna lagrådsremiss göra en jämförelse av hur direktivet har genomförts i samtliga medlemsstater. Det bör vidare beaktas att direktivet är ett så kallat minimidirektiv och att det därmed finns utrymme för medlemsstaterna att införa krav som går längre än direktivets. Det är ofrånkomligt att direktivet i viss utsträckning kommer att genomföras på olika sätt i olika medlemsstater utifrån de tolkningar och överväganden om behov som görs i de nationella lagstiftningsärendena.

Utredningen föreslår att lagen ska benämnas lag om cybersäkerhet. *Netnod AB* för ett resonemang om att den nya lagen tar sikte på det som brukar kallas för ledningssystem för informationssäkerhet och inte kan anses beröra cybersäkerhet i dess helhet. *Malmö kommun* anser att rubriken även bör innefatta uttrycket informationssäkerhet. Regeringen bedömer, vilket utvecklas i avsnitt 5.2, att uttrycket informationssäkerhet inte tillför något i sak i förhållande till uttrycket cybersäkerhet. Regeringen bedömer vidare att den nya lagen, med hänvisning till sitt innehåll och trots Netnod AB:s invändningar, bör kallas cybersäkerhetslag.

5.2 Uttryck i lagen och hänvisningar till EU-rättsakter

Regeringens förslag: Vissa uttryck som används i den nya lagen ska definieras.

Hänvisningar i lagen till EU-direktiv ska vara statiska medan hänvisningar till EU-förordningar ska vara dynamiska.

Regeringens bedömning: Definitionerna bör i huvudsak motsvara dem som finns i direktivet.

Utredningens förslag och bedömning överensstämmer delvis med regeringens. Utredningen föreslår att ett flertal uttryck som inte används i lagen ska definieras i densamma. Utredningen bedömer att definitionerna som utgångspunkt ska utformas utifrån den systematik och terminologi som används i nationell rätt. Utredningens hänvisningar till EU-rättsakter är dynamiska.

Remissinstanserna: Ett flertal remissinstanser, bland andra *Svensk Handel* och *Tillväxtverket*, stödjer användningen av vedertagna begrepp.

Certezza AB anser att det tydligt bör framgå av definitionen av uttrycket utlokaliserade säkerhetstjänster att tjänsterna har en koppling till leverantörer som tillhandahåller utlokaliserade driftstjänster. *Hi3G Access AB (Tre)* bedömer att definitionerna rent författningstekniskt bör utformas på ett mer enhetligt sätt än vad utredningen föreslår. Tre påpekar att till exempel uttrycket betydande cyberhot definieras i lagen, medan det i en annan definition finns en hänvisning till EU:s cybersäkerhetsakt. Många remissinstanser, däribland *Malmö kommun* och *Post- och telestyrelsen (PTS)*, invänder mot att uttrycket cybersäkerhet ska ersätta det mer väletablerade uttrycket informationssäkerhet eller efterfrågar klargöranden i fråga om hur de olika begreppen förhåller sig till varandra. *Sparbankernas Riksförbund* anser att det bör övervägas att direkt i den nya lagen ange vilka verksamhetsutövare som lagen gäller för i stället för att hänvisa till bilagor till NIS 2-direktivet. *Sveriges advokatsamfund* påpekar att många av de uttryck som definieras i direktivet används i olika sammanhang och definieras på olika sätt i olika EU-rättsakter, vilket riskerar att leda till begreppsförvirring. Även *Stockholms universitet* påtalar att den lagstiftningsteknik som används i lagen, där flera uttryck definieras genom hänvisning till andra rättskällor, inte bidrar till att underlätta läsningen och att ett grundkrav är att explicit förklara de uttryck som används i lagen.

Skälen för regeringens förslag och bedömning: I artikel 6 i NIS 2-direktivet finns definitioner av uttryck som används i direktivet. Motsvarande uttryck bör som utgångspunkt även definieras i den nya lagen under förutsättning att de används i lagen. Utredningen anser att direktivet inte ska införlivas direktivnära i detta avseende utan att förslagen ska utformas utifrån den systematik och terminologi som används i svensk rätt.

I direktivet används en rad facktermer, förkortningar och uttryck, till exempel DNS-tjänster och utlokaliserad driftstjänst. Flera av dessa härrör från andra EU-rättsakter på cyberområdet. Uttrycken kan antingen anpassas så långt det är möjligt till ett språkbruk som ligger närmare nationell lagstiftning eller så kan den terminologi som används i EU-rättsakterna användas även i den nya lagen.

Regeringen har förståelse för bland annat *Svensk Handels* ståndpunkt att etablerade begrepp bör användas i den nya lagen och delar även *Tres* uppfattning att en enhetlig systematik är eftersträvansvärd. En direktivsnära terminologi underlättar dock både anpassningen till och tolkningen av den nya lagen. Att avvika från den terminologi som används i NIS 2-direktivet och de rättsakter som direktivet hänvisar till skulle kunna innebära ett felaktigt eller otillräckligt genomförande av direktivet och även motverka ett harmoniserat genomförande av direktivet inom EU.

Övervägande skäl talar således enligt regeringen för att terminologin som används i den nya lagen så långt det är möjligt ska stämma överens med terminologin i NIS 2-direktivet, även om viss anpassning till nationell rätt måste göras för att underlätta tillämpningen. I linje med detta bör författningstexten som utgångspunkt följa direktivets utformning.

Lagtexten bör, som *Stockholms universitet* nämner, vara lättillgänglig. Det framstår dock inte som ändamålsenligt att återge innehållet i bilagorna till NIS 2-direktivet i lagen som *Sparbankernas Riksförbund* föreslår. Hänvisningar till EU-rättsakter kan också i vissa andra fall, med hänvisning till bland annat i vilken takt förändringar sker på cybersäkerhetsområdet, vara en mer ändamålsenlig lösning än att skriva ut innebörden av ett visst uttryck i lagen.

För att säkerställa att ändringarna i de EU-rättsakter som är förordningar får omedelbart genomslag bör hänvisningarna till dessa vara dynamiska. När det rör sig om hänvisningar till direktiv i lagen bör dock hänvisningarna vara statiska och därmed avse EU-rättsakten i dess lydelse vid en viss tidpunkt. Som *Sveriges advokatsamfund* påpekar används det i NIS 2-direktivet begrepp som också förekommer i andra rättsakter. Regeringen kan inte se att denna omständighet bör påverka hur definitionerna utformas i den lag som genomför direktivet.

Definitionerna i den nya lagen bör alltså som utgångspunkt motsvara definitionerna i direktivet. Vissa rättelser har gjorts av direktivet som utredningen inte har kunnat ta hänsyn till. Uttrycken hanterade säkerhetstjänster och hanterade tjänster, som används i utredningens förslag till lag, bör ersättas med termerna utlokaliserade säkerhetstjänster och utlokaliserade driftstjänster. Som *Certezza AB* påpekar krävs enligt direktivet att en leverantör av hanterade säkerhetstjänster även är en leverantör av utlokaliserade driftstjänster, vilket bör framgå av definitionen.

Flera remissinstanser, däribland *PTS*, anser att uttrycket cybersäkerhet inte är heltäckande utan att uttrycket informationssäkerhet bör användas i lagen. Syftet med NIS 2-direktivet är att uppnå en hög cybersäkerhetsnivå. Uttrycket cybersäkerhet definieras i direktivet som all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot. Att använda uttrycket informationssäkerhet i lagen skulle enligt regeringens mening inte tillföra något i förhållande till uttrycket cybersäkerhet i angiven betydelse.

5.3 Lagens tillämpningsområde

5.3.1 Benämning av dem som omfattas av lagen

Regeringens förslag: De som omfattas av lagen ska benämnas verksamhetsutövare och delas in i enskilda verksamhetsutövare respektive offentliga verksamhetsutövare.

Hela verksamheten hos en verksamhetsutövare ska som utgångspunkt omfattas av lagen.

Utredningens förslag överensstämmer i allt väsentligt med regeringens. Utredningen föreslår att uttrycket verksamhetsutövare ska definieras som en fysisk eller juridisk person som bedriver verksamhet. Utredningen föreslår också att det ska anges att uttrycket är en samlingsterm för bland annat leverantör, producent, vårdgivare, leverantör eller tillhandahållare.

Remissinstanserna: Flera remissinstanser, bland annat flera länsstyrelser och *Transportstyrelsen*, anser att uttrycket verksamhetsutövare är ett lämpligt samlingsbegrepp för dem som träffas av lagen. *Advokatfirman Kahn Pedersen* och *Affärsverket svenska kraftnät* motsätter sig att uttrycket används. Affärsverket svenska kraftnät påtalar att det inte framgår av den föreslagna definitionen vilken sorts aktivitet som avses med formuleringen bedriver verksamhet och anser att definitionen inte innebär en tillräcklig avgränsning. Advokatfirman Kahn Pedersen pekar på att den nya lagen och säkerhetsskyddslagen (2018:585) i vissa fall har ett helt eller delvis överlappande tillämpningsområde och att det därför är olyckligt om samma term används för att definiera vilka som omfattas av respektive lag.

Merparten av länsstyrelserna tillstyrker förslaget att verksamhetsutövaren som helhet ska omfattas av lagen och framhåller att ett fullgott informationssäkerhetsarbete bygger på att hela verksamheten integreras då informationssystem har kopplingar till verksamheten i stort. Många remissinstanser, bland andra *Företagarna*, *Lantmännen*, *Svenskt Näringsliv* och *Tele2 Sverige AB (Tele2)* motsätter sig dock att förslaget om att hela verksamheten ska omfattas genomförs. Exempelvis Svenskt Näringsliv bedömer att förslaget i denna del innebär en överimplementering av direktivet. *Scrive AB* menar att artikel 21 i NIS 2-direktivet ger stöd åt tolkningen att endast vissa nätverks- och informationssystem ska omfattas av direktivets krav på riskhanteringsåtgärder. *Eskilstuna Kommunfastigheter* anser att förslaget innebär ett oproportionerligt tillämpningsområde. *AMF Fastigheter*, *Netnod AB* och *Stiftelsen för internetinfrastruktur (Internetstiftelsen)* framför att utredningens förslag kan slå orimligt hårt mot mindre aktörer.

Drivkraft Sverige och *Energiföretagen Sverige* efterfrågar vägledning från tillsynsmyndigheterna i fråga om hur säkerhetsåtgärder ska appliceras på de delar av verksamheten som inte är av betydelse för den samhällsviktiga verksamheten. *Myndigheten för samhällsskydd och beredskap (MSB)* föreslår att lagens tillämpningsområde ska anpassas efter beredskapslagstiftningen. MSB anser även att myndigheten bör få i uppdrag att ta fram underlag för att utvidga tillämpningsområdet så att det omfattar de sektorer som är betydelsefulla ur ett totalförsvarsperspektiv.

Skälen för regeringens förslag

De som omfattas av lagen bör benämnas verksamhetsutövare

I direktivet benämns de som omfattas av regleringen som entiteter. En entitet definieras i artikel 6 som en fysisk eller juridisk person som bildats och erkänts som sådan och som i eget namn får utöva rättigheter och ha skyldigheter. Av direktivets bilaga 1 och 2 framgår att det är fysiska eller juridiska personer som bedriver verksamhet inom vissa områden som omfattas av direktivet.

I likhet med utredningen anser regeringen att utformningen av lagen i största möjliga mån ska präglas av ett enkelt och lättillgängligt språkbruk. Utredningen föreslår att uttrycket verksamhetsutövare ska användas i lagen i stället för entitet och att uttrycket ska definieras som en fysisk eller juridisk person som bedriver verksamhet. Verksamhetsutövare är ett vedertaget begrepp och används exempelvis i säkerhetsskyddslagen. Regeringen anser inte att det skäl som *Advokatfirman Kahn Pedersen* framför talar emot att uttrycket används även i den nya lagen.

I säkerhetsskyddslagen knyts uttrycket verksamhetsutövare till en viss typ av verksamhet och avser den som till någon del bedriver säkerhetskänslig verksamhet. Som *Affärsverket svenska kraftnät* påtalar framgår det inte av den definition som utredningen föreslår vilken slags aktivitet som avses med formuleringen bedriver verksamhet.

Regeringen anser, till skillnad mot utredningen, inte att det krävs någon definition av uttrycket verksamhetsutövare. Däremot bör de som omfattas av lagen benämnas verksamhetsutövare som ett samlingsbegrepp. De som omfattas av lagen bör, som utredningen föreslår, delas in i enskilda verksamhetsutövare respektive offentliga verksamhetsutövare (se vidare avsnitt 5.3.2–5.3.4).

Verksamhetsutövaren bör som utgångspunkt omfattas i sin helhet

En verksamhetsutövare kan, som utredningen nämner, bedriva verksamhet inom flera olika områden varav endast ett faller inom någon av de sektorer som föreslås omfattas av lagen. Frågan är då om enbart den del av verksamhetsutövarens verksamhet som omfattas av en utpekad sektor ska träffas av den nya lagen eller om verksamhetsutövaren i sin helhet ska omfattas i enlighet med utredningens förslag.

Det framgår inte av direktivet om enbart den verksamhetsgren som omfattas av en av de utpekade sektorerna omfattas av direktivets tillämpningsområde. Flera remissinstanser, bland andra *Tele2*, bedömer att NIS 2-direktivet, i likhet med NIS-direktivet, endast omfattar de nätverks- och informationssystem som används för att tillhandahålla den reglerade tjänsten. Regeringen anser att frågan om hur lagen ska utformas i detta avseende måste besvaras utifrån direktivets syfte.

Syftet med NIS 2-direktivet är att förbättra den inre marknadens funktion genom att fastställa åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen. Ett av direktivets mål är att undanröja skillnaderna i medlemsstaternas genomförande av NIS-direktivet genom att bland annat föreskriva minimiregler för ett fungerande samordnat regelverk. Regeringen delar utredningens uppfattning att direktivets utformning talar för att hela verksamhetsutövaren bör omfattas av lagens tillämpningsområde.

Regeringen gör exempelvis motsatt tolkning av artikel 21.1 i NIS 2-direktivet jämfört med den som *Scrive AB* redogör för. Enligt bestämmelsen ska medlemsstaten säkerställa att entiteter vidtar vissa åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster. Scrive AB anser att uttrycket verksamhet syftar på de i bilagorna utpekade verksamheterna. Enligt regeringens mening bör uttrycket dock ta sikte på verksamhetsutövarens verksamhet i sin helhet eftersom artikeln behandlar medlemsstaters tillsynsansvar i förhållande till verksamhetsutövare som omfattas av direktivet.

Oavsett tolkning av direktivets innebörd kan det också konstateras att direktivet är ett så kallat minimidirektiv vilket innebär att medlemsstaterna får införa bestämmelser som ger en högre cybersäkerhetsnivå än vad direktivet kräver. Regeringen bedömer, i likhet med till exempel *Eskilstuna Kommunfastigheter* och *Internetstiftelsen*, att lagens tillämpningsområde inte får bli oproportionerligt omfattande. Regeringen ser emellertid en risk med att låta endast en del av verksamhetsutövarens verksamhet omfattas av lagens tillämpningsområde. En incident i en del av verksamheten som inte omfattas av lagens krav skulle kunna påverka även andra delar av verksamheten. Det skulle också kunna uppstå gränsdragningsproblem när det gäller att bestämma vilka system i en verksamhet som omfattas av lagen och därmed olika tolkningar bland verksamhetsutövarna. Regeringen anser därför att en verksamhetsutövare som bedriver verksamhet inom någon av de utpekade sektorerna, och som i övrigt uppfyller de föreslagna kriterierna för att omfattas av lagen, bör omfattas av regelverkets krav i sin helhet i enlighet med utredningens förslag (jfr dock avsnitt 5.4.2).

Flera remissinstanser, bland andra *Svenskt Näringsliv*, anser att utredningens förlag är en överimplementering av direktivet och att en sådan kan få negativa konsekvenser för svenska företags konkurrenskraft och även öka företagens administrativa kostnader. Som anges ovan bedömer regeringen att direktivets utformning talar för att hela verksamheten ska omfattas och att det därmed inte är fråga om ett genomförande som går utöver direktivets krav. I fråga om vilken inverkan förslagen kan få på svenska företags konkurrenskraft kan det konstateras att direktivet har genomförts på motsvarande sätt som utredningen föreslår i bland annat Finland (RP 57/2024 rd, s. 150). Som utvecklas i avsnitt 14.3 kan förslagen innebära vissa kostnader och administrativa bördor för enskilda verksamhetsutövare. Det saknas utrymme att inom ramen för denna lagrådsremiss ge uppdrag om vägledning som *Drivkraft Sverige* och *Energiföretagen Sverige* efterfrågar. Det finns inte heller utrymme för att föreslå ett ändrat tillämpningsområde eller ge ett uppdrag i enlighet med MSB:s synpunkter.

5.3.2 Vilka ska omfattas av lagen?

Regeringens förslag: Lagen ska gälla för en verksamhetsutövare som i Sverige tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster.

Lagen ska även gälla för en verksamhetsutövare som har huvudsakligt etableringsställe i Sverige, eller en företrädare som är etablerad i Sverige, och som är en registreringsenhet för toppdomäner eller erbjuder DNS-tjänster eller domännamnsregistreringstjänster.

Lagen ska vidare gälla för en verksamhetsutövare som har huvudsakligt etableringsställe i Sverige, eller en företrädare som är etablerad i Sverige, storleksmässigt motsvarar eller är större än ett medelstort företag, och erbjuder molntjänster, datacentraltjänster, nätverk för leverans av innehåll, utlokaliserade driftstjänster, utlokaliserade säkerhetstjänster, marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster.

Lagen ska även gälla för en verksamhetsutövare som är etablerad i Sverige och tillhandahåller betrodda tjänster.

Lagen ska också gälla för en verksamhetsutövare som omfattas av bilaga 1 eller 2 till NIS 2-direktivet i övrigt och är etablerad i Sverige samt en verksamhetsutövare som erbjuder molntjänster, datacentraltjänster, nätverk för leverans av innehåll, utlokaliserade driftstjänster, utlokaliserade säkerhetstjänster, marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster, om

- verksamhetsutövaren är den enda leverantören av en tjänst i Sverige som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet,
- en störning av den tjänst som verksamhetsutövaren tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa eller kan medföra betydande systemrisker, eller
- verksamhetsutövaren har särskild betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer som är beroende av verksamhetsutövaren.

Lagen ska därutöver gälla för en annan verksamhetsutövare som omfattas av bilaga 1 eller 2 till NIS 2-direktivet i övrigt, om verksamhetsutövaren är etablerad i Sverige och storleksmässigt motsvarar eller är större än ett medelstort företag.

Ett medelstort företag ska i lagen definieras som ett företag som, utan beaktande av artikel 3.4, räknas som ett medelstort företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela ytterligare föreskrifter om kriterier för när verksamhetsutövare ska omfattas av lagen med hänvisning till sin särskilda betydelse och för när sådana ska räknas som väsentliga verksamhetsutövare.

Regeringen eller den myndighet som regeringen bestämmer ska också få meddela föreskrifter om vad som utgör huvudsakligt etableringsställe och om undantag från skyldigheterna enligt lagen för vissa partnerföretag och anknutna företag.

Regeringen eller den myndighet som regeringen bestämmer ska, i enskilda fall, om det finns särskilda skäl, få besluta om undantag från skyldigheterna enligt lagen för vissa partnerföretag och anknutna företag.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen benämner vissa enskilda verksamhetsutövare som gränsöverskridande verksamhetsutövare. Utredningen föreslår att lagen som utgångspunkt ska gälla för en enskild verksamhetsutövare som bland annat överskrider villkoren för medelstort företag och lämnar inget förslag om reglering gällande undantaget för företag som kontrolleras av ett offentligt organ. Utredningen föreslår att det ska regleras i förordning vad som avses med huvudsakligt etableringsställe men lämnar inget förslag om att det även ska kunna regleras i andra föreskrifter på lägre normgivningsnivå än lag. Utredningen föreslår att regeringen eller den myndighet som regeringen bestämmer i föreskrifter ska få meddela undantag i enskilda fall från storlekskravet avseende partnerföretag eller anknutna företag som inte i sig uppfyller storlekskravet. Utredningen föreslår ingen definition av begreppet medelstort företag. Utredningen föreslår att en verksamhetsutövare ska omfattas av lagen bland annat om verksamheten är väsentlig för att upprätthålla kritiska funktioner i samhället och ekonomiska funktioner.

Remissinstanserna: Ett mycket stort antal remissinstanser, bland andra *Lantbrukarnas riksförbund*, *Livsmedelsverket* och *Naturvårdsverket*, efterfrågar förtydliganden kring vilka verksamhetsutövare som omfattas av respektive sektor som nämns i bilaga 1 och 2 till direktivet. Bland andra *Statens energimyndighet* föreslår, i likhet med utredningen, att regeringen ska ge tillsynsmyndigheten i uppdrag att med stöd av Myndigheten för samhällsskydd och beredskap (MSB) utforma vägledning till stöd för enskilda verksamhetsutövare. *Post- och telestyrelsen (PTS)* och *Tech Sverige* förordar en restriktiv tolkning av leverantör av DNS-tjänster och anser att uttryckets innebörd bör tydliggöras. *Transportstyrelsen* anser att tillämpningsområdet är svårtolkat och att MSB med stöd av berörd tillsynsmyndighet bör bemyndigas att meddela föreskrifter om den närmare innebörden av vilka verksamheter som omfattas av lagen.

PTS efterfrågar ett förtydligande i fråga om leverantörer av internetknutpunkter ska anses vara tillhandahållare av allmänna elektroniska kommunikationsnät enligt LEK och därmed omfattas av lagen oavsett om de uppfyller storlekskravet.

Advokatfirman Kahn Pedersen framhåller att NIS 2-direktivet innehåller ett undantag från artikel 3.4 i kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag, vilket också bör gälla enligt lagen. *Energiföretagen Sverige* påpekar att direktivet kräver att verksamhetsutövaren ska vara den enda leverantören av en tjänst som är väsentlig för att upprätthålla kritiska funktioner i samhället och ekonomiska funktioner och inte enbart att verksamhetsutövaren är väsentlig för att upprätthålla sådana funktioner. Organisationen saknar en motivering om varför utredningen föreslår en utvidgning av tillämpningsområdet i förhållande till detta krav. *Integritetsskyddsmyndigheten (IMY)* påpekar bland annat att uttrycket huvudsakligt etableringsställe också används i EU:s dataskyddsförordning.

Skälen för regeringens förslag

Högkritiska och andra kritiska sektorer enligt direktivet

I NIS 2-direktivets bilaga 1 pekas elva så kallade högkritiska sektorer ut. Dessa är energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvårdssektorn, dricksvatten, avloppsvatten, digital infrastruktur, förvaltning av IKT-tjänster mellan företag, offentlig förvaltning och rymden. Dessa sektorer motsvarar i hög grad de sektorer som omfattas av NIS-lagen. Vilka delsektorer som omfattas anges också i bilagan.

I direktivets bilaga 2 pekas sju andra sektorer ut, kallade andra kritiska sektorer. Dessa är post- och budtjänster; avfallshantering; tillverkning, produktion och distribution av kemikalier; produktion, bearbetning och distribution av livsmedel; digitala leverantörer; forskning; och tillverkning. I den sistnämnda sektorn ingår bland annat delsektorerna tillverkning av medicintekniska produkter, elektronikvaror och transportmedel. Vid en jämförelse med NIS-direktivet och NIS-lagen är dessa sektorer i stort sett nya.

I direktivet ställs det upp olika krav för att entiteter inom angivna sektorer ska omfattas av tillämpningsområdet för direktivet. En redogörelse för dessa krav följer nedan.

Storlekskravet i direktivet

Enligt artikel 2.1 i NIS 2-direktivet är direktivet tillämpligt på offentliga eller privata entiteter av den typ som avses i bilaga 1 eller 2 som betecknas som medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG (härefter bilagan till kommissionens rekommendation) eller överstiger de trösklar för medelstora företag som avses i punkt 1 i den artikeln och som tillhandahåller sina tjänster eller bedriver sin verksamhet i unionen. Storlekskravet innebär att en entitet som har minst 50 anställda eller en balansomslutning och årsomsättning som överstiger 10 000 000 euro per år omfattas av direktivet.

I artikel 3 i bilagan till kommissionens rekommendation anges vilka typer av företag som beaktas vid beräkning av personalstyrkan och de finansiella beloppen. Det anges också vad som avses med uttrycken fristående företag, partnerföretag och anknutna företag. Med anknutna företag avses företag som det finns viss förbindelse mellan. Fyra olika kriterier skapar var för sig en sådan förbindelse. Det första är att det ena företaget ska ha ett stort inflytande över det andra genom ett innehav av en majoritet av rösterna för aktierna eller andelarna (a). Det andra kriteriet är att det ena företaget har rätt att utse eller entlediga en majoritet av ledamöterna i det andra företagets styrelse, ledning eller tillsynsorgan (b). Det tredje kriteriet innebär att det ska finnas rätt att utöva bestämmande inflytande över ett det andra företaget enligt avtal eller enligt företagets stadgar (c). Det fjärde kriteriet innebär att företaget på grund av överenskommelser med vissa andra förfogar ensamt över en majoritet av rösterna för aktierna eller andelarna i det andra företaget (d).

Med partnerföretag avses, enligt artikel 3.2 i bilagan till kommissionens rekommendation, företag som inte betecknas som anknutna, men som har en annan förbindelse. Det ena företaget ska ensamt eller tillsammans med ett eller flera andra anknutna företag inneha en kapital- eller röstandel på minst 25 procent i ett annat företag. Detta innebär att även företag som inte

når upp till storlekskravet som egen juridisk person kan göra det på grund av sambandet med exempelvis ett moderbolag. Ett företag kan dock enligt artikelns andra stycke betecknas som fristående, och alltså inte anses ha ett partnerföretag, även om tröskelvärdet på 25 procent har uppnåtts eller överskridits, om det gäller vissa uppräknade kategorier av investerare och dessa enskilt eller tillsammans inte är anknutna i visst avseende till det berörda företaget.

I artikel 3.4 finns ett undantag som anger att ett företag, utom i de fall som avses i artikel 3.2 andra stycket, inte kan anses tillhöra kategorin mikroföretag eller små och medelstora företag om 25 procent eller mer av dess kapital eller dess röstandel direkt eller indirekt kontrolleras av ett eller flera offentliga organ, individuellt eller gemensamt.

I artikel 2.1 i NIS 2-direktivet anges att artikel 3.4 i bilagan till kommissionens rekommendation inte är tillämplig i förhållande till direktivet. I skäl 16 i direktivet anges att medlemsstaterna, för att undvika att entiteter som har partnerföretag eller som är anknutna företag betraktas som väsentliga eller viktiga entiteter när detta vore oproportionellt, kan ta hänsyn till vilken grad av oberoende som entiteten åtnjuter i förhållande till sin partner eller de anknutna företagen vid tillämpningen av artikel 6.2 i bilagan till kommissionens rekommendation. I synnerhet kan medlemsstaterna ta hänsyn till att en entitet är oberoende av sin partner eller de anknutna företagen med avseende på de nätverks- och informationssystem som entiteten använder vid tillhandahållandet av sina tjänster och med avseende på de tjänster som entiteten tillhandahåller. På grundval av detta kan medlemsstaterna när det är lämpligt anse att en sådan entitet inte betraktas som ett medelstort företag enligt artikel 2 i bilagan till kommissionens rekommendation, eller inte överstiger de trösklar för ett medelstort företag som fastställs i punkt 1 i den artikeln, om entiteten, med hänsyn tagen till dess grad av oberoende, inte skulle ha ansetts betraktas som ett medelstort företag eller överstiga dessa trösklar om bara dess egna data hade tagits i beaktande. Detta påverkar inte skyldigheterna enligt direktivet för partnerföretag och anknutna företag som omfattas av direktivets tillämpningsområde.

Entiteter kan omfattas av direktivet även om de inte uppfyller storlekskravet

Artikel 2.2 a–e i NIS 2-direktivet innehåller särskilda kvalificeringsgrunder för entiteter som omfattas av bilaga 1 eller 2, men som inte uppfyller storlekskravet.

De två första kvalificeringsgrunderna finns i artikel 2.2 a och avser tjänster som tillhandahålls av tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster (i) och tjänster som tillhandahålls av tillhandahållare av betrodda tjänster (ii).

Elektronisk kommunikation regleras i lagen (2022:482) om elektronisk kommunikation (LEK). Begreppet allmänt elektroniskt kommunikationsnät definieras i den lagen som ett elektroniskt kommunikationsnät som helt eller huvudsakligen används för att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster och som stöder informationsöverföring mellan nätanslutningspunkter (1 kap. 7 §). Allmänna elektroniska

kommunikationsnät som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster får, med vissa undantag, endast tillhandahållas efter anmälan till PTS enligt 2 kap. 1 § samma lag.

Med uttrycket elektronisk kommunikationstjänst i NIS 2-direktivet avses detsamma som i LEK. Därmed avses en tjänst som vanligen tillhandahålls mot ersättning via elektroniska kommunikationsnät och som – med undantag för dels tjänster i form av tillhandahållande av innehåll som överförs med hjälp av elektroniska kommunikationsnät och elektroniska kommunikationstjänster, dels tjänster som innebär utövande av redaktionellt ansvar över sådant innehåll – uppfyller vissa krav. Det kan exempelvis vara fråga om en internetanslutningstjänst enligt artikel 2.2 i Europaparlamentets och rådets förordning (EU) 2015/2120 av den 25 november 2015 om åtgärder rörande en öppen internetanslutning och slutkundsavgifter för reglerad kommunikation inom EU och om ändring av direktiv 2002/22/EG och förordning (EU) nr 531/2012. I annat fall ska det röra sig om en interpersonell kommunikationstjänst, eller tjänst som utgörs helt eller huvudsakligen av överföring av signaler, såsom överföringstjänster som används för tillhandahållande av maskin-till-maskin-tjänster eller för rundradio. Att en elektronisk kommunikationstjänst är allmänt tillgänglig innebär att tjänsten erbjuds till någon annan. Den som själv överför signaler i ett nät för eget bruk tillhandahåller inte allmänt tillgängliga elektroniska kommunikationstjänster (jfr prop. 2021/22:136 s. 406 och prop. 2002/03:110 s. 120).

Internetknutpunkter anses i svensk rätt utgöra sådana allmänna elektroniska kommunikationsnät som omfattas av LEK. Som *PTS* påpekar ingår leverantörer av internetknutpunkter i sektorn digital infrastruktur som uttryckligen omfattas av bilaga 1 till NIS 2-direktivet. Regeringen anser dock att leverantörer av internetknutpunkter även i aktuellt sammanhang bör räknas som tillhandahållare av allmänna elektroniska kommunikationsnät enligt LEK (jfr prop. 2017/18:205 s. 25).

Den andra kvalificeringsgrunden gäller i förhållande till tillhandahållare av så kallade betrodda tjänster. I artikel 6.24 och 6.25 i NIS 2-direktivet hänvisas beträffande uttrycken betrodd tjänst och tillhandahållare av betrodd tjänst till 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 (EU:s förordning om elektronisk identifiering). EU:s förordning om elektronisk identifiering reviderades under 2024 genom 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 (ändringsförordningen).

I artikel 3.16 i EU:s förordning om elektronisk identifiering definieras betrodd tjänst som en elektronisk tjänst som vanligen tillhandahålls mot ersättning och som består av någon av vissa utpekade funktioner. Med uttrycket tillhandahållare av betrodda tjänster avses, enligt artikel 3.19 i samma förordning, en fysisk eller juridisk person som tillhandahåller en eller flera betrodda tjänster, antingen i egenskap av kvalificerade eller icke kvalificerade tillhandahållare av betrodda tjänster.

Den tredje kvalificeringsgrunden gäller, enligt artikel 2.2 a i NIS 2-direktivet, registreringsenheter för toppdomäner och leverantörer av domännamnssystemtjänster (DNS-tjänster). Uttrycket registreringsenhet för toppdomäner definieras i artikel 6.21 i direktivet. Regeringen anser att definitionen i lagen i sak bör motsvara den i direktivet. Enligt regeringen bör det av lagen framgå att uttrycket registreringsenhet för toppdomäner avser en verksamhetsutövare som har delegerats en specifik toppdomän och som ansvarar för administrationen av den, dock inte om toppdomänen endast används för registreringsenhetens eget bruk (se vidare avsnitt 10).

Med domännamnssystem, eller DNS, avses enligt artikel 6.19 i direktivet ett hierarkiskt distribuerat namnsystem som möjliggör identifieringen av tjänster och resurser på internet, vilket gör det möjligt för slutanvändarenheter att använda internetrouting- och internetuppkopplingstjänster för att nå dessa tjänster och resurser. Uttrycket leverantör av DNS-tjänster definieras enligt artikel 6.20 i direktivet som en entitet som tillhandahåller allmänna rekursiva tjänster för att lösa domännamnsfrågor till internetslutanvändare (a) eller auktoritativa tjänster för att lösa domännamnsfrågor för användning av tredje part, med undantag för rotnamnsservrar (b).

Av artikel 2.2 b–e i NIS 2-direktivet följer ytterligare fyra kvalificeringsgrunder som innebär att entiteter kan omfattas av tillämpningsområdet för direktivet, trots att storlekskravet inte är uppfyllt. En sådan kvalificeringsgrund är att entiteten är den enda leverantören i en medlemsstat av en tjänst som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet (b). Därutöver omfattas en entitet av direktivet om en störning av den tjänst som entiteten tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa (c) eller kan medföra betydande systemrisker, särskilt för de sektorer där sådana störningar kan få gränsöverskridande konsekvenser (d). En entitet omfattas också om den är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer som är beroende av denna entitet (e).

NIS 2-direktivet är vidare, oavsett entiteternas storlek, tillämpligt på entiteter som identifieras som kritiska entiteter enligt CER-direktivet, det vill säga Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (artikel 2.3) och på entiteter som tillhandahåller domännamnsregistreringstjänster (artikel 2.4).

Direktivet i fråga om jurisdiktion

Enligt huvudregeln ska entiteter som omfattas av direktivet enligt artikel 26.1 i NIS 2-direktivet anses omfattas av jurisdiktionen i den medlemsstat där de är etablerade, utom när det gäller vissa särskilt angivna entiteter. I fråga om tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster gäller att de omfattas av jurisdiktionen i den medlemsstat där de tillhandahåller sina tjänster (artikel 26.1 a).

När det gäller leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokali-

serade tjänster och leverantörer av utlokaliserade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster gäller särskilda regler. Dessa entiteter ska enligt artikel 26.1 b anses omfattas av jurisdiktionen i den medlemsstat där de har sitt huvudsakliga etableringsställe i unionen i enlighet med artikel 26.2.

Enligt artikel 26.2 ska en entitet som omfattas av artikel 26.1 b anses ha sitt huvudsakliga etableringsställe i unionen i den medlemsstat där besluten om riskhanteringsåtgärder för cybersäkerhet i huvudsak fattas. Om en sådan medlemsstat inte kan fastställas eller om sådana beslut inte fattas i unionen ska det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där cybersäkerhetsoperationer utförs. Om en sådan medlemsstat inte kan fastställas ska det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där den berörda entiteten har det etableringsställe som har flest anställda i unionen.

Om en entitet som omfattas av artikel 26.1 b inte är etablerad i unionen, men erbjuder tjänster inom unionen, ska den enligt artikel 26.3 utse en företrädare i unionen. Företrädaren ska vara etablerad i en av de medlemsstater där tjänsterna erbjuds och entiteten ska anses omfattas av jurisdiktionen i den medlemsstat där företrädaren är etablerad. Om det inte finns en sådan utsedd företrädare i unionen får varje medlemsstat där entiteten tillhandahåller tjänster vidta rättsliga åtgärder mot entiteten för överträdelsen av direktivet. Det faktum att en entitet inte har utsett en företrädare ska inte påverka eventuella rättsliga åtgärder mot entiteten i sig (artikel 26.4).

Om entiteten tillhandahåller tjänster eller är etablerad i mer än en medlemsstat bör den omfattas av dessa medlemsstaters separata och parallella jurisdiktioner samtidigt (skäl 113). Det framgår även bland annat att de behöriga myndigheterna i de berörda medlemsstaterna bör samarbeta samt att efterkontrollsåtgärder och sanktioner inte bör påföras mer än en gång för samma handling enligt principen om ne bis in idem, det vill säga dubbelbestraffningsförbudet. Av skäl 114 framgår att kriteriet för etableringsställe i direktivet förutsätter att verksamhet faktiskt bedrivs genom en stabil struktur. Den rättsliga formen för en sådan struktur, oavsett om det är en filial eller ett dotterföretag med status som juridisk person, bör inte vara den avgörande faktorn i detta avseende. Huruvida kriteriet är uppfyllt bör inte vara beroende av om nätverks- och informationssystemen är fysiskt belägna på en viss plats.

Hur ska de som omfattas av lagen benämnas? Och vad ska gälla i fråga om jurisdiktion?

I avsnitt 5.3.1 föreslår regeringen att uttrycket verksamhetsutövare ska användas i lagen för att beteckna dem som omfattas av lagen. Utredningen föreslår att uttrycket enskilda verksamhetsutövare ska definieras i lagen och att det ska avse fysiska och juridiska personer som inte är en myndighet, region eller en kommun och som bedriver verksamhet. Regeringen bedömer att uttrycket enskild verksamhetsutövare i lagen bör avse en verksamhetsutövare som inte är en offentlig sådan (se vidare avsnitt 5.3.3).

Enligt artikel 26.1 ska entiteter som omfattas av bilaga 1 eller 2 till direktivet anses omfattas av jurisdiktionen i den medlemsstat där de är

etablerade, utom när det gäller vissa särskilt angivna entiteter. I fråga om tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster gäller att de omfattas av jurisdiktionen i den medlemsstat där de tillhandahåller sina tjänster (artikel 26.1 a). Huvudregeln om krav på etablering gäller därmed inte för sådana verksamhetsutövare. Till skillnad mot utredningen anser regeringen därför att dessa aktörer endast ska omfattas av lagen om de tillhandahåller näten eller tjänsterna i Sverige.

För de verksamhetsutövare som räknas upp i artikel 26.1 b gäller också en särskild reglering i fråga om jurisdiktion. Utredningen benämner dessa verksamhetsutövare som gränsöverskridande verksamhetsutövare. Regeringen bedömer att det saknas skäl för att införa en särskild samlingsterm för dessa aktörer i lagen. Regeringen delar däremot utredningens uppfattning att verksamhetsutövare som erbjuder molntjänster, datacentraltjänster, nätverk för leverans av innehåll, utlokaliserade driftstjänster, utlokaliserade säkerhetstjänster, marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster bör omfattas av lagen om de har sitt huvudsakliga etableringsställe i Sverige eller en företrädare som är etablerad här och uppfyller direktivets storlekskrav.

Vid bedömningen av vad som utgör huvudsakligt etableringsställe ska enligt utredningens förslag till förordning beaktas plats för beslut om riskhanteringsåtgärder för cybersäkerhet, plats för cybersäkerhetsverksamhet, eller plats där verksamhetsutövaren har flest anställda. Regeringen bedömer, i likhet med utredningen, att det tydligt bör anges på lägre normgivningsnivå än i lag vad som avses med huvudsakligt etableringsställe. Det bör finnas möjlighet att reglera detta i såväl förordning som i föreskrifter som meddelas av en myndighet.

Som *IMY* påpekar används uttrycket huvudsakligt etableringsställe även i 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 dataskyddsförordning) med en annan innebörd än den som anges i utredningens förordningsförslag. Mot bakgrund av ställningstagandet att det bör regleras på lägre föreskriftsnivå än i lag vad som avses med uttrycket, finns det inte anledning att närmare beröra innebörden av uttrycket i denna lagrådsremiss. Regeringen konstaterar dock att utredningens förslag i stort följer artikel 26.2 i NIS 2-direktivet och att det är ofrånkomligt att samma uttryck kan komma att användas med olika innebörd i olika rättsakter.

Tillhandahållare av betrodda tjänster omfattas av sektorn digital infrastruktur i bilaga 1 till NIS 2-direktivet. Som utredningen föreslår bör verksamhetsutövare som är etablerade i Sverige och som tillhandahåller betrodda tjänster omfattas av lagen oavsett om de uppfyller storlekskravet.

Ett mycket stort antal remissinstanser, däribland *Naturvårdsverket*, efterfrågar förtydliganden kring vilka verksamhetsutövare som omfattas av respektive sektor som nämns i bilagorna till direktivet. Utredningen och ett antal remissinstanser, till exempel *Transportstyrelsen*, föreslår att regeringen ska ge i uppdrag att utforma vägledning för den enskilda verksamhetsutövaren om vem som omfattas av sektorerna. Regeringen

konstaterar att det inte finns utrymme för att ge ett sådant uppdrag inom ramen för denna lagrådsremiss.

Storlekskravet i lagen

Utredningen föreslår att storlekskravet ska uttryckas som att en verksamhetsutövare uppfyller kraven för medelstort företag enligt artikel 2 och 3.1–3.3 i bilagan till kommissionens rekommendation. Enligt artikel 2.1 i NIS 2-direktivet är direktivet, när det gäller storlekskravet, tillämpligt på entiteter som betecknas som medelstora företag eller överstiger trösklarna för medelstora företag. För att tydliggöra det sistnämnda bör det framgå av lagen att storlekskravet innebär att verksamhetsutövaren ska storleksmässigt motsvara eller vara större än ett medelstort företag.

En definition av uttrycket medelstort företag bör föras in i lagen och i den bör en hänvisning till artikel 2 i bilagan till kommissionens rekommendation göras. Av den artikeln framgår att ett medelstort företag sysselsätter färre än 250 personer och har en årsomsättning som inte överstiger 50 000 000 euro eller en balansomslutning som inte överstiger 43 000 000 euro per år. Ett medelstort företag ska samtidigt vara större än sådana företag som kategoriseras som små företag. Ett medelstort företag ska därför sysselsätta minst 50 personer eller ha en årsomsättning och balansomslutning som överstiger 10 000 000 euro per år. I likhet med vad *Advokatfirman Kahn Pedersen* framför bör undantaget som gäller enligt artikel 2.1 i NIS 2-direktivet, i förhållande till artikel 3.4 i bilagan till kommissionens rekommendation, framgå av lagen. Artikel 3.4 i bilagan till kommissionens rekommendation ska således inte tillämpas vid beräkning av storleken.

Registreringsenheter för toppdomäner, DNS-tjänster och domännamnsregistreringstjänster

I enlighet med artiklarna 2.2 a och 2.4 i NIS 2-direktivet bör storlekskravet inte gälla för verksamhetsutövare som är registreringsenheter för toppdomäner eller som erbjuder domännamnssystemtjänster eller domännamnsregistreringstjänster. Bland annat skyldigheten för registreringsenheter för toppdomäner och verksamhetsutövare som erbjuder domännamnsregistreringstjänster att föra register över domännamn behandlas i avsnitt 10.

Utredningen föreslår att domännamnssystemtjänster (DNS-tjänster) i lagen ska definieras som allmänna rekursiva tjänster för att lösa domännamnsfrågor till internetslutanvändare, eller auktoritativa tjänster för att lösa domännamnsfrågor för användning av tredje part, med undantag för rotnamnsservrar. *Post- och telestyrelsen (PTS)* och *Tech Sverige* anser att det bör tydliggöras vad som avses med uttrycket. PTS lyfter att det bör göras en avgränsning så att företag som inte tillhandahåller en DNS-tjänst men som innehar en auktoritativ namnserver för egna domäner faller utanför lagens tillämpningsområde. PTS anger att webbplatser hos stora företag kan tänkas inbegripa auktoritativa namnservrar. Sådana företag bör enligt myndigheten falla utanför NIS 2-direktivets tillämpningsområde utifrån en tolkning av uttrycken leverantör och tillhandahålla. Trots att dessa namnservrar skulle kunna beskrivas som allmänt tillgängliga, så torde det enligt PTS inte röra sig om en tjänst som tillhandahålls till andra

utan snarare om ett verktyg som organisationen använder inom ramen för sin egen verksamhet. Även Tech Sverige anser att DNS-servrar som endast används i den egna verksamheten faller utanför direktivets tillämpningsområde.

Varje domännamn har minst en namnserver på internet som är auktoritativ för den. En auktoritativ namnserver innehåller bland annat information om vilken ip-adress som gäller för domännamnet. Som PTS anger kan det förekomma att till exempel företag innehar en auktoritativ namnserver för egna domäner. En förutsättning för att en tjänst ska räknas som en DNS-tjänst enligt utredningens förslag är dock bland annat att tjänsten löser domännamnsfrågor till internetslutanvändare eller för användning av tredje part. Regeringen bedömer att uttrycket bör definieras i lagen på samma sätt som i NIS 2-direktivet och att det dessutom är tydligt att den som innehar en auktoritativ namnserver enbart för egna domäner faller utanför tillämpningsområdet.

Vilka ska i övrigt omfattas av lagen med hänvisning till sin särskilda betydelse i samhället?

Utredningen föreslår att vissa verksamhetsutövare som omfattas av bilagorna till NIS 2-direktivet och är etablerade i Sverige ska omfattas av lagen med hänvisning till sin särskilda betydelse och oavsett om de uppfyller storlekskravet. Regeringen instämmer i allt väsentligt i utredningens uppfattning om vilka som bör omfattas av lagen med hänvisning till sin särskilda betydelse i samhället, men gör vissa andra bedömningar än utredningen.

Utredningen föreslår bland annat att ett krav ska vara att verksamheten är väsentlig för att upprätthålla kritiska funktioner i samhället och ekonomiska funktioner. Regeringen anser dock att det i stället bör krävas att verksamhetsutövaren är den enda leverantören av en tjänst i Sverige som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet. Ett krav på att verksamhetsutövaren ska vara den enda leverantören av en sådan tjänst stämmer, som *Energiföretagen Sverige* påpekar, bättre överens med direktivets utformning och regeringen anser inte att det finns skäl att avvika från den.

I fråga om när en tjänst ska anses vara väsentlig för att upprätthålla angiven verksamhet bör viss ledning kunna tas från definitionen av uttrycket samhällsviktig tjänst i NIS-lagen. I den lagen beskrivs en samhällsviktig tjänst som en tjänst som är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet. I förarbetena till NIS-lagen framgår att det rör sig om tjänster som är viktiga för samhällets funktionalitet i sin helhet och där ett avbrott i tjänsten hindrar genomförandet av ekonomisk verksamhet, genererar omfattande förluster, undergräver användarnas förtroenden och medför allvarliga konsekvenser för landets och unionens ekonomi (se prop. 2017/18:205 s. 34).

Som utredningen föreslår bör ett annat krav enligt lagen vara att en störning av den tjänst som verksamhetsutövaren tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa eller medföra betydande systemrisker. Allmän säkerhet avser, som framgår av avsnitt 5.4.2, skydd av en medlemsstats institutioner, dess väsentliga offentliga tjänster och dess invånares över-

levnad. Enligt regeringens mening bör störningens gränsöverskridande effekt beaktas i bedömningen av om en tjänst kan medföra betydande systemrisker, men det bör inte lyftas fram som en omständighet att beakta särskilt som utredningen föreslår. Lagen bör också, som utredningen bedömer, gälla för en verksamhetsutövare som har särskild betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer som är beroende av verksamhetsutövaren.

Regeringen eller den myndighet som regeringen bestämmer bör som utredningen föreslår få meddela föreskrifter om kriterier för när en verksamhetsutövare ska omfattas av lagen med hänvisning till sin betydelse.

Undantag från storlekskravet för partnerföretag och anknutna företag

Det finns med stöd av skäl 16 i NIS 2-direktivet en möjlighet att meddela undantag från tillämpningsområdet för lagen för vissa partnerföretag och anknutna företag. Undantag får meddelas om det skulle vara oproportionerligt att partnerföretag eller anknutna företag som inte i sig uppfyller storlekskravet, men gör det genom sin anknytning till en annan verksamhet, omfattas av regleringen. Utredningen föreslår att regeringen, eller den myndighet som regeringen bestämmer, ska få meddela föreskrifter om undantag för partnerföretag eller anknutna företag som inte i sig uppfyller storlekskravet. Utredningen föreslår även att det ska regleras i förordning att sådana undantag får meddelas efter ansökan till tillsynsmyndigheten och när skäl finns. Skäl kan, enligt utredningens resonemang, finnas när den juridiska personen inte i sig uppfyller storlekskravet och därutöver vid en sammantagen bedömning, med utgångspunkt från lagens syfte, inte behöver omfattas.

För att åstadkomma den ordning som utredningen föreslår bör regeringen eller den myndighet som regeringen bestämmer i enskilda fall, och om det finns särskilda skäl, få besluta om undantag från skyldigheterna enligt lagen för partnerföretag eller anknutna företag som annars skulle ha omfattats av lagen med hänvisning till att aktören omfattas av bilaga 1 eller 2 till NIS 2-direktivet, är etablerad i Sverige och storleksmässigt motsvarar eller är större än ett medelstort företag. Skäl för undantag kan finnas om verksamhetsutövaren inte i sig uppfyller storlekskravet och därutöver vid en sammantagen bedömning, och med utgångspunkt från lagens syfte, inte behöver omfattas av densamma. Enligt regeringen framstår det dock inte som ändamålsenligt att i lag uttömmande reglera möjligheten till undantag. Regeringen eller den myndighet som regeringen bestämmer bör därför därutöver bemyndigas att meddela föreskrifter om undantag från skyldigheterna enligt lagen för partnerföretag eller anknutna företag.

5.3.3 Offentlig verksamhet som i övrigt ska omfattas av lagen

Regeringens förslag: Statliga myndigheter som har befogenhet att fatta beslut som påverkar fysiska eller juridiska personers rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital ska omfattas av lagen. Därutöver ska de statliga myndigheter som regeringen bestämmer omfattas av lagen. Regeringen, Regerings-

kansliet, utlandsmyndigheter, kommittéväsendet, myndigheter under riksdagen, domstolar och nämnder som utövar rättskipning ska däremot inte omfattas av lagen.

Även regioner, kommuner och kommunalförbund, med undantag för fullmäktige och förbundsdirektion, ska omfattas av lagen.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår att samtliga statliga myndigheter ska omfattas av lagen som utgångspunkt. Utredningen bedömer att myndigheter som lyder under riksdagen ska undantas men föreslår endast ett undantag för Riksrevisionen, Riksdagens ombudsmän, Sveriges riksbank och Riksdagsförvaltningen. Utredningen föreslår att undantag ska göras för Sveriges domstolar. I utredningens förslag nämns inte kommunalförbund.

Remissinstanserna: Flera remissinstanser, bland andra *Kemikalieinspektionen* och *Kronofogdemyndigheten*, ser positivt på att lagen föreslås omfatta offentlig förvaltning. *Brottsförebyggande rådet (Brå)* anser att det kan diskuteras om inte utredningen tolkar innebörden av ett av kriterierna för att räknas som offentlig förvaltningsentitet enligt direktivet väl extensivt. *Livsmedelsverket* anser att förslaget om att samtliga statliga myndigheter ska omfattas går utöver NIS 2-direktivets krav eftersom direktivet i huvudsak är avsett att tillämpas i förhållande till myndigheter som kan påverka rörlighet och handel inom unionen. Livsmedelsverket anser att den föreslagna utvidgningen bör föregås av en fördjupad konsekvensanalys då förslaget kan medföra höga kostnader för den som träffas av det. *Myndigheten för psykologiskt försvar (MPF)* anser att lagen bör omfatta hela den offentliga förvaltningen men att kraven bör differentieras för de olika statliga myndigheterna, regionerna och kommunerna beroende på behov.

Domstolsverket och *Rymdstyrelsen* framhåller att Sveriges domstolar inte är ett vedertaget begrepp. Domstolsverket påpekar att utredningen använder både uttrycket Sveriges Domstolar och uttrycket Sveriges domstolar och att uttrycken har olika betydelse. Domstolsverket nämner att de allmänna domstolarna, de allmänna förvaltningsdomstolarna, hyres- och arrendenämnderna, Rättshjälpsmyndigheten, Rättshjälpsnämnden och Domstolsverket omfattas av det inarbetade uttrycket Sveriges Domstolar.

Sveriges Kommuner och Regioner (SKR) menar att regioner och kommuner inte per automatik omfattas av NIS 2-direktivets tillämpningsområde. Regioner och kommuner är uppdelade i nämnder som inte är juridiska personer. SKR accepterar dock att dessa omfattas av lagens tillämpningsområde, givet säkerhetsläget. Bland andra *Göteborgs kommun* och *Salems kommun* efterfrågar förtydliganden i fråga om hur ansvaret ska fördelas avseende den kommunala nämndorganisationen. Ett antal kommuner, bland andra *Karlstads kommun* och *Umeå kommun*, ställer sig positiva till att kommunerna som helhet omfattas av lagen. Till exempel *Gävle kommun* och *Linköpings kommun* gör dock motsatt bedömning och anser att varje nämnd borde ses som en egen enhet. Bland andra *Region Stockholm* och *Malmö kommun* efterfrågar ett förtydligande i frågan om huruvida ett kommunalförbund omfattas av lagen enligt utredningens förslag. Exempelvis *Sveriges advokatsamfund* pekar på att det enligt dataskyddsregleringen är varje enskild nämnd och inte

kommunen som helhet som är personuppgiftsansvarig för den personuppgiftsbehandling som den kommunala myndigheten bedriver.

Skälen för regeringens förslag

Direktivets definition av offentlig förvaltning

Offentlig förvaltning är en av de sektorer som pekas ut i NIS 2-direktivets bilaga 1. Uttrycket avser i bilagan offentliga förvaltningsentiteter hos nationella regeringar eller på regional nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt. Av artikel 6.35 i direktivet följer att en offentlig förvaltningsentitet enligt direktivet definieras som en entitet som erkänts som sådan i en medlemsstat i enlighet med nationell rätt, med undantag för rättsväsendet, parlament och centralbanker. Därutöver ska fyra kriterier uppfyllas.

Det första kriteriet innebär att entiteten ska ha inrättats för att tillgodose ett behov i det allmännas intresse och att verksamheten inte har industriell eller kommersiell karaktär (a). Det andra kriteriet är att entiteten har ställning som juridisk person eller har lagstadgad rätt att agera för en annan entitet som har ställning som juridisk person (b). Det tredje kriteriet innebär att entiteten ska finansieras till största delen av staten, regionala myndigheter eller andra offentligrättsliga organ, ska stå under administrativ tillsyn av dessa myndigheter eller organ, eller ha ett förvaltnings-, lednings-, eller kontrollorgan där mer än hälften av ledamöterna utses av staten, regionala myndigheter eller andra offentligrättsliga organ (c). Det sista kriteriet är att entiteten ska ha befogenhet att rikta administrativa eller reglerande beslut till fysiska eller juridiska personer som påverkar deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital (d).

Storlekskravet som nämns i avsnitt 5.3.2 gäller som utgångspunkt även för offentliga förvaltningsentiteter som omfattas av bilaga 1 och 2 till direktivet (se artikel 2.1). Av artikel 2.2 f framgår dock att storlekskravet inte gäller för offentliga förvaltningsentiteter på statlig nivå. Det gäller inte heller för offentliga förvaltningsentiteter på regional nivå om entiteten enligt en riskbaserad bedömning tillhandahåller tjänster vars störning kan ha en betydande effekt på kritisk samhällelig eller ekonomisk verksamhet.

Endast vissa statliga myndigheter bör omfattas av lagen

Regeringen bedömer, i likhet med utredningen, att uttrycket offentliga förvaltningsentiteter hos nationella regeringar för svensk del bör anses motsvara statliga myndigheter. Direktivets definition är visserligen något motsägelsefull då den dels innebär att det ska vara fråga om en entitet som definieras som en fysisk eller juridisk person i artikel 6.38, dels anger att entiteten ska ha ställning som juridisk person eller ha lagstadgad rätt att agera för annan juridisk person (artikel 6.35 b). Det sistnämnda bör innebära att det är tillräckligt med företrädesrätt för att räknas som offentlig förvaltningsentitet och att det inte behöver vara fråga om en egen juridisk person. Statliga myndigheter i Sverige är inte egna juridiska personer. De har dock rätt att företräda den juridiska personen staten.

Kriterierna i artikel 6.35 a och c i direktivet, som bland annat innebär att entiteten ska ha inrättats för att tillgodose behov i det allmännas intresse,

stämmer väl överens med vad som gäller för svenska statliga myndigheter. Det fjärde kriteriet i artikel 6.35 d, det vill säga att entiteten ska ha befogenhet att fatta vissa beslut med koppling till gränsöverskridande rörlighet för personer, varor, tjänster eller kapital, är som utredningen anger mer svårtolkat. Utifrån en EU-rättslig kontext brukar uttrycket gränsöverskridande rörlighet tolkas i linje med de fyra friheterna för EU:s inre marknad enligt fördraget om Europeiska unionens funktionssätt (EUF-fördraget), det vill säga fri rörlighet för varor, tjänster, personer och kapital.

Många statliga myndigheter kan sägas ha befogenhet att fatta beslut som påverkar fysiska och juridiska personers gränsöverskridande rättigheter. Som utredningen nämner gäller detta till exempel Polismyndighetens rätt att i vissa fall frihetsberöva personer och Tullverkets befogenheter att omhänderta gods. Vilka statliga myndigheter som kan sägas uppfylla kriteriet beror dock på hur man ser på olika besluts påverkan i förlängningen. Det skulle kunna argumenteras för att även beslut som indirekt påverkar exempelvis möjligheten för en individ att studera, arbeta eller etablera sig i en annan medlemsstat, eller beslut som rör offentlig upphandling med potentiella gränsöverskridande effekter, innebär att kriteriet i artikel 6.35 d är uppfyllt. Med det resonemanget skulle till exempel varje myndighets beslut om anställning indirekt kunna anses ha sådana effekter. Regeringen bedömer dock, i linje med *Brå,* att det skulle innebära en för extensiv tolkning av kriteriet.

Utredningen föreslår att samtliga statliga myndigheter, med vissa undantag, ska omfattas av lagen oavsett innebörden av artikel 6.35 d. Regeringen konstaterar att direktivet är ett så kallat minimidirektiv, vilket innebär att medlemsstaterna får införa bestämmelser som kan anses bidra till en högre cybersäkerhetsnivå. Som bland annat *Kemikalieinspektionen* framhåller är det positivt att offentlig förvaltning omfattas av lagen. Regeringen bedömer dock, i likhet med *Livsmedelsverket*, att det inte är motiverat att låta samtliga statliga myndigheter omfattas av den nya lagens krav utan att ta hänsyn till kriteriet som anges i artikel 6.35 d. Detta innebär, enligt regeringens mening, att endast de statliga myndigheter som har befogenhet att fatta beslut som påverkar fysiska eller juridiska personer och deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital bör omfattas av lagen i enlighet med direktivets krav. Till exempel bör en myndighet som kan fatta beslut om tillhandahållandet av varor på inre marknaden, däribland Livsmedelsverket, anses fatta sådana beslut som avses i direktivet. En statlig myndighet kan även omfattas av lagen om den bedriver sådan verksamhet som behandlas i avsnitt 5.3.2.

Det kan finnas skäl att låta även vissa andra statliga myndigheter, som inte fattar beslut i enlighet med artikel 6.35 d i direktivet, omfattas av lagens krav. I beredskapssektorerna ingår 61 beredskapsmyndigheter. Det är myndigheter med särskild betydelse för samhällets krisberedskap och totalförsvar. Myndigheterna ska ha god förmåga att motstå hot och risker, förebygga sårbarheter, hantera fredstida krissituationer och genomföra sina uppgifter vid höjd beredskap. Det är motiverat att en stor andel av beredskapsmyndigheterna omfattas av den nya lagens krav. Med hänvisning till förslaget i avsnitt 5.4.2 om undantag för verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller brottsbekämpande

verksamhet bör dock inte samtliga beredskapsmyndigheter omfattas av lagen. Det bör i stället införas en bestämmelse i den nya lagen som innebär att de myndigheter som regeringen bestämmer, med beaktande av de undantag som gäller enligt lagen, ska omfattas av den nya lagen och räknas som offentliga verksamhetsutövare.

Regeringen anser att kravet i bilaga 1 till direktivet om att offentliga förvaltningsentiteter ska finnas ”hos” nationella regeringar exkluderar regeringen och myndigheter som lyder under riksdagen. Det bör därför göras ett undantag i lagen för sådana myndigheter. Regeringen konstaterar att det finns fler myndigheter som lyder under riksdagen än de myndigheter som utredningen räknar upp i sitt förslag. I stället för en uppräkning av enskilda myndigheter bör det anges att undantaget gäller generellt för myndigheter under riksdagen. Även Regeringskansliet, utlandsmyndigheter och kommittéväsendet bör undantas från tillämpningsområdet i enlighet med utredningens förslag. Uttrycket utlandsmyndigheter inbegriper ambassader, karriärkonsulat, representationer och delegationer vid internationella organisationer som EU, FN, OECD och Nato.

Rättsväsendet faller utanför direktivets definition av offentlig förvaltningsentitet och bör därför undantas från lagens tillämpningsområde. Utredningen föreslår att undantag ska göras för Sveriges domstolar. Som *Domstolsverket* och *Rymdstyrelsen* framhåller har uttrycket ingen entydig innebörd. Rättsväsendet omfattar de institutioner som ansvarar för rättssäkerhet och rättstrygghet i Sverige. I den engelska språkversionen av direktivet används uttrycket ”the judiciary”, vilket har en snävare innebörd. Enligt regeringens mening bör undantaget träffa rättskipningsorgan såsom domstolar och nämnder som utövar rättskipning. Detta innebär att specialdomstolar, såsom Arbetsdomstolen och Försvarsunderrättelsedomstolen, undantas från lagens krav. Exempelvis Rättshjälpsnämnden, Notarienämnden och Överklagandenämnden för nämndemannauppdrag omfattas också av undantaget. Däremot bör, till skillnad mot vad utredningen resonerar kring, inte Domarnämnden och Rättshjälpsmyndigheten omfattas av undantaget.

Regioner och kommuner bör omfattas av lagen

I likhet med utredningen anser regeringen att offentliga förvaltningsentiteter på regional nivå bör anses omfatta regionerna. Regionerna uppfyller, som utredningen resonerar kring, både storlekskravet och kravet som uppställs i artikel 2.2 f. Regionerna bör därför, med undantag för regionfullmäktige i varje region, omfattas av lagen i enlighet med utredningens förslag.

Kommunernas verksamhet ryms inte i sektorn offentlig förvaltning enligt bilaga 1 till direktivet. Enligt artikel 2.5 a i direktivet får dock medlemsstaterna föreskriva att direktivet ska tillämpas på offentliga förvaltningsentiteter på lokal nivå. Som utredningen anger bedriver en stor del av alla kommuner sådan verksamhet som omfattas av bilaga 1 eller 2, till exempel hemsjukvård och avfallshantering. Kommuner som uppfyller storlekskravet omfattas därmed av direktivet redan på den grunden och måste därmed omfattas även av lagen. Regeringen bedömer dock, i likhet med utredningen, att det är av värde att samtliga kommuner omfattas av lagen och utredningens förslag i denna del bör därmed genomföras.

Utredningen föreslår att kommunerna i sin helhet ska omfattas av lagen medan bland andra *Gävle kommun* och *Linköpings kommun* anser att respektive nämnd i en kommun bör räknas som en verksamhetsutövare på samma sätt som en enskild statlig myndighet räknas som en sådan. Till exempel *Sveriges advokatsamfund* pekar också på att det enligt dataskyddsregleringen är varje enskild nämnd, och inte kommunen som helhet, som är personuppgiftsansvarig för den personuppgiftsbehandling som den kommunala myndigheten bedriver. Bland andra *Göteborgs kommun* och *Salems kommun* efterfrågar förtydliganden i fråga om hur ansvaret enligt utredningens förslag ska fördelas avseende den kommunala nämndorganisationen.

Regeringen konstaterar till att börja med att dataskyddsregelverket och NIS 2-direktivet har olika syften. Regeringen bedömer också att NIS 2-direktivets utformning talar för att en kommun i sin helhet ska ses som en verksamhetsutövare. Det måste också beaktas, vilket *SKR* påpekar, att en kommunal nämnd inte är en egen juridisk person. En kommunal nämnd får inte heller, till skillnad från en statlig myndighet, företräda staten vid domstol inom sitt verksamhetsområde (jfr 27 § myndighetsförordningen [2007:515]). I fråga om kommunala myndigheter krävs det att kommunfullmäktige lämnar uppdrag åt en nämnd att föra en viss talan eller att det framgår av annan lag eller författning (se vidare 6 kap. 15 § kommunallagen [2017:725]). Regeringen anser mot denna bakgrund, i likhet med utredningen och bland annat *Karlstads kommun*, att det är lämpligast att kommunen som helhet omfattas av lagen. Undantag bör dock göras för kommunfullmäktige i enlighet med utredningens förslag.

Som utredningen nämner kan inte ett aktie- eller handelsbolag rikta administrativa eller andra beslut mot fysiska eller juridiska personer som påverkar deras gränsöverskridande rörlighet (jfr artikel 6.35 d). Detta innebär att om en verksamhet bedrivs genom kommunalt bolag är det inte kommunen som räknas som verksamhetsutövare. De kommunala bolagen omfattas dock av lagen om de uppfyller kraven som behandlas i avsnitt 5.3.2.

Bland andra *Region Stockholm* efterfrågar ett förtydligande i frågan om huruvida ett kommunalförbund omfattas av lagen enligt utredningens förslag. Ett kommunalförbund är en offentligrättslig juridisk person för samverkan mellan kommuner eller regioner och det är fristående i förhållande till sina medlemskommuner. Huvudregeln enligt 3 kap. 8 § kommunallagen är att vilken kommunal angelägenhet som helst får anförtros ett kommunalförbund, vilket även innefattar obligatoriska uppgifter som kommuner och regioner har att sköta utifrån olika författningar. Frågorna om vad samarbetet ska avse och hur arbetet bör bedrivas är i allt väsentligt överlämnat till den kommunala självstyrelsen. Kommunalförbund får utan särskilt lagstöd ha hand om myndighetsutövning. Bedrivs verksamheten genom ett kommunalförbund är det enligt regeringens mening inte kommunen som är verksamhetsutövare utan kommunalförbundet. Det bör tydliggöras i lagen att även kommunalförbund omfattas av densamma, dock med undantag för förbundets fullmäktige och direktion.

MPF anser att lagen bör omfatta hela den offentliga förvaltningen men att kraven bör differentieras för de olika myndigheterna, regionerna och kommunerna. Regeringen konstaterar att det finns möjligheter att göra

nyanserade bedömningar i fråga om vilka åtgärder som verksamhetsutövare ska vidta utifrån utformningen av bland annat kravet på säkerhetsåtgärder (se vidare avsnitt 6.4). Det finns därför inte anledning att ställa upp olika krav i lagen beroende på vilken slags offentlig verksamhetsutövare det är fråga om.

5.3.4 Vilka lärosäten ska omfattas av lagen?

Regeringens förslag: En enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen om tillstånd att utfärda examina ska omfattas av lagen, om utbildningsanordnaren är etablerad i Sverige och storleksmässigt motsvarar eller är större än ett medelstort företag.

En enskild utbildningsanordnare med angivet slags tillstånd ska också omfattas av lagen, om utbildningsanordnaren är etablerad i Sverige och har särskild betydelse i samhället.

Regeringen eller den myndighet som regeringen bestämmer ska i enskilda fall, om det finns särskilda skäl, få besluta om undantag från skyldigheterna enligt lagen för enskilda utbildningsanordnare med tillstånd att utfärda examina.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår att samtliga lärosäten med examenstillstånd ska omfattas av lagen och föreslår inte att vissa enskilda utbildningsanordnare ska kunna undantas genom beslut. Utredningen anser att samtliga statliga universitet och högskolor ska omfattas av lagen eftersom de är statliga myndigheter och omfattas av sektorn offentlig förvaltning.

Remissinstanserna: Ett antal remissinstanser, bland andra *Lunds universitet* och *Totalförsvarets forskningsinstitut*, tillstyrker utredningens förslag.

Ett flertal remissinstanser, bland andra *Karolinska institutet (KI)* och *Stockholms universitet*, är kritiska till förslaget att samtliga lärosäten ska omfattas av lagen trots att detta inte följer av direktivet. Stockholms universitet anser att i vart fall mindre lärosäten med mindre omfattande forskningsverksamhet bör undantas från tillämpningsområdet samt att lärosäten bör räknas som viktiga verksamhetsutövare eftersom det skulle minska den administrativa bördan för dessa. *Uppsala universitet* framhåller att ekonomiska resurser måste tillföras lärosäten för att de ska kunna uppfylla kraven som lagen innebär. Därtill anser universitetet att det är för stort fokus på att bygga upp kontrollsystem, i stället för att identifiera och uppmärksamma de alltmer trängande behov som lärosätena har av stöd och dialog med myndigheter som har expertkunskap inom cybersäkerhetsområdet. *Vetenskapsrådet* anser att det krävs förtydliganden i fråga om vilka som omfattas av utredningens förslag.

Skälen för regeringens förslag

Direktivets reglering om forskningsorganisationer och utbildningsinstitut

Forskning är en sektor som omfattas av NIS 2-direktivet och en, i förhållande till NIS-direktivet, ny sådan. Sektorn omnämns i bilaga 2 till direktivet och omfattar forskningsorganisationer. Forskningsorganisat-

ioner definieras i artikel 6.41 i direktivet som en entitet vars främsta mål är att bedriva tillämpad forskning eller experimentell utveckling i syfte att utnyttja resultaten av denna forskning i kommersiellt syfte, men som inte inbegriper utbildningsinstitutioner.

Som utvecklas i avsnitt 5.3.3 är direktivet enligt artikel 2.2 f, oavsett om en entitet uppfyller angivet storlekskrav, tillämpligt på entiteter av en typ som avses i bilaga 1 eller 2 till direktivet, om entiteten är en offentlig förvaltningsentitet på statlig eller regional nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt. Enligt artikel 2.5 b i direktivet får medlemsstaterna föreskriva att direktivet ska tillämpas på utbildningsinstitut, särskilt om de utför kritisk forskningsverksamhet. I direktivet saknas en definition av uttrycket utbildningsinstitut.

Högre utbildning och forskning i Sverige

Högre utbildning och forskning bedrivs dels vid statliga universitet och högskolor som omfattas av högskolelagen (1992:1434), dels vid enskilda utbildningsanordnare som har fått tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina. I denna lagrådsremiss benämns universitet och högskolor, som har staten som huvudman och som omfattas av högskolelagen, statliga universitet och högskolor. Enskilda utbildningsanordnare som har fått tillstånd att utfärda examina enligt lagen om tillstånd att utfärda vissa examina benämns i lagrådsremissen enskilda utbildningsanordnare. Med uttrycket lärosäten avses, som utredningen redogör för, såväl statliga universitet och högskolor som enskilda utbildningsanordnare. De statliga universiteten och högskolorna är statliga myndigheter.

Det finns 16 statliga universitet och 15 statliga högskolor samt 18 enskilda utbildningsanordnare med tillstånd att utfärda examina. Regeringen delar utredningens uppfattning att det bör vara lärosäten som avses med utbildningsinstitut i NIS 2-direktivet.

Samtliga lärosäten bör inte omfattas av lagen

Vetenskapsrådet anser att det krävs förtydliganden i fråga om vilka lärosäten som omfattas av utredningens förslag. Utredningens förslag innebär att samtliga lärosäten, såväl statliga universitet och högskolor som de enskilda utbildningsanordnare som uppfyller i avsnitt 5.3.2 angivet storlekskrav, omfattas av lagen. Som utvecklas i avsnitt 5.3.3 anser regeringen, till skillnad mot utredningen, att endast sådana statliga myndigheter som har befogenhet att fatta beslut som påverkar fysiska eller juridiska personers rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital bör omfattas av lagen (se artikel 6.35 d i direktivet). De statliga universitet och högskolor som har befogenhet att fatta sådana beslut bör därför enligt regeringen omfattas av lagens tillämpningsområde. Utredningens förslag om att samtliga statliga universitet och högskolor ska omfattas av lagen enbart med hänvisning till att de är statliga myndigheter, och oavsett om de uppfyller kravet i artikel 6.35 d, bör dock inte genomföras.

När det gäller enskilda utbildningsanordnare delar regeringen *KI:s* uppfattning att svenska lärosäten inte bör hamna i en ofördelaktig situation – i jämförelse med lärosäten i övriga medlemsstater – genom den reglering

som genomför direktivet i Sverige, om det inte är motiverat. Det finns en möjlighet för medlemsstaterna att låta direktivet tillämpas på utbildningsinstitut, särskilt om de utför kritisk forskningsverksamhet (artikel 2.5 b i direktivet). Enligt regeringens mening är det viktigt att enskilda utbildningsanordnare som bedriver sådan kritisk forskningsverksamhet som nämns i artikel 2.5 b når upp till en hög cybersäkerhetsnivå. Regeringen bedömer därför att enskilda utbildningsanordnare med tillstånd att utfärda examina bör omfattas av lagens tillämpningsområde som utgångspunkt, under förutsättning att de uppfyller storlekskravet.

I avsnitt 5.3.2 föreslår regeringen att vissa verksamhetsutövare som omfattas av bilagorna till NIS 2-direktivet och är etablerade i Sverige ska omfattas av lagen med hänvisning till deras särskilda betydelse i samhället, oavsett om de uppfyller storlekskravet. Detsamma bör gälla för enskilda utbildningsanordnare med tillstånd att utfärda examina som är etablerade i Sverige.

Vissa enskilda utbildningsanordnare bör undantas från lagens tillämpningsområde

Regeringen bedömer, i linje med vad *Stockholms universitet* anför som ett alternativ, att det kan finnas skäl att undanta vissa enskilda utbildningsanordnare från lagens tillämpningsområde. Forskningsverksamhetens omfattning och innehåll bör vara sådana omständigheter som utgör grund för att det föreligger särskilda skäl för undantag. Detta innebär att en enskild utbildningsanordnare som exempelvis bedriver forskningsverksamhet som är av mindre omfattning eller inte är kritisk bör kunna undantas från skyldigheterna i lagen, bland annat utifrån den typ av forskning som bedrivs vid lärosätet. Eftersom bedömningen av vilka enskilda utbildningsanordnare som bör undantas kan variera över tid bör det inte fastslås i lag vilka som är undantagna. Regeringen föreslår därför att regeringen eller den myndighet som regeringen bestämmer, om det finns särskilda skäl, ska få besluta om undantag från skyldigheterna enligt lagen för enskilda utbildningsanordnare med tillstånd att utfärda examina.

Frågor om finansiering som *Uppsala universitet* väcker behandlas i avsnitt 14.

5.3.5 Väsentliga och viktiga verksamhetsutövare

Regeringens förslag: Följande verksamhetsutövare ska betecknas som väsentliga:

- en verksamhetsutövare som är en statlig myndighet,
- en verksamhetsutövare som är en kommun eller en region och som är större än ett medelstort företag,
- en verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster och som storleksmässigt motsvarar eller är större än ett medelstort företag,
- en verksamhetsutövare som är en kvalificerad tillhandahållare av betrodda tjänster,

- en verksamhetsutövare som är en registreringsenhet för toppdomäner eller erbjuder DNS-tjänster, eller
- en verksamhetsutövare som är större än ett medelstort företag och som i övrigt omfattas av bilaga 1 till NIS 2-direktivet eller som är en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen om tillstånd att utfärda vissa examina.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela ytterligare föreskrifter om när verksamhetsutövare som omfattas av lagen med hänvisning till sin särskilda betydelse i samhället ska räknas som väsentliga.

Verksamhetsutövare som inte är väsentliga ska räknas som viktiga verksamhetsutövare.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår, när det gäller storlekskravet för verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster, att det ska röra sig om en verksamhet som är ett medelstort företag. Utredningen föreslår att verksamhetsutövare, som omfattas av lagen med hänvisning till sin särskilda betydelse i samhället, ska anses vara väsentliga om de har identifierats som sådana i förordning. Kommuner och regioner anges inte uttryckligen i utredningens lagförslag.

Remissinstanserna: *Advokatfirman Kahn Pedersen* anser att det bör förtydligas att även regioner är väsentliga verksamhetsutövare. *Finansiell ID-Teknik BID AB (BID)* anser att utfärdare av svensk e-legitimation på tillitsnivå 3 och 4 bör räknas som väsentliga verksamhetsutövare eftersom utfärdare av svensk elektronisk legitimation annars kan undgå att träffas av lagens tillämpningsområde. *Post- och telestyrelsen (PTS)* och *Scrive AB* efterfrågar ett förtydligande i fråga om hur lagen ska tillämpas i de situationer då en verksamhetsutövare tillhandahåller tjänster som gör att verksamhetsutövaren både klassificeras som väsentlig och viktig.

Skälen för regeringens förslag: Av artikel 3 i NIS 2-direktivet följer att entiteter antingen ska anses vara väsentliga eller viktiga. Följande entiteter ska anses vara väsentliga enligt artikel 3.1:

- Entiteter av en typ som avses i bilaga 1 som överstiger trösklarna för medelstora företag som fastställs i artikel 2.1 i bilagan till kommissionens rekommendation (a).
- Kvalificerade tillhandahållare av betrodda tjänster och registreringsenheter för toppdomäner samt leverantörer av DNS-tjänster, oavsett storlek (b).
- Tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster som betraktas som medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation (c).
- Offentliga förvaltningsentiteter som avses i artikel 2.2 f i (d).
- Alla andra entiteter av en typ som avses i bilaga 1 eller 2 som av en medlemsstat identifierats som väsentliga entiteter i enlighet med artikel 2.2 b–e (e).
- Entiteter som identifierats som kritiska entiteter enligt CER-direktivet, som avses i artikel 2.3 i NIS 2-direktivet (f).

- Entiteter som medlemsstaterna före den 16 januari 2023 har identifierat som leverantörer av samhällsviktiga tjänster i enlighet med NIS-direktivet eller nationell rätt, om så föreskrivs av medlemsstaten (g).

Vid tillämpningen av direktivet ska, enligt artikel 3.2, alla entiteter av en typ som avses i bilaga 1 eller 2 och som inte betraktas som väsentliga entiteter betraktas som viktiga entiteter. Detta inkluderar entiteter som av en medlemsstat identifierats som viktiga entiteter i enlighet med artikel 2.2 b–e.

De sektorer som avses i bilaga 1 och som nämns i artikel 3.1 a är de så kallade högkritiska sektorerna, det vill säga energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, förvaltning av IKT-tjänster mellan företag, offentlig förvaltning och rymden. I likhet med utredningen anser regeringen att en verksamhetsutövare som bedriver verksamhet som omfattas av bilagan bör räknas som en väsentlig verksamhetsutövare om verksamhetsutövaren är större än ett medelstort företag. Storlekskravet innebär att verksamhetsutövaren ska sysselsätta minst 250 personer eller ha en årsomsättning på minst 50 000 000 euro och en balansomslutning på minst 43 000 000 euro per år. I enlighet med resonemanget i avsnitt 5.3.2 bör inte undantaget i artikel 3.4 i bilagan till kommissionens rekommendation tillämpas vid bedömningen av om storlekskravet är uppfyllt.

Regeringen anser, i likhet med *Advokatfirman Kahn Pedersen*, att det bör förtydligas i lagtexten under vilka förhållanden regioner räknas som väsentliga verksamhetsutövare. En region räknas som en offentlig förvaltningsentitet på regional nivå enligt bilaga 1 och kommer därmed att vara väsentlig om den uppfyller storlekskravet. En kommun räknas som väsentlig verksamhetsutövare om den uppfyller storlekskravet och bedriver verksamhet inom de sektorer som avses i bilaga 1. Som utredningen anger bedriver merparten av kommunerna exempelvis hemsjukvård och omfattas därmed av bilaga 1. Regeringen anser, i likhet med utredningen, att samtliga kommuner som uppfyller storlekskravet bör räknas som väsentliga verksamhetsutövare.

Artikel 3.1 b omfattar tre olika kategorier av entiteter. Innebörden av uttrycken betrodd tjänst, registreringsenhet för toppdomäner och DNS-tjänster framgår av avsnitt 5.3.2. Skillnaden mellan tillhandahållare av en betrodd tjänst och kvalificerad tillhandahållare av en betrodd tjänst är att den sistnämnda ska ha beviljats status som kvalificerad av tillsynsorganet enligt artikel 3.20 i EU:s förordning om elektronisk identifiering. Därutöver är ett krav att en kvalificerad tillhandahållare tillhandahåller en eller flera kvalificerade betrodda tjänster. Som *BID* påpekar kommer utfärdare av elektronisk legitimation – om de inte också tillhandahåller en betrodd tjänst eller bedriver någon annan verksamhet som omfattas av lagen – inte att omfattas av lagens tillämpningsområde. Regeringen bedömer dock att regleringen i den nya lagen bör ligga nära direktivets utformning i detta avseende.

Innebörden av begreppen tillhandahållare av allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster, som nämns i artikel 3.1 c, behandlas i avsnitt 5.3.2. Det bör i sammanhanget uppmärksammas att storlekskravet för dessa entiteter

skiljer sig från det som anges i artikel 3.1 a. Sådana verksamhetsutövare bör enligt den nya lagen räknas som väsentliga om de storleksmässigt motsvarar eller är större än ett medelstort företag. Detta innebär att verksamheten ska sysselsätta minst 50 personer eller ha en omsättning och balansomslutning som överstiger 10 000 000 euro per år.

De offentliga förvaltningsentiteter som avses i artikel 3.1 d motsvarar statliga myndigheter som har befogenhet att fatta beslut som påverkar fysiska eller juridiska personer och deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital i enlighet med resonemanget i avsnitt 5.3.3. En statlig myndighet kan emellertid omfattas av lagen även om den inte räknas som en offentlig förvaltningsentitet enligt direktivet. Regeringen bedömer att en statlig myndighet som omfattas av lagen bör anses vara väsentlig, oavsett skälet till att myndigheten omfattas av lagen. Ett lärosäte omfattas, som utvecklas i avsnitt 5.3.4, av lagen om det antingen är en offentlig verksamhetsutövare eller är en enskild verksamhetsutövare. Regeringens bedömning, vilken överensstämmer med utredningens, är att en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen om tillstånd att utfärda examina bör räknas som väsentlig om den är större än ett medelstort företag.

Regeringen instämmer i utredningens uppfattning att medlemsstaterna, i enlighet med artiklarna 3.1 e och 3.2 i direktivet, får bestämma om de entiteter som avses i artikel 2.2 b–e är väsentliga eller viktiga. I avsnitt 5.3.2 föreslås att regeringen eller den myndighet som regeringen bestämmer ska få rätt att meddela ytterligare föreskrifter om kriterier för när verksamhetsutövare ska omfattas av lagen med hänvisning till sin särskilda betydelse i samhället. Utredningen föreslår att dessa verksamhetsutövare ska anses vara väsentliga om de har identifierats som sådana i den förordning som hör till lagen. I utredningens förslag till förordning lämnas förslag som innebär att Myndigheten för samhällsskydd och beredskap i föreskrifter får ange vilka verksamhetsutövare som omfattas av lagen med hänvisning till sin särskilda betydelse och om verksamhetsutövaren är väsentlig. Med hänvisning till att föreskrifter ska vara generellt tillämpbara bör det förtydligas att det handlar om en rätt att meddela föreskrifter om kriterier för när sådana verksamhetsutövare ska anses vara väsentliga snarare än utpekande av vissa fysiska eller juridiska personer som sådana.

Enligt artikel 3.1 g ska entiteter som identifierats som kritiska enligt CER-direktivet vara väsentliga. Utredningens förslag i slutbetänkandet om genomförandet av CER-direktivet bereds inom Regeringskansliet och är inte föremål för denna lagrådsremiss.

Av artikel 3.1 g följer att medlemsstater får föreskriva att entiteter som före den 16 januari 2023 har identifierats som leverantörer av samhällsviktiga tjänster i enlighet med NIS-direktivet eller nationell rätt är väsentliga. Som utredningen anger innebär detta att det är möjligt att föreskriva att samtliga leverantörer som tillhandahåller en samhällsviktig tjänst och som fram till och med den 15 januari 2023 omfattades av NIS-lagen ska kategoriseras som väsentliga. Regeringen instämmer i utredningens uppfattning att det inte finns något behov av att införa särskild reglering för de leverantörer som omfattas av den lagen.

PTS och *Scrive AB* efterfrågar ett förtydligande i fråga om hur lagen ska tillämpas i de situationer då en verksamhetsutövare tillhandahåller tjänster som gör att verksamhetsutövaren både kategoriseras som väsentlig och viktig. Kategoriseringen som väsentlig respektive viktig är av betydelse för vilka tillsynsåtgärder som kan vidtas och vilka ingripanden som kan komma i fråga i förhållande till verksamhetsutövaren (se vidare avsnitt 7 och 8). Om verksamhetsutövaren tillhandahåller någon tjänst som gör att denne är att betrakta som väsentlig så blir det avgörande för vilka tillsynsåtgärder och ingripande som kan bli aktuella i förhållande till denne.

5.4 Undantag från lagens tillämpningsområde

5.4.1 Undantag på grund av krav i andra författningar

Regeringens förslag: Om det i lag eller annan författning finns bestämmelser som innehåller krav på säkerhetsåtgärder eller incidentrapportering ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt den nya lagen, med beaktande av bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna.

Lagen ska inte tillämpas på sådana verksamheter som har undantagits enligt artikel 2.4 i 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 (DORA-förordningen).

Skyldigheterna enligt lagen, frånsett anmälningsskyldigheten och skyldigheten att utse företrädare, ska inte gälla för en verksamhetsutövare som omfattas av DORA-förordningen.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att regeringen i föreskrifter ska få ange vilka andra bestämmelser om riskhanteringsåtgärder och incidentrapportering som har motsvarande verkan. Utredningen föreslår inget undantag i lagen för verksamhetsutövare som omfattas av DORA-förordningen men däremot att det ska framgå av förordning.

Remissinstanserna: Flera remissinstanser, bland andra *Finansinspektionen*, *Sparbankernas Riksförbund* och *Svenska Bankföreningen*, tillstyrker utredningens förordningsförslag om undantag för verksamhetsutövare som omfattas av DORA-förordningen. Bland andra Finansinspektionen menar att det bör övervägas om undantaget ska regleras i lag. Sparbankernas riksförbund anser att det bör övervägas om de fåtal bestämmelser som träffar verksamhetsutövare som omfattas av DORA-förordningen kan införas i annan reglering än i den nya lagen. På så sätt skulle verksamhetsutövare som omfattas av DORA-förordningen helt kunna undantas från den nya lagens tillämpningsområde, vilket skulle bidra till ökad överskådlighet på området.

Euroclear vill se ett förtydligande av vilket genomslag det får att vissa verksamhetsutövare som endast träffas av anmälningsskyldigheten och tillhörande sanktioner omfattas av lagen. *Finansbolagens förening* efter-

lyser ett förtydligande av hur utredningens förordningsförslag gällande CSIRT-enhetens uppgifter förhåller sig till finansiella företag som omfattas av DORA-förordningen. *Länsstyrelsen i Västerbottens län* bedömer att det, för att uppnå en god cybersäkerhet i samhället, krävs regler som är enkla och tillgängliga. Förslaget om att den nya lagen ska vara subsidiär vid krav på riskhanteringsåtgärder eller incidentrapportering med motsvarande verkan i annan reglering bedöms bidra till oklarheter om tillämpningsområdet. Om den nya lagen ska vara subsidiär behöver det enligt länsstyrelsen framgå tydligt vilka rättsregler som har företräde.

Skälen för regeringens förslag: I artikel 2.10 i NIS 2-direktivet anges att direktivet inte är tillämpligt på entiteter som medlemsstaterna har undantagit från tillämpningsområdet för 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 (DORA-förordningen) i enlighet med artikel 2.4 i den förordningen.

I artikel 4.1 i NIS 2-direktivet finns också ett särskilt undantag kopplat till sektorsspecifika unionsrättsakter. Om det i sektorsspecifika unionsrättsakter föreskrivs att väsentliga eller viktiga entiteter ska anta riskhanteringsåtgärder för cybersäkerhet eller underrätta om betydande incidenter, och dessa krav har minst samma verkan som de skyldigheter som fastställs i direktivet, ska de relevanta bestämmelserna i direktivet, inbegripet bestämmelserna om tillsyn och efterlevnadskontroll, inte tillämpas på sådana entiteter. Om de sektorsspecifika unionsrättsakterna inte omfattar alla entiteter inom en viss sektor som omfattas av tillämpningsområdet, ska de relevanta bestämmelserna i direktivet fortsätta att tillämpas på de entiteter som inte omfattas av dessa sektorsspecifika unionsrättsakter.

De krav som avses i artikel 4.1 ska enligt artikel 4.2 anses ha samma verkan som de skyldigheter som fastställs i direktivet, om riskhanteringsåtgärderna minst är likvärdiga de åtgärder som föreskrivs i artikel 21.1 och 21.2 (a). Detsamma ska gälla om respektive sektorsspecifik unionsrättsakt föreskriver omedelbar, och när det är lämpligt automatisk och direkt, tillgång till incidentunderrättelser från CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna enligt NIS 2-direktivet och om kraven på underrättelse av betydande incidenter har minst samma verkan som de krav som fastställs i artikel 23.1–23.6 (b). Slutligen framgår av artikel 4 att kommissionen ska tillhandhålla riktlinjer som klargör tillämpningen av artikel 4.1 och 4.2. Sådana riktlinjer har publicerats i september 2023. Av meddelandet Kommissionens riktlinjer för tillämpningen av artikel 4.1 och 4.2 i direktiv (EU) 2022/2555 (NIS 2-direktivet) framgår att DORA-förordningen bör betraktas som en sektorsspecifik unionsakt och att medlemsstaterna inte bör tillämpa direktivets bestämmelser om riskhanterings- och rapporteringsskyldigheter på finansiella verksamhetsutövare som omfattas av den förordningen.

I 9 § NIS-lagen anges att om det i lag eller annan författning finns bestämmelser som innehåller krav på säkerhetsåtgärder och incidentrapportering ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt lagen, med beaktande av bestäm-

melsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelsen. I förarbetena till lagen anges att motsvarande bestämmelser om säkerhetsåtgärder och incidentrapportering kan finnas till exempel inom sjöfartssektorn, banksektorn och sektorn för finansmarknadsinfrastruktur. Däremot skulle kraven enligt den numera upphävda förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap eller kraven i EU:s dataskyddsförordning inte anses innebära motsvarande krav. I förarbetena anges att leverantörer därmed kan behöva tillämpa NIS-lagen och dessa regelverk parallellt (se prop. 2017/18:205 s. 29).

Regeringen delar utredningens uppfattning att ett undantag som motsvarar det som finns i NIS-lagen bör gälla enligt den nya lagen och oavsett om bestämmelserna finns i EU-rättsakter eller i nationell författning. Enligt regeringen inbegriper krav om säkerhetsåtgärder och incidentrapportering även de närliggande kraven på utbildning och information (se avsnitt 6.5 och 6.6.3). Innebörden av undantaget bör därmed vara att skyldigheten att, i förekommande fall, utse företrädare och att göra en anmälan ska gälla (se vidare avsnitt 6.1 och 6.2). För vissa verksamhetsutövare gäller också en skyldighet att föra register, vilken behandlas i avsnitt 10.

Undantaget i NIS 2-direktivet tar sikte på författningar som innehåller krav på säkerhetsåtgärder eller incidentrapportering med motsvarande verkan. Det kan uppkomma situationer då enstaka bestämmelser i annan reglering innehåller krav på säkerhetsåtgärder eller incidentrapportering. I dessa fall anser regeringen inte att dessa enstaka bestämmelser ska gälla i stället för motsvarande bestämmelser i den nya lagen. I likhet med resonemanget som fördes kring motsvarande bestämmelse i NIS-lagen anser inte regeringen att en sådan ordning är ändamålsenlig (se prop. 2017/18:205 s. 29).

Utredningen föreslår att det i en bilaga till förordningen som hör till lagen ska framgå vilka författningar som innehåller bestämmelser med krav på riskhanteringsåtgärder och rapportering om betydande incidenter som motsvarar verkan av skyldigheterna enligt lagen. I den nämns endast DORA-förordningen. Regeringen delar *Länsstyrelsen i Västerbottens läns* uppfattning att rättsregler bör vara enkla och tillgängliga. Det är dock inte görbart att sammanställa samtliga rättsregler som kan anses ha motsvarande verkan.

I likhet med till exempel *Finansinspektionen* anser regeringen att det bör framgå redan av lagen att krav om exempelvis säkerhetsåtgärder och incidentrapportering inte ska gälla en verksamhetsutövare som omfattas av DORA-förordningen. Det rör sig om de kreditinstitut som omfattas av sektorn bankverksamhet och de operatörer av handelsplatser och centrala motparter som omfattas av sektorn finansmarknadsinfrastruktur i bilaga 1 till NIS 2-direktivet. För dessa verksamhetsutövare bör endast anmälningsskyldigheten och, i förekommande fall, skyldigheten att utse en företrädare samt de tillsyns- och ingripandemöjligheter som finns kopplat till dessa skyldigheter gälla.

Euroclear vill se ett förtydligande av vilket genomslag det får att vissa verksamhetsutövare endast träffas av en begränsad del av lagen. Regeringen konstaterar att skyldigheten att utse företrädare och göra en anmälan är en följd av direktivets utformning. Det finns därför inte

utrymme för att föreslå en ordning där vissa verksamhetsutövare även är undantagna från dessa skyldigheter.

Finansbolagens förening efterlyser ett förtydligande av hur CSIRT-enhetens uppgifter enligt 29 och 30 §§ i utredningens förslag till förordning, som kan avse finanssektorn, är tänkt att fungera när det gäller finansiella företag som omfattas av DORA-förordningen. I nämnda paragrafer föreslås CSIRT-enheten bland annat övervaka och analysera cyberhot, ta emot incidentrapport och få möjlighet att utföra vissa typer av skanningar. CSIRT-enhetens uppgifter följer bland annat av artikel 11 i NIS 2-direktivet. Utredningens förslag till förordning är inte föremål för denna lagrådsremiss och regeringen bedömer inte heller att det krävs något sådant förtydligande som Finansbolagens förening efterfrågar bland annat med hänvisning till direktivets innehåll.

Sparbankernas riksförbund anser att det bör övervägas om de fåtal bestämmelser som träffar de verksamhetsutövare som omfattas av DORA-förordningen kan införas i annan reglering än som nu föreslås. Exempelvis skulle, enligt förbundet, regler för verksamhetsutövare att rapportera uppgifter till tillsynsmyndigheten kunna införas i lagen med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn som föreslås i promemorian Digital operativ motståndskraft för finanssektorn (Fi2024/00073). Lagen (2024:1278) med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn (kompletteringslagen) trädde i kraft den 17 januari 2025. Regeringen anser att det finns ett värde i att samla de bestämmelser som krävs för genomförandet av NIS 2-direktivet i samma lag. Det bör därför inte föras in några andra bestämmelser i kompletteringslagen som krävs för genomförandet av direktivet.

För Sveriges del är Svenska skeppshypotekskassan en sådan entitet som kan undantas från DORA-förordningen. Möjligheten enligt artikel 2.4 i DORA-förordningen att göra undantag för vissa enheter har inte utnyttjats (se prop. 2024/25:44 s. 73). Regeringen bedömer oavsett detta, givet artikel 2.10 i NIS 2-direktivet, att det bör införas ett sådant undantag som utredningen föreslår i förhållande till DORA-förordningen.

5.4.2 Undantag för viss säkerhetskänslig verksamhet och brottsbekämpande verksamhet

Regeringens förslag: Lagen ska inte gälla för en enskild verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet.

Lagen ska inte gälla för en statlig myndighet som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet. Lagen ska inte heller gälla för en enskild verksamhetsutövare som enbart erbjuder tjänster till en sådan statlig myndighet.

För andra verksamhetsutövare som till någon del bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet eller till någon del erbjuder tjänster till en sådan statlig myndighet som anges ovan ska skyldigheterna enligt lagen, frånsett skyldigheten att utse företrädare och anmälningsskyldigheten, inte gälla i förhållande till den säkerhets-

känsliga verksamheten eller brottsbekämpande verksamheten eller den verksamhet som erbjuder tjänsterna.

Undantagen ska inte gälla för en verksamhetsutövare som tillhandahåller betrodda tjänster.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att enskilda verksamhetsutövare som enbart bedriver brottsbekämpande verksamhet ska undantas från lagens tillämpningsområde. Utredningen föreslår att regeringen i föreskrifter ska få ange vilka statliga myndigheter som bedriver säkerhetskänslig verksamhet eller brottsbekämpning till övervägande del.

Remissinstanserna: Bland andra *Försvarsmakten* och *Försvarsunderrättelsedomstolen* tillstyrker utredningens förslag att statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet ska undantas från lagens tillämpningsområde.

Många länsstyrelser, däribland *länsstyrelserna i Blekinge*, *Dalarnas* och *Värmlands län*, anser att undantag inte bör göras för säkerhetskänslig verksamhet och brottsbekämpande verksamhet. Det skulle, enligt länsstyrelserna, underlätta tillämpningen och öka acceptansen för regelverket om samtliga aktörer omfattas av lagens tillämpningsområde. Flera remissinstanser, bland andra *Myndigheten för samhällsskydd och beredskap (MSB)* och *Säkerhetspolisen*, menar att även den säkerhetskänsliga verksamheten bör omfattas av kraven på att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete, vidta säkerhetsåtgärder och genomföra utbildning.

Kustbevakningen och *Myndigheten för totalförsvarsanalys (MTFA)* anser att det är otydligt vad som avses med att en verksamhetsutövare till övervägande del bedriver säkerhetskänslig verksamhet. Det bör enligt Kustbevakningen särskilt noteras att NIS 2-direktivet inte kräver att någon av de uppräknade verksamheterna, endast sedd för sig, bedrivs till övervägande del för att undantag från direktivets tillämpningsområde ska vara tillåtet. Det bör alltså enligt Kustbevakningen finnas utrymme för att i stället göra en helhetsbedömning av den verksamhet som en myndighet sammantaget bedriver på de aktuella områdena. Kustbevakningen nämner också att vad som anses utgöra säkerhetskänslig verksamhet enligt säkerhetsskyddslagen är föränderligt och att förslaget kan ge upphov till gränsdragningsproblem vid tillämpningen av den föreslagna paragrafen. MTFA resonerar kring myndighetens uppdrag och bedömer att uppdragets karaktär i praktiken gör den säkerhetskänsliga delen odelbar från den övriga. Att stå under tillsyn från såväl Försvarsmakten som en tillsynsmyndighet enligt den nya lagen kommer att medföra osäkerheter gällande gränsdragningar och otydliga ansvarsförhållanden. Ett flertal remissinstanser, bland andra *Tullverket*, resonerar kring om de bör omfattas av lagen eller inte med hänvisning till att de bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet.

Ett stort antal remissinstanser, bland andra *Drivkraft Sverige* och *Skatteverket*, anser att förhållandet mellan den nya lagen och säkerhetsskyddsregleringen bör förtydligas. *Netnod AB* menar att förslaget kan medföra att en verksamhetsutövare föredrar att verksamheten lyder under säkerhetsskyddslagstiftningen, eftersom den är mindre betungande och därför utvidgar säkerhetsanalysen därefter. *Göteborgs kommun* efterfrågar

ett förtydligande i fråga om innebörden av brottsbekämpande verksamhet i förhållande till kommunerna. Flera remissinstanser, till exempel *Myndigheten för psykologiskt försvar (MPF)* och *Statens energimyndighet*, anser att det i den fortsatta beredningen bör tas fram en beskrivning över hur NIS 2- och CER-regleringarna förhåller sig till beredskapssystemet. Ett antal remissinstanser, såsom *Strålsäkerhetsmyndigheten (SSM*), anser att regeringen bör överväga att tillsätta en utredning efter att NIS 2- och CER-direktiven har införlivats i svensk rätt med uppdrag att se över hur de nya lagarna förhåller sig till beredskapsregleringen.

Post- och telestyrelsen (PTS) påpekar att det för närvarande inte finns någon statlig myndighet som är en tillhandahållare av en betrodd tjänst men att det kan ändras framöver på grund av EU-reglering.

Skälen för regeringens förslag

Undantaget i direktivet

Av artikel 2.6 i NIS 2-direktivet framgår att direktivet inte påverkar medlemsstaternas ansvar att skydda nationell säkerhet och deras befogenhet att skydda andra väsentliga statliga funktioner, inbegripet att säkerställa statens territoriella integritet och upprätthålla lag och ordning. Av artikel 2.7 följer att direktivet inte är tillämpligt på offentliga förvaltningsentiteter som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott.

Undantaget för offentliga förvaltningsentiteter bör enligt skäl 8 i direktivet omfatta entiteter vars verksamhet till övervägande del bedrivs på de områdena som avses i artikel 2.7. Offentliga förvaltningsentiteter vars verksamhet endast marginellt hänför sig till dessa områden bör dock, enligt samma skäl, inte vara undantagna från direktivets tillämpningsområde. Vid tillämpningen av direktivet anses vidare entiteter med tillsynsbefogenheter inte bedriva verksamhet på brottsbekämpningsområdet, och de är därför inte undantagna från tillämpningsområdet för direktivet. Däremot är offentliga förvaltningsentiteter som inrättats gemensamt med ett tredjeland i enlighet med ett internationellt avtal undantagna från direktivets tillämpningsområde enligt samma skäl. Direktivet är inte heller tillämpligt på medlemsstaters diplomatiska och konsulära beskickningar i tredjeländer eller på deras nätverks- och informationssystem, såvida dessa system är belägna inom beskickningen eller drivs för användare i ett tredjeland.

Medlemsstaterna får enligt artikel 2.8 undanta särskilda entiteter som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott, eller som tillhandahåller tjänster uteslutande till en offentlig förvaltningsentitet som avses i artikel 2.7 från skyldigheterna i artiklarna 21 eller 23, som handlar om riskhanteringsåtgärder och rapporteringsskyldigheter, med avseende på sådan verksamhet eller sådana tjänster. I sådana fall ska, enligt artikel 2.8, tillsyns- och efterlevnadskontrollåtgärder inte tillämpas på den specifika verksamheten eller de specifika tjänsterna. Om entiteterna bedriver verksamhet eller tillhandahåller tjänster uteslutande av aktuell typ, får medlemsstaterna besluta att befria dessa entiteter också från skyldig-

heterna i artiklarna 3 och 27 som handlar om skyldighet att lämna vissa uppgifter om väsentliga och viktiga entiteter.

I skäl 9 anges vidare att medlemsstaterna bör kunna vidta de åtgärder som är nödvändiga för att skydda väsentliga nationella säkerhetsintressen, upprätthålla allmän ordning och säkerhet och möjliggöra förebyggande, utredning, upptäckt och lagföring av brott. I detta syfte bör medlemsstaterna kunna undanta särskilda entiteter som bedriver verksamhet på områdena, nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott, från vissa skyldigheter i direktivet med avseende på sådan verksamhet. Om en entitet tillhandahåller tjänster uteslutande för en offentlig förvaltningsentitet som är undantagen från direktivets tillämpningsområde bör medlemsstaterna enligt nyss nämnda skäl kunna undanta den entiteten från vissa skyldigheter med avseende på dessa tjänster.

I artikel 2.9 anges att undantagen i artikel 2.7 och 2.8 inte ska gälla för en entitet som agerar som en tillhandahållare av betrodda tjänster.

Vad tar undantagen sikte på för verksamhet?

NIS 2-direktivet är inte tillämpligt på offentliga förvaltningsentiteter som bedriver verksamhet inom områdena nationell säkerhet, allmän säkerhet, försvar och brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott. Det utvecklas inte närmare i direktivet vad som avses med uttrycken. För att genomföra direktivet på korrekt sätt i nationell rätt krävs en tolkning av vad de avser för slags verksamhet i Sverige.

Som utredningen anger är uttrycket nationell säkerhet ett vedertaget begrepp inom unionsrätten, men saknar en tydlig definition i densamma. I Sverige används uttrycket Sveriges säkerhet i olika sammanhang. Som utredningen anger har innebörden av uttrycket behandlats i flera lagstiftningsärenden de senaste åren (se till exempel prop. 2022/23:116 s. 21). Uttrycket tar sikte på förhållanden av grundläggande betydelse för Sverige. 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 för detta skyddsintresse. En slutsats av det anförda är att direktivet bland annat inte är tillämpligt på säkerhetskänslig verksamhet.

Uttrycket allmän säkerhet i direktivet bör, i likhet med vad utredningen anger, anses 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. Vilken verksamhet som uttrycket försvar avser i direktivet bör enligt regeringen inte kräva någon närmare analys.

NIS 2-direktivet är inte tillämpligt på offentliga förvaltningsentiteter som bedriver verksamhet inom området brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott. Utredningen bedömer att undantaget tar sikte på de myndigheter som betecknas som rättsvårdande myndigheter.

Med brottsbekämpande verksamhet avses, i bland annat lagen (2025:170) om skyldighet att lämna uppgifter till de brottsbekämpande

myndigheterna, sådan verksamhet som en brottsbekämpande myndighet bedriver för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda eller lagföra brott. Verksamhet för att verkställa straffrättsliga påföljder, upprätthålla allmän ordning och säkerhet och sådan kontrollverksamhet som brottsbekämpande myndigheter i vissa fall bedriver omfattas inte av uttrycket i lagen (se prop. 2024/25:65 s. 201).

I förarbetena till lagen om skyldighet att lämna uppgifter till de brottsbekämpande myndigheterna anges att det är underrättelseverksamhet som avses när formuleringen förebygga, förhindra eller upptäcka brottslig verksamhet används. Med att utreda brott avses vidare i lagen framför allt att genomföra förundersökning enligt 23 kap. rättegångsbalken. Med brott avses ett konkret brott. Med uttrycket lagföra brott avses i lagen framför allt åklagares beslut i åtalsfrågor och om åtalsunderlåtelser samt brottmålsförfarandet i allmän domstol. Enligt regeringens mening bör uttrycket brottsbekämpande verksamhet i den nya lagen ha samma innebörd som i lagen om skyldighet att lämna uppgifter till de brottsbekämpande myndigheterna.

Undantag för statliga myndigheter som till övervägande del bedriver aktuell verksamhet

Flera remissinstanser, däribland många länsstyrelser, *MSB* och *Säkerhetspolisen*, anser att undantag inte bör göras för säkerhetskänslig verksamhet och brottsbekämpande verksamhet. Säkerhetsskyddsregleringen gäller för de mest skyddsvärda verksamheterna i samhället och verksamhetsutövare som omfattas av säkerhetsskyddslagen står under tillsyn enligt den lagen. Regeringen bedömer att det inte skulle vara en ändamålsenlig lösning att låta dessa verksamhetsutövare omfattas av krav och även stå under tillsyn enligt den nya lagen. Att det skulle underlätta tillämpningen och öka acceptansen för regelverket om samtliga aktörer omfattas av lagens tillämpningsområde bedömer regeringen inte heller utgör tillräckligt skäl för att låta myndigheter som bedriver brottsbekämpande verksamhet till övervägande del omfattas.

Enligt regeringens uppfattning, vilken överensstämmer med utredningens, bör de offentliga verksamhetsutövare som undantas helt från lagens tillämpningsområde vara de verksamhetsutövare som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen eller brottsbekämpande verksamhet. Detta innebär, i linje med utredningens resonemang, att endast statliga myndigheter bör undantas i sin helhet från lagens tillämpningsområde. Regeringen anser inte att det är en lämplig ordning, som utredningen föreslår, att det av en förordning ska framgå vilka statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet. Det finns inte heller skäl för att i en förordning ange vilka myndigheter som till övervägande del bedriver brottsbekämpande verksamhet. Det bör inte införas något sådant bemyndigande för regeringen som utredningen föreslår i denna del.

Eftersom undantaget i en del knyts till säkerhetsskyddslagens tillämpningsområde finns det inte skäl för att, trots vissa remissinstansers begäran om förtydliganden, resonera kring vilka enskilda myndigheter som kommer att anses omfattas av detsamma. Vilka myndigheter som bedriver

säkerhetskänslig verksamhet till övervägande del får bedömas i varje enskilt fall.

Kustbevakningen och *MTFA* anser att det är otydligt vad som avses med att en verksamhetsutövare till övervägande del bedriver viss slags verksamhet. Med övervägande del bör avses att myndighetens huvudsakliga verksamhet rör säkerhetskänslig verksamhet eller utgör brottsbekämpning. *Göteborgs kommun* efterfrågar ett förtydligande i fråga om innebörden av undantaget för brottsbekämpande verksamhet i förhållande till kommunerna. Som Göteborgs kommun påpekar har kommunerna ett ansvar att bedriva brottsförebyggande arbete vilket bland annat framgår av lagen (2023:196) om kommunernas ansvar för brottsförebyggande arbete. Regeringen konstaterar dock att detta inte kan anses innebära att kommuner omfattas av undantaget.

Kustbevakningen anser att direktivet inte kräver att någon av de uppräknade verksamheterna, endast sedd för sig, bedrivs till övervägande del för att undantaget ska vara tillåtet. Myndigheten bedömer därför att det bör finnas utrymme för att göra en helhetsbedömning av den verksamhet som en myndighet sammantaget bedriver på de aktuella områdena. Om en verksamhetsutövare till någon mindre del, än till övervägande del, bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet föreslås endast kravet på anmälan och, i förekommande fall, kravet på att utse företrädare gälla för den delen av verksamheten (se avsnittet nedan). Regeringen bedömer att detta är en ändamålsenlig lösning och att det inte bör göras en sådan helhetsbedömning som Kustbevakningen nämner.

Regeringen konstaterar att frågan om att tillsätta en sådan utredning och ta fram en sådan beskrivning som *SSM* och bland andra *MPF* föreslår ligger utanför sådant som kan behandlas inom ramen för denna lagrådsremiss.

I vissa fall bör endast en del av verksamheten vara undantagen

I likhet med utredningen anser regeringen att en särregel bör gälla för offentliga verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet men inte till övervägande del. För dessa verksamhetsutövare bör den säkerhetskänsliga delen av verksamheten och verksamheten som avser brottsbekämpning undantas från kravet på att vidta bland annat säkerhetsåtgärder och genomföra incidentrapportering. Innebörden blir att den säkerhetskänsliga delen av verksamheten och den del som avser brottsbekämpning endast kommer att omfattas av anmälningsskyldigheten som behandlas i avsnitt 6.2 samt ingripanden kopplat till detta krav (se avsnitt 8). För den övriga verksamheten bör lagen gälla i sin helhet. Även om regeringen har förståelse för *Kustbevakningens* och *MTFA:s* synpunkter att det kan vara svårt att särskilja vilken del av verksamheten som är undantagen från den övriga anser regeringen inte att artikel 2.7 i direktivet, utifrån formuleringen i skäl 8, ger utrymme för en annan lösning.

Bland andra *Skatteverket* önskar förtydliganden i fråga om hur lagen förhåller sig till säkerhetskyddsregleringen och till exempel *Statens energimyndighet* efterfrågar en beskrivning om hur lagen förhåller sig till beredskapssystemet. Regeringen konstaterar att regelverken kommer att gälla parallellt. En beskrivning av hur rapporteringsskyldigheten enligt

lagen förhåller sig till skyldigheter enligt säkerhetsskyddslagen finns i avsnitt 6.6.2.

Undantag för enskilda verksamhetsutövare

Regeringens bedömning, vilken överensstämmer med utredningens, är att innebörden av artikel 2.8 i NIS 2-direktivet är att enskilda verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet helt bör undantas från lagens krav. Detsamma bör gälla för en enskild verksamhetsutövare som enbart erbjuder tjänster till en statlig myndighet som är helt undantagen från lagens tillämpningsområde med hänvisning till att den bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet. Utredningen föreslår ett undantag för enskilda verksamhetsutövare som enbart bedriver brottsbekämpande verksamhet men utvecklar inte vilka som skulle omfattas av ett sådant undantag. I motsats till utredningen kan regeringen inte se att det finns anledning att göra undantaget.

För övriga enskilda verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller erbjuder tjänster till en statlig myndighet som är undantagen från lagens tillämpningsområde men i annan utsträckning, bör bland annat kraven på säkerhetsåtgärder och incidentrapportering inte gälla för den säkerhetskänsliga delen av verksamheten eller den del av verksamheten som erbjuder tjänsterna. Innebörden blir att den delen av verksamheten kommer att omfattas av anmälningsskyldigheten och, i förekommande fall, skyldigheten att utse en företrädare, som behandlas i avsnitt 6.1 respektive 6.2, samt tillsyn och ingripanden kopplat till dessa krav (se avsnitt 7 och 8). För den delen av verksamheten som inte är säkerhetskänslig eller tillhandahåller tjänsterna gäller lagen i dess helhet.

Netnod AB anser att en oönskad effekt av förslaget är att verksamhetsutövare föredrar att verksamheten lyder under säkerhetsskyddslagstiftningen, eftersom den är mindre betungande och därför utvidgar säkerhetsanalysen därefter. Regeringen konstaterar att säkerhetsskyddslagen och den nya lagen har olika tillämpningsområden och syften. Införandet av den nya lagen innebär inte några förändrade krav enligt säkerhetsskyddslagen. De verksamhetsutövare som omfattas av den lagstiftningen ska alltjämt göra noggranna säkerhetsskyddsanalyser och vidta de säkerhetsskyddsåtgärder som bedöms nödvändiga utifrån den analysen.

Undantagen i artikel 2.7 och 2.8 gäller inte för en verksamhetsutövare som agerar som en tillhandahållare av betrodda tjänster. Vad som avses med sådana tjänster behandlas i avsnitt 5.3.2. Tillhandahållare av betrodda tjänster ska således omfattas av lagen oavsett om verksamhetsutövaren bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet eller enbart erbjuder sådana tjänster till en statlig myndighet som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet. Regeringen delar *PTS* uppfattning att det inte kan uteslutas att en myndighet framöver kan vara tillhandahållare av en betrodd tjänst.

5.4.3 Undantag för säkerhetsskyddsklassificerade uppgifter

Regeringens förslag: Skyldigheterna att lämna uppgifter enligt lagen ska inte gälla säkerhetsskyddsklassificerade uppgifter.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Flera remissinstanser, bland andra *Försvarets materielverk* och *Säkerhetspolisen*, tillstyrker förslaget. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: Av artikel 2.6 i NIS 2-direktivet följer att direktivet inte påverkar medlemsstaternas ansvar för att skydda nationell säkerhet och andra väsentliga statliga funktioner inbegripet att säkerställa statens territoriella integritet och upprätthålla lag och ordning. Av skäl 9 framgår att ingen medlemsstat bör vara skyldig att lämna information vars avslöjande skulle strida mot dess väsentliga intressen i fråga om nationell säkerhet, allmän säkerhet eller försvar. I detta sammanhang bör även unionsregler eller nationella regler till skydd för säkerhetsskyddsklassificerade uppgifter, sekretessavtal samt informella sekretessavtal såsom Traffic Light Protocol beaktas.

Med säkerhetsskyddsklassificerade uppgifter avses i 1 kap. 2 § säkerhetsskyddslagen 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. I bland annat avsnitt 6.2 föreslås att verksamhetsutövare ska vara skyldiga att lämna ut uppgifter med stöd av den nya lagen. För att säkerställa att säkerhetsskyddsklassificerade uppgifter inte lämnas ut med stöd av den nya lagen är det, som utredningen anger, inte tillräckligt att vissa verksamhetsutövare som bedriver säkerhetskänslig verksamhet undantas från lagens tillämpningsområde. Det bör införas ett undantag som innebär att skyldigheter att lämna ut uppgifter enligt lagen inte avser säkerhetsskyddsklassificerade uppgifter.

6 Verksamhetsutövares skyldigheter

6.1 Vissa enskilda verksamhetsutövare ska utse en företrädare

Regeringens förslag: Verksamhetsutövare som erbjuder vissa tjänster i Sverige, men saknar etablering inom EES, ska utse en företrädare med etablering i Sverige eller i något annat land inom EES där tjänsterna erbjuds.

Skyldigheten ska gälla om verksamhetsutövaren är en registreringsenhet för toppdomäner eller erbjuder DNS-tjänster eller domännamnsregistreringtjänster. Skyldigheten ska också gälla om verksamhetsutövaren storleksmässigt motsvarar eller större än ett medelstort företag och erbjuder molntjänster, datacentraltjänster, nätverk för leverans av innehåll, utlokaliserade driftstjänster, utlokaliserade säkerhetstjänster,

marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna har inga synpunkter på eller yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: Om en entitet som avses i artikel 26.1 b i NIS 2-direktivet inte är etablerad i unionen, men erbjuder tjänster inom unionen, ska den enligt artikel 26.3 utse en företrädare i unionen. Företrädaren ska enligt artikel 26.3 vara etablerad i en av de medlemsstater där tjänsterna erbjuds. Om det inte finns en utsedd företrädare i unionen får varje medlemsstat där entiteten tillhandahåller tjänster vidta rättsliga åtgärder mot entiteten för överträdelsen av direktivet. I artikel 26.4 anges att det faktum att en entitet har underlåtit att utse en företrädare inte ska påverka eventuella rättsliga åtgärder mot entiteten i sig.

I avsnitt 5.3.2 behandlas vilka entiteter som avses i artikel 26.1 b. Regeringen föreslår i det avsnittet att lagen ska gälla för en verksamhetsutövare som har sitt huvudsakliga etableringsställe i Sverige, eller en företrädare som är etablerad i Sverige, om verksamhetsutövaren storleksmässigt motsvarar eller är större än ett medelstort företag och erbjuder molntjänster, datacentraltjänster, nätverk för leverans av innehåll, marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster, eller är en leverantör av utlokaliserade driftstjänster eller utlokaliserade säkerhetstjänster. Lagen föreslås även gälla för en verksamhetsutövare som har sitt huvudsakliga etableringsställe i Sverige, eller en företrädare som är etablerad i Sverige, och som är en registreringsenhet för toppdomäner eller erbjuder DNS-tjänster eller domännamnsregistreringstjänster. Dessa verksamhetsutövare bör som utredningen föreslår vara skyldiga att utse en företrädare med etablering i Sverige eller något annat land inom Europeiska ekonomiska samarbetsområdet (EES) där tjänsterna erbjuds, om etablering saknas inom EES.

Utifrån ordalydelsen av artikel 26.3 är det ett alternativ att låta verksamhetsutövaren utse en företrädare i EU i stället för inom EES. Något beslut om att införliva NIS 2-direktivet i EES-avtalet har inte fattats, men NIS-direktivet införlivades genom beslut den 3 februari 2023. Regeringen anser, mot denna bakgrund, att utredningens förslag i denna del bör genomföras.

6.2 Samtliga verksamhetsutövare ska göra en anmälan

Regeringens förslag: Verksamhetsutövare ska så snart det kan ske anmäla sig till den myndighet som regeringen bestämmer.

Verksamhetsutövare ska anmäla en förändring avseende i anmälan lämnade uppgifter så snart det kan ske, dock senast 14 dagar efter det att förändringen ägde rum.

Utredningens förslag överensstämmer delvis med regeringens förslag. Utredningen föreslår att anmälan ska göras till tillsynsmyndigheten, att det ska regleras i lag vilka uppgifter anmälan ska innehålla och att ändrade uppgifter ska anmälas inom 14 dagar. Utredningen lämnar inget förslag

om när verksamhetsutövare ska göra en anmälan. Utredningen föreslår ett bemyndigande i fråga om anmälans innehåll.

Remissinstanserna: Ett stort antal remissinstanser, bland andra *Livsmedelsverket*, *Läkemedelsverket*, *Länsstyrelsen i Norrbottens län* och *Myndigheten för samhällsskydd och beredskap (MSB)*, anser att det vore mer ändamålsenligt och resurseffektivt med ett centralt system för insamling och hantering av anmälningar än vad utredningen föreslår. Några remissinstanser, däribland MSB, *Skatteverket* och *Statens energimyndighet*, understryker att anmälningarna kommer att innehålla vissa känsliga uppgifter och att de därför bör göras i ett system med en tillräckligt hög nivå av säkerhet. De förordar därför att MSB, i egenskap av gemensam kontaktpunkt enligt utredningens förslag till förordning, ska få i uppdrag att tillhandahålla en gemensam plattform som möjliggör detta. *Post- och telestyrelsen (PTS)* tillstyrker å andra sidan utredningens förslag om att verksamhetsutövare ska göra en anmälan till respektive tillsynsmyndighet. Även *Telenor Sverige AB (Telenor)* anser att PTS, i egenskap av sådan tillsynsmyndighet, bör hantera anmälningarna gällande sektorn digital infrastruktur på samma sätt som myndigheten hanterar registret för tillhandahållare av elektroniska kommunikationsnät och kommunikationstjänster.

Certezza AB anser att det inte behöver framgå av lag inom vilken tid förändringar ska anmälas, utan menar att detta kan regleras på lägre föreskriftsnivå. Livsmedelsverket föreslår att ändrade uppgifter ska anmälas utan dröjsmål.

Certezza AB och *Finansiell ID-Teknik BID AB (BID)* yttrar sig över utredningens förslag om anmälans innehåll. Certezza AB anser att innehållet bör kunna regleras på lägre föreskriftsnivå än i lag.

Strålsäkerhetsmyndigheten (SSM) bedömer att det bör göras ett tillägg i bestämmelsen om anmälningsskyldighet som tydliggör att kraven på anmälan inte inbegriper de system och den delen av verksamheten som omfattas av säkerhetsskyddslagen.

Skälen för regeringens förslag

Identifiering av verksamhetsutövare genom anmälan

Enligt artikel 3.3 i NIS 2-direktivet ska medlemsstaterna senast den 17 april 2025 upprätta en förteckning över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster. Medlemsstaterna ska enligt samma artikel regelbundet och minst vartannat år därefter se över förteckningen och uppdatera den när det är lämpligt. Enligt artikel 3.5 ska de behöriga myndigheterna bland annat underrätta kommissionen om antalet väsentliga och viktiga entiteter som ingår i förteckningen. Syftet med förteckningen är att skapa en tydlig överblick över de entiteter som omfattas av direktivets tillämpningsområde (skäl 18). Vid upprättandet av förteckningen ska medlemsstaterna enligt artikel 3.4 ålägga entiteterna att lämna vissa uppgifter och medlemsstaterna får inrätta nationella mekanismer som gör det möjligt för entiteterna att registrera sig själva. Entiteterna ska enligt samma bestämmelse meddela alla ändringar av de uppgifter som de har lämnat in utan dröjsmål och under alla omständigheter inom två veckor från datumet för ändringen.

Av artikel 27.1 framgår att Enisa ska skapa och upprätthålla ett register över de entiteter som avses i avsnitt 6.1. Medlemsstaterna ska ålägga berörda entiteter att lämna vissa uppgifter om verksamheten samt säkerställa att entiteterna underrättar om eventuella ändringar av uppgifterna utan dröjsmål och under alla omständigheter inom tre månader från dagen för ändring (artikel 27.2 och 27.3). Informationen ska medlemsstaterna vidarebefordra till Enisa via den gemensamma kontaktpunkten (artikel 27.4). Av artikel 27.5 följer att informationen som avses i artikel 27.2 och 27.3 i tillämpliga fall ska lämnas genom den nationella mekanism för självregistrering som avses i artikel 3.4.

För att Sverige ska kunna uppfylla sina skyldigheter enligt nämnda bestämmelser bör det, som utredningen föreslår, införas en bestämmelse om anmälningsplikt för verksamhetsutövare i den nya lagen. *SSM* gör gällande att det bör förtydligas att anmälningsskyldigheten inte gäller för den del av verksamheten som omfattas av säkerhetsskyddslagen. Enligt förslaget i avsnitt 5.4.2 gäller inte lagen för statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet och inte heller för enskilda verksamhetsutövare som enbart bedriver sådan verksamhet. Lagen föreslås därutöver inte gälla för verksamhetsutövare som enbart erbjuder tjänster till statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet. För andra verksamhetsutövare som till någon del bedriver säkerhetskänslig verksamhet eller erbjuder sådana tjänster gäller inte flertalet av skyldigheterna enligt lagen för den delen av verksamheten. Däremot gäller skyldigheten att göra en anmälan även för den delen av verksamheten som bedriver säkerhetskänslig verksamhet eller som tillhandahåller tjänsterna och i förekommande fall även skyldigheten att utse en företrädare. Skyldigheten att lämna uppgifter enligt den nya lagen föreslås dock inte gälla för uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen. Regeringen bedömer att det inte behövs något förtydligande om att kraven på anmälan inte inbegriper den delen av verksamheten som omfattas av säkerhetsskyddslagen som SSM efterfrågar.

Anmälan bör göras till den myndighet som regeringen bestämmer

I avsnitt 7.1 föreslår regeringen att den myndighet som regeringen bestämmer ska utöva tillsyn bland annat över att den nya lagen och föreskrifter som har meddelats i anslutning till lagen följs. Remissutfallet är blandat i fråga om utredningens förslag om att anmälan ska göras till tillsynsmyndigheten. Regeringen konstaterar att flera av de verksamhetsutövare som kommer att omfattas av den nya lagen bedriver verksamhet inom olika sektorer och de kommer därmed att falla in under flera olika tillsynsmyndigheters ansvarsområden. Detta skulle, som bland annat *Läkemedelsverket* påpekar, kunna innebära ett förhållandevis komplicerat anmälningsförfarande för verksamhetsutövaren om en anmälan ska göras till varje tillsynsmyndighet. Dessutom skulle en sådan ordning innebära att samtliga tillsynsmyndigheter behöver utveckla och tillhandahålla system som kan hantera anmälningarna med en tillräcklig nivå av säkerhet.

Enligt artikel 8 i NIS 2-direktivet ska varje medlemsstat utse en gemensam kontaktpunkt. Som utredningen föreslår bör utpekande av den svenska kontaktpunkten inte ske i lag. MSB har i ett regeringsuppdrag som

beslutades den 27 februari 2025 pekats ut som bland annat gemensam kontaktpunkt (Fö2025/00387). Flera remissinstanser förordar som redovisas ovan att den gemensamma kontaktpunkten får ett samlat ansvar för bland annat anmälningsförfarandet och svarar för att informera tillsynsmyndigheterna om vilka verksamhetsutövare som har anmält sig inom respektive sektor. *PTS* och *Telenor* motsätter sig dock en sådan ordning. Regeringen anser att det av lag endast bör framgå att anmälan ska ske till den myndighet som regeringen bestämmer.

Anmälans innehåll

Utredningen föreslår att anmälans innehåll ska regleras i lag och att anmälan ska innehålla uppgift om identitet, kontaktuppgift, ip-adressintervall, verksamhet och uppgift om i vilka länder verksamheten bedrivs. Sådana verksamhetsutövare som avses i avsnitt 6.1 ska enligt utredningens förslag även lämna uppgift om huvudsakligt etableringsställe och i förekommande fall kontaktuppgift till en företrädare. Enligt regeringen framstår det inte som ändamålsenligt att i lag reglera vilka uppgifter en anmälan ska innehålla. Detta kan i stället, som till exempel *Certezza AB* förordar, regleras i förordning men också på lägre föreskriftsnivå än i lag med stöd av 8 kap. 7 § regeringsformen och utan ett sådant bemyndigande i lagen som utredningen föreslår.

Tidpunkt för anmälan och ändring av uppgifter

Utredningen lämnar inget förslag i fråga om när anmälan ska göras, men föreslår samtidigt att en utebliven anmälan ska kunna leda till ingripanden. Regeringen anser att det, i linje med vad som gäller enligt 23 § NIS-lagen, bör framgå av lagen att verksamhetsutövaren ska göra anmälan så snart det kan ske. Att en anmälan ska göras så snart det kan ske innebär att en anmälan ska göras i omedelbar anslutning till att lagen träder i kraft, om det rör sig om en vid tidpunkten för ikraftträdandet redan etablerad verksamhetsutövare. Om en aktör startar en sådan verksamhet som gör att denne omfattas av lagen, och därmed räknas som en verksamhetsutövare, bör en anmälan göras i samband med att verksamheten börjar bedrivas. Detsamma gäller om en verksamhet utvecklas så att aktören uppfyller kraven för att omfattas av lagen. Det kommer i det enskilda fallet vara tillsynsmyndigheten och ytterst domstolarna som avgör om en anmälan har gjorts i rätt tid.

Medlemsstaterna är enligt artikel 3.3 i NIS 2-direktivet skyldiga att regelbundet se över förteckningen över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster och uppdatera den när det är lämpligt. Enligt artikel 3.4 ska entiteterna vid upprättandet av förteckningen lämna vissa uppgifter och meddela alla ändringar av de uppgifter som de har lämnat in utan dröjsmål och under alla omständigheter inom två veckor från datumet för ändringen. Med hänsyn till detta bör det införas en bestämmelse i den nya lagen om att verksamhetsutövare ska anmäla förändringar avseende uppgifter som har lämnats i en anmälan senast 14 dagar efter det att ändringen ägde rum. Till skillnad från utredningen anser regeringen att det, som *Livsmedelsverket* föreslår, även bör framgå av lagen att en anmälan om ändrade uppgifter ska göras så snart det kan ske och att 14 dagar är en bortre tidsgräns.

Eftersom även ett åsidosättande av skyldigheten att anmäla ändrade uppgifter kan leda till ingripanden, anser regeringen att tidsgränsen bör framgå av lag och inte på förordningsnivå som *Certezza AB* förordar.

6.3 Ingen särskild reglering om systematiskt och riskbaserat informationssäkerhetsarbete

Regeringens bedömning: Det bör inte införas en särskild bestämmelse om att verksamhetsutövare ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.

Utredningens förslag överensstämmer inte med regeringens bedömning. Utredningen föreslår, utöver att det ska införas en bestämmelse om att verksamhetsutövare ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete, att regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om arbetet.

Remissinstanserna: *Hi3G Access AB* tillstyrker utredningens förslag.

Drivkraft Sverige, *Energiföretagen i Sverige* och *Post- och telestyrelsen (PTS)* anser att kravet att verksamhetsutövare ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete är en sådan riskhanteringsåtgärd som avses i artikel 21 i NIS 2-direktivet. Remissinstanserna anser att utredningens förslag innebär en dubbelreglering. Flera remissinstanser, bland andra *Myndigheten för samhällsskydd och beredskap (MSB)*, *Svensk Handel* och *Transportstyrelsen*, anser att skyldigheten bör framgå av den nya lagen, men att formuleringen systematiskt och riskbaserat informationssäkerhetsarbete bör kompletteras med uttrycket cybersäkerhetsarbete. *Sveriges Kommuner och Regioner (SKR)* påpekar att kravet inte följer av direktivet samt bedömer att förslaget innebär en inskränkning av det kommunala självstyret eftersom kommuner och regioner inte längre kommer att styra sitt informationssäkerhetsarbete själva. *Tech Sverige* och *Teknikföretagen* anser att det är skillnad mellan ett systematiskt säkerhetsarbete och direktivets krav på ett riskbaserat arbete och att denna skillnad kan påverka svenska företags konkurrenskraft.

Ett flertal remissinstanser, bland andra *Inspektionen för vård och omsorg*, *Länsstyrelsen i Stockholms län*, MSB och *Teracom*, föreslår till skillnad mot utredningen att tillsynsmyndigheterna ska ges möjlighet att ingripa mot verksamhetsutövares brister i det systematiska och riskbaserade informationssäkerhetsarbetet. MSB anför att flera undersökningar visar att detta slags arbete inte prioriteras och att detta leder till incidenter som hade kunnat undvikas. *Sveriges advokatsamfund* menar att det i vart fall bör övervägas om tillsynsmyndigheterna ska ges möjligheter att ingripa. Om en särskild skyldighet att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete införs i lagen är det enligt PTS, som alltså motsätter sig att en skyldighet införs, mycket viktigt att skyldigheten förenas med ingripandemöjligheter.

Ett antal remissinstanser, bland andra *Patent- och registreringsverket (PRV)* och *Umeå kommun*, ser ett behov av ytterligare vägledning i fråga om vad ett systematiskt och riskbaserat informationssäkerhetsarbete innebär.

Skälen för regeringens bedömning: Uttrycket cybersäkerhet definieras i artikel 6.3 i NIS 2-direktivet, genom en hänvisning till EU:s cybersäkerhetsakt, som all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot. Av definitionen i artikel 6.2 framgår att säkerhet i nätverks- och informationssystem avser systemens förmåga att med en viss tillförlitlighetsnivå motstå händelser som kan undergräva tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via systemen.

Eftersom hot mot säkerheten i nätverks- och informationssystem kan ha olika ursprung bör, enligt skäl 79 i direktivet, riskhanteringsåtgärder för cybersäkerhet bygga på en allriskansats som syftar till att skydda nätverks- och informationssystem och dessa systems fysiska miljö mot händelser såsom stöld, brand, översvämning, telekommunikations- eller elavbrott eller obehörig fysisk åtkomst till och skada eller störning på en väsentlig eller viktig entitets information och informationsbehandlingsresurser, som kan undergräva tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem.

Utredningen föreslår att den nya lagen, utöver kravet på säkerhetsåtgärder som behandlas i avsnitt 6.4, ska innehålla ett uttryckligt krav på att verksamhetsutövare ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Detta krav följer inte uttryckligen av vare sig NIS-direktivet eller, som utredningen och *SKR* påpekar, av NIS 2-direktivet. Däremot gäller kravet enligt 11 § NIS-lagen. Ett systematiskt informationssäkerhetsarbete innebär enligt förarbetena till den lagen bland annat att arbetet ska bedrivas långsiktigt, kontinuerligt och metodiskt samt att det finns en tydlig rollfördelning med särskilt utpekat ansvar (se prop. 2017/18:205 s. 39). Kravet är dock inte förenat med någon möjlighet för tillsynsmyndigheterna att ingripa, varken genom förelägganden eller sanktionsavgift.

Utredningen anger att innebörden av informationssäkerhetsarbete är att skydda uppgifter som lagras, behandlas, hämtas eller överförs. Utredningen resonerar bland annat om att informationssäkerhetsarbete även tar sikte på skydd av uppgifter som inte finns i digital form i enlighet med skäl 79. Utredningen nämner också att begreppet täcker in fysisk hantering av uppgifter som kan påverkas av till exempel tillträde till lokaler.

Kravet på ett systematiskt och riskbaserat informationssäkerhetsarbete är visserligen genom NIS-lagen väletablerat och svarar mot existerande arbetssätt och standarder. Utredningens förslag kan inte, som bland annat *Teknikföretagen* hävdar, nödvändigtvis anses innebära en konkurrensmässig nackdel. Att ett företag bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete är något som enligt regeringen kan skapa förtroende och signalera att det är tryggt att investera i företaget. Regeringen anser dock, i likhet med bland andra *PTS,* att utredningens förslag i denna del innebär en dubbelreglering jämfört med förslaget om säkerhetsåtgärder i avsnitt 6.4. Det bör därför inte införas någon sådan bestämmelse som utredningen föreslår.

6.4 Skyldighet att vidta säkerhetsåtgärder

Regeringens förslag: Verksamhetsutövare ska vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och systemens fysiska miljö mot incidenter (säkerhetsåtgärder).

Säkerhetsåtgärderna ska utgå från ett allriskperspektiv och säkerställa en nivå på säkerheten i nätverks- och informationssystemen som är lämplig i förhållande till risken. Säkerhetsåtgärderna ska åtminstone avse

1. strategier för riskanalys och för nätverks- och informationssystemens säkerhet,
2. incidenthantering,
3. kontinuitetshantering och krishantering,
4. säkerhet i leveranskedjan,
5. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem,
6. strategier och förfaranden för att bedöma effektiviteten i säkerhetsåtgärderna,
7. grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,
8. strategier och förfaranden för användning av kryptografi samt, vid behov, kryptering,
9. personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning, och
10. vid behov användning av lösningar för autentisering, säkrade kommunikationer och säkrade nödkommunikationssystem.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela ytterligare föreskrifter om säkerhetsåtgärder.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår att åtgärderna ska benämnas riskhanteringsåtgärder. Utredningen föreslår att åtgärderna ska vara proportionella i förhållande till risken och att det ska anges att åtgärderna ska utgå från en riskanalys och utvärderas. I utredningens förslag finns inget krav på att åtgärderna ska vara lämpliga och att åtgärderna ska säkerställa en nivå på säkerheten som är lämplig i förhållande till den föreliggande risken. I förhållande till utredningens förslag har det förtydligats vilka nätverks- och informationssystem som avses. Vad gäller punkt 3 nämner utredningen inte krishantering. Vad gäller punkt 5 föreslår utredningen att det särskilt ska anges att kravet inbegriper hantering av sårbarheter och sårbarhetsinformation. I förhållande till utredningens förslag motsvarande punkt 8 och 10 har det förtydligats att vissa krav endast gäller vid behov. Utredningen lämnar inget förslag motsvarande punkt 1, 6 och 7.

Remissinstanserna: Ett antal remissinstanser yttrar sig gällande utredningens förslag om att uttrycket riskhanteringsåtgärder ska användas för att beteckna de åtgärder som verksamhetsutövare är skyldiga att vidta enligt lagen. *Teracom Group AB* tillstyrker utredningens förslag. Flera andra remissinstanser, bland andra *Certezza AB*, *Malmö kommun* och

Myndigheten för samhällsskydd och beredskap (MSB), anser dock att ”säkerhetsåtgärder” bör användas i stället, som i NIS-lagen.

Ett flertal remissinstanser, bland andra *Hi3G Access AB (Tre)* och *Region Jönköpings län*, yttrar sig gällande förslaget att verksamhetsutövare ska vidta tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter och ber om ett förtydligande av vilka åtgärder som avses. *Stokab AB* och *Svenska stadsnätsföreningen* anser att åtgärderna ska vara proportionella i förhållande till risken i enlighet med utredningens förslag. Bland andra *Affärsverket svenska kraftnät* och *Myndigheten för digital förvaltning (Digg)* anser att det också bör framgå att åtgärderna även ska vara lämpliga på det sätt som framgår av direktivet.

Vissa remissinstanser, däribland Certezza AB, *Inspektionen för vård och omsorg (IVO)*, *Netnod AB* och *Post- och telestyrelsen (PTS),* har synpunkter på utredningens förslag om att åtgärderna ska utgå från ett allriskperspektiv och en riskanalys samt vara proportionella i förhållande till risken och efterfrågar bland annat förtydliganden av förslagets innebörd. Stokab AB anser att det är viktigt att åtgärderna ska utgå från ett allriskperspektiv. Certezza AB ser positivt på att riskanalys ska göras men lyfter att det finns flera olika sätt att analysera risker på. Det vore enligt företaget värdefullt om regeringen i det fortsatta lagstiftningsarbetet resonerar kring kvantitativ och erfarenhetsbaserade riskbedömning. *Livsmedelsverket* anser att flera riskanalyser kan vara nödvändiga. Tre anser även att det är oklart om samtliga i lagen uppräknade åtgärder ska grunda sig på en riskanalys.

Ett stort antal remissinstanser, bland andra *Drivkraft Sverige*, *Energiföretagen Sverige*, *Sveriges advokatsamfund* och *Transportstyrelsen*, har synpunkter på åtgärderna som anges i lagen eller anser att det krävs förtydliganden i fråga om vad kraven innebär eller att utformningen av paragrafen bör ligga närmare direktivets utformning. Enligt Certezza AB bör ett dokumentationskrav avseende säkerhetsåtgärderna införas. *Lantbrukarnas riksförbund* anser att kraven på åtgärder är för omfattande för primärproducenter. *Tullverket* bedömer att genomförandet av förslaget riskerar att leda till ökad administrativ börda och ta resurser i anspråk som i dag används för att vidta säkerhetsåtgärder. Enligt Tullverket arbetar många myndigheter redan i dag med etablerade processer och arbetsmetoder som överlappar förslagen och för de myndigheter som bedriver såväl säkerhetskänslig som brottsbekämpande verksamhet, utöver verksamhet som inte kan kategoriseras som någondera av dem, blir gränsdragningen än besvärligare. Tullverket ifrågasätter om förslaget i praktiken kommer att innebära ökad cybersäkerhet, eller åtminstone i vilken utsträckning och på bekostnad av vad.

En *arbetsgrupp inom Cybernoden*, *Försvarets radioanstalt (FRA)* och Tre ifrågasätter utredningens slutsats att det inte skulle vara möjligt att ställa upp krav på användningen av standarder. FRA ifrågasätter om NIS 2-direktivets krav i denna del kan anses vara till fullo genomfört genom utredningens förslag.

Ett antal kommuner och *Patent- och registreringsverket (PRV)* ser ett behov av ytterligare vägledning. *Göteborgs kommun* och MSB föreslår att MSB ges ett bemyndigande att utfärda bland annat föreskrifter med grundläggande krav. Även *Karlstads kommun* anser att MSB bör få ett utökat

ansvar i fråga om föreskrifter. *Tech Sverige* önskar att möjligheten för PTS att meddela undantag från skyldigheten att vidta säkerhetsåtgärder som finns i LEK överförs till den nya lagen.

Skälen för regeringens förslag

Krav på åtgärder enligt direktivet

I artikel 21 i NIS 2-direktivet finns bestämmelser om riskhanteringsåtgärder för cybersäkerhet. Enligt första stycket i artikel 21.1 ska medlemsstaterna säkerställa att väsentliga och viktiga 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.

Med uttrycket nätverks- och informationssystem avses enligt artikel 6.1 i NIS 2-direktivet ett elektroniskt kommunikationsnät enligt definitionen i artikel 2.1 i Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (härefter kodexen) (a). Med uttrycket avses även en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter (b). Med nätverks- och informationssystem avses också digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av leden a och b för att de ska kunna drivas, användas, skyddas och underhållas. Definitionen motsvarar NIS-direktivets definition, frånsett att hänvisning sker till artikel 2.1 i kodexen i stället för artikel 2 a i Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv), som har upphävts genom kodexen.

NIS 2-direktivets skäl 83 anger att entiteterna bör säkerställa säkerheten i de nätverks- och informationssystem som de använder i sin verksamhet samt att det framför allt rör sig om privata nätverks- och informationssystem som antingen förvaltas av entiteternas interna it-personal eller vilkas säkerhet har lagts ut på entreprenad. Bland annat riskhanteringsåtgärderna bör enligt samma skäl tillämpas på entiteterna oavsett om entiteterna underhåller sina nätverks- och informationssystem internt eller lägger ut underhållet på entreprenad.

Med risk avses enligt artikel 6.9 i NIS 2-direktivet 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 en sådan incident inträffar.

Med beaktande av de senaste, och i tillämpliga fall, relevanta europeiska och internationella standarder samt genomförandekostnaderna, ska dessa åtgärder enligt andra stycket i artikel 21 säkerställa en nivå på säkerheten i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken. Vid bedömningen av dessa åtgärders proportionalitet ska vederbörlig hänsyn tas till entitetens grad av riskexponering, entitetens storlek samt sannolikheten för att incidenter inträffar och deras allvarlighetsgrad, inbegripet deras samhälleliga och ekonomiska konsekvenser.

Enligt artikel 21.2 i NIS 2-direktivet ska de åtgärder som avses i artikel 21.1 baseras på en allriskansats som syftar till att skydda nätverks- och informationssystem och dessa systems fysiska miljö från incidenter och i artikeln finns även en uppräkning av vad åtgärderna måste innefatta som ett minimum. Där anges bland annat, i artikel 21.2 a, strategier för riskanalys och informationssystemens säkerhet.

De verksamhetsutövare som omfattas av NIS 2-regleringen ska alltså vidta vissa åtgärder till skydd för säkerheten i nätverks- och informationssystem. I jämförelse med NIS-regleringen är åtgärderna mer omfattande. Nedan följer bland annat en redogörelse för hur regeringen anser att åtgärderna ska benämnas, vad som ska vara deras syfte och vilka perspektiv som de ska utgå ifrån.

Det bör noteras att EU-kommissionen har antagit en genomförandeförordning med stöd av artikel 21.5 och 23.11 i NIS 2-direktivet som bland annat syftar till att fastställa specifikationer för riskhanteringsåtgärder när det gäller vissa angivna entiteter. Det rör sig om 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 driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster (härefter genomförandeförordningen). Genomförandeförordningen är direkt tillämplig och motsvarande specifikationer behöver därför inte införas i den nya lagen. Det finns inte heller utrymme för att nationellt reglera delar som omfattas av genomförandeförordningen.

Hur bör åtgärderna benämnas?

Utredningen föreslår att de åtgärder som verksamhetsutövarna ska vara skyldiga att vidta enligt den nya lagen ska benämnas riskhanteringsåtgärder. Uttrycket förekommer inte i NIS-direktivet. Där används däremot, precis som i NIS-lagen, uttrycket säkerhetsåtgärder. I artikel 16 i NIS-direktivet anges att medlemsstaterna ska säkerställa att leverantörer av digitala tjänster utarbetar och vidtar ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder när de tillhandahåller sådana tjänster som avses i bilaga 3 till det direktivet inom unionen.

Som utredningen påpekar är kraven i NIS 2-direktivet både strängare och mer omfattande än de krav som anges i NIS-direktivet. Samtidigt rör det sig, som *MSB* påpekar, inte primärt om nya åtgärder, utan om en utveckling och i viss mån konkretisering av de åtgärder som nämns i NIS-direktivet. Som utvecklas i avsnitt 5.2 anser regeringen att det, som utgångspunkt, finns ett värde i att vid genomförandet av NIS 2-direktivet använda definitioner som motsvarar de definitioner som finns i direktivet.

Det faktum att uttrycket säkerhetsåtgärder redan är väletablerad på området talar dock enligt regeringens uppfattning för att den bör användas även i den nya lagen. Därutöver används säkerhetsåtgärder, som *Malmö kommun* påpekar, i standardserien ISO 27000 som bland annat rör cybersäkerhet. Regeringen bedömer därför, i likhet med *Certezza AB*, Malmö kommun och MSB och till skillnad från utredningen och *Teracom Group AB*, att uttrycket säkerhetsåtgärder bör användas i den nya lagen.

Säkerhetsåtgärdernas syfte och allriskperspektivet

Utredningen föreslår att verksamhetsutövare ska vidta tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. *Region Jönköping* föreslår att åtgärderna i stället ska syfta till att skapa förmågor för att skydda, upptäcka, reagera och återställa nätverks- och informationssystem. Regeringen bedömer att utredningens förslag, som ligger närmare utformningen av NIS 2-direktivet, bör genomföras. *Tre* anser att det är otydligt om kraven enbart omfattar nätverks- och informationssystem som tillhandahållaren använder för den samhällsviktiga tjänsten, eller om kraven omfattar alla nätverks- och informationssystem som används i verksamheten. Det bör, i förhållande till utredningens förslag, förtydligas att kravet gäller de system som en verksamhetsutövare använder för sin verksamhet eller för att tillhandahålla sina tjänster.

Åtgärderna ska enligt utredningens förslag bland annat utgå från ett allriskperspektiv. Bland andra *Certezza AB* efterfrågar ett förtydligande av vad detta innebär. *Netnod AB* anser att den grundläggande ansatsen i NIS 2-direktivet och i betänkandet, att cybersäkerhet baserad på en allriskansats är bättre än ett mer begränsat riskperspektiv, saknar vetenskaplig grund.

Vad som avses med allriskansats utvecklas i skäl 79 i direktivet. I skälet anges det att riskhanteringsåtgärderna, eftersom hot mot säkerheten i nätverks- och informationssystem kan ha olika ursprung, bör bygga på en allriskansats som syftar till att skydda nätverks- och informationssystem och dessa systems fysiska miljö mot händelser såsom stöld, brand, översvämning, telekommunikations- eller elavbrott eller obehörig fysisk åtkomst till och skada eller störning på en väsentlig eller viktig entitets information och informationsbehandlingsresurser, som kan undergräva tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem. Riskhanteringsåtgärderna bör därför också, enligt nämnda skäl, omfatta den fysiska säkerheten och miljösäkerheten i nätverks- och informationssystem genom att inbegripa åtgärder för att skydda sådana system mot systemfel, mänskliga misstag, avsiktligt skadliga handlingar eller naturfenomen i överensstämmelse med europeiska och internationella standarder, såsom de åtgärder som ingår i ISO/IEC 27000-serien. I detta avseende bör väsentliga och viktiga entiteter som ett led i sina riskhanteringsåtgärder för cybersäkerhet också ägna sig åt personalsäkerhet och inrätta lämpliga strategier för åtkomstkontroll. Det anges också att åtgärderna bör vara förenliga med CER-direktivet.

I enlighet med artikel 21.1 och skäl 79 bör en allriskansats anses innebära att verksamhetsutövarna arbetar för att minska sårbarheter inom ett brett område. För att genomföra NIS 2-direktivet i svensk rätt krävs, oavsett vad Netnod AB anför, en reglering som utgår ifrån nämnda ansats. Därutöver ställer sig regeringen bakom ståndpunkten att det krävs en allriskansats för att åstadkomma en hög gemensam cybersäkerhetsnivå i hela unionen. Uttrycket bör dock, i enlighet med utredningens förslag, i den nya lagen ersättas med allriskperspektiv som är ett etablerat uttryck på cybersäkerhetsområdet. Allriskperspektivet innebär att verksamhetsutövare ska sträva efter att bedöma alla risker för systemen som ska skyddas och att analysera alla möjliga orsaker till att en risk realiseras. Regeringen anser inte att det krävs något närmare förtydligande av innebörden av uttrycket i lagen.

Riskanalys

Utredningen föreslår att det i lagen ska finnas en uppräkning över vilka åtgärder verksamhetsutövare är skyldiga att vidta som ett minimum och att det i lagen ska anges att åtgärderna ska utgå från en riskanalys. *IVO* önskar ett förtydligande av vad som avses med riskanalys och förordar att regleringen i denna del i stället överensstämmer med direktivets utformning. *PTS* uttrycker motsvarande synpunkt och gör gällande att det med utredningens förslag riskerar att bli otydligt att föreskriftsrätten för tillsynsmyndigheterna även omfattar denna typ av åtgärder.

I artikel 21.2 a i NIS 2-direktivet finns en uppräkning av vad åtgärderna minst ska inbegripa. En redogörelse för regeringens bedömning om hur artikeln ska genomföras i svensk rätt finns nedan. Det kan dock konstateras att strategier för riskanalys och informationssystemens säkerhet nämns i uppräkningen i direktivet. Regeringen anser i likhet med IVO och PTS att det inte finns skäl att avvika från direktivets utformning i denna del. Att verksamhetsutövare ska ha strategier för riskanalys och informationssystemens säkerhet bör därför i stället anges i uppräkningen av de åtgärder som de åtminstone är skyldiga att vidta.

Säkerhetsåtgärderna bör vara både lämpliga och proportionella

De åtgärder som ska vidtas ska enligt första stycket i artikel 21.1 i NIS 2-direktivet bland annat vara lämpliga och proportionella. Enligt artikelns andra stycke ska åtgärderna vidare säkerställa en nivå på säkerheten i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken, med beaktande av vissa standarder och genomförandekostnader. Det anges även att det, vid bedömningen av åtgärdernas proportionalitet, ska tas vederbörlig hänsyn till entitetens grad av riskexponering, entitetens storlek samt sannolikheten för att incidenter inträffar och deras allvarlighetsgrad, inbegripet deras samhälleliga och ekonomiska konsekvenser.

Utredningen, liksom *Stokab AB* och *Svenska stadsnätsföreningen*, anser att åtgärderna ska vara proportionella i förhållande till risken. Utredningen anser att de i artikel 21.1 angivna omständigheterna – det vill säga graden av riskexponering, storleken, sannolikheten för incidenter och allvarlighetsgraden – tar sikte på själva risken och att åtgärderna bör vara proportionella i förhållande till denna. Utredningen anser att detta bör

komma till uttryck i lagen, men att skrivningen i direktivet om att åtgärderna ska vara lämpliga och proportionella samt därutöver säkerställa en nivå på säkerheten som är lämplig i förhållande till risken inte tillför något. Ett antal remissinstanser, däribland *Affärsverket svenska kraftnät* och *Digg*, gör en annan bedömning i sistnämnda del.

Regeringen bedömer, i likhet med utredningen, att ovannämnda omständigheter främst bör vara hänförliga till riskbedömningen. Det kan enligt regeringens mening dock vara så att en säkerhetsåtgärd är proportionell men inte lämplig. Enligt Digg handlar lämplighet om att vidta rätt åtgärd i förhållande till en viss specifik risk, medan proportionaliteten handlar om hur omfattande åtgärden måste vara för att motverka eller eliminera risken. Även om proportionalitets- och lämplighetsbedömningen i många fall kan ge samma resultat, delar regeringen uppfattningen att det finns en skillnad mellan dessa bedömningar och att båda bedömningarna bör ingå.

Det bör mot denna bakgrund anges i lagtexten att åtgärderna ska vara både lämpliga och proportionella samt att åtgärderna ska säkerställa en nivå på säkerheten som är lämplig i förhållande till risken. Den sistnämnda lämplighetsbedömningen innebär, till skillnad från den förstnämnda som tar sikte på vilka åtgärder som vidtas, att nivån på säkerheten i systemen ska vara anpassad till risken. Samtliga åtgärder bör alltså grunda sig på en proportionalitets- och lämplighetsbedömning. I en sådan bedömning ingår även beaktande av kostnader och tillgänglig teknik, vilket *PTS* lyfter fram. Föreslagen reglering innebär att det finns goda möjligheter att anpassa åtgärderna efter den egna verksamheten och till skillnad från *Lantbrukarnas riksförbund* anser regeringen att kraven på åtgärderna inte kan anses vara för betungande för primärproducenter.

Utredningen föreslår att det ska framgå att säkerhetsåtgärderna ska utvärderas. Som redovisas nedan föreslår regeringen att verksamhetsutövaren ska ha strategier och förfaranden för att bedöma effektiviteten i säkerhetsåtgärder. Det behöver därmed inte införas ytterligare en bestämmelse om att utvärdering ska ske.

Regeringen anser inte heller att det bör införas ett dokumentationskrav kopplat till säkerhetsåtgärderna som *Certezza AB* föreslår. Dokumentation är visserligen en naturlig del av cybersäkerhetsarbetet. Av skäl 122 framgår dock bland annat att viktiga entiteter inte bör vara skyldiga att systematiskt dokumentera efterlevnad av riskhanteringsåtgärderna. Enligt regeringen bör det mot denna bakgrund inte införas något generellt dokumentationskrav i lagen.

Även om regeringen har förståelse för *Tullverkets* synpunkt att krav på säkerhetsåtgärder kan innebära svårigheter för verksamhetsutövare vars verksamhet delvis är undantagen från lagens tillämpningsområde, anser regeringen att regleringen är ändamålsenlig för att uppnå lagens syfte. En närmare analys av förslagens konsekvenser finns i avsnitt 14.

Vad ska säkerhetsåtgärderna innefatta som ett minimum?

I artikel 21.2 anges tio punkter (a–j) som säkerhetsåtgärderna minst ska inbegripa. Utredningen föreslår att merparten av dessa ska föras över till den nya lagen, dock med vissa undantag och förändringar. Ett stort antal remissinstanser, däribland *Sveriges advokatsamfund*, efterfrågar ändringar

som innebär att bestämmelserna i denna del i stället formuleras i enlighet med motsvarande bestämmelser i NIS 2-direktivet. Flera av dem understryker vikten av enhetliga regleringar för verksamhetsutövare som är verksamma i flera unionsländer.

Regeringen konstaterar att flera av de länder som hittills har genomfört direktivet, däribland Belgien, Kroatien och Italien, i sin nationella lagstiftning har valt att återge punkterna så som de är angivna i direktivet. Mot bland annat denna bakgrund anser regeringen att bestämmelserna närmare bör följa direktivets utformning än vad utredningen föreslår.

En bestämmelse bör, som anges ovan, ta sikte på verksamhetsutövares skyldighet att ha strategier för riskanalys men även för nätverks- och informationssystemens säkerhet. Strategierna kan exempelvis utformas som rutiner. Riskanalysen ska ligga till grund för valet av säkerhetsåtgärder. Verksamhetsutövaren bör bland annat ta hänsyn till att det finns olika modeller för riskanalys och att flera riskanalyser kan vara nödvändiga, som *Certezza AB* och *Livsmedelsverket* anför.

En bestämmelse om incidenthantering bör, som utredningen föreslår, också finnas med i lagen. Incidenthantering definieras i artikel 6.8 i direktivet som alla åtgärder och förfaranden som syftar till att förebygga, upptäcka, analysera, begränsa eller reagera på och återhämta sig från en incident.

I artikel 21.2 c nämns ”driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering, och krishantering”. Regeringen anser, i likhet med utredningen, att uttrycket driftskontinuitet bör ersättas av det mer etablerade uttrycket kontinuitetshantering. Till skillnad från utredningen bedömer regeringen dock inte att krishantering nämns i direktivet som ett exempel på driftskontinuitet, utan som en självständig beståndsdel. Krishantering bör därför, som *Digg* föreslår, nämnas särskilt. Enligt regeringen behöver däremot inte hantering av säkerhetskopiering, i motsats till vad Digg gör gällande, och katastrofhantering anges eftersom dessa utgör exempel på vad som ingår i kontinuitetshantering och krishantering. Kontinuitetshantering och krishantering innebär att verksamhetsutövaren ska planera för och ha förmåga att upprätthålla sin verksamhet på en tolerabel nivå oavsett vilken störning den utsätts för eller om en kris inträffar. Det kan till exempel röra sig om störningar som innebär att personalen inte kan komma till arbetet, att lokalerna inte går att använda, att strömavbrott inträffar eller att leveranser av viktiga varor och tjänster inte når verksamhetsutövaren.

Enligt direktivets formulering inbegriper säkerhet i leveranskedjan säkerhetsaspekter som rör förbindelserna mellan varje entitet och dess direkta leverantörer eller tjänsteleverantörer (artikel 21.2 d). Regeringen anser, likt utredningen, att det är tillräckligt att endast ange uttrycket säkerhet i leveranskedjan i lagen. Flera remissinstanser önskar dock förtydliganden av vad bestämmelsen innebär för krav.

Medlemsstaterna ska enligt artikel 21.3 i NIS 2-direktivet säkerställa att entiteter, när de överväger lämpliga åtgärder enligt 21.2 d, beaktar de sårbarheter som är specifika för varje direktleverantör och tjänsteleverantör och den övergripande kvaliteten på deras leverantörers och tjänsteleverantörers produkter och cybersäkerhetspraxis, inbegripet deras förfaranden för säker utveckling. Enligt samma bestämmelse ska medlemsstaterna vidare säkerställa att entiteter därvid är skyldiga att

beakta resultatet av de samordnade säkerhetsriskbedömningar av kritiska leveranskedjor som utförs i enlighet med artikel 22.1.

Av skäl 85 framgår att entiteter bland annat bör bedöma och beakta den övergripande kvaliteten och resiliensen hos produkter och tjänster och riskhanteringsåtgärder som är inbyggda i dem samt cybersäkerhetspraxis hos leverantörer. Av samma skäl framgår att entiteter bör uppmuntras att införliva riskhanteringsåtgärder i avtal med sina direkta leverantörer och att entiteterna kan beakta risker som härrör från leverantörer på andra nivåer.

Regeringen instämmer i utredningens uppfattning att kravet på säkerhet i leveranskedjan i artikel 21.2 d visserligen endast omfattar säkerhetsaspekter i förhållande till direkta leverantörer och tjänsteleverantörer, men anser att verksamhetsutövare även bör beakta risker som härrör från leverantörer på andra nivåer. *Integritetsskyddsmyndigheten (IMY)* delar inte utredningens uppfattning om hur kravet i artikel 21.2 d ska tolkas. Det kan enligt IMY i vissa fall krävas att verksamhetsutövaren upprätthåller förmåga att effektivt hämta in och reagera på information från andra källor än direkta leverantörer om kända brister i säkerhetsnivån hos leverantörens underleverantörer under den tid som ett avtal löper.

Som IMY påpekar kan en verksamhetsutövare till exempel behöva vidta åtgärder med anledning av kända brister hos underleverantörer. Som Digg anmärker kan en verksamhetsutövare exempelvis behöva bedöma risker i flera led, om inte annat för att avtalsvis kunna reglera vilka åtgärder som leverantören i första ledet behöver vidta och svara för i de följande leverantörsleden. Den närmare innebörden av kravet på säkerhet i leveranskedjan, inklusive vilka krav som finns på ett avtals innehåll och hur kraven gäller i förhållande till befintliga avtalsförhållanden, bör dock inte anges i lag. Det får avgöras i varje enskilt fall om en verksamhetsutövare har vidtagit tillräckliga åtgärder i detta avseende, inbegripet åtgärder för att revidera befintliga avtal. Även resultatet av samordnade säkerhetsriskbedömningar på unionsnivå av kritiska leveranskedjor bör beaktas.

Artikel 21.2 e i NIS 2-direktivet rör säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem och bör, som utredningen föreslår, ingå i uppräkningen av vad säkerhetsåtgärderna åtminstone ska avse. Enligt direktivets formulering och utredningens förslag inbegriper denna del hantering av sårbarheter och sårbarhetsinformation. Till skillnad från utredningen anser regeringen inte att det sistnämnda behöver nämnas i lagen.

MSB har till utredningen föreslagit att ordet förvärv ersätts med ”anskaffning” för att signalera att kraven gäller även när något inte har köpts, exempelvis vid utkontraktering. Även *Statens servicecenter* och *Tillväxtverket* anser att en bredare term bör användas för att bland annat fånga utkontrakterade tjänster och licensierade system. Att förvärva något innebär att överta något med äganderätt. Att en verksamhetsutövare behöver vidta åtgärder även vid utkontraktering och licensiering följer av kravet på säkerhet vid utveckling och underhåll av systemen och till viss del även av kravet på säkerhet i leveranskedjan. Detta gäller även i förhållande till de system som Statens servicecenter nämner som tillhandahålls av verksamhetsutövaren i egen regi.

I artikel 21.2 f i NIS 2-direktivet nämns strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet. Detta krav bör komma till uttryck i lagen och bland annat innebära att säkerhetsåtgärderna ska utvärderas.

Artikel 21.2 g i NIS 2-direktivet rör grundläggande praxis för cyberhygien och utbildning i cybersäkerhet. Praxis för cyberhygien bör omfatta ett brett spektrum av grundläggande rutiner, som exempelvis programuppdateringar, åtkomsthantering och användarmedvetenhet. Kravet på utbildning i cybersäkerhet kan innebära att verksamhetsutövare bör erbjuda viss personal att genomgå sådan utbildning. Enligt regeringen motsvarar inte kravet på utbildning i cybersäkerhet enligt artikel 21.2 g utbildningskravet i artikel 20.2, som främst riktar sig till verksamhetsutövares ledningsorgan (se vidare avsnitt 6.5). Regeringen anser, likt Certezza AB, Digg och *Transportstyrelsen* och till skillnad från utredningen, att kraven bör framgå uttryckligen av lagen.

I artikel 21.2 h anges ”strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering”. *FRA* anmärker på att det i direktivet finns ett lämplighetskrav kopplat till kryptering, vilket utredningen har utelämnat i sitt förslag utan vidare motivering. Regeringen bedömer att det i paragrafen bör finnas ett generellt krav på att säkerhetsåtgärderna ska vara lämpliga, vilket överensstämmer med direktivet. Det bör dock, som FRA påpekar, förtydligas att kryptering endast ska användas vid behov.

Bestämmelsen i lagen som motsvarar artikel 21.2 i, som rör personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning, bör enligt regeringen utformas som i direktivet och inte delas upp som utredningen föreslår. Flera remissinstanser önskar förtydliganden av vad personalsäkerhet innebär. *Orange Cyberdefense* och *Tre* ställer sig frågande till om uttrycket personalsäkerhet även omfattar bakgrundskontroller och pekar på att bakgrundskontroller, men även personuppgiftsbehandling, kan kräva lagstöd.

Av skäl 79 i direktivet framgår bland annat att riskhanteringsåtgärderna bör omfatta den fysiska säkerheten och miljösäkerheten i nätverks- och informationssystem genom att inbegripa åtgärder för att skydda systemen mot mänskliga misstag och avsiktligt skadliga handlingar samt att entiteterna i detta avseende bör ägna sig åt personalsäkerhet och inrätta lämpliga strategier för åtkomstkontroll som bör vara förenliga med CER-direktivet. Syftet med personalsäkerhet är enligt regeringen att förebygga att personal orsakar incidenter på grund av olämplighet eller okunskap. Kravet på personalsäkerhet kan enligt regeringen bland annat innebära att verksamhetsutövaren genomför insatser för att höja kompetensen och kunskapen hos personalen om frågor som rör cybersäkerhet för att motverka mänskliga misstag. En aspekt på personalsäkerhet kan därmed vara utbildning av personal. Det finns ingen vedertagen definition av uttrycket bakgrundskontroller, men personalsäkerhet kan också innebära att olika typer av kontroller genomförs exempelvis i form av verifiering av olika kvalifikationer bland annat för att motverka avsiktligt skadliga handlingar.

I uttrycket åtkomstkontroll ingår sådana funktioner som syftar till att reglera och kontrollera en användares åtkomst till information och resurser. Det rör sig bland annat om behörighetsstyrning i form av

tilldelning, återkallande och hantering av behörigheter samt uppföljning av åtkomst till information och resurser, till exempel genom loggar och andra hjälpmedel.

Punkten j i direktivet rör användning inom entiteten, när så är lämpligt, av lösningar för multifaktorautentisering eller kontinuerlig autentisering samt säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem. Regeringen anser att motsvarande bestämmelse i lagen kan formuleras på ett mer lättillgängligt sätt än det som utredningen föreslår. Regeringen anser också, av det skäl som anförs ovan kopplat till genomförandet av artikel 21.2 h, att det bör anges särskilt att användningen endast ska ske vid behov. Lösningar för autentisering kan bland annat ta sikte på att kontrollera en uppgiven identitet vid exempelvis inloggning i ett system. Säkrad kommunikation bör bland annat vara skyddad mot obehörig avlyssning eller upptagning och bör, om behovet finns, kunna användas både i den dagliga verksamheten och i nödsituationer. Förtydliganden om vad dessa lösningar närmare avser, som Tre efterfrågar, bör inte ske i lag.

Krav på användningen av standarder

En arbetsgrupp inom Cybernoden och *Tre* ifrågasätter utredningens slutsats att det inte skulle vara möjligt att ställa upp krav på användningen av standarder. *FRA* ifrågasätter om kraven i NIS 2-direktivet på att medlemsstaterna ska uppmuntra till användning av standarder kan anses vara till fullo genomfört genom utredningens förslag.

I artikel 25.1 i NIS 2-direktivet anges att medlemsstaterna för att främja en enhetlig tillämpning av artikel 21.1 och 21.2 ska uppmuntra användningen av europeiska och internationella standarder och tekniska specifikationer av relevans för säkerheten i nätverks- och informationssystem (se även skäl 80). Detta ska enligt bestämmelsen ske utan att föreskriva eller gynna användning av en viss typ av teknik. I bestämmelsen om åtgärderna anges det att relevanta standarder ska beaktas (artikel 21.1 andra stycket). Bestämmelser om internationella standarder fanns även i artikel 16.1 e respektive artikel 19.1 i NIS-direktivet.

Regeringen bedömde i samband med genomförandet av NIS-direktivet att bestämmelser i fråga om säkerhetsåtgärder och standarder skulle meddelas i förordning eller i föreskrifter som meddelas av en myndighet (se prop. 2017/18:205 s. 43). Av NIS-förordningen framgår att leverantörer ska beakta vissa standarder och specifikationer vid utformningen av säkerhetsåtgärder (5 §) och att efterlevnaden av internationella standarder ska beaktas vid bedömningen av om säkerhetsåtgärderna säkerställer en viss nivå på säkerheten (6 §). Därutöver anges det i MSB:s föreskrifter att varje leverantör ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av vissa särskilt angivna standarder (5 § i MSBFS 2018:8).

Utredningen bedömer att innebörden av bestämmelserna rörande standarder i NIS 2-direktivet bör vara att medlemsstaterna inte kan ställa upp krav om standarder och att det därför inte är möjligt att i lag föreskriva att standarder ska beaktas. I stället menar utredningen att användningen av standarder bör uppmuntras på andra sätt. Regeringen gör dock samma bedömning som till exempel Tre och anser att bestämmelser som främjar

användningen av europeiska eller internationella standarder och tekniska specifikationer av relevans för säkerheten i nätverks- och informationssystem bör meddelas på lägre föreskriftsnivå än i lag på motsvarande sätt som gäller enligt NIS-regleringen.

Bemyndigande men inget beslut om undantag

Den nya lagen kommer att gälla för ett stort antal sektorer och verksamhetsutövare. Det finns därför behov av att konkretisera regleringen på såväl förordningsnivå som i föreskrifter som meddelas av en myndighet som bland andra *Drivkraft Sverige*, *Energiföretagen Sverige* och *PRV* bedömer. Lagen bör därför innehålla ett bemyndigande som ger regeringen eller den myndighet som regeringen bestämmer rätt att meddela ytterligare föreskrifter om säkerhetsåtgärder. Det finns, givet direktivets krav, inget utrymme för att införa ytterligare möjlighet att meddela undantag från skyldigheten att vidta säkerhetsåtgärder som *Tech Sverige* föreslår (se vidare avsnitt 11).

6.5 Ledningen ska genomgå utbildning

Regeringens förslag: Ledningen för en verksamhetsutövare ska genomgå utbildning om säkerhetsåtgärder.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om utbildningen.

Regeringens bedömning: Det behöver inte införas någon särskild reglering om att ledningen ska godkänna säkerhetsåtgärder och övervaka genomförandet av dem.

Utredningens förslag och bedömning överensstämmer i huvudsak med regeringens. Utredningen föreslår att även anställda ska erbjudas utbildning.

Remissinstanserna: *Drivkraft Sverige*, *Kollegiet för svensk bolagsstyrning* och *Svenskt Näringsliv* delar utredningens uppfattning att det såvitt avser aktiebolag förefaller rimligt att styrelsen och verkställande direktör ska anses utgöra ledningen. Dessa remissinstanser anser också att det saknas anledning att reglera styrelsens ansvar för säkerhetsåtgärder eftersom det redan följer av aktiebolagslagen (2005:551) att styrelsen svarar för bolagets organisation och förvaltningen av dess angelägenheter. Kollegiet för svensk bolagsstyrning anser att det är av principiell betydelse att styrelsens frihet att själv avgöra vad som är en lämplig form för bolagets organisation och förvaltning inte inskränks i onödan. *Energiföretagen Sverige* anser att det är underförstått att en styrelse har ansvaret för att förbereda, formulera och prioritera rätt frågor för företagets affärsnytta.

Certezza AB och *Statens energimyndighet* anser att direktivets krav på att ledningsorgan ska godkänna och övervaka säkerhetsåtgärder måste anges i lagen. Statens energimyndighet konstaterar att det, enligt den tillsyn som har utförts enligt NIS-lagen, inte har varit tillräckligt tydligt vem som bär ansvar och bedömer att ett förtydligande i denna del dessutom kan användas som ett stöd för att involvera ledningen i cybersäkerhetsarbetet. *Sveriges advokatsamfund* bedömer att utredningens

slutsatser kring ledningens ansvar inte är i linje med direktivets krav och delar inte utredningens uppfattning att ansvaret inte behöver regleras i den nya lagen. Advokatsamfundet noterar att det inte enbart är aktiebolags ledningsorgan som kommer att omfattas av skyldigheterna och att det dessutom inte finns någon tydlig reglering som motsvarar direktivets krav i aktiebolagslagen, annan associationsrättslig lagstiftning eller lagstiftning för andra utpekade verksamhetsutövare.

Ett antal remissinstanser, bland andra Energiföretagen Sverige och *Lantmäteriet*, ber om förtydliganden i olika avseenden. Bland annat anser *Mittuniversitetet* och *Tele2 Sverige AB (Tele2)* att uttrycket utbildning behöver preciseras. Enligt Certezza AB måste det vara fråga om utbildningar som bidrar till ökad kompetens för att direktivets krav ska anses vara uppfyllda.

Flens kommun, *Karlstads kommun*, *Nynäshamns kommun* och *Umeå kommun* anser att även andra kommunala nämnder än kommunstyrelsen bör omfattas av utbildningskravet. *Region Gotland* ställer sig frågande till om lagstiftaren kan kräva att folkvalda ska genomgå utbildning och om detta är förenligt med det kommunala självstyret.

Ett antal remissinstanser yttrar sig särskilt över utredningens förslag om att anställda ska erbjudas utbildning. *En arbetsgrupp inom Cybernoden* anser att kravet på utbildning bör gälla verksamhetsutövaren i sin helhet på samma sätt som gäller för exempelvis brandsäkerhetskraven, arbetsmiljökraven och hållbarhetskraven. Mittuniversitetet efterfrågar ett förtydligande i fråga om utbildningen till anställda ska motsvara den utbildning som ledningen ska genomgå eller om utbildningen kan anpassas. Enligt bland andra Svenskt Näringsliv och *Tech Sverige* är det för långtgående att kräva att anställda ska erbjudas utbildning eftersom direktivet endast föreskriver att verksamhetsutövarna ska uppmuntras att erbjuda sådan utbildning. *Trafikverket* anser att kravet på obligatorisk utbildning även ska gälla för anställda, åtminstone för anställda hos väsentliga verksamhetsutövare.

Flera remissinstanser, bland andra *Lantmäteriet* och Trafikverket, anser att en myndighet bör ges i uppdrag att ta fram och utveckla anpassade utbildningar på området med hänvisning till resurseffektivitet. *Salems kommun* föreslår att den myndighet som får i uppdrag att meddela föreskrifter om utbildning även bör få detta uppdrag. *Myndigheten för samhällsskydd och beredskap (MSB)* föreslår att myndigheten ges bemyndigande att utfärda bland annat föreskrifter med grundläggande krav på utbildning.

Strålsäkerhetsmyndigheten (SSM) föreslår att det införs ett krav i den nya lagen på att verksamhetsutövare ska ha en cybersäkerhetschef och att krav på utbildning bör införas i säkerhetsskyddslagen.

Skälen för regeringens förslag och bedömning

Skyldigheter kopplade till säkerhetsåtgärder enligt NIS 2-direktivet

Av artikel 20.1 i NIS 2-direktivet framgår att medlemsstaterna ska säkerställa att entiteters ledningsorgan godkänner de riskhanteringsåtgärder som entiteterna vidtar för att följa artikel 21, övervakar genomförandet av dem och kan ställas till svars för entiteternas överträdelser av den artikeln. Enligt artikel 20.1 andra stycket påverkar inte tillämpningen av artikel 20.1

nationell rätt när det gäller de ansvarsregler som är tillämpliga på offentliga institutioner samt ansvaret för statligt anställda och valda eller utnämnda tjänstepersoner. Därutöver följer av artikel 20.2 att medlemsstaterna ska säkerställa att medlemmarna i entiteternas ledningsorgan är skyldiga att genomgå utbildning och ska uppmuntra entiteter att regelbundet erbjuda liknande utbildning till sina anställda för att de ska få tillräckligt med kunskap och kompetens för att kunna identifiera risker och bedöma riskhanteringspraxis för cybersäkerhet och deras inverkan på de tjänster som tillhandahålls av entiteten.

NIS 2-direktivet ställer alltså krav på att ledningsorgan ska ansvara för säkerhetsåtgärder på visst sätt och genomgå utbildning med anledning av detta. Enligt regeringen omfattas ledningsorgan i både offentliga och privata entiteter av skyldigheterna, även om nationell rätt om bland annat ansvarsregler som är tillämpliga på offentliga institutioner och ansvaret för statligt anställda inte ska påverkas enligt direktivet.

Ledningen ansvarar för säkerhetsåtgärder utan särskild reglering

Regeringen anser att uttrycket ledningsorgan som används, men inte definieras, i NIS 2-direktivet i ett svenskt sammanhang motsvaras av uttrycket ledning. Detta uttryck har ingen vedertagen entydig innebörd och eftersom den nya lagen kommer att omfatta många olika typer av verksamhetsutövare måste en bedömning av vem som anses utgöra ledningen göras från fall till fall.

För ett aktiebolag får ledningen, som utredningen anger, primärt avse styrelsen. Av 8 kap. 4 § aktiebolagslagen framgår att styrelsens svarar för ett aktiebolags organisation och förvaltningen av bolagets angelägenheter. Enligt 8 kap. 27 och 29 §§ aktiebolagslagen ska den verkställande direktören utses av styrelsen och sköta den löpande förvaltningen enligt styrelsens riktlinjer och anvisningar. Den verkställande direktören är med andra ord underställd styrelsen. Som utredningen anger är NIS 2-direktivet utformat för att tillämpas inom EU där medlemsstaterna har mycket skiftande bolagsrättsliga traditioner. Med hänsyn till utformningen och innebörden av artikel 20.1 anser regeringen, likt utredningen, att ledningen i det här sammanhanget bör omfatta styrelsen, den verkställande direktören och ersättare för dessa. Motsvarande ordning som redovisas ovan gäller för ekonomiska föreningar enligt 7 kap. 4 och 29 §§ lagen (2018:672) om ekonomiska föreningar. För handelsbolag gäller enligt lagen (1980:1102) om handelsbolag och enkla bolag att bolagsmännen ansvarar för förvaltningen.

Lantmäteriet önskar ett förtydligande av vad som avses med uttrycket ledning särskilt i fråga om styrelsemyndigheter. *Statens servicecenter* anser att det bör klargöras om uttrycket ska ges en annan betydelse i den nya lagen än i myndighetsförordningen för myndigheter under regeringen. I 2 § myndighetsförordningen finns, som Statens servicecenter påpekar, en definition av ledning. Enligt denna paragraf framgår att huvudregeln är att en myndighet under regeringen leds av en myndighetschef om det är en enrådighetsmyndighet, en styrelse om det är en styrelsemyndighet och en nämnd om det är en nämndmyndighet. Av samma paragraf framgår att myndighetens ledningsform anges i myndighetens instruktion eller i någon

annan författning. Regeringen anser inte att uttrycket bör ges någon annan betydelse i den nya lagen.

För kommuner och regioner instämmer regeringen i utredningens uppfattning att ledningen utgörs av kommun- respektive regionstyrelsen i enlighet med 6 kap. 1 § kommunallagen. Av paragrafen framgår att styrelsen ska leda och samordna förvaltningen av kommunens eller regionens angelägenheter och ha uppsikt över bland annat övriga nämnders verksamhet.

Ledningen i enskilda och offentliga verksamhetsutövare ansvarar alltså för att godkänna säkerhetsåtgärder och övervaka genomförandet av dem på sätt som framgår av artikel 20 i direktivet utan särskild reglering. Regeringen bedömer därmed, till skillnad från *Certezza AB*, *Statens energimyndighet* och *Sveriges advokatsamfund*, att direktivets krav i denna del inte behöver regleras i lagen.

Energiföretagen Sverige anser att det är otydligt, i de fall ett dotterbolag omfattas av direktivet på grund av sitt samband med moderbolaget, vilket ledningsorgan som är ytterst ansvarigt. Alla bolag som omfattas av regleringen omfattas av kraven på att vidta säkerhetsåtgärder och det är därmed ledningen i varje bolag som ansvarar för de skyldigheter som följer med anledning av densamma.

Det finns inget utrymme att inom ramen för denna lagrådsremiss genomföra de förslag som *SSM* lämnar.

Ledningens skyldighet att genomgå utbildning bör regleras

Enligt artikel 20.2 i NIS 2-direktivet ska medlemsstaterna säkerställa att medlemmarna i entiteters ledningsorgan är skyldiga att genomgå utbildning. Medlemsstaterna ska enligt samma artikel också uppmuntra entiteter att regelbundet erbjuda liknande utbildning till sina anställda.

Utbildningskravet bör, som utredningen föreslår, lyftas fram särskilt i den nya lagen. Enligt direktivet avser utbildningsskyldigheten verksamhetsutövarnas ledningsorgan och kravet bör därför avse verksamhetsutövares ledningar. Uttrycket ledning bör omfatta styrelsen och verkställande direktören samt ersättare för dessa i aktiebolag och ekonomiska föreningar, bolagsmännen i handelsbolag, ledning som den definieras i myndighetsförordningen för myndigheter samt styrelsen för kommuner och regioner. Enligt regeringen utgör inte förslagen i denna lagrådsremiss en inskränkning i den kommunala självstyrelsen som *Region Gotland* bedömer, vilket utvecklas i avsnitt 14.4.

Kravet på utbildning innebär att ledningen för enskilda och offentliga verksamhetsutövare ska genomgå utbildning. Ett antal remissinstanser, bland andra *Certezza AB* och *Tele2*, ber om förtydliganden i olika avseenden kopplat till kravet på utbildning. *Umeå kommun* anser att kravet på utbildning även bör omfatta utbildning i informationssäkerhetsarbete. Utbildningen ska enligt artikel 20.2 i direktivet syfta till att den som genomgår utbildningen ska få tillräckligt med kunskap och kompetens för att kunna identifiera risker och bedöma riskhanteringspraxis för cybersäkerhet och deras inverkan på de tjänster som tillhandahålls av entiteten. Eftersom utbildningskravet har en koppling till skyldigheten för ledningen att godkänna och övervaka genomförandet av säkerhetsåtgärder bör utbildningen enligt regering handla om säkerhetsåtgärder. Utbild-

ningen bör alltså därmed bland annat syfta till att ledningen ska ha tillräcklig kompetens för att kunna identifiera risker och kunna bedöma vilka säkerhetsåtgärder som bör vidtas av verksamhetsutövaren. Hur utbildningen bör utformas närmare kan variera beroende på sektoriella skillnader och behov. Det bör därför införas ett bemyndigande som möjliggör för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om utbildningen. Genom sådana föreskrifter kan det, i enlighet med exempelvis *Mittuniversitetets* önskemål, preciseras vad som avses med utbildning och vad denna ska innefatta. Frågan om vilken myndighet som bör ges föreskriftsrätt, som *MSB* väcker, behandlas inte i denna lagrådsremiss.

Ett antal remissinstanser är kritiska till utredningens förslag om att anställda ska erbjudas utbildning, medan andra anser att utbildningskravet bör gälla samtliga anställda. Några remissinstanser, bland andra *Flens kommun* och *Nynäshamns kommun*, anser vidare att andra kommunala nämnder än kommunstyrelsen bör omfattas av utbildningskravet. NIS 2-direktivet innebär endast krav på att medlemsstaterna ska uppmuntra verksamhetsutövare att erbjuda utbildning till sina anställda. Som bland andra *Svenskt Näringsliv* påpekar går utredningens förslag därmed längre än direktivets krav. Enligt regeringen finns det inte tillräckliga skäl att utsträcka utbildningskravet på det sätt som utredningen föreslår. Kravet på utbildning i denna del bör därför endast gälla ledningar. I enlighet med regeringens förslag i avsnitt 6.4 ska dock verksamhetsutövare vidta säkerhetsåtgärder, som bland annat ska innefatta grundläggande praxis för cyberhygien och utbildning i cybersäkerhet samt personalsäkerhet. Redan genom dessa krav uppmuntras verksamhetsutövare att regelbundet erbjuda utbildning till sina anställda, inklusive i de kommunala nämnderna, på området för cybersäkerhet, även i det syfte som anges i artikel 20.2.

Flera remissinstanser, bland andra *Lantmäteriet* och *Trafikverket,* lämnar förslag om uppdrag som det inte finns möjlighet att ta om hand inom ramen för en lagrådsremiss.

6.6 Incidentrapportering och informationsskyldighet

6.6.1 Ord och uttryck

Regeringens förslag: En incident ska i lagen definieras som en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem.

En betydande incident ska definieras som en incident som har orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller en incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande skada.

Ett cyberhot ska definieras som en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka

nätverks- och informationssystem, användare av dessa system och andra personer.

Ett betydande cyberhot ska definieras som ett cyberhot som, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på en verksamhetsutövares nätverks- och informationssystem eller användarna av verksamhetsutövarens tjänster genom att vålla betydande skada.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela ytterligare föreskrifter om vad som utgör en betydande incident.

Utredningens förslag överensstämmer i huvudsak med regeringens. I utredningens förslag till definitionen av uttrycket incident anges inte att det ska röra sig om tjänster som är tillgängliga via nätverks- och informationssystem. Utredningen föreslår att cyberhot ska definieras genom en hänvisning till EU:s cybersäkerhetsakt. Utredningen föreslår att även begreppet tillbud ska definieras i lagen. Utredningen föreslår att regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om vad som utgör en betydande incident.

Remissinstanserna: Flera remissinstanser, däribland *Energiföretagen Sverige*, *Skatteverket*, *Tillväxtverket* och *Umeå kommun*, anser att det bland annat finns behov av att förtydliga vad som avses med incident, betydande incident och tillbud. *Göteborgs kommun* bedömer att definitionen av uttrycket betydande incident är för bred i sin utformning och menar att detta kan leda till att fler incidenter rapporteras än vad som är tanken. Det är därmed mycket angeläget enligt kommunen att Myndigheten för samhällsskydd och beredskap så snart som möjligt meddelar föreskrifter som närmare preciserar betydelsen av begreppet. *Hi3G Access AB (Tre)* påpekar att definitionen av uttrycket incident skiljer sig från säkerhetsincident som används i LEK. *Stokab AB* bedömer att en särskild svårighet i lagstiftningsärendet är att vissa sektorsspecifika bestämmelser i LEK föreslås upphävas och ersättas med en ny sektorsövergripande lag. Stokab AB pekar bland annat på skillnaderna mellan lagarna och bedömer att det är oklart huruvida en kabelskada ska anses utgöra en incident i den nya lagens bemärkelse. Bolaget instämmer i utredningens uppfattning att det i det fortsatta lagstiftningsarbetet bör övervägas om skillnaden i omfattning mellan lagstiftningarna medför ett behov av vidare åtgärder. *Telefonaktiebolaget LM Ericsson (Ericsson)* anser att det bör finnas en möjlighet för företag att definiera vad som utgör en betydande incident utifrån sin storlek och verksamhet.

Skälen för regeringens förslag

Uttrycken incident och betydande incident i direktivet

I NIS 2-direktivet fastställs en flerstegsstrategi för rapportering av betydande incidenter för att hitta rätt balans mellan, å ena sidan, snabb rapportering som bidrar till att begränsa den potentiella spridningen av betydande incidenter och gör det möjligt för väsentliga och viktiga entiteter att söka bistånd och, å andra sidan, ingående rapportering som drar värdefulla lärdomar av enskilda incidenter och med tiden förbättrar cyberresiliensen hos enskilda entiteter och hela sektorer (skäl 101).

Enligt samma skäl bör direktivet omfatta rapportering av incidenter som, baserat på en första bedömning som utförts av den berörda entiteten, kan orsaka allvarliga störningar i tjänsterna eller ekonomiska förluster för den berörda entiteten eller påverka andra fysiska eller juridiska personer genom att orsaka betydande materiell eller immateriell skada. En sådan inledande bedömning bör bland annat ta hänsyn till de drabbade nätverks- och informationssystemen, särskilt deras betydelse för tillhandahållandet av entitetens tjänster, allvaret i och de tekniska egenskaperna hos cyberhotet och eventuella underliggande sårbarheter som utnyttjas, samt entitetens erfarenhet av liknande incidenter. Indikatorer såsom i vilken utsträckning tjänstens funktion påverkas, hur länge incidenten pågår eller hur många tjänstemottagare som drabbas kan också, enligt skäl 101, spela en viktig roll när man fastställer om tjänstens driftsstörning är allvarlig.

För att säkerställa ett smidigt tillhandahållande av tjänster som levereras av väsentliga och viktiga entiteter är det, enligt skäl 97 i NIS 2-direktivet, viktigt att alla tillhandahållare av allmänna elektroniska kommunikationsnät har infört lämpliga riskhanteringsåtgärder för cybersäkerhet och rapporterar betydande incidenter i samband med dessa. Medlemsstaterna bör enligt samma skäl säkerställa att säkerheten i de allmänna elektroniska kommunikationsnäten upprätthålls och att deras vitala säkerhetsintressen skyddas mot sabotage och spionage. Eftersom internationell konnektivitet förstärker och påskyndar en konkurrenskraftig digitalisering av unionen och dess ekonomi bör incidenter som påverkar undervattenskablar rapporteras till CSIRT-enheten eller i förekommande fall den behöriga myndigheten. Den nationella strategin för cybersäkerhet bör också när så är relevant, i enlighet med skäl 97, beakta cybersäkerheten för undervattenskablar och inbegripa kartläggning av potentiella cybersäkerhetsrisker och riskreduceringsåtgärder för att säkerställa högsta skyddsnivå för dem.

Bestämmelserna om incidentrapportering finns i artikel 23 i NIS 2-direktivet. Av artikel 23.1 följer att medlemsstaterna ska säkerställa att entiteter utan onödigt dröjsmål underrättar sin CSIRT-enhet, eller i tillämpliga fall sin behöriga myndighet, om sådana incidenter som enligt direktivet räknas som betydande.

Enligt definitionen i artikel 6.6 avses med incident en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem. En incident ska enligt artikel 23.3 anses vara betydande om den har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för den berörda entiteten eller om den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada. I bland annat den engelska och danska språkversionen anges det att incidenten ska anses vara betydande om den har orsakat eller är kapabel att orsaka (”is capable of causing” respektive ”er i stand til att forårsage”) nämnda konsekvenser. I dessa språkversionen anges även att incidenten ska anses vara betydande om den har påverkat eller är kapabel att påverka (”is capable of affecting” respektive ”er i stand til att påvirke”) på visst sätt.

Hur ska uttrycken definieras i lagen?

Som *Tre* påpekar skiljer sig definitionen av incident enligt NIS 2-regleringen från definitionen av säkerhetsincident enligt LEK. En säkerhetsincident enligt 1 kap. 7 § LEK avser en händelse med en faktisk negativ inverkan på bland annat tillgängligheten hos ett nät eller en tjänst, hos vissa uppgifter eller hos vissa närliggande tjänster eller på förmågan att motstå sådana händelser.

I avsnitt 11 föreslås bland annat att bestämmelserna som rör rapportering av vissa säkerhetsincidenter i LEK ska upphävas. De verksamhetsutövare som omfattas av LEK föreslås i stället rapportera incidenter enligt den nya lagen. Regeringen anser, likt utredningen, att det inte finns skäl att ge incidentbegreppet enligt den nya lagen samma innebörd som i LEK. Enligt regeringen bör direktivets definition i stället användas i den nya lagen.

En incident bör, i linje med vad som anges i NIS 2-direktivet, definieras i lagen som en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem. En incident är alltså varje händelse som på så sätt äventyrar uppgifternas eller tjänsternas skyddsvärda egenskaper. Tjänster som erbjuds genom eller är tillgängliga via ett elektroniskt kommunikationsnät inbegriper såväl grossisttjänster som slutkunds-tjänster.

Göteborgs kommun bedömer att den av utredningen föreslagna definitionen av uttrycket betydande incident är för bred i sin utformning och menar att detta kan leda till att fler incidenter rapporteras än vad som är tanken. Regeringen anser dock, likt utredningen, att det finns skäl att låta definitionen i lagen i stort överensstämma med direktivets utformning. En betydande incident bör därför definieras som en incident som har orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande skada. Som utredningen föreslår bör uttrycket ekonomisk skada användas i stället för ekonomisk förlust som nämns i artikel 23.3 i NIS 2-direktivet. Till skillnad från utredningen anser regeringen att endast uttrycket skada bör användas i definitionens andra led i stället för materiell eller immateriell skada. Innebörden av uttrycket skada bör motsvara det som avses med materiell eller immateriell skada i direktivet, i den engelska språkversionen ”material or non-material”, det vill säga bland annat sakskada och ren förmögenhetsskada. En bedömning bör göras i varje enskilt fall av vad som utgör en betydande incident, men uttrycket i sig bör inte, som *Ericsson* föreslår, ges en individuell innebörd.

Regeringen instämmer i utredningens och Göteborgs kommuns uppfattning om att innebörden av uttrycket betydande incident bör preciseras. Genomförandeförordningen, som nämns i avsnitt 6.4, syftar bland annat till att närmare ange i vilka fall en incident ska anses vara betydande enligt artikel 23.3 i NIS 2-direktivet. De verksamhetsutövare som berörs av genomförandeförordningen är registreringsenheter för toppdomäner samt leverantörer av DNS-tjänster, molntjänster, data-centraltjänster, nätverk för leverans av innehåll, utlokaliserade driftstjäns-ter, utlokaliserade säkerhetstjänster, marknadsplatser online, sökmotorer,

plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster. Eftersom genomförandeförordningen är direkt tillämplig behöver inte motsvarande bestämmelser införas i nationell rätt. Det finns vidare inte utrymme för att införa nationella bestämmelser i de delar som omfattas av genomförandeförordningen. Regeringen eller den myndighet som regeringen bestämmer bör dock, i övrigt, få meddela ytterligare föreskrifter om vad som utgör en betydande incident.

I skäl 95 i NIS 2-direktivet anges att befintliga nationella riktlinjer som har antagits för att införliva kodexens bestämmelser om säkerhetsåtgärder bör beaktas, när så är lämpligt och för att undvika onödiga störningar, vid införlivandet av NIS 2-direktivet för att ta fasta på den kunskap och kompetens som redan förvärvats inom ramen för kodexen avseende säkerhetsåtgärder och incidentunderrättelser. Detta innebär att Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster (PTSFS 2022:11) så långt möjligt bör beaktas också i det kommande föreskriftsarbetet när det gäller tillhandahållare av allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster.

En jämförelse med LEK

I avsnitt 6.6.2 lämnas förslag om hur rapporteringsskyldigheten vid betydande incidenter ska fullgöras. Både *Stokab AB* och *Tre* resonerar kring skillnaderna mellan den i det avsnittet föreslagna rapporteringsskyldigheten och rapporteringsskyldigheten enligt LEK. Tre påpekar bland annat att definitionen av uttrycket betydande incident skiljer sig från uttrycket säkerhetsincident som används i LEK.

Regeringen anser visserligen, som framgår ovan, att det inte finns skäl att ge incidentbegreppet enligt den nya lagen samma innebörd som i LEK. En händelse som har fysisk påverkan på ett allmänt tillgängligt kommunikationsnät och som äventyrar tillgängligheten till exempelvis nät- eller slutkundstjänster bör dock anses utgöra en incident även enligt den nya lagen. En händelse som orsakar en kabelskada i ett sådant nät, som Stokab AB resonerar kring, kan därmed räknas som en incident. För att föranleda rapporteringsskyldighet krävs dock att även ovan angivna rekvisit för att incidenten ska räknas som en betydande incident är uppfyllda.

När det gäller fysisk skada på ledningar för elektronisk kommunikation är det viktigt att tillsynsmyndigheten får underlag för att kunna kontrollera att det förebyggande arbetet mot oönskad påverkan på nätet bedrivs på ett lämpligt sätt med hänsyn till risken (jfr skäl 97 och 101). Att elektroniska kommunikationsnät fungerar på ett säkert sätt och med tillräcklig redundans är av mycket stor betydelse för bland annat totalförsvaret (jfr prop. 2024/25:34 s. 129 f.). Det rådande omvärldsläget innebär ökade risker i form av så kallade hybridhot mot nät och tjänster, där antagonistiska aktörer försöker påverka genom dolda sabotage som kan vara flera och samverkande. Mot den bakgrunden utgör information om fysiska skador på nät numera en viktigare del i operatörernas långsiktiga strategiska driftssäkerhetsarbete och i tillsynen.

När det gäller ett ledningsbrott i ett elektroniskt kommunikationsnät kan en incident vara betydande även när den är sådan som typiskt sett medför

allvarlig driftsstörning eller avbrott i ett nät eller en tjänst men som inte har gjort det i det enskilda fallet. Huruvida en driftsstörning är att se som allvarlig kan vara beroende av omfattningen av ett kapacitetsbortfall eller hur många aktiva anslutningar eller hur stort område som påverkats av incidenten. Även en störning eller risk för störning som skulle kunna vålla betydande skada i form av påverkan på redundans eller viktiga samhällsfunktioner kvalificerar som en betydande incident.

Regeringen bedömer sammanfattningsvis, trots att begreppsanvändningen i den nya lagen föreslås vara en annan än i LEK, att rapporteringsskyldigheten beträffande tillhandahållare av allmänna elektroniska kommunikationsnät och av allmänt tillgängliga elektroniska kommunikationstjänster i allt väsentligt kommer att vara densamma sett till vilka slags incidenter som ska rapporteras. Det finns därför inget behov av ytterligare åtgärder som Stokab AB nämner.

Cyberhot och betydande cyberhot

Av artikel 23.2 i NIS 2-direktivet följer en viss underrättelseskyldighet för entiteterna, som beskrivs mer ingående i avsnitt 6.6.3, avseende betydande cyberhot. I artikel 6.10 definieras uttrycket cyberhot som ett cyberhot enligt definitionen i artikel 2.8 i EU:s cybersäkerhetsakt. Ett cyberhot definieras därmed i NIS 2-direktivet som en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare av dessa system och andra personer. Ett cyberhot kan utnyttja en sårbarhet, till exempel ett bristfälligt skyddat informationssystem. Definitionen förutsätter inte att omständighetens, händelsens eller handlingens påverkan realiseras. Uttrycket betydande cyberhot definieras i artikel 6.11 i direktivet som ett cyberhot som, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på en entitets nätverks- och informationssystem eller användarna av entitetens tjänster genom att vålla betydande materiell eller immateriell skada. Cyberhot och betydande cyberhot bör i lagen definieras på samma sätt som i direktivet, med den skillnaden att uttrycket materiell eller immateriell inte bör anges i lagen i enlighet med resonemanget ovan. Det bör dock framgå direkt av lagen vad som avses med uttrycket cyberhot.

Ingen definition av eller rapporteringsskyldighet vid tillbud

Ett antal remissinstanser, till exempel *Energiföretagen Sverige*, resonerar kring rapportering av tillbud. Uttrycket tillbud definieras i artikel 6.5 i NIS 2-direktivet som en händelse som kunde ha undergrävt tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem, men som framgångsrikt hindrades från att utvecklas eller som inte uppstod.

Ordet tillbud nämns endast i artiklarna 29 och 30, som rör möjligheterna för entiteter att lämna frivilliga underrättelser eller på frivillig basis utbyta relevant information om bland annat tillbud jämte bestämmelser om exempelvis CSIRT-enhetens skyldigheter i anledning av detta. Det finns alltså ingen rapporteringsskyldighet för verksamhetsutövare kopplad till tillbud enligt direktivet och detta är inte heller något som utredningen

föreslår. Utredningen föreslår däremot att uttrycket tillbud ska definieras i lagen. Eftersom uttrycket inte används i lagen i övrigt, utan endast i utredningens förslag till förordning, bör definitionen inte anges i lagen.

6.6.2 Verksamhetsutövare ska rapportera betydande incidenter

Regeringens förslag: Verksamhetsutövare ska upplysa den myndighet som regeringen bestämmer om en betydande incident så snart det kan ske, dock senast 24 timmar efter det att verksamhetsutövaren har fått kännedom om den betydande incidenten.

Verksamhetsutövare ska till samma myndighet göra en incidentanmälan om den betydande incidenten så snart det kan ske, dock senast 72 timmar efter det att verksamhetsutövaren har fått kännedom om den betydande incidenten. För verksamhetsutövare som tillhandahåller betrodda tjänster ska anmälan i stället göras senast 24 timmar efter sådan kännedom.

På begäran av myndigheten ska verksamhetsutövare lämna en delrapport med relevanta statusuppdateringar för den betydande incidenten.

Senast en månad efter incidentanmälan ska verksamhetsutövare lämna en slutrapport till myndigheten. Om den betydande incidenten fortfarande är pågående ska i stället en lägesrapport lämnas vid denna tidpunkt och därefter en slutrapport inom en månad efter det att den betydande incidenten har hanterats.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om incidentrapporteringen.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att ordet varning ska användas i stället för upplysning. Utredningen föreslår att rapporteringen ska ske till CSIRT-enheten och att enheten ska få begära ytterligare information av verksamhetsutövaren, men har inget förslag om att CSIRT-enheten ska upplysas så snart det kan ske och förslaget innehåller inte heller ordet delrapport. Utredningen lämnar förslag om vad en varning, anmälan och rapport ska innehålla för uppgifter.

Remissinstanserna: Ett antal remissinstanser, däribland *Hi3G Access AB (Tre)* och *Myndigheten för samhällsskydd och beredskap (MSB)*, anser att ett annat ord än varning bör användas för den första underrättelsen som ska skickas till CSIRT-enheten. MSB föreslår ordet notifiering som ett alternativ. *Telenor Sverige AB (Telenor)* anser att det finns ett behov av att kunna dra tillbaka underrättelsen. Telenor tillhör vidare de remissinstanser som anser att det är otydligt vad den första underrättelsen ska innehålla för uppgifter.

Advokatfirman Kahn Pedersen påpekar bland annat att det inte framgår på vilket sätt varningen ska uppdateras i incidentanmälan och föreslår en mer direktivnära formulering av bestämmelsen om anmälan än den som utredningen föreslår. MSB har synpunkter på utredningens förslag om anmälans innehåll och anser i likhet med *Region Stockholm* att bestämmelsen bör utformas på ett mer direktivnära sätt. Enligt Tre bör

innebörden av uttrycket angreppsindikatorer, som nämns i utredningens förslag gällande anmälans innehåll, förtydligas.

Göteborgs kommun efterfrågar ett förtydligande av vad som utgör en sådan incident som ska föranleda rapportering. Bland andra *Skatteverket* och Telenor pekar på svårigheterna för en verksamhetsutövare att bedöma huruvida en omständighet kan orsaka en allvarlig driftstörning eller ekonomisk skada, inte minst när det gäller att bedöma risken för potentiell skada för andra. Enligt Telenor krävs det tydlig och konkret vägledning i detta avseende. *Lantmännen* och *Livsmedelsverket* gör gällande att förslaget innebär att flera verksamhetsutövare inom samma koncern kan omfattas av kraven och att detta kan leda till att en enskild incident måste rapporteras flera gånger. *Statens veterinärmedicinska anstalt* anser att det finns en otydlighet gällande hur många rapporter som kan krävas. *Teracom Group AB* understryker vikten av att rapporterna i största möjliga mån bör ses som en möjlighet till lärande, att verksamhetsutövare får information om incidenter från andra verksamhetsutövare och att rapportering inte automatiskt ska leda till tillsyn och sanktioner.

Flera remissinstanser har synpunkter på förslagen om tidsfrister. *Drivkraft Sverige* föreslår att tidsfristen ska börja löpa när en mer grundlig bedömning av incidenten har gjorts. Enligt Livsmedelsverket bör den första underrättelsen göras redan inom 6 timmar, men *Svensk Dagligvaruhandel* ser positivt på underrättelsen ska ges in inom 24 timmar. *Trafikverket* och *Transportstyrelsen* anser, i likhet med vissa andra instanser, att det i enlighet med direktivet bör framgå att tidsfristerna ska ses som en bortre tidsgräns. Flera remissinstanser, däribland *Region Gotland* och *Salems kommun*, påpekar att tidsfristerna kan bli utmanande att hålla för de verksamhetsutövare som inte har bemanning dygnet runt. *Svensk Handel* föreslår att tidsfristerna förlängs.

Ett antal remissinstanser har synpunkter på förslaget om att incidentrapportering endast ska ske till CSIRT-enheten. Bland andra *Tillväxtverket* framför att förslaget innebär risk för att tillsynsmyndigheterna inte får tillräcklig kännedom om inträffade incidenter och *Östhammars kommun* anser att det borde finnas en sammanhållande myndighet som kan ges i uppdrag att vidareförmedla information till berörda myndigheter. Flertalet remissinstanser, till exempel *Länsstyrelsen i Västernorrlands län* och *Svenskt Vatten*, resonerar kring hur förslaget förhåller sig till säkerhetsskyddsregelverket. Flera remissinstanser, bland andra *Post- och telestyrelsen (PTS)* och *Scrive AB*, önskar att bestämmelserna om incidentrapportering harmoniseras med andra regelverk. Enligt PTS och Scrive AB behöver regleringen om incidentrapporteringen i den nya lagen förhålla sig till den incidentrapportering som ska ske enligt EU:s förordning om elektronisk identifiering. Göteborgs kommun nämner att det är av stor vikt att lämplig återkoppling sker från den myndighet som har mottagit rapporteringen till verksamhetsutövaren. Kommunen efterfrågar även ett förtydligande av hur inrapporterade uppgifter ska användas på regional nivå och på unionsnivå.

Ett antal remissinstanser, däribland PTS och *Stokab AB*, resonerar kring förslaget om möjligheten att meddela föreskrifter. PTS anför bland annat att det är av vikt att den myndighet som ges föreskriftsrätt avseende incidentrapportering, om det skulle vara en annan än PTS, beaktar redan framtagna regler och rapporteringströsklar avseende incidentrapportering

samt samverkar föreskrifterna med PTS. Stokab AB anger att det är av vikt att föreskrifterna utfärdas av den myndighet som utövar tillsyn.

Några remissinstanser, däribland *Svenskt Näringsliv*, anser att incidentrapporteringen innebär vissa problem eftersom rapporterna kan innefatta personuppgifter och uppgifter som omfattas av sekretess.

Skälen för regeringens förslag

Rapportering av betydande incidenter enligt direktivet

I NIS 2-direktivet fastställs en flerstegsstrategi för rapportering av betydande incidenter för att hitta rätt balans mellan, å ena sidan, snabb rapportering som bidrar till att begränsa den potentiella spridningen av betydande incidenter och gör det möjligt för väsentliga och viktiga entiteter att söka bistånd och, å andra sidan, ingående rapportering som drar värdefulla lärdomar av enskilda incidenter och med tiden förbättrar cyberresiliensen hos enskilda entiteter och hela sektorer (skäl 101). Vad som avses med uttrycket cyberresiliens utvecklas inte i direktivet men uttrycket tar typiskt sett sikte på förmågan hos en organisation att förbereda sig för, hantera och återhämta sig från cyberattacker.

Enligt artikel 23.1 i NIS 2-direktivet ska varje medlemsstat säkerställa att entiteter utan onödigt dröjsmål underrättar sin CSIRT-enhet eller, i tillämpliga fall, sin behöriga myndighet på visst sätt om alla incidenter som har en betydande inverkan på tillhandahållandet av deras tjänster och som definieras som en betydande incident. Enligt samma artikel ska entiteterna också underrätta mottagarna av deras tjänster om betydande incidenter och även om betydande cyberhot (se vidare avsnitt 6.6.3).

Enligt artikel 23.4 ska rapporteringen ske i olika steg. Först ska en tidig varning lämnas och därefter en incidentanmälan. När incidenten är hanterad ska en slutrapport lämnas och i vissa fall även en lägesrapport dessförinnan. Allt detta ska ske inom vissa angivna tidsfrister. Om mottagande myndighet begär det, ska verksamhetsutövaren utöver övriga underrättelser lämna en delrapport. Bestämmelser som motsvarar denna flerstegsstrategi bör, som utredningen föreslår, införas i den nya lagen på sätt som framgår nedan.

Enligt artikel 23.6 i NIS 2-direktivet ska, när så är lämpligt och särskilt om en betydande incident berör två eller flera medlemsstater, CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten utan onödigt dröjsmål informera andra berörda medlemsstater och Enisa om den betydande incidenten. Sådan information ska åtminstone inbegripa den typ av information som har mottagits i enlighet med artikel 23.4, det vill säga inom ramen för entiteternas rapporteringsskyldighet. Därvid ska CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten, i enlighet med unionsrätten eller nationell rätt, bevara entitetens säkerhets- och affärsintressen samt den tillhandahållna informationens konfidentialitet. På begäran av CSIRT-enheten eller den behöriga myndigheten ska den gemensamma kontaktpunkten också enligt artikel 23.8 vidarebefordra underrättelser som mottagits i enlighet med 23.1 till de gemensamma kontaktpunkterna i andra berörda medlemsstater.

Rapportering bör ske till den myndighet som regeringen bestämmer

Hur uttrycket betydande incident, som används i artikel 23, ska tolkas och vilka överväganden som ska göras i bedömningen av om en sådan har inträffat behandlas i avsnitt 6.6.1. Utredningen föreslår att all rapportering av betydande incidenter ska ske till en enda myndighet och att det då, i enlighet med utgångspunkten i artikel 23, är CSIRT-enheten som rapportering ska ske till. Majoriteten av remissinstanserna instämmer i uppfattningen att denna ordning bör gälla. Bland andra *Tillväxtverket* framför dock att förslaget innebär risk för att tillsynsmyndigheterna inte får tillräcklig kännedom om inträffade incidenter och *Östhammars kommun* anser att det borde finnas en sammanhållande myndighet som kan ges i uppdrag att vidareförmedla information till berörda myndigheter.

I förarbetena till NIS-lagen gjordes bedömningen att rapportering skulle ske till CSIRT-enheten men att uttrycket inte skulle användas i lagen (se prop. 2017/18:205 s. 47 f.). Av NIS-lagen framgår endast att rapporteringen ska göras till den myndighet som regeringen bestämmer, medan det av 11 § NIS-förordningen framgår att rapporteringen ska göras till CSIRT-enheten. Det är, som bland andra Tillväxtverket resonerar kring, av vikt att tillsynsmyndigheterna får tillräcklig kännedom om inträffade incidenter. Regeringen anser dock inte att det heller i den nya lagen finns anledning att peka ut till vilken myndighet som rapportering ska ske. Det bör i stället finnas en flexibilitet i regleringen och i lag anges att rapportering ska ske till den myndighet som regeringen bestämmer. Det finns inte utrymme för att inom ramen för denna lagrådsremiss ge ett sådant uppdrag som Östhammars kommun efterfrågar.

Det generella syftet med att rapportera incidenter är bland annat att begränsa skada och förebygga liknande händelser (jfr skäl 101 i direktivet). Som *Teracom Group AB* nämner är incidentrapporterna en möjlighet till lärande. Det är enligt regeringen inte möjligt att göra något generellt uttalande om när en rapporterad incident ska leda till tillsyn eller ingripande. Som framgår av avsnitt 7 är tillsynsmyndigheternas uppdrag att utöva tillsyn över att regleringen följs och för viktiga verksamhetsutövare får dessutom tillsynsåtgärder endast vidtas när tillsynsmyndigheten har anledning att anta att regleringen inte följs. I vilka fall ingripande föreslås kunna ske framgår av avsnitt 8.

Som *Göteborgs kommun* nämner är det av stor vikt att lämplig återkoppling sker från den myndighet som har mottagit rapporteringen till verksamhetsutövaren. Detta är dock inte något som kräver reglering i lag och därmed inte heller en fråga som bör behandlas i denna lagrådsremiss. Kommunen efterfrågar även ett förtydligande av hur inrapporterade uppgifter ska användas på regional nivå och på unionsnivå. Uppgifterna kommer, i enlighet med skäl 101 i NIS 2-direktivet, att användas för olika syften. De kommer, i linje med vad som anges i skälet, bland annat att användas för att begränsa effekterna av incidenten. De inrapporterade uppgifterna kommer också i enlighet med artikel 23.6 och 23.8 att användas på unionsnivå. Som utvecklas i avsnitt 12 gäller krav på konfidentialitet i direktivet och i avsnittet lämnas även förslag som syftar till att skydda känsliga uppgifter som utbyts.

Verksamhetsutövaren bör först upplysa om en betydande incident

Av artikel 23.4 a följer att entiteter, utan onödigt dröjsmål och under alla omständigheter inom 24 timmar efter att de har fått kännedom om den betydande incidenten, ska lämna en tidig varning.

Den första underrättelsen som en verksamhetsutövare ska lämna bör enligt regeringen, som bland andra *MSB* gör gällande, benämnas på ett annat sätt än varning för att undvika sammanblandning med andra liknande uttryck och för att tydliggöra att syftet med underrättelsen främst är att så tidigt som möjligt underrätta om incidenten. I direktivet används i artikel 23.1 underrättelser som ett samlingsbegrepp för alla rapporteringsåtgärder. Regeringen anser därför att det är lämpligare att den första underrättelsen benämns upplysning.

Utredningen anser att artikeln ska tolkas som att kravet enbart innebär att upplysningen ska lämnas inom 24 timmar. Regeringen bedömer emellertid, som bland andra *Transportstyrelsen*, att det i lagen bör framhållas att upplysningen ska lämnas så snart det kan ske, dock senast 24 timmar efter det att verksamhetsutövaren har fått kännedom om incidenten. Tidsfristen om 24 timmar bör alltså ses som en bortre tidsgräns. Med hänsyn till den övriga hantering som en betydande incident innebär för en verksamhetsutövare anser regeringen inte att tidsgränsen bör sättas kortare på sätt som *Livsmedelsverket* föreslår. Enligt regeringen är det inte heller möjligt att sätta en längre tidsfrist än vad som anges i direktivet, som bland andra *Svensk Handel* resonerar kring.

Tidsfristen bör i enlighet med vad som anges i NIS 2-direktivet börja löpa från det att verksamhetsutövaren har fått kännedom om den betydande incidenten och inte, som *Drivkraft Sverige* föreslår, från det att en mer grundlig bedömning av incidenten har gjorts. Det följer av syftet med upplysningen, att snabbt uppmärksamma den mottagande myndigheten på incidenten och ge verksamhetsutövaren möjlighet att vid behov få hjälp, att det inte kan ställas krav på en mer omfattande utredning. Detta kan, som till exempel *Telenor* påpekar, leda till att verksamhetsutövare upplyser om incidenter i större utsträckning än vad som visar sig vara nödvändigt i efterhand. Om och på vilket sätt en incidentrapport ska kunna återkallas bör regleras på lägre föreskriftsnivå än i lag.

Verksamhetsutövare bör sammanfattningsvis upplysa den myndighet som regeringen bestämmer om en betydande incident så snart det kan ske, dock senast 24 timmar efter det att verksamhetsutövaren har fått kännedom om incidenten. Enligt artikel 23.4 a ska det i samband med upplysningen i tillämpliga fall anges om den betydande incidenten misstänks ha orsakats av olagliga eller avsiktligt skadliga handlingar eller kan ha gränsöverskridande verkningar. Utredningen föreslår att det ska framgå av lagen att det i upplysningen ska anges om det finns misstanke om incidenten orsakats uppsåtligen och om incidenten kan ha gränsöverskridande effekter. Regeringen anser att det är lämpligare att innehållet i en upplysning regleras på lägre föreskriftsnivå än i lag.

Verksamhetsutövaren bör därefter göra en incidentanmälan

Det andra steget i rapporteringen av betydande incidenter utgörs av en incidentanmälan. Av artikel 23.4 b framgår att entiteter, utan onödigt dröjsmål och under alla omständigheter inom 72 timmar efter att ha fått

kännedom om den betydande incidenten, ska lämna en incidentanmälan. Dessutom ska incidentanmälan, i tillämpliga fall, uppdatera den information som avses i artikel 23.4 a. Av sista stycket i artikel 23.4 följer ett undantag avseende tidsfristen för tillhandahållare av betrodda tjänster, som i stället ska lämna en incidentanmälan utan onödigt dröjsmål och under alla omständigheter inom 24 timmar efter att ha fått kännedom om den betydande incidenten.

Regeringen instämmer i allt väsentligt i utredningens uppfattning om hur skyldigheterna avseende incidentanmälan bör regleras i den nya lagen. Det bör enligt regeringen även framgå av lagen att anmälan ska göras så snart det kan ske, dock senast 24 timmar av tillhandahållare av betrodda tjänster och 72 timmar av övriga verksamhetsutövare efter det att verksamhetsutövaren har fått kännedom om incidenten. Tidsfristerna bör alltså ses som en bortre tidsgräns.

Vad en incidentanmälan ska innehålla behandlas i artikel 23.4 b. Enligt denna artikel ska det i incidentanmälan finnas en inledande bedömning av den betydande incidenten, dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer. I tillämpliga fall ska samma incidentanmälan även innehålla en uppdatering av den information som ingår i underrättelsen. Utredningen föreslår att incidentanmälan enligt den nya lagen ska innehålla en inledande bedömning av hur allvarlig den betydande incidenten är, konsekvenserna av den och förekomsten av angreppsindikatorer. Dessutom föreslår utredningen att den tidigare underrättelsen ska uppdateras.

Ett flertal remissinstanser, bland andra *Region Stockholm*, har synpunkter på utredningens förslag om anmälans innehåll och anser att bestämmelsen bör utformas på ett mer direktivnära sätt än vad utredningen föreslår. Regeringen anser att det är lämpligare att innehållet i incidentanmälan regleras på lägre föreskriftsnivå än i lag. Det finns därmed inte skäl att närmare beröra eller göra förtydliganden i förhållande till utredningens förslag i denna lagrådsremiss.

Delrapport, slutrapport och lägesrapport

Av artikel 23.4 c i direktivet framgår att medlemsstaterna ska säkerställa att berörda entiteter på begäran av en CSIRT-enhet eller, i tillämpliga fall, den behöriga myndigheten, lämnar en delrapport om relevanta statusuppdateringar. Det utvecklas inte närmare i direktivet när en sådan delrapport kan begäras.

I utredningens förslag genomförs artikeln genom att det i lagen anges att CSIRT-enheten får begära ytterligare information av verksamhetsutövaren men utredningen utvecklar inte när sådan information ska få begäras. Regeringen bedömer att det i stället bör införas en bestämmelse om att verksamhetsutövare, på begäran av den myndighet som regeringen bestämmer, ska lämna en delrapport med relevanta statusuppdateringar för den betydande incidenten. Det bör, utifrån skäl 101, bland annat kunna vara aktuellt att begära en delrapport om det krävs ytterligare information från verksamhetsutövaren för att begränsa den potentiella spridningen av den betydande incidenten. Det kommer att vara upp till den myndighet som regeringen bestämmer att bedöma om det finns behov av en

delrapport och om en begäran är proportionerlig utifrån bland annat 5 § tredje stycket förvaltningslagen (2017:900).

Enligt artikel 23.4 d ska medlemsstaterna säkerställa att berörda entiteter senast en månad efter incidentanmälan lämnar en slutrapport. Slutrapporten ska enligt samma artikel innehålla en detaljerad beskrivning av incidenten, inbegripet dess allvarlighetsgrad och konsekvenser, den typ av hot eller grundorsak som sannolikt har utlöst incidenten, tillämpade och pågående begränsande åtgärder samt, i tillämpliga fall, incidentens gränsöverskridande verkningar. Av artikel 23.4 e framgår att entiteterna, för det fall incidenten är pågående vid tidpunkten för inlämnandet av slutrapporten, i stället ska tillhandahålla en lägesrapport vid den tidpunkten och en slutrapport inom en månad efter det att de har hanterat incidenten.

Regeringen bedömer, i likhet med utredningen, att direktivets reglering avseende slut- och lägesrapport bör införas i svensk rätt genom en särskild bestämmelse i den nya lagen. En incident ska anses ha hanterats när det inte längre vidtas några åtgärder för att förebygga, upptäcka, analysera, begränsa eller reagera på eller återhämta sig från incidenten. Regeringen anser dock att innehållet i rapporterna, på samma sätt som för övriga underrättelser, bör regleras på lägre föreskriftsnivå än i lag.

Frivillig underrättelse kan lämnas utan särskild reglering

Enligt artikel 30.1 i NIS 2-direktivet ska medlemsstaterna säkerställa att underrättelser, utöver den underrättelseskyldighet som föreskrivs i artikel 23 om rapporteringsskyldigheter, kan lämnas in på frivillig basis. Detta gäller enligt artikeln såväl väsentliga och viktiga entiteter som andra entiteter, oberoende om de omfattas av NIS 2-direktivet, med avseende på incidenter, cyberhot och tillbud. Av artikel 30.2 följer att myndigheterna ska behandla dessa frivilliga underrättelser i enlighet med det förfarande som gäller för rapporteringsskyldigheten enligt artikel 23.

Utredningen bedömer att kravet på att möjliggöra frivilliga underrättelser inte behöver regleras särskilt i den nya lagen, utan att 19 § förvaltningslagen är tillräcklig i sammanhanget. Enligt den paragrafen ska en enskild formlöst kunna inleda ett ärende hos en myndighet genom en ansökan, anmälan eller annan framställning. Med enskild avses inte bara fysiska personer, utan också företag, föreningar, organisationer och liknande privaträttsliga subjekt. Däremot omfattas exempelvis inte myndigheter.

NIS 2-direktivet innehåller inga begränsningar om att möjligheten att frivilligt lämna uppgifter endast ska gälla privaträttsliga subjekt. Vidare är en stor andel av de verksamhetsutövare som omfattas av NIS 2-regleringen myndigheter, regioner och kommuner. Det som stadgas i 19 § förvaltningslagen är därmed i sig inte tillräckligt för att kraven i artikel 30.1 ska anses vara uppfyllda. Däremot finns det inget hinder mot att statliga myndigheter, kommuner och regioner lämnar en sådan frivillig underrättelse som direktivet nämner. Direktivets krav innebär endast att det ska finnas möjlighet att lämna en sådan underrättelse och enligt regeringen krävs det därför inte någon särskild reglering för att uppfylla direktivets krav i denna del.

Förhållandet till säkerhetsskyddslagen

Ett flertal remissinstanser resonerar kring förslagets förhållande till säkerhetsskyddsregleringen. Bland annat *Länsstyrelsen i Västernorrlands län* ber om ett förtydligande i fråga om att berörda aktörer inte ska behöva rapportera incidenter enligt såväl den nya lagen som säkerhetsskyddsregleringen. *Skatteverket* önskar förtydliganden om hur incidenter ska hanteras när det rör sig om både en säkerhetshotande händelse och när det finns ett allmänt behov av omedelbar rapportering till mottagande myndighet enligt den nya lagen.

Av 1 kap. 1 § säkerhetsskyddslagen framgår att lagen gäller för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet). Enligt 2 kap. 1 § samma lag ska en verksamhetsutövare bland annat anmäla och rapportera sådant som är av vikt för säkerhetsskyddet.

Med säkerhetsskydd avses, enligt 1 kap. 2 § säkerhetsskyddslagen, skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter. Med säkerhetsskyddsklassificerade uppgifter avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt OSL eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig.

Enligt 2 kap. 4 § säkerhetsskyddsförordningen (2021:955) ska en verksamhetsutövare skyndsamt göra en anmälan till Säkerhetspolisen vid säkerhetshotande händelser eller verksamhet. Detta gäller bland annat om det inträffat en it-incident i ett informationssystem som verksamhetsutövaren är ansvarig för och som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet. Om verksamhetsutövaren tillhör Försvarsmaktens tillsynsområde ska anmälan göras också till Försvarsmakten. Säkerhetspolisen ska underrätta verksamhetsutövarens tillsynsmyndighet om en anmälan som gjorts.

I avsnitt 5.4.2 föreslås att den nya lagen inte ska gälla för bland annat statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet och inte heller för enskilda verksamhetsutövare som enbart bedriver sådan verksamhet eller enbart erbjuder tjänster till en statlig myndighet som till övervägande del bedriver säkerhetskänslig verksamhet. För andra verksamhetsutövare som till någon del bedriver säkerhetskänslig verksamhet eller till någon del erbjuder tjänster till en statlig myndighet som i sin tur till övervägande del bedriver säkerhetskänslig verksamhet gäller inte vissa krav, bland annat rapporteringsskyldigheten, för den del av verksamheten som är säkerhetskänslig eller tillhandahåller tjänsterna. För övriga delar föreslås lagen gälla i dess helhet. I avsnitt 5.4.3 föreslås att skyldigheten att lämna uppgifter inte ska gälla säkerhetsskyddsklassificerade uppgifter.

Förslaget gällande rapportering enligt den nya lagen följer i allt väsentligt NIS 2-direktivets krav och är därmed nödvändigt för att genomföra direktivet i nationell rätt. Om annan författning innehåller bestämmelser om krav på säkerhetsåtgärder eller incidentrapportering med motsvarande verkan gäller, enligt regeringens förslag i avsnitt 5.4.1, inte

kraven i den nya lagen för verksamhetsutövaren. *Region Gotland* ställer sig frågande till att det ställs högre krav i fråga om incidentanmälan och slutrapport i utredningens förslag än i säkerhetsskyddsregelverket.

Det skulle visserligen kunna uppstå en situation då samma incident både påverkar den säkerhetskänsliga verksamhet som verksamhetsutövaren bedriver och övrig verksamhet. För verksamhetsutövare som endast undantas från rapporteringsskyldigheten i vissa delar kan det då bli fråga om att rapportera incidenten enligt båda regelverken. Regeringen tar frågan om vilka negativa konsekvenser som parallella regelverk kan föra med sig på allvar. Det finns dock inget utrymme, givet direktivets innehåll och regelverkens olika syften och tillämpningsområden, att till exempel låta ett av regelverken vara subsidiärt i förhållande till det andra. Mot bakgrund av att hanteringen av anmälningarna enligt den nya lagen och säkerhetsskyddslagen sker av olika myndigheter, utifrån olika befogenheter och ur olika perspektiv, bedömer regeringen att det inte finns risk för att verksamhetsutövare ska uppleva otydlighet i fråga om vad skyldigheterna innebär. Regeringen kan därför inte se att incidentrapporteringen enligt den nya lagen kan komma i konflikt med säkerhetsskyddsregleringen som *Svenskt Vatten* anför. Den administrativa börda som dubbla anmälningar kan innebära är vidare godtagbar. Med hänvisning till de föreslagna undantagen för säkerhetskänslig verksamhet finns det ingen anledning att bedöma huruvida säkerhetsskyddsregelverket innebär krav med motsvarande verkan som Region Gotland resonerar om.

Förhållandet till EU:s förordning om elektronisk identifiering

Rapporteringsskyldigheten i artikel 23 i NIS 2-direktivet träffar alla som omfattas av direktivet, bland annat de tillhandahållare av betrodda tjänster som omfattas av direktivet (se avsnitt 5.3.2). Vilka som anses vara tillhandahållare av betrodda tjänster framgår av EU:s förordning om elektronisk identifiering, som under 2024 har reviderats genom ändringsförordningen.

I enlighet med EU:s förordning om elektronisk identifiering ska både icke-kvalificerade och kvalificerade tillhandahållare av betrodda tjänster anmäla alla säkerhetsincidenter eller störningar som har en betydande inverkan på den tillhandahållna betrodda tjänsten eller de personuppgifter som lagras däri till bland annat tillsynsorganet (artiklarna 19 a.1 b och 24.2 fb). Anmälan ska ske utan onödigt dröjsmål och under alla omständigheter inom 24 timmar från säkerhetsincidenten eller störningen.

Enligt *PTS* och *Scrive AB* behöver regleringen om incidentrapporteringen i den nya lagen förhålla sig till den incidentrapportering som ska ske enligt EU:s förordning om elektronisk identifiering. PTS anser att bestämmelserna om incidentrapportering enligt de båda regelverken överlappar varandra. PTS anser därför att det bör tydliggöras under vilket regelverk som tillhandahållare av betrodda tjänster ska rapportera incidenter. Scrive AB anser att incidentrapportering enligt direktivet och förordningen bör ske på ett sammanhållet sätt till samma myndighet och med samma metoder och samma innehåll.

Av NIS 2-direktivet framgår att tillhandahållare av betrodda tjänster som omfattas av EU:s förordning om elektronisk identifiering bör omfattas av NIS 2-direktivet, bland annat för att rationalisera de skyldigheter som åläggs dem och för att göra det möjligt för dem och för de behöriga

myndigheterna enligt EU:s förordning om elektronisk identifiering att dra nytta av den rättsliga ram som inrättas genom NIS 2-direktivet (skäl 11 och 92). De cybersäkerhetsskyldigheter som fastställs i NIS 2-direktivet bör, enligt skäl 93, anses komplettera de krav som åläggs tillhandahållare av betrodda tjänster enligt EU:s förordning om elektronisk identifiering och tillhandahållare av betrodda tjänster bör vara skyldiga att bland annat rapportera incidenter enligt direktivet. Medlemsstaterna kan, enligt skäl 94, bland annat använda den gemensamma kontaktpunkt som har inrättats för att uppnå en gemensam och automatisk rapportering av incidenter till både tillsynsorganet enligt EU:s förordning om elektronisk identifiering och CSIRT-enheten eller den behöriga myndigheten enligt NIS 2-direktivet.

Av ändringsförordningen framgår att tillhandahållare av betrodda tjänster ska anmäla incidenter enligt NIS 2-direktivet samt att kraven och rapporteringsskyldigheterna enligt NIS 2-direktivet bör ses som komplement till de krav som införs för tillhandahållare av betrodda tjänster enligt förordningen (skäl 50). Vidare framgår att nationella förfaranden eller riktlinjer som fastställts med avseende på genomförandet av säkerhets- och rapporteringskraven och övervakningen av efterlevnaden av sådana krav enligt förordningen i tillämpliga fall bör fortsätta att tillämpas av de behöriga myndigheter som utses enligt NIS 2-direktivet (skäl 50). Vederbörlig hänsyn bör tas för att säkerställa ett effektivt samarbete mellan de tillsynsorgan som utses i enlighet med förordningen och NIS 2-direktivet (skäl 51).

Till skillnad från NIS 2-direktivets krav på flerstegsrapportering avser kravet i EU:s förordning om elektronisk identifiering endast en anmälan. Dessutom finns det inte i förordningen en lika tydligt avgränsad definition av vad som avses med en rapporteringspliktig säkerhetsincident eller störning, mer än att den ska ha en betydande inverkan på den tillhandahållna betrodda tjänsten eller de personuppgifter som lagras däri. Enligt regeringen är incidentrapporteringen som ska ske enligt de olika regelverken därmed inte helt överlappande. Regeringen bedömer därför att rapportering inte enbart kan ske enligt något av regelverken när det gäller tillhandahållare av betrodda tjänster och att det inte heller finns utrymme för att göra undantag i lagen för sådana incidenter som ska rapporteras enligt EU:s förordning om elektronisk identifiering (jfr avsnitt 5.4.1).

En tillhandahållare av betrodda tjänster kan alltså, i enlighet med vad som också framgår av skälen till NIS 2-direktivet och EU:s förordning om elektronisk identifiering, i vissa fall behöva rapportera en incident enligt både NIS 2-regelverket och EU:s förordning om elektronisk identifiering. Det är PTS som i egenskap av tillsynsorgan ska motta en anmälan enligt EU:s förordning om elektronisk identifiering. Vilken myndighet som ska motta incidentrapporter enligt den nya cybersäkerhetslagen bör inte regleras i lag. Regeringen anser dock, i linje med vad som anges i både direktivet och förordningen, att det är av stor vikt att de myndigheter som ska motta incidentrapporter enligt regelverken samverkar.

Övriga frågor om incidentrapportering

Som *Lantmännen* och *Livsmedelsverket* bedömer kan förslaget innebära att flera verksamhetsutövare, som exempelvis ingår i en koncern och som

påverkas av samma incident, kan behöva rapportera incidenten. Regeringen kan inte se att det finns utrymme för att åstadkomma en annan ordning givet direktivets krav. *Statens veterinärmedicinska anstalt* anser att det finns en otydlighet gällande hur många rapporter som kan krävas. Förslaget innebär att verksamhetsutövaren ska lämna en upplysning, göra en incidentanmälan samt lämna en slutrapport. Verksamhetsutövaren ska också i vissa fall lämna en lägesrapport och, på begäran, en delrapport.

Hur uttrycket betydande incident ska definieras och vilka överväganden som ska göras i bedömningen av om en sådan har inträffat behandlas i avsnitt 6.6.1. Bland andra *Skatteverket* och *Telenor* pekar på svårigheterna för en verksamhetsutövare att bedöma huruvida en omständighet kan orsaka en allvarlig driftstörning eller ekonomisk skada, inte minst när det gäller att bedöma risken för potentiell skada för andra. I avsnitt 6.6.1 lämnas förslag om att regeringen eller den myndighet som regeringen bestämmer ska få meddela ytterligare föreskrifter om vad som utgör en betydande incident. Den närmare reglering om formerna för incidentrapporteringen bör också finnas på lägre föreskriftsnivå än i lag, bland annat i fråga om vad underrättelserna ska innehålla och hur uppgifterna som rapporteras ska användas och vidareförmedlas. Regeringen eller den myndighet som regeringen bestämmer bör därför få meddela föreskrifter om incidentrapporteringen. Föreskrifterna kommer enligt regeringens mening att utgöra sådan tydlig och konkret vägledning som Telenor efterfrågar.

Frågan om vilken myndighet som ska utfärda föreskrifter, som PTS och *Stokab AB* väcker, föreslås inte regleras i lag och är därför inte en fråga som behandlas i denna lagrådsremiss. Frågor om sekretess och personuppgiftsbehandling, som bland andra *Svenskt Näringsliv* lyfter, behandlas i avsnitt 12.

6.6.3 Information till mottagare av tjänsterna

Regeringens förslag: Om det är lämpligt ska verksamhetsutövare så snart det kan ske informera mottagarna av deras tjänster om en betydande incident som sannolikt inverkar negativt på tillhandahållandet av tjänsterna.

Vid ett betydande cyberhot ska verksamhetsutövare så snart det kan ske informera mottagarna av deras tjänster som kan påverkas av hotet om skydds- och motåtgärder som mottagarna kan vidta. Om det är lämpligt ska verksamhetsutövare även informera om själva hotet.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om informationsskyldigheten.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår att verksamhetsutövare, i samband med incidentanmälan, ska informera kunder som kan antas påverkas av den betydande incidenten och att kunderna vid behov ska informeras om avhjälpande åtgärder. Utredningen föreslår att samma informationsskyldighet ska gälla vid betydande cyberhot.

Remissinstanserna: Ett antal remissinstanser, bland andra *Post- och telestyrelsen (PTS)* och *Transportstyrelsen*, anser att informationsskyldig-

heten bör utformas mer direktivnära än i utredningens förslag. Information om själva hotet bör enligt PTS endast lämnas när så är lämpligt och det kan, enligt myndigheten, i vissa fall vara olämpligt att informera kunderna om själva hotet. Vissa instanser, däribland *Affärsverket svenska kraftnät* och *Myndigheten för digital förvaltning (Digg)*, resonerar kring utredningens förslag om att ”kunder” ska användas som begrepp för den krets som ska motta informationen. *Advokatfirman Kahn Pedersen* menar att det bör bedömas i det enskilda fallet, och beroende på vilken typ av tjänst det är fråga om, vem som ska anses vara mottagare och förordar att informationsskyldigheten begränsas till sådana direkta mottagare som verksamhetsutövaren känner till eller rimligtvis bör känna till.

Bland andra *Energiföretagen Sverige* och *Hi3G Access AB (Tre)* anser att det bör regleras på vilket sätt informationen ska förmedlas och hur detaljerad informationen ska vara. Enligt Tre är det svårt att, utifrån definitionen av uttrycket betydande cyberhot, bedöma när informationsskyldigheten inträder och företaget betonar behovet av en restriktiv tillämpning. *Sveriges Kommuner och Regioner (SKR)* anser att det bör vara möjligt att avstå från att underrätta kunder när en sådan underrättelse skulle inverka menligt på incidenthanteringen och att det av samma skäl inte att det bör införas några tidsfrister för underrättelserna. *Region Skåne* framhåller att kravet på att informera kunder, som för regionens del omfattar bland annat patienter och resenärer, innebär stora utmaningar om det ska göras inom den av utredningen föreslagna tiden. *Svenskt Näringsliv* och *Tech Sverige* menar att informationsskyldigheten bör inträda först när vederhäftiga bedömningar kunnat göras. De framför också att värdet av information om en incident eller ett hot som kan få allvarliga konsekvenser är begränsat och att informationsskyldigheten kan leda till olämplig spridning av information som utgör en säkerhetsrisk och osäker information som riskerar att vara börspåverkande.

Skälen för regeringens förslag

Skyldighet att informera mottagare enligt direktivet

Av artikel 23.1 i NIS 2-direktivet framgår att entiteter, när så är lämpligt, utan onödigt dröjsmål ska underrätta mottagarna av deras tjänster om betydande incidenter som sannolikt inverkar negativt på tillhandahållandet av tjänsterna. I tillämpliga fall ska medlemsstaterna vidare enligt artikel 23.2 säkerställa att entiteter utan onödigt dröjsmål underrättar de mottagare av deras tjänster som kan påverkas av ett betydande cyberhot om eventuella åtgärder eller avhjälpande arrangemang som dessa mottagare kan vidta som svar på hotet. När så är lämpligt ska entiteterna också informera dessa mottagare om själva det betydande cyberhotet.

Skyldighet att informera vid betydande incidenter enligt lagen

Utredningen föreslår att verksamhetsutövare, i samband med en incidentanmälan, ska informera kunder som kan antas påverkas av den betydande incidenten. Regeringen anser, i likhet med bland andra *Digg*, att uttrycket kunder bör ersättas för att åstadkomma en reglering som är mer direktivnära och för att markera att även andra mottagare av tjänster, som inte kan betecknas som kunder, omfattas av regleringen. Vidare anser regeringen

att informationsskyldigheten även i övrigt bör utformas mer direktivnära än vad utredningen föreslår. Verksamhetsutövare bör, mot denna bakgrund, informera mottagarna av deras tjänster om betydande incidenter som sannolikt inverkar negativt på tillhandahållandet av tjänsterna. Vem som räknas som sådan mottagare får, som *Advokatfirman Kahn Pedersen* resonerar kring, bedömas i det enskilda fallet. Det är endast mottagare av de tjänster som den betydande incidenten sannolikt inverkar negativt på som bör omfattas av informationsskyldigheten.

Regeringen anser även att verksamhetsutövare, i enlighet med vad som gäller enligt direktivet och som bland andra *PTS* anför, endast bör informera om betydande incidenter om det är lämpligt. Det kan förekomma situationer då det, exempelvis av säkerhetsskäl, framstår som mindre lämpligt att informera om en betydande incident. Detta gäller till exempel om informationslämnande skulle innebära att integritetskänsliga eller på annat sätt känsliga uppgifter behöver delas. Lämplighetsbedömningen bör också kunna resultera i att endast vissa mottagare informeras om incidenten.

Vad gäller tidpunkten för när informationsskyldigheten bör inträda anges det i direktivet att information bör lämnas utan onödigt dröjsmål. Utredningen föreslår att verksamhetsutövare ska vara skyldiga att informera om den betydande incidenten samtidigt som en incidentanmälan görs (se avsnitt 6.6.2). *Svenskt Näringsliv* och *Tech Sverige* menar att informationsskyldigheten bör inträda först när vederhäftiga bedömningar kunnat göras. *Region Skåne* framhåller att kravet på att informera kunder innebär stora utmaningar om det ska göras inom den av utredningen föreslagna tiden.

Verksamhetsutövaren bör vid den tidpunkt då en incidentanmälan görs i och för sig ha hunnit vidta vissa inledande åtgärder och skaffa sig en tydlig bild av situationen. Samtidigt kan en skyldighet att informera mottagare av tjänster få andra konsekvenser än en rapport till en myndighet. Det kan också vara förenat med betydande svårigheter att identifiera vem informationen ska riktas till och på vilket sätt. Vidare kan det finnas anledning att göra särskilda överväganden kring vilken information som ska lämnas. Enligt regeringen är det därför inte lämpligt att ange en särskild tidpunkt för när information ska lämnas. Det bör däremot anges att information ska lämnas så snart det kan ske.

Verksamhetsutövaren bör göra en bedömning av när informationen kan lämnas utifrån bland annat vilken typ av incident och tjänst det är fråga om. I enlighet med förslaget i avsnitt 8.5 får tillsynsmyndigheten förelägga en verksamhetsutövare att fullgöra informationsskyldigheten inom en viss tid.

Bland andra *Energiföretagen Sverige* och *Tre* anser att det bör regleras på vilket sätt informationen ska förmedlas och hur detaljerad informationen ska vara. Hur informationsskyldigheten ska fullgöras bör dock regleras på lägre föreskriftsnivå än i lag. Regeringen eller den myndighet som regeringen bestämmer bör därför få rätt att meddela föreskrifter om informationsskyldigheten.

Skyldighet att informera vid betydande cyberhot enligt lagen

Uttrycket mottagare av tjänster bör användas även avseende den informationsskyldighet som avses i artikel 23.2. Till skillnad från vad som föreslås gälla för betydande incidenter bör dock mottagarna som kan påverkas av det betydande cyberhotet informeras och en lämplighetsbedömning bör endast ske kopplat till skyldigheten att informera om hotet. I enlighet med vad regeringen föreslår i fråga om betydande incidenter bör ingen närmare tidsangivelse anges i lagen utan informationen bör i stället lämnas så snart det kan ske, med ledning i bland annat vilken typ av hot det är fråga om och på vilket sätt mottagarna kan påverkas av hotet.

Enligt *Tre* är det svårt att, utifrån den föreslagna definitionen av uttrycket betydande cyberhot, bedöma när informationsskyldigheten inträder (jfr avsnitt 6.6.1). Regeringen bedömer, till skillnad från Tre, att det inte finns anledning att betona behovet av en restriktiv tillämpning av den föreslagna bestämmelsen, men bedömer däremot att det krävs ytterligare reglering som ger vägledning i fråga om skyldighetens innebörd. Hur informationsskyldigheten avseende betydande cyberhot närmare bör utformas och fullgöras bör dock framgå på lägre föreskriftsnivå än i lag. Regeringen eller den myndighet som regeringen bestämmer bör få rätt att meddela föreskrifter om informationsskyldigheten.

6.7 Ingen reglering om användning av vissa tjänster, produkter och processer

Regeringens bedömning: Det bör inte införas något krav på användning av vissa certifierade IKT-produkter, IKT-tjänster och IKT-processer i lagen eller någon särskild reglering i lagen som uppmuntrar till användning av kvalificerade betrodda tjänster.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Swedac* delar utredningens uppfattning om att det är rimligt att avvakta EU-kommissionens beslut innan certifieringskrav införs, men anser att kopplingarna mellan certifiering och cybersäkerhet hade behövt belysas ytterligare. *Swedsoft* och *Teknikföretagen* anser att det är viktigt att regeringen, om och när kommissionen inleder ett arbete med delegerade akter, har en dialog med svenskt näringsliv. *Telefonaktiebolaget LM Ericsson* välkomnar att direktivet uppmuntrar medlemsstaterna att främja användningen av standarder och tekniska specifikationer och rekommenderar bland annat att fördel ska dras av EU:s cybersäkerhetsakt och EU:s kommande cyberresiliensakt.

Försvarets materielverk (FMV) anser att behovet av nationella certifieringskrav inte har analyserats tillräckligt och påpekar bland annat att flera certifieringsordningar är antagna eller under framtagande. *ISACA Sweden Chapter* betonar vikten av att införa certifieringskrav i nationell lagstiftning för att motverka cyberhot på sätt som har skett i andra länder.

Övriga remissinstanser yttrar sig inte särskilt över bedömningen.

Skälen för regeringens bedömning: Av artikel 24.1 i NIS 2-direktivet framgår att medlemsstaterna får ålägga entiteter att, för att visa att vissa krav enligt artikel 21 angående riskhanteringsåtgärder är uppfyllda,

använda särskilda IKT-produkter, IKT-tjänster och IKT-processer som har utvecklats av entiteten eller upphandlats från tredje parter som är certifierade enligt europeiska ordningar för cybersäkerhetscertifiering som har antagits i enlighet med artikel 49 i EU:s cybersäkerhetsakt. Enligt samma artikel ska medlemsstaterna dessutom uppmuntra entiteter att använda kvalificerade betrodda tjänster.

Förkortningen IKT står för informations- och kommunikationsteknik. Enligt artikel 6.12–14 i NIS 2-direktivet ska begreppen IKT-produkt, IKT-tjänst och IKT-process förstås på samma sätt som i artikel 2.12–14 i EU:s cybersäkerhetsakt. Uttrycket IKT-produkt definieras således som en del, eller en grupp av delar i nätverks- och informationssystem, IKT-tjänst som en tjänst som helt eller huvudsakligen består i överföring, lagring, hämtning eller behandling av information via nätverks- och informationssystem samt IKT-process som verksamhet som utförs för att utforma, utveckla, tillhandahålla eller underhålla en IKT-produkt eller IKT-tjänst.

En kvalificerad betrodd tjänst ska enligt artikel 6.26 i NIS 2-direktivet förstås på samma sätt som i artikel 3.17 i EU:s förordning om elektronisk identifiering och definieras således som en betrodd tjänst som uppfyller tillämpliga krav i förordningen. Enligt artikel 3.16 i samma förordning avser en betrodd tjänst en elektronisk tjänst som vanligen tillhandahålls mot ersättning och som består av vissa närmare angivna tjänster, exempelvis utfärdande eller validering av certifikat för elektroniska underskrifter eller stämplar samt skapande eller validering av sådana elektroniska underskrifter eller stämplar.

I artikel 24.2 i NIS 2-direktivet ges EU-kommissionen befogenhet att anta delegerade akter på visst sätt för att komplettera direktivet genom att ange vilka kategorier av 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 enligt samma artikel antas om det har fastställts att cybersäkerhetsnivån är otillräcklig och ska omfatta en genomförandeperiod. Några delegerade akter har ännu inte antagits.

Utredningen anser att det inte bör införas några certifieringskrav i lagen och lämnar heller inget förslag i fråga om hur en sådan reglering skulle ha kunnat utformas. I artikel 24.1 i NIS 2-direktivet anges endast att medlemsstaterna får ålägga entiteterna att använda vissa certifierade IKT-produkter, IKT-tjänster och IKT-processer. Regeringen instämmer i bland annat *FMV:s* uppfattning om att certifieringskrav kan vara viktiga verktyg för att öka säkerheten i nätverks- och informationssystem. Regeringen anser dock, i likhet med utredningen och till exempel *Swedac*, att det i vart fall inte bör införas sådana innan kommissionen har antagit delegerade akter.

Digitala transaktioner behöver ske på ett säkert och effektivt sätt. Det handlar till exempel om att elektroniska underskrifter ska vara korrekta och spårbara. En del av lösningen för en säker digital miljö är betrodda tjänster enligt EU:s förordning om elektronisk identifiering. Leverantörer av betrodda tjänster kan vara antingen kvalificerade eller icke-kvalificerade. Alla företag som erbjuder betrodda tjänster måste följa förordningens säkerhetskrav, men för de kvalificerade leverantörerna är kraven i vissa fall högre. Kvalificerade betrodda tjänster kan användas som

en del av de säkerhetsåtgärder som vidtas i enlighet med förslaget i avsnitt 6.4. Det behöver inte införas någon särskild reglering i lagen som uppmuntrar till användningen av kvalificerade betrodda tjänster.

7 Tillsyn

7.1 Tillsynsmyndigheterna ska pekas ut i förordning

Regeringens förslag: Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet.

Tillsynsmyndigheten ska utöva tillsyn över att lagen och föreskrifter som har meddelats i anslutning till lagen följs. Tillsynsmyndigheten ska också utöva tillsyn över att sådana rättsakter följs som har antagits med stöd av NIS 2-direktivet.

Utredningens förslag överensstämmer i allt väsentligt med regeringens. Utredningen föreslår inte att tillsynsmyndigheten också ska utöva tillsyn över att sådana rättsakter följs som har antagits med stöd av NIS 2-direktivet.

Remissinstanserna: *Affärsverket svenska kraftnät* anser att det behöver tydliggöras om det ska finnas en eller flera tillsynsmyndigheter.

Ett stort antal remissinstanser, bland andra *Livsmedelsverket*, *Läkemedelsverket*, *Post- och telestyrelsen (PTS)*, *Stockholms universitet*, *Strålsäkerhetsmyndigheten*, *Transportstyrelsen* och ett flertal länsstyrelser, yttrar sig över utredningens förslag om vilka myndigheter som föreslås utöva tillsyn över olika sektorer och vissa begär förtydliganden av innebörden av utredningens förslag till förordning. *Malmö kommun*, *Naturvårdsverket*, *Tillväxtverket* och *Totalförsvarets forskningsinstitut* ifrågasätter det system för tillsyn som utredningen föreslår och anför att förutsättningarna för ett alternativt förslag med exempelvis en central tillsynsmyndighet borde ha analyserats noggrannare.

Flera remissinstanser, bland andra *Inspektionen för vård och omsorg (IVO)*, *Myndigheten för digital förvaltning*, *Myndigheten för samhällsskydd och beredskap (MSB)*, *Swedish Medtech*, *Tech Sverige*, *Teknikföretagen* och många kommuner och regioner, betonar vikten av samordning mellan tillsynsmyndigheterna.

Skälen för regeringens förslag: Enligt artiklarna 8 och 31.1 i NIS 2-direktivet ska varje medlemsstat utse eller inrätta en eller flera behöriga myndigheter med ansvar för att övervaka och vidta de åtgärder som krävs för att säkerställa att direktivet efterlevs. Av artikel 31.2 framgår att medlemsstaterna får tillåta sina behöriga myndigheter att prioritera tillsyn med grund i en riskbaserad metod.

Statens energimyndighet, Finansinspektionen, IVO, Livsmedelsverket, PTS och Transportstyrelsen är tillsynsmyndigheter för leverantörer av samhällsviktiga tjänster inom sju olika sektorer enligt NIS-lagen. NIS 2-direktivet innebär att antalet sektorer utökas till 18 och att det även tillkommer delsektorer och nya typer av verksamhetsutövare. Utredningen bedö-

mer att det bör utses en tillsynsmyndighet för varje sektor vid genomförandet av direktivet och föreslår att utpekande av tillsynsmyndigheterna ska ske i förordning. Utredningen föreslår att Statens energimyndighet, Transportstyrelsen, Finansinspektionen, IVO, Livsmedelsverket, Läkemedelsverket, PTS och vissa länsstyrelser ska pekas ut som tillsynsmyndigheter i förordning.

Regeringen delar utredningens uppfattning att det bör finnas flera tillsynsmyndigheter. De sektorer som föreslås omfattas av lagen sträcker sig över många sakområden och har en anknytning till olika myndigheters ansvarsområden enligt andra regelverk. Det finns skäl att hålla samman myndigheternas ansvar så att de får ett helhetsansvar över berörda områden. Till skillnad från vad bland andra *Naturvårdsverket* och *Tillväxtverket* anför anser regeringen därmed att det inte finns tillräckliga skäl att frångå det tillsynssystem som gäller i dag och peka ut en central tillsynsmyndighet.

Vilka myndigheter som bör utöva tillsyn över den nya lagen kan variera över tid och regeringen bedömer att det inte är ändamålsenligt att reglera i lag vilka myndigheter som ska vara tillsynsmyndigheter. Detta bör i stället regleras i förordning. Det bör därför föras in en bestämmelse i lagen om att den myndighet som regeringen bestämmer ska vara tillsynsmyndighet samt att tillsynsmyndigheten ska utöva tillsyn över att lagen och föreskrifter som har meddelats i anslutning till lagen följs. Tillsynsmyndigheten bör även utöva tillsyn över att sådana rättsakter som har antagits med stöd av artiklarna 21.5 och 23.11 i NIS 2-direktivet följs, som den genomförandeförordning som nämns i avsnitt 6.4. Formuleringen överensstämmer med motsvarande bestämmelser i säkerhetsskyddslagen och LEK och utesluter inte att flera tillsynsmyndigheter utses. Bestämmelsen bör därför inte ändras som *Affärsverket svenska kraftnät* resonerar kring. Det som flera remissinstanser, bland andra *PTS*, framför i fråga om vilka myndigheter som ska ha tillsynsansvar och avgränsningen av tillsynsområdena mellan tillsynsmyndigheterna är frågor som rör förordningens utformning och dessa frågor behandlas därför inte inom ramen för denna lagrådsremiss.

Flera remissinstanser, bland andra *MSB*, *Tech Sverige* och flera kommuner och regioner, betonar vikten av samordning mellan tillsynsmyndigheterna. En myndighet ska, enligt 6 § myndighetsförordningen, verka för att genom samarbete med bland annat andra myndigheter ta till vara de fördelar som kan vinnas för enskilda och för staten som helhet. Enligt 8 § förvaltningslagen ska en myndighet vidare inom sitt verksamhetsområde samverka med andra myndigheter och i rimlig utsträckning hjälpa den enskilde genom att själv inhämta upplysningar eller yttranden från andra myndigheter. Regeringen utgår ifrån att samverkan mellan tillsynsmyndigheterna kommer att fungera väl när det gäller bland annat sådana frågor som behöver hanteras gemensamt.

7.2 Tillsynsmyndigheternas befogenheter

7.2.1 Tillgång till uppgifter, handlingar och utrymmen

Regeringens förslag: Den som står under tillsyn ska vara skyldig att på begäran tillhandahålla tillsynsmyndigheten de uppgifter eller handlingar som myndigheten behöver för sin tillsyn.

Tillsynsmyndigheten ska ha rätt att i den omfattning det behövs för tillsynen få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamheten.

Tillsynsmyndigheten ska få begära handräckning av Kronofogdemyndigheten för att genomföra tillsynsåtgärderna. Vid handräckning ska bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande gälla.

Tillsynsmyndigheten ska få besluta att förelägga verksamhetsutövaren att tillhandahålla uppgifterna eller handlingarna och att ge tillträde. Ett föreläggande ska få förenas med vite. Ett vitesföreläggande ska även få riktas mot staten.

Utredningens förslag överensstämmer i allt väsentligt med regeringens. Utredningen föreslår att det ska införas en bestämmelse om att tillsynsmyndigheten ska få bestämma att ett föreläggande ska gälla omedelbart.

Remissinstanserna: Majoriteten av remissinstanserna yttrar sig inte särskilt över förslaget. *Myndigheten för digital förvaltning (Digg)* anser att det bör övervägas om tillsynsmyndigheternas befogenheter också ska innefatta åtkomst till it-system. *Region Skåne* anser att det är otydligt om tillsynen och rätten till tillträde även gäller i förhållande till en driftsleverantör i de fall där tjänster eller it-driften är utlokaliserad.

Skälen för regeringens förslag

Tillsynsmyndighetens uppdrag kräver vissa befogenheter

Enligt artiklarna 32.2 och 33.2 i NIS 2-direktivet ska medlemsstaterna säkerställa att behöriga myndigheter, när de utövar sina tillsynsuppgifter avseende väsentliga respektive viktiga entiteter, har befogenhet att vidta åtminstone vissa i artiklarna uppräknade åtgärder. De behöriga myndigheterna ska bland annat ha möjlighet att genomföra inspektioner på plats och distansbaserad tillsyn och få begära tillgång till uppgifter, handlingar och information som behövs för att de ska kunna utföra sina tillsynsuppgifter. Åtgärderna i artiklarna skiljer sig i några mindre avseenden åt. Enligt artiklarna 32.3 och 33.3 ska de behöriga myndigheterna, när de begär information, ange syftet med begäran och specificera den begärda informationen.

Behöriga myndigheters utförande av tillsynsuppgifter bör, enligt skäl 123 i NIS 2-direktivet, inte i onödan hämma den berörda entitetens affärsverksamhet. När behöriga myndigheter utför sina tillsynsuppgifter avseende väsentliga entiteter, bland annat genom inspektioner på plats och distansbaserad tillsyn, utredning av överträdelser av direktivet, säkerhets-

revisioner eller säkerhetsskanningar, bör de minimera konsekvenserna för den berörda entitetens affärsverksamhet.

En effektiv tillsyn kan inte bygga på antagandet att verksamhetsutövaren i samtliga fall kommer att medverka till tillsynen. Regeringen anser, i likhet med utredningen, att det finns skäl att ge tillsynsmyndigheterna vissa befogenheter för att de ska kunna utföra sitt uppdrag.

Uppgiftsskyldighet för verksamhetsutövaren

Utredningen föreslår att verksamhetsutövaren ska vara skyldig att tillhandahålla tillsynsmyndigheten den information som myndigheten behöver för sin tillsyn och anger att denna skyldighet inbegriper en skyldighet att tillhandahålla de handlingar som behövs för tillsynen. Formuleringen av den föreslagna bestämmelsen överensstämmer med 24 § NIS-lagen och 6 kap. 2 § säkerhetsskyddslagen. I bland annat 25 § lagen (2023:560) om granskning av utländska direktinvesteringar används uttrycket uppgifter och handlingar i stället för ordet information. Regeringen anser i likhet med utredningen att verksamhetsutövaren bör ha en uppgiftsskyldighet men att uttrycket uppgifter och handlingar bör användas även i den nya lagen eftersom det tydliggör innebörden av skyldigheten. Uttrycket handling bör ha samma innebörd som i andra kapitlet tryckfrihetsförordningen och därmed omfatta såväl skriftligt material som material som har lagrats digitalt och som kan läsas, avlyssnas eller på annat sätt uppfattas endast med hjälp av tekniska hjälpmedel.

Som *Digg* bedömer kan det finnas behov av att tillsynsmyndigheten undersöker hur säkerhetsåtgärder har fått genomslag i verksamhetsutövarens it-infrastruktur. Behovet möts delvis genom att lagen föreslås innehålla en bestämmelse som ger möjlighet för en tillsynsmyndighet att genomföra säkerhetsrevisioner och säkerhetsskanning (se avsnitt 7.2.2 och 7.2.3). Det finns dock inte utrymme för att inom ramen för denna lagrådsremiss föreslå en ordning som innebär att tillsynsmyndigheterna även ska få annan åtkomst till it-infrastruktur än den som utredningen föreslår i enlighet med Diggs förslag.

Tillsynsmyndigheten bör ha viss tillträdesrätt

Utredningen föreslår att tillsynsmyndigheten i den utsträckning som behövs för tillsynen ska ha rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som omfattas av lagen bedrivs. Motsvarande bestämmelser om tillträdesrätt finns i bland annat 25 § NIS-lagen och 6 kap. 3 § säkerhetsskyddslagen.

Enligt 2 kap. 6 § första stycket regeringsformen är var och en skyddad mot husrannsakan och liknande intrång. I förarbeten används uttrycket husrannsakan för att beteckna varje av myndighet företagen undersökning av hus, rum eller slutet förvaringsställe oavsett syftet med undersökningen (jfr prop. 1973:90 s. 246 och prop. 1975/76:209 s. 147). Skyddet mot husrannsakan kan enligt 2 kap. 20 och 21 §§ regeringsformen begränsas genom lag, men en sådan begränsning får endast göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle och får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den.

Av artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) följer att var och en har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens. Inskränkningar i skyddet kan godtas, under förutsättning att de har stöd i lag och är nödvändiga i ett demokratiskt samhälle för att tillgodose något av de i artikeln uppräknade intressena, däribland den nationella säkerheten.

Att tillsynsmyndigheterna kan få tillträde till områden, lokaler och andra utrymmen där verksamhet som omfattas av lagen bedrivs är av avgörande betydelse för att de ska kunna kontrollera att lagen följs. Med hänsyn till de skyddsvärden som är i fråga och vilken krets som berörs av förslaget är den föreslagna tillträdesrätten en godtagbar inskränkning av enskildas fri- och rättigheter. Tillsynsmyndigheten är skyldig att i varje enskilt fall göra en bedömning av om en mindre ingripande åtgärd än tillträde kan vidtas i första hand och om undersökningsåtgärden är proportionerlig (se 5 § tredje stycket förvaltningslagen). Nämnda krav i regeringsformen och Europakonventionen är mot denna bakgrund uppfyllda.

Region Skåne anser att det är otydligt om tillsynen och rätten till tillträde till områden, lokaler och andra utrymmen även gäller en driftsleverantör i de fall där tjänster och/eller it-driften är utlokaliserad. De föreslagna befogenheterna gäller endast i förhållande till en verksamhetsutövare som omfattas av lagen.

Förelägganden som ska kunna förenas med viten

Om en verksamhetsutövare inte samarbetar med tillsynsmyndigheten vid tillsynen bör myndigheten kunna meddela de förelägganden som behövs för att verksamhetsutövaren ska tillhandahålla de uppgifter och handlingar och ge det tillträde som behövs för tillsynen. Tillsynsmyndigheten bör dock som utgångspunkt i första hand försöka förmå verksamhetsutövaren att tillhandahålla uppgifterna och handlingarna och ge tillträdet på frivillig väg (se 5 § tredje stycket förvaltningslagen). Tillsynsmyndigheten måste göra en proportionalitetsbedömning i varje enskilt fall.

Föreläggandena bör kunna förenas med vite. Den allmänna regleringen om viten finns i lagen (1985:206) om viten (viteslagen). Regeringen delar utredningens uppfattning att bestämmelserna i viteslagen är lämpliga att använda för myndigheternas vitesförelägganden.

Ett vitesföreläggande kan som huvudregel inte riktas mot staten. I förarbetena till viteslagen överlämnas frågan om ett vitesföreläggande ska kunna riktas mot staten till rättstillämpningen, dock med kommentaren att sådana viten bör komma i fråga främst i situationer där staten i så utpräglad grad uppträder som privaträttsligt subjekt, till exempel på det marknadsrättsliga området, att det skulle vara onaturligt om vitesmöjligheten inte stod till buds. Vidare uttalas att det utanför det marknadsrättsliga området bör krävas att ett helt speciellt undantagsfall är för handen för att ett vitesföreläggande mot en statlig aktör ska vara godtagbart (se prop. 1984/85:96 s. 99 f.). I likhet med resonemanget som förs i förarbetena till säkerhetsskyddslagen anser regeringen att det finns skäl för att vite ska kunna riktas mot staten även enligt den nya cybersäkerhetslagen främst eftersom staten, i situationer när ett vitesföreläggande skulle kunna aktualiseras, agerar utanför sin rent offentligrättsliga kapacitet (se prop.

2020/21:194 s. 66 och 67). Regeringen bedömer även att en statlig myndighet i de flesta fall kommer att följa tillsynsmyndighetens uppmaning på frivillig väg och att tillsynsmyndigheten endast undantagsvis bör behöva förena ett föreläggande med vite. Regeringen anser därmed att det finns skäl att låta tillsynsmyndigheten förena ett föreläggande med vite även mot statliga aktörer.

Frågor om utdömande av viten ska enligt viteslagen prövas av förvaltningsrätt på ansökan av den myndighet som har utfärdat vitesföreläggandet. Det finns inte anledning att i den nya lagen införa bestämmelser som avviker från viteslagen.

Av artikel 6.1 i Europakonventionen följer bland annat att den som är anklagad för brott har rätt att inte belasta sig själv vid utredningen av anklagelsen, den så kallade passivitetsrätten. En skyldighet att lämna uppgifter och handlingar vid vite kan vara oförenlig med passivitetsrätten. Detta kan innebära att ett föreläggande om att tillhandahålla uppgifter eller handlingar inte bör förenas med vite om det rör en överträdelse som kan jämföras med en brottsanklagelse. Tillsynsmyndigheterna är skyldiga att vid beslut om vitesföreläggande beakta om ett sådant föreläggande kan vara oförenligt med passivitetsrätten. Skyldigheten att beakta passivitetsrätten gäller även för en domstol som överprövar ett beslut om ett vitesföreläggande.

Enligt 38 § NIS-lagen kan en tillsynsmyndighet besluta om att ett föreläggande enligt lagen ska gälla omedelbart. Utredningen föreslår att detta även ska gälla ett beslut om föreläggande enligt den nya lagen. Enligt 35 § tredje stycket förvaltningslagen får en myndighet verkställa ett beslut omedelbart om ett väsentligt allmänt eller enskilt intresse kräver det. Myndigheten ska dock, enligt samma bestämmelse, först noga överväga om det finns skäl att avvakta med att verkställa beslutet på grund av att beslutet medför mycket ingripande verkningar för någon enskild, att verkställigheten inte kan återgå om ett överklagande av beslutet leder till att det upphävs eller någon annan omständighet. Mot bakgrund av möjligheterna som förvaltningslagen ger i detta avseende i förhållande till enskilda bedömer regeringen att det inte behöver införas någon sådan bestämmelse som utredningen föreslår.

Handräckning av Kronofogdemyndigheten

Tillsynsmyndigheterna bör i första hand försöka förmå berörd verksamhetsutövare att tillhandahålla uppgifter och handlingar och ge tillträde på frivillig väg. Om en verksamhetsutövare, trots förelägganden, vägrar att ge tillsynsmyndigheten uppgifter och handlingar eller tillträde, kan dock tvångsåtgärder behöva användas.

Tillsynsmyndigheterna kommer inte att ha befogenheter att vidta tvångsåtgärder. Det finns inte anledning att anta att det kommer att finnas risk för hot eller handgripligheter i samband med utförandet av en tillsynsmyndighets uppdrag. De eventuella hinder som kan uppstå får i stället antas vara av fysiskt art. För att tillsynsmyndigheten i en sådan situation ska kunna få tillgång till uppgifter och handlingar och få tillträde bör myndigheten kunna begära handräckning av Kronofogdemyndigheten. Det bör därför, som utredningen föreslår, införas en bestämmelse om att tillsynsmyndigheten ska ha rätt att begära sådan handräckning.

Det bör framgå av lagen att bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande gäller vid handräckning.

7.2.2 Riktade och regelbundna säkerhetsrevisioner

Regeringens förslag: Tillsynsmyndigheten ska, om det finns särskilda skäl, få utföra eller låta ett oberoende organ utföra riktade säkerhetsrevisioner av den som står under tillsyn.

Tillsynsmyndigheten ska få utföra regelbundna säkerhetsrevisioner av väsentliga verksamhetsutövare eller anlita ett oberoende organ för att utföra regelbundna säkerhetsrevisioner av sådana verksamhetsutövare.

Tillsynsmyndigheten ska få förelägga verksamhetsutövare att medverka till säkerhetsrevisioner. Ett föreläggande ska få förenas med vite. Ett vitesföreläggande ska även få riktas mot staten.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om säkerhetsrevisioner.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår att tillsynsmyndigheten om det finns särskilda skäl ska få ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att redovisa resultatet för tillsynsmyndigheten. Utredningen föreslår ingen uttrycklig reglering i fråga om att tillsynsmyndigheten har befogenhet att utföra säkerhetsrevisioner. Utredningen föreslår att endast regeringen ska få meddela föreskrifter om säkerhetsrevisioner. Utredningen föreslår inte att det ska vara möjligt för tillsynsmyndigheten att besluta om förelägganden vid vite i syfte att förmå verksamhetsutövaren att medverka till en säkerhetsrevision.

Remissinstanserna: Ett antal remissinstanser, bland andra *Stokab AB* och *Strålsäkerhetsmyndigheten (SSM)*, tillstyrker förslaget om att tillsynsmyndigheter ska kunna besluta om riktad säkerhetsrevision. SSM anser att det bör förtydligas att säkerhetsrevision innebär att tillsynsmyndigheten ska beredas faktisk tillgång till nätverks- och informationssystemen.

Några remissinstanser, bland andra *Skatteverket* och *Tele2 Sverige AB (Tele2),* anser att innebörden av uttrycket säkerhetsrevision och kravet på särskilda skäl bör förtydligas. *Hi3G Access AB (Tre)* anser att det bör framgå av lagen att åtgärderna inte får orsaka större kostnad eller olägenhet än vad som är nödvändigt och att de inte i onödan får hämma verksamhetsutövarens affärsverksamhet. *Länsstyrelserna i Norrbottens* och *Stockholms län* anser att förslaget är otydligt i fråga om vem som ska finansiera säkerhetsrevisioner. Länsstyrelsen i Stockholms län ställer sig frågande till om regelbundna säkerhetsrevisioner kommer att genomföras om dessa ska finansieras inom ramen för tillsynsuppdraget. *Telenor Sverige AB (Telenor)* bedömer att det i stället för särskilda skäl bör krävas synnerliga skäl. *Trelleborgs kommun* efterfrågar ett förtydligande av vilka moment som ska ingå i en säkerhetsrevision. Kommunen anser också att det behöver framgå att det är tillsynsmyndigheten som tar kostnaden för

revisionen. *Tullverket* ser vissa potentiella praktiska hinder med förslaget. Tullverket nämner att det kan förekomma situationer där en it-miljö också stödjer brottsbekämpande och säkerhetskänslig verksamhet och att säkerhetsrevisionernas omfattning i sådana fall måste begränsas. Myndigheten anser att värdet av säkerhetsrevisionerna då riskerar att gå förlorat.

Bolagsverket, Tech Sverige och *Teknikföretagen* ställer sig tveksamma till att tillsynsmyndigheterna ska kunna ålägga verksamhetsutövaren att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision. *Försvarets materielverk (FMV)* anför att det kan leda till olika kvalitet i hur säkerhetsrevisioner genomförs om det är upp till en tillsynsmyndighet att avgöra vad som är ett oberoende organ. *Plikt- och prövningsverket (PPV)* anser att förslaget kan leda till att det finns en lojalitets- och intressekonflikt mellan den verksamhetsutövare som beställer och finansierar revisionen och det organ som utför revisionen. Vidare framhåller myndigheten vikten av att kompetens kopplat till tillsyn och säkerhetsrevision inte enbart finns inom de myndigheter som svarar för tillsynen, utan också hos de myndigheter som blir föremål för tillsyn. *Skatteverket* bedömer att det behöver tydliggöras vilka krav som ställs på ett oberoende organ, exempelvis om det krävs en viss certifiering för att genomföra revisioner.

Skälen för regeringens förslag

Krav på säkerhetsrevisioner enligt direktivet

Enligt artikel 32.2 b och c i NIS 2-direktivet ska medlemsstaterna säkerställa att behöriga myndigheter, när de utövar sina tillsynsuppgifter avseende väsentliga entiteter, har befogenhet att underställa dessa entiteter regelbundna och riktade säkerhetsrevisioner som utförs av ett oberoende organ eller en behörig myndighet. Vidare ska de ha befogenhet att utföra ad hoc-revisioner, inbegripet när detta är motiverat på grund av en betydande incident eller av en väsentlig entitets överträdelse av direktivet. När det gäller viktiga entiteter ska de behöriga myndigheterna endast ha befogenhet att underställa dessa entiteter riktade säkerhetsrevisioner (artikel 33.2 b).

Enligt artiklarna 32.2 och 33.2 ska de riktade säkerhetsrevisionerna baseras på riskbedömningar som utförs av den behöriga myndigheten eller den granskade entiteten eller på annan tillgänglig riskrelaterad information. Enligt samma artiklar ska resultaten av alla riktade säkerhetsrevisioner göras tillgängliga för den behöriga myndigheten. Kostnaderna för riktade säkerhetsrevisioner som utförs av ett oberoende organ ska vidare betalas av den granskade entiteten, utom i vederbörligen motiverade fall när den behöriga myndigheten beslutar något annat.

Behöriga myndigheters utförande av tillsynsuppgifter bör enligt direktivet inte i onödan hämma den berörda entitetens affärsverksamhet (skäl 123). När behöriga myndigheter utför sina tillsynsuppgifter avseende väsentliga entiteter, bland annat genom säkerhetsrevisioner, bör de enligt direktivet också minimera konsekvenserna för den berörda entitetens affärsverksamhet.

Säkerhetsrevisioner enligt den nya lagen

Direktivet reglerar alltså tre olika slags revisioner: regelbundna säkerhetsrevisioner, riktade säkerhetsrevisioner och ad hoc-revisioner. Regelbundna säkerhetsrevisioner och ad hoc-revisioner får endast utföras gentemot väsentliga entiteter, medan riktade säkerhetsrevisioner även får utföras gentemot viktiga entiteter.

Det utvecklas inte i direktivet vad som avses med regelbundna säkerhetsrevisioner, riktade säkerhetsrevisioner och ad hoc-revisioner. Utredningen bedömer att ad hoc-revisioner bör avse en typ av granskning som är oplanerad och händelsestyrd och som kan motiveras av till exempel en incident eller en förändrad hotbild. En regelbunden säkerhetsrevision är enligt utredningens bedömning i stället planerad och återkommande. Riktade säkerhetsrevisioner får enligt utredningen anses syfta på granskning av något specifikt område eller med anledning av någon viss omständighet som är hänförlig till verksamhetsutövaren, eller granskning utifrån ett specifikt säkerhetskrav i regleringen.

Utredningen anser att det inte behöver regleras särskilt att tillsynsmyndigheten på egen hand får utföra säkerhetsrevisioner eftersom det ingår i uppgiften att bedriva tillsyn. Enligt regeringens mening bör rätten att utföra säkerhetsrevisioner regleras på ett tydligare sätt i lagen dels eftersom säkerhetsrevisioner skiljer sig från övriga tillsynsåtgärder som myndigheten har befogenhet att vidta, dels eftersom regelbundna säkerhetsrevisioner endast får riktas mot väsentliga verksamhetsutövare. I fråga om riktade säkerhetsrevisioner anser regeringen, till skillnad mot utredningen, att dessa bör få utföras av såväl tillsynsmyndigheten som ett oberoende organ.

Uttrycket ad hoc-revisioner bör ta sikte på liknande åtgärder som vidtas vid regelbundna och riktade säkerhetsrevisioner. Tillsynsmyndighetens befogenhet att utföra regelbundna säkerhetsrevisioner inom ramen för den löpande tillsynen av väsentliga verksamhetsutövaren får också anses innefatta rätten att utföra ad hoc-revisoner. Det krävs därför ingen särskild reglering avseende tillsynsmyndighetens möjlighet att utföra sistnämnda slags revisioner. I linje med vad utredningen föreslår anser regeringen att det bör införas en bestämmelse i lagen om att tillsynsmyndigheterna ska få anlita ett oberoende organ för att utföra regelbundna säkerhetsrevisioner avseende en väsentlig verksamhetsutövare.

Tullverket anför att syftet med en säkerhetsrevision riskerar att gå förlorat därför att revisionen behöver begränsas för att inte omfatta den brottsbekämpande och säkerhetskänsliga delen av en verksamhet som en it-miljö också stödjer. En utgångspunkt för NIS 2-direktivet är att regelverket inte ska tillämpas på verksamheter som omfattas av nationell säkerhet eller räknas som brottsbekämpande (se vidare avsnitt 5.4.2). Det innebär dock inte att sådana tillsynsåtgärder, som säkerhetsrevisioner, inte kan utföras på angränsande verksamheter eller tjänster som omfattas av regelverket. Beroende på verksamhetens art och it-miljö kan det givetvis uppstå gränsdragningssvårigheter i praktiken. Ett tillvägagångssätt som möjliggör en för syftet avgränsad säkerhetsrevision är dock något som lämpligen verksamhetsutövaren och tillsynsmyndigheten eller det organ som utför revisionen får utarbeta i det enskilda fallet.

Vilka moment ska ingå i säkerhetsrevisioner?

Några remissinstanser, bland andra *Skatteverket* och *Tele2*, framför att innebörden av uttrycket säkerhetsrevision bör förtydligas. *Trelleborgs kommun* efterfrågar ett förtydligande av vilka moment som ska ingå i en säkerhetsrevision. I artikel 6.2 i NIS 2-direktivet definieras uttrycket säkerhet i nätverks- och informationssystem som nätverks- och informationssystems förmåga att med en viss tillförlitlighetsnivå motstå händelser som kan undergräva tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via dessa system.

En säkerhetsrevision inom ramen för den föreslagna lagen bör innebära att det sker en granskning av säkerheten i nätverks- och informationssystemen hos verksamhetsutövaren. Syftet med revisionen är att bedöma om de åtgärder som en verksamhetsutövare har vidtagit för att skydda systemen och säkerställa efterlevnad av lagens krav är ändamålsenliga och effektiva. De granskningsmoment som vidtas vid en säkerhetsrevision behöver vara sådana att resultatet av en revision kan visa på nivån av säkerheten i nätverks- och informationssystem.

En säkerhetsrevision bör kunna omfatta både tekniska och icke-tekniska moment, till exempel granskning av en verksamhets it-miljö, riskhanteringssystem och rutiner samt den dokumentation som finns gällande verksamhetsutövarens efterlevnad av tillämpliga regelverk och användning av standarder. Att tillsynsmyndigheten ska beredas faktisk tillgång till nätverks- och informationssystemen, som *SSM* nämner, bör vara en grundläggande förutsättning för en revision. Frågan om vilka moment som ska ingå i en säkerhetsrevision och hur de närmare ska utföras är dock något som inte bör regleras i lagen.

Utredningen föreslår att regeringen ska få rätt att meddela föreskrifter om säkerhetsrevisioner. Regeringen bedömer dock att det också kan krävas reglering som är bättre lämpad att utformas i föreskrifter som meddelas av en myndighet med särskild kompetens på området. Därmed bör regeringen eller den myndighet som regeringen bestämmer få meddela föreskrifter om säkerhetsrevisioner.

Regeringen delar *PPV:s* uppfattning att det är viktigt att även de myndigheter som är föremål för tillsyn har egen kompetens att utföra kontroller i verksamheten.

Det bör krävas särskilda skäl för en riktad säkerhetsrevision

Utredningen föreslår att det ska krävas särskilda skäl för att ålägga en verksamhetsutövare att genomgå en riktad säkerhetsrevision. *Tele2* anser att innebörden av kravet på särskilda skäl bör förtydligas och *Telenor* bedömer att det i stället bör krävas synnerliga skäl.

Enligt 8 kap. 2 § LEK får tillsynsmyndigheten om det finns särskilda skäl ålägga den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst att på egen bekostnad låta ett oberoende kvalificerat organ utföra en säkerhetsgranskning av hela eller delar av verksamheten och att redovisa resultatet av granskningen för myndigheten.

Vid införandet av regleringen i LEK framfördes det att en säkerhetsgranskning kan vara arbetskrävande och kostsam för den verksamhetsutövare som är skyldig att genomgå den (se prop. 2021/22:136 s. 318). En sådan granskning bör därför, enligt förarbetena, i första hand komma i fråga om tillsynsmyndigheten har tagit del av uppgifter eller bedrivit tillsyn där det framkommit att ytterligare granskning behövs. I förarbetena anges vidare att möjligheten att kräva utförande av säkerhetsgranskningar inte heller kan befria tillsynsmyndigheten från dess uppgift att upprätthålla en egen grundläggande kompetens och förmåga att granska säkerheten i verksamheter. Regeringen bedömde att skyldigheten endast skulle gälla om det finns särskilda skäl.

Regeringen anser att en riktad säkerhetsrevision endast bör få utföras om det finns särskilda skäl, även om kostnaden föreslås bäras av tillsynsmyndigheten (se nedan). Ett krav på särskilda skäl överensstämmer även med utformningen av artiklarna 32.2 och 33.2 av vilka det framgår att en riktad säkerhetsrevision ska baseras på riskbedömningar som utförs av den behöriga myndigheten eller den granskade entiteten eller på annan tillgänglig riskrelaterad information. Att i stället ställa upp ett krav på synnerliga skäl, som Telenor föreslår, skulle innebär en alltför hög tröskel som riskerar att motverka syftet med lagen. Kravet på särskilda skäl kan till exempel vara uppfyllt om det har framkommit någon omständighet vid tillsyn som föranleder bedömningen att ytterligare granskning krävs.

Proportionalitet

Regeringen delar *Tres* uppfattning att säkerhetsrevisionen inte bör vålla större kostnad eller olägenhet än vad som är nödvändigt och inte i onödan får hämma verksamhetsutövarens affärsverksamhet. Att tillsynsmyndighetens åtgärd ska vara proportionerlig kommer bland annat till uttryck i 5 § tredje stycket förvaltningslagen. Det behöver inte särskilt framgå av lagen att tillsynsmyndigheterna ska beakta proportionaliteten i de åtgärder som de vidtar inom ramen för sin tillsyn, däribland beslut om säkerhetsrevisioner.

Oberoende organ och kostnadsansvaret

Vad som avses med ett oberoende organ framgår inte av direktivet. Regeringen instämmer dock i utredningens uppfattning att det i lagens bemärkelse till exempel bör vara fråga om ett företag som genomför säkerhetsrevisioner och som är oberoende i förhållande till tillsynsmyndigheten och den verksamhetsutövare vars verksamhet ska granskas. Organet bör ha den sakkunskap som krävs för revisionen. Enligt regeringen är det, trots de synpunkter som framförs av bland andra *FMV* och *Skatteverket*, inte lämpligt att närmare reglera i lagen vilka krav som ska ställas på ett oberoende organ. Detta bör lämpligen utformas inom ramen för föreskrifter på en lägre normgivningsnivå och utifrån samordning mellan tillsynsmyndigheterna. Risken för sådana intresse- och lojalitetskonflikter som *PPV* nämner minimeras enligt regeringens mening på ett ändamålsenligt sätt genom kravet i lagen på att det ska vara ett oberoende organ som anlitas.

Länsstyrelserna i Norrbottens och *Stockholms län* och *Trelleborgs kommun* anser att förslaget är otydligt i fråga om vem som ska finansiera

säkerhetsrevisioner. Utredningen föreslår att tillsynsmyndigheten, om det finns särskilda skäl, ska få ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att redovisa resultatet för tillsynsmyndigheten. I likhet med vad bland andra *Tech Sverige* och *Teknikföretagen* framhåller, anser regeringen att kostnadsansvaret för en riktad säkerhetsrevision som utförs av ett oberoende organ inte bör belasta verksamhetsutövaren. En säkerhetsrevision kan vara arbetsam för den verksamhetsutövare som är skyldig att genomgå den. Att verksamhetsutövaren därutöver ska bära kostnaden blir enligt regeringens mening orimligt betungande. En riktad säkerhetsrevision bör därför utföras antingen av tillsynsmyndigheten eller av ett oberoende organ på tillsynsmyndighetens bekostnad.

Länsstyrelsen i Stockholms län ställer sig också frågande till om regelbundna säkerhetsrevisioner kommer att genomföras om de ska finansieras inom ramen för tillsynsuppdrag. Regeringen bedömer dock att finansieringen för tillsyn, som behandlas i avsnitt 14, ger utrymme för att genomföra såväl riktade som regelbundna säkerhetsrevisioner i lämplig utsträckning.

Möjlighet att besluta om vitesförelägganden

Utredningen föreslår att en överträdelse av lagen ska anses vara allvarlig om verksamhetsutövaren har hindrat säkerhetsrevisioner eller tillsynsåtgärder som tillsynsmyndigheten beslutat om (se vidare avsnitt 8.4.2). Utredningen resonerar dock inte i övrigt om konsekvenserna av att en verksamhetsutövare hindrar en säkerhetsrevision. Utredningen lämnar inte heller något förslag om vilka åtgärder tillsynsmyndigheten ska kunna vidta i en sådan situation. En effektiv tillsyn kan inte bygga på antagandet att verksamhetsutövaren i samtliga fall kommer att medverka till tillsynen. Regeringen anser, till skillnad från utredningen, att det även bör vara möjligt för tillsynsmyndigheten att besluta om förelägganden vid vite i syfte att förmå verksamhetsutövaren att medverka till en säkerhetsrevision. I enlighet med resonemanget i avsnitt 7.2.1 anser regeringen att skäl finns för att tillsynsmyndigheten även ska få rikta vitesföreläggande mot staten.

7.2.3 Säkerhetsskanningar

Regeringens förslag: Tillsynsmyndigheten ska få genomföra säkerhetsskanningar hos den som står under tillsyn.

En säkerhetsskanning ska ske i samarbete med verksamhetsutövaren.

Tillsynsmyndigheten ska få förelägga verksamhetsutövaren att medverka till en säkerhetsskanning. Ett föreläggande ska få förenas med vite. Ett vitesföreläggande ska även få riktas mot staten.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om säkerhetsskanningar.

Utredningens förslag överensstämmer delvis med regeringens förslag. Utredningen föreslår inte att tillsynsmyndigheten ska få besluta om förelägganden och föreslår inte heller något bemyndigande.

Remissinstanserna: *Strålsäkerhetsmyndigheten (SSM)* tillstyrker utredningens förslag om att tillsynsmyndigheterna ska kunna besluta om säkerhetsskanningar. SSM anser att det bör förtydligas att säkerhetsskanning innebär att tillsynsmyndigheten ska beredas faktisk tillgång till nätverks- och informationssystemen. *Försvarsmakten* och *Livsmedelsverket* tillstyrker förslaget om att en säkerhetsskanning alltid ska ske i samarbete med verksamhetsutövaren.

Lantmännen framhåller att många verksamheter redan utför regelbundna sårbarhetsskanningar som en del av deras interna säkerhetsprotokoll. Skanningar som utförs av tillsynsmyndigheter kan påverka verksamhetens kontinuitet och leda till oplanerade störningar, kostnader och förluster samt innebära integritets- och sekretessrisker. Livsmedelsverket anser att det behöver förtydligas vilka begränsningar som gäller för skanningarna, hur de ska utföras och vilka delar av en teknisk miljö de får avse. Myndigheten bedömer att det kan vara lämpligt att meddela tydliggörande föreskrifter, som även reglerar hur ett resultat av en säkerhetsskanning ska hanteras. *Länsstyrelsen i Norrbottens län* anser att det är otydligt vem som ska genomföra säkerhetsskanningarna. *Malmö kommun*, *Skatteverket* och *Svensk dagligvaruhandel* föreslår att innebörden av en säkerhetsskanning ska förtydligas. Svensk dagligvaruhandel anser vidare att tillsynsmyndighetens mandat behöver specificeras så att det likställs med CSIRT-enheternas mandat att utföra icke-inkräktande skanning av allmänt tillgängliga nätverks- och informationssystem. *Region Skåne* efterfrågar ett förtydligande gällande vad förslaget har för konsekvenser för en verksamhetsutövare som har en utlokaliserad it-driftmiljö samt för leverantören av den utlokaliserade it-miljön. Skatteverket anför att det finns stora risker med genomförande av skanning av it-miljöer varför en överprövningsmekanism bör införas om samråd inte leder till en samsyn mellan parterna. *Statens veterinärmedicinska anstalt (SVA)* ställer sig frågande till att en metod för att hitta sårbarheter i nätverk genom säkerhetsskanning kodifieras i lag. SVA:s uppfattning är att cybersäkerhetsverktyg förändras över tid och inte ska beskrivas i lagtext. *Trelleborgs kommun* anför att det behöver tydliggöras vem som tar kostnaden för att genomföra säkerhetsskanningar.

Hi3G Access AB (Tre) anser att det är otydligt varför två myndigheter, MSB i egenskap av nationell CSIRT-enhet och PTS, enligt utredningens förslag ska ha befogenhet att utföra skanningar för till synes samma syfte. *Energiföretagen Sverige* anser att det finns behov av att närmare utreda möjligheten att ge nationella CSIRT-enheten befogenhet att inhämta information via sårbarhetsskanningar för att kunna varna och skydda samhällskritisk verksamhet.

Skälen för regeringens förslag: Enligt artiklarna 32.2 d och 33.2 c i NIS 2-direktivet ska en behörig myndighet ha befogenhet att underställa entiteter säkerhetsskanningar på grundval av objektiva, icke-diskriminerande, rättvisa och transparenta riskbedömningskriterier, vid behov i samarbete med den berörda entiteten. Direktivet innehåller ingen definition av vad som avses med uttrycket säkerhetsskanning. Behöriga myndigheters utförande av tillsynsuppgifter bör enligt direktivet inte i onödan hämma den berörda entitetens affärsverksamhet (skäl 123). När behöriga myndigheter utför sina tillsynsuppgifter avseende väsentliga

entiteter, bland annat genom säkerhetsskanningar, bör de enligt direktivet minimera konsekvenserna för den berörda entitetens affärsverksamhet.

Med hänsyn till direktivets krav bör det införas en bestämmelse i den nya lagen om säkerhetsskanningar. Enligt regeringens mening kan metoderna för sådana skanningar variera över tid, men till skillnad från *SVA* och med hänvisning till bland annat direktivets innehåll, anser regeringen att det bör framgå av lagen att tillsynsmyndigheterna har befogenhet att underställa verksamhetsutövare sådana skanningar. Som svar på *Länsstyrelsen i Norrbottens läns* och *Trelleborgs kommuns* frågor om vem som ska utföra skanningen och stå för kostnaden kan det konstateras att bestämmelsen tar sikte på när tillsynsmyndigheten inom ramen för sitt tillsynsuppdrag låter utföra eller själv utför en säkerhetsskanning och att det är tillsynsmyndigheten som står för kostnaderna. Förslaget innebär alltså att tillsynsmyndigheten både kan genomföra säkerhetsskanningen på egen hand och via en extern aktör. För att förtydliga detta bör bestämmelsen omformuleras något i förhållande till utredningens förslag.

Bland andra *Malmö kommun* och *Skatteverket* efterfrågar förtydliganden i fråga om vad som avses med säkerhetsskanning. Regeringen delar utredningens uppfattning att sådana skanningar innebär en typ av skanning som kan göras avseende verksamhetsutövarens nätverks- och informationssystem i syfte att upptäcka sårbarheter eller osäkert konfigurerade delar av systemet. Säkerhetsskanningar är en slags sårbarhetsskanning. Sårbarhetsskanningar sker normalt med automatiserade verktyg som identifierar och klassificerar sårbarheter i datorer, nätverk och applikationer genom att matcha dem mot redan kända systembrister.

Icke-inkräktande skanningar innebär att it-systemens integritet och säkerhet säkerställs under genomförandet av skanningen (jfr andra stycket i artikel 11.3 NIS 2-direktivet). Som utredningen framhåller får inte en säkerhetsskanning ha någon negativ inverkan på hur verksamhetsutövarnas nätverks- och informationssystem fungerar. Det innebär att de eventuella risker som en sådan kan medföra, vilka *Lantmännen* lyfter, ska minimeras. Av proportionalitetskravet som framgår av bland annat 5 § tredje stycket förvaltningslagen följer att påverkan på it-system ska minimeras så att de i möjlig utsträckning kan fortsätta prestera obehindrat samtidigt som potentiella hot och sårbarheteter identifieras. Regeringen anser till skillnad från *Svensk dagligvaruhandel* att det inte bör framgå av lagen att endast icke-inkräktande säkerhetsskanningar får genomföras. Något motsvarande absolut krav finns inte i NIS 2-direktivet utan där anges enbart att konsekvenserna för den berörda entitetens affärsverksamhet bör minimeras.

Utredningen anför att en säkerhetsskanning behöver ske i samarbete med verksamhetsutövaren för att den inte ska ha någon negativ inverkan på hur verksamhetsutövarnas nätverks- och informationssystem fungerar. Regeringen delar utredningens uppfattning och anser också att det bör framgå av lagen att en säkerhetsskanning ska ske i samarbete med verksamhetsutövaren. Att säkerhetsskanningar ska ske i samarbete innebär endast att tillsynsmyndigheten ska involvera verksamhetsutövaren vid utförandet av säkerhetsskanningen, men det betyder inte att det måste finnas en samsyn i hur skanningen ska genomföras.

En effektiv tillsyn kan inte bygga på antagandet att verksamhetsutövaren i samtliga fall kommer att medverka till tillsynen. Regeringen anser, till skillnad från utredningen, att det även bör vara möjligt för tillsynsmyndigheten att besluta om förelägganden vid vite i syfte att förmå verksamhetsutövaren att medverka vid en säkerhetsskanning. Som framgår av resonemanget i avsnitt 7.2.1 anser regeringen att tillsynsmyndigheten även ska få rikta ett vitesföreläggande mot staten. Ett sådant beslut får, med stöd av förslaget i avsnitt 9, överklagas till allmän förvaltningsdomstol. Det behöver inte införas någon särskild överprövningsmekanism med anledning av *Skatteverkets* kritik.

Som *SSM* anför innebär en säkerhetsskanning att tillsynsmyndigheten bereds faktisk tillgång till berörda nätverks- och informationssystem. Liksom i frågan om säkerhetsrevisioner ger NIS 2-direktivet inte någon vägledning om vad säkerhetsskanningar ska omfatta för moment. Däremot framgår det av direktivet att säkerhetsskanningar ska ske på grundval av objektiva, icke-diskriminerande, rättvisa och transparenta riskbedömningskriterier. Säkerhetsskanningar kan bestå av olika moment, vilka också kan förändras över tid, varför det inte är lämpligt att reglera innehållet eller omfattningen av säkerhetsskanningar i lag. Det kan lämpligen ske på lägre normgivningsnivå, i enlighet med vad *Livsmedelsverket* förespråkar. Regeringen föreslår därför, till skillnad från utredningen, att regeringen eller den myndighet som regeringen bestämmer ska få rätt att meddela föreskrifter på området.

Region Skåne lyfter frågan om vad som gäller för säkerhetsskanningar vid utlokaliserade it-driftsmiljöer och för leverantörer. Den föreslagna bestämmelsen om säkerhetsskanningar gäller endast den verksamhetsutövare som är föremål för tillsyn, vilket innebär att skanning endast kan ske av de informations- och nätverkssystem som verksamhetsutövaren har rådighet över inom ramen för sin verksamhet.

I artikel 11 i NIS 2-direktivet anges även att CSIRT-enheten får utföra proaktiva, icke-inkräktande skanningar av verksamhetsutövarnas allmänt tillgängliga nätverks- och informationssystem i syfte att upptäcka sårbara eller osäkert konfigurerade system, vilket *Tre* lyfter fram. En CSIRT-enhet är inte nödvändigtvis ett tillsynsorgan och den skanning som en sådan enhet utför får därför anses ha ett annat syfte än de säkerhetsskanningar som utförs inom ramen för tillsynsmyndighetens uppdrag. CSIRT-enhetens uppgifter föreslås inte regleras i lagen. Vilka befogenheter en CSIRT-enhet bör ha i fråga om säkerhetsskanningar, som *Energiföretagen Sverige* resonerar om, är därmed inte en fråga för denna lagrådsremiss.

7.2.4 Tillsynsåtgärder i förhållande till viktiga verksamhetsutövare

Regeringens förslag: Tillsynsåtgärder när det gäller viktiga verksamhetsutövare ska endast få vidtas när tillsynsmyndigheten har anledning att anta att lagen, de föreskrifter som har meddelats i anslutning till lagen eller sådana rättsakter som har antagits med stöd av NIS 2-direktivet inte följs.

Utredningens förslag överensstämmer i allt väsentligt med regeringens. Utredningen föreslår att tillsynsåtgärderna endast ska få vidtas när tillsynsmyndigheten har befogad anledning att anta att lagen eller de föreskrifter som har meddelats i anslutning till lagen inte följs.

Remissinstanserna: *Mittuniversitetet* påtalar att uttrycket befogad anledning kan tolkas på olika sätt och anser att innebörden av uttrycket behöver förtydligas. Universitetet efterfrågar även ett förtydligande om tillsynsmyndigheten har en skyldighet att redovisa anledningen till sin tillsynsåtgärd och hur redovisningen i sådant fall ska ske. *Strålsäkerhetsmyndigheten (SSM)* anför att kravet på befogad anledning gör det svårt för tillsynsmyndigheten att arbeta preventivt eftersom tillsynsmyndigheternas kontrollmöjligheter kommer att vara begränsade till i huvudsak efterhandstillsyn.

Skälen för regeringens förslag: Enligt artikel 33.1 i NIS 2-direktivet ska medlemsstaterna, när de får bevis, indikationer på eller information om att en viktig entitet påstås underlåta att fullgöra kraven i direktivet, särskilt kraven på riskhanteringsåtgärder i artikel 21 och rapporteringsskyldigheter enligt artikel 23, säkerställa att de behöriga myndigheterna vid behov vidtar åtgärder i form av tillsynsåtgärder i efterhand. Medlemsstaterna ska säkerställa att dessa åtgärder är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall.

I skäl 122 anges att väsentliga entiteter bör omfattas av ett heltäckande tillsynssystem med förhandstillsyn och efterhandstillsyn, medan viktiga entiteter bör omfattas av enklare tillsyn, endast i efterhand. Den efterhandstillsyn som görs av viktiga enheter kan enligt samma skäl utlösas av uppgifter som tillsynsmyndigheten mottar från andra myndigheter, entiteter, medborgare, medier, eller andra källor eller härröra från annan verksamhet som tillsynsmyndigheten bedriver i samband med fullgörandet av sina uppgifter. För väsentliga verksamhetsutövare gäller alltså inte begränsningen i artikel 33.1 i direktivet om när åtgärder får vidtas. I avsnitt 5.3.5 behandlas frågan om vilka verksamhetsutövare som ska betraktas som väsentliga respektive viktiga.

När det gäller tillsyn över leverantörer av digitala tjänster enligt NIS-lagen gjordes bedömningen i förarbetena att tillsynsmyndigheten inte skulle ha någon allmän skyldighet att utöva tillsyn (se prop. 2017/18:205 s. 60). Medlemsstaterna skulle enligt artikel 17 i NIS-direktivet säkerställa att tillsynsmyndigheterna vid behov vidtar åtgärder genom tillsynsåtgärder i efterhand, när de har mottagit bevis på att en leverantör av digitala tjänster inte uppfyller kraven i direktivet. Bakgrunden till skillnaderna i tillsynsuppdragen enligt NIS-direktivet är, enligt skäl 60 i samma direktiv, att leverantörer av digitala tjänster bör omfattas av mindre ingripande, reaktiv efterhandstillsyn som är anpassad till deras tjänsters och verksamheters art.

Enligt 22 § NIS-lagen står leverantörer av digitala tjänster endast under så kallad reaktiv tillsyn. Tillsynsåtgärder när det gäller leverantörer av sådana tjänster får vidtas endast när tillsynsmyndigheten har befogad anledning att anta att en leverantör inte uppfyller vissa uppräknade krav. Det innebär att tillsynsmyndigheten måste ha uppgifter som ger objektivt stöd för en överträdelse (se prop. 2017/18:205 s. 97). Enligt förarbetena kan tillsynsmyndigheten få sådana uppgifter av leverantören av digitala

tjänster själv, en annan tillsynsmyndighet eller en tjänsteanvändare. Även incidentrapporteringen kan enligt förarbetena innehålla information som gör att tillsynsmyndigheten har befogad anledning att anta att lagen inte följs.

Utredningen föreslår att tillsynsåtgärderna endast ska få vidtas när tillsynsmyndigheten har befogad anledning att anta att lagen eller de föreskrifter som har meddelats i anslutning till lagen inte följs. *Mittuniversitetet* anser att innebörden av kravet på befogad anledning behöver förtydligas och *SSM* anför att kravet gör det svårt för tillsynsmyndigheten att arbeta preventivt. Regeringen anser, till skillnad från utredningen, att den nya lagen bör innehålla en bestämmelse om att tillsynsåtgärder i förhållande till viktiga verksamhetsutövare får vidtas endast när en tillsynsmyndighet har anledning att anta att lagen eller de föreskrifter som har meddelats i anslutning till lagen inte följs. Eftersom NIS 2-direktivet, till skillnad från NIS-direktivet, inte kräver att det ska finnas bevis för att en överträdelse har skett bör det inte uppställas ett krav på befogad anledning i den nya lagen. Tillsynsåtgärder när det gäller viktiga verksamhetsutövare bör också få vidtas när en tillsynsmyndighet har anledning att anta att sådana rättsakter som har antagits med stöd av NIS 2-direktivet inte följs (se avsnitt 7.1).

Kravet på att tillsynsmyndigheten ska ha anledning att anta att en överträdelse har skett innebär att tillsynsåtgärder får vidtas när det finns bevis eller indikationer på att verksamhetsutövaren inte uppfyller lagens krav, till exempel utifrån information från andra tillsynsmyndigheter eller via incidentrapporteringen. Om det kan anses finnas anledning i det enskilda fallet får avgöras av tillsynsmyndigheten.

Regeringen anser inte att kravet innebär att det blir svårt för tillsynsmyndigheterna att arbeta förebyggande. Preventiva insatser behöver inte alltid ske inom ramen för ett tillsynsärende, utan kan även genomföras med bred ansats i syfte att främja efterlevnaden av regelverket. Väsentliga verksamhetsutövare bör, som utredningen föreslår, omfattas av ett tillsynssystem där tillsyn kan ske fortlöpande och även i efterhand.

Mittuniversitetet anser att det behövs ett förtydligande i fråga om tillsynsmyndigheten har en skyldighet att redovisa anledningen till sin tillsynsåtgärd och hur redovisningen i sådant fall ska ske. Regeringen vill här framhålla att en sådan skyldighet redan följer av 32 § förvaltningslagen enligt vilken ett beslut som kan antas påverka någons situation på ett inte obetydligt sätt ska innehålla en klargörande motivering, om det inte är uppenbart obehövligt. En sådan motivering ska innehålla uppgifter om vilka föreskrifter som har tillämpats och vilka omständigheter som varit avgörande för myndighetens ställningstagande. En motivering får helt eller delvis utelämnas bland annat om det är nödvändigt med hänsyn till rikets säkerhet, skyddet för enskildas personliga eller ekonomiska förhållanden eller något annat jämförbart förhållande. Hur ett beslut om att inleda ett tillsynsärende ska utformas i det enskilda fallet blir en fråga för tillsynsmyndigheten och behöver varken regleras i förhållande till offentliga eller enskilda verksamhetsutövare.

7.3 Avgift för tillsyn med koppling till viss digital infrastruktur

Regeringens förslag: Tillsynsmyndigheten ska få ta ut en handläggningsavgift och en årlig avgift av en verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster i Sverige och som har anmält sin verksamhet enligt lagen.

Handläggningsavgiften ska motsvara myndighetens kostnader för handläggningen av ärendet. De årliga avgifterna ska sammantagna motsvara de kostnader som myndigheten, utöver kostnaderna för handläggning av ärendet, har för sin verksamhet enligt lagen när det gäller nämnda slags verksamhetsutövare. Avgifterna ska fördelas med skälig andel på var och en av verksamhetsutövarna.

Utredningens förslag överensstämmer inte med regeringens. Utredningen föreslår att tillsynen ska finansieras genom ökade anslag.

Remissinstanserna: Som redovisas i avsnitt 14 yttrar sig ett flertal remissinstanser över de ekonomiska konsekvenserna av förslagen. *Post- och telestyrelsen (PTS)* ser ett behov av 15 årsarbetskrafter motsvarande drygt 20 000 000 kronor med anledning av det av utredningen föreslagna tillsynsansvaret. En tilldelning begränsad till 2 000 000 kronor, som utredningen föreslår, skulle enligt PTS inte möjliggöra föreslagen tillsynsverksamhet och skulle innebära en kraftigt sänkt ambitionsnivå jämfört med det arbete som myndigheten bedriver i dag enligt LEK.

Skälen för regeringens förslag

Finansiering av tillsyn enligt NIS-lagen och LEK

I samband med genomförandet av NIS-direktivet gavs Statskontoret i uppdrag att utreda de ekonomiska konsekvenserna för de myndigheter som enligt direktivet skulle utföra tillsyn (Ju2017/08091). Statskontoret ansåg inte att tillsynen enligt NIS-direktivet skulle finansieras med avgifter. Det som ansågs tala emot avgiftsfinansiering var risken för konkurrenssnedvridande effekter, jämförelsevis höga administrationskostnader, svårigheter att utforma tillsynen över sektorerna på ett enhetligt sätt och svårigheten att påvisa en tydlig motprestation för avgiften. Statskontoret föreslog att tillsynen enligt NIS-direktivet skulle finansieras med anslag, vilket också blev fallet (jfr prop. 2017/18:205 s. 89).

Enligt 14 kap. 1 § LEK och 1 kap. 5 § förordningen (2022:511) om elektronisk kommunikation får PTS ta ut en handläggningsavgift av den som anmäler verksamhet enligt 2 kap. 1 § samma lag, vilket ska göras av den som tillhandahåller sådana allmänna elektroniska kommunikationsnät som vanligen tillhandahålls mot ersättning, eller allmänt tillgängliga elektroniska kommunikationstjänster. Handläggningsavgiften ska motsvara myndighetens kostnader för handläggningen av ärendet.

PTS ska vidare enligt 14 kap. 2 § LEK ta ut en årlig avgift av den som bedriver verksamhet som är anmäld enligt 2 kap. 1 §. De årliga avgifterna ska sammantagna motsvara de kostnader som myndigheten, utöver 14 kap. 1 §, har för sina verksamheter enligt lagen. Avgifterna ska fördelas med

skälig andel på var och en av dem som omfattas av anmälningsplikten enligt lagen.

Ordningen med avgiftsfinansiering, som gällde enligt telelagen (1993:597), behölls vid införandet av lagen (2003:389) om elektronisk kommunikation bland annat med hänvisning till innehållet i artikel 12 i Europaparlamentets och rådets direktiv 2002/20/EG av den 7 mars 2002 om auktorisation för elektroniska kommunikationsnät och kommunikationstjänster (auktorisationsdirektiv), där det enkelt uttryckt föreskrivs att företag som tillhandahåller aktuellt slags nät eller tjänst får åläggas att betala en administrativ avgift (se vidare prop. 2002/03:110 s. 289).

I förarbetena anges att spännvidden mellan de företag som är anmälda skulle bli mycket stor både vad gäller omsättning och den del de tar i anspråk av tillsynsverksamhet och annan verksamhet (se prop. 2002/03:110 s. 291). Det anges vidare att förhållandet att kostnaderna för myndighetsverksamheten är olika för till exempel skilda slag av radioanvändning eller verksamheter bör återspeglas i avgiftsuttaget. De minsta operatörerna bedömdes komma att orsaka tillsynskostnader eller andra kostnader i sådan begränsad omfattning att det ansågs rimligt att föreskriva att dessa inte ska erlägga avgift för verksamhet som är anmäld. Å andra sidan bedömdes det vara mycket resurskrävande att behandla en ansökan om radiotillstånd vid ett inbjudningsförfarande, varför denna engångsavgift kan uppgå till ett större belopp.

Det finns skäl för avgifter i förhållande till vissa verksamhetsutövare

Utredningen föreslår, som redovisas i avsnitt 7.1, att bland annat PTS ska pekas ut som tillsynsmyndighet i förordning. PTS föreslås av utredningen utöva tillsyn över bland annat sektorn digital infrastruktur. PTS föreslås därmed bland annat utöva tillsyn över den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst. Som redovisas närmare i avsnitt 14 anser utredningen att de föreslagna tillsynsmyndigheterna, förutom Finansinspektionen, bör få en skönsmässig ökning av anslag om 2 000 000 kronor men att regeringen också bör ge Statskontoret i uppdrag att göra en kartläggning av kostnaderna för tillsynsverksamheten.

Regeringen är av uppfattningen att det inte bör regleras i lag vilken eller vilka myndigheter som ska vara tillsynsmyndigheter. Det kan dock konstateras att samtliga tillsynsmyndigheter som utredningen föreslår ska pekas ut som tillsynsmyndigheter, förutom Finansinspektionen, i budgetpropositionen för 2025 fick ökade anslag med sammanlagt 28 000 000 kronor med anledning av deras utökade ansvar i samband med NIS 2-direktivet och kommande nationell lagstiftning (prop. 2024/25:1). Regeringen gav den 24 oktober 2024 Statskontoret i uppdrag att utreda de ekonomiska konsekvenserna för tillsynsmyndigheternas verksamhet till följd av NIS 2-direktivet och föreslå lämpliga finansieringsmodeller för tillsyn inom sektorn för elektronisk kommunikation med hänsyn tagen till sektorns särskilda förutsättningar (Fö2024/01753). Statskontoret redovisade uppdraget den 11 april 2025. I Statskontorets rapport Tillsynsmyndigheternas kostnader till följd av NIS2-direktivet (2025:8) föreslår Statskontoret att tillsynen för sektorn elektronisk kommunikation ska finansieras med anslag i likhet med övrig tillsyn enligt NIS 2-

direktivet. Statskontoret bedömer att en avgiftsfinansiering skulle skapa en inkonsekvent finansieringsmodell inom samma regelverk och även riskera att leda till diskussioner om avgiftsnivåer och motprestationer.

I avsnitt 11 föreslår regeringen att bestämmelserna i 8 kap. 1–4§§ LEK om skyldighet för den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst att vidta åtgärder för att hantera risker som hotar säkerheten i nät och tjänster, låta utföra säkerhetsgranskning samt rapportera och informera om vissa säkerhetsincidenter ska upphävas. Regeringen gör i avsnittet, i likhet med utredningen, bedömningen att den krets som träffas av 8 kap. 1–4 §§ LEK i stället kommer att träffas av den föreslagna lagen. Vidare gör regeringen bedömningen att de ingripanden och tillsynsbefogenheter som i aktuella delar följer av LEK motsvaras av innehållet i förslaget till ny lag.

Utredningens och Statskontorets förslag i fråga om finansiering innebär i förlängningen att PTS, vid utpekande som tillsynsmyndighet enligt den nya lagen, förlorar rätten att ta ut avgifter trots att avgiftsfinansiering sedan lång tid tillbaka bedömts vara befogad för tillsyn över aktuell sektor. Detta framstår inte som ändamålsenligt och skulle, som *PTS* anför, kunna innebära en sänkt ambitionsnivå jämfört med det arbete som myndigheten bedriver i dag enligt LEK. Det bör därför införas bestämmelser i den nya lagen som ger den tillsynsmyndighet som regeringen pekar ut i förordning rätt att ta ut avgifter av en enskild verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster i Sverige och som har anmält sin verksamhet enligt lagen. Handläggningsavgiften bör motsvara myndighetens kostnader för handläggningen av ärendet. De årliga avgifterna bör sammantagna motsvara de kostnader som myndigheten, utöver kostnaderna för handläggning av ärendet, har för sin verksamhet enligt lagen när det gäller nämnda slags verksamhetsutövare. Avgifternas storlek behöver inte anges i lagen utan kan regleras i verkställighetsföreskrifter. Avgifterna bör fördelas med skälig andel på var och en av verksamhetsutövarna. Det sistnämnda ger utrymme för att bland annat beakta att kostnaderna för myndighetens verksamhet är olika för skilda slag av verksamheter.

8 Ingripanden

8.1 Administrativa eller straffrättsliga sanktioner?

Regeringens bedömning: Överträdelser av bestämmelser i lagen bör inte vara straffsanktionerade. I stället bör en tillsynsmyndighet kunna besluta om administrativa sanktioner.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna yttrar sig inte över bedömningen. *Stiftelsen för internetinfrastruktur* (*Internetstiftelsen)* ställer sig bakom utredningens bedömning. *Netnod AB* håller med om att överträdelser inte bör vara straffsanktionerade, men ser en större proble-

matik i att det saknas en harmonisering i fråga om ansvarsutkrävande inom unionen.

En arbetsgrupp inom Cybernoden anser att det är både lämpligt och nödvändigt att införa straffrättsliga sanktioner för den som avsiktligt eller av grov oaktsamhet orsakar betydande skada genom att underlåta att hålla en hög nivå av cybersäkerhet.

Skälen för regeringens bedömning: Medlemsstaterna ska enligt artikel 31.1 i NIS 2-direktivet säkerställa att deras behöriga myndigheter på ett ändamålsenligt sätt övervakar och vidtar de åtgärder som krävs för att säkerställa att direktivet efterlevs. Enligt artiklarna 32.1 och 33.1 ska medlemsstaterna bland annat säkerställa att de efterlevnadskontrollåtgärder som åläggs entiteter angående de skyldigheter som anges i direktivet är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall.

I artiklarna 32.4 och 33.4 anges vilka särskilda typer av efterlevnadskontrollåtgärder som medlemsstaterna ska säkerställa att deras behöriga myndigheter har befogenhet att vidta. Medlemsstaterna ska enligt artikel 36 fastställa regler om sanktioner för överträdelse av nationella åtgärder som har antagits enligt direktivet och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas.

I skäl 4 och 5 anges bland annat att en översyn av NIS-direktivet har visat på stora skillnader i medlemsstaternas genomförande och att NIS 2-direktivets mål är att undanröja dessa skillnader, bland annat genom att föreskriva effektiva rättsmedel och efterlevnadskontrollåtgärder, vilket är centralt för att upprätthålla en effektiv kontroll av att dessa skyldigheter efterlevs. I skäl 131 anges att medlemsstaterna bör kunna fastställa bestämmelser om straffrättsliga påföljder för överträdelser av de nationella bestämmelser som införlivar direktivet. I skäl 132 anges vidare att medlemsstaterna, när direktivet inte harmoniserar administrativa sanktioner eller när så är nödvändigt i andra fall till exempel i händelse av en allvarlig överträdelse av direktivet, bör genomföra ett system med effektiva, proportionella och avskräckande sanktioner. Dessa påföljders art, och frågan om de är straffrättsliga eller administrativa, bör enligt samma skäl fastställas i nationell rätt.

Vid genomförandet av NIS-direktivet gjordes bedömningen att överträdelser av NIS-lagen inte skulle vara straffsanktionerade, utan att det vore både effektivare och i övrigt lämpligare med administrativa sanktioner än med straff (se prop. 2017/18:205 s. 64 f.). En fördel med administrativa sanktioner är att dessa kan vara en kännbar reaktion mot en juridisk person som inte kan bli föremål för samtliga straffrättsliga åtgärder. Regeringen anser, till skillnad från *en arbetsgrupp inom Cybernoden*, att administrativa sanktioner på ett bättre sätt kan göra att man uppnår syftet med sanktionsbestämmelserna, nämligen att säkerställa att verksamhetsutövarna uppfyller de skyldigheter som lagen innebär för dem. Regeringen anser därför, likt utredningen, att de sanktioner som införs till följd av NIS 2-direktivet bör vara administrativa.

NIS 2-direktivets mål är visserligen, som anges i skäl 5, att undanröja skillnader mellan medlemsstaterna i fråga om efterlevnadskontrollåtgärder. Det har samtidigt överlämnats till medlemsstaterna att, med beaktande av regleringen i direktivet, utforma vilka ingripandeåtgärder som ska kunna komma i fråga i nationell rätt. Som *Netnod AB* resonerar kring kan

detta innebära att det saknas en harmonisering av regelverken inom EU. Detta är en följd av direktivets utformning och en godtagbar effekt.

8.2 Vilka överträdelser ska kunna leda till ingripande?

Regeringens förslag: Tillsynsmyndigheten ska ingripa om en verksamhetsutövare har åsidosatt sina skyldigheter att utse företrädare, göra en anmälan, vidta säkerhetsåtgärder, låta ledningen genomgå utbildning, rapportera betydande incidenter eller informera vid betydande incidenter och betydande cyberhot enligt lagen eller enligt föreskrifter som har meddelats i anslutning till lagen. Tillsynsmyndigheten ska också ingripa om verksamhetsutövaren har åsidosatt sina skyldigheter enligt sådana rättsakter som har antagits med stöd av NIS 2-direktivet.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår inte att tillsynsmyndigheten ska kunna ingripa om verksamhetsutövaren har åsidosatt sina skyldigheter enligt rättsakter som har antagits med stöd av NIS 2-direktivet.

Remissinstanserna: *Netnod AB* tillstyrker utredningens förslag.

Hi3G Access AB (Tre) avstyrker förslaget att överträdelser av anmälningsskyldigheten och utbildningsskyldigheten ska kunna leda till sanktionsavgift eftersom dessa skyldigheter inte är sanktionsavgiftsgrundande enligt direktivet. *Naturvårdsverket* ifrågasätter om det är möjligt att föreskriva att en tillsynsmyndighet alltid ska ingripa vid överträdelser. Enligt *Sveriges advokatsamfund* är syftet med direktivet och de föreslagna bestämmelserna inte i första hand att reagera på inträffade fel eller brister, utan att det så långt som det är möjligt ska försöka undvikas att de ens uppkommer. Detta uppnås inte effektivt genom olika slags ingripanden i efterhand mot verksamhetsutövarna, när incidenten redan har inträffat och skadan redan är för handen. *Tech Sverige* efterfrågar ett förtydligande om vad som ska gälla i fråga om sanktionsmöjligheter vid underlåtenhet att lämna information till användare om betydande cyberhot.

Ett flertal remissinstanser, bland andra *Myndigheten för samhällsskydd och beredskap (MSB)* och *Teracom*, föreslår att tillsynsmyndigheterna ska ges möjlighet att ingripa mot verksamhetsutövares brister i det systematiska och riskbaserade informations- och cybersäkerhetsarbetet.

Skälen för regeringens förslag: Som *Tre* påpekar anges det i artikel 34.4 och 34.5 i NIS 2-direktivet endast att medlemsstaterna ska säkerställa att entiteter som överträder artiklarna 21 och 23, som handlar om riskhanteringsåtgärder och rapporteringsskyldighet, påförs administrativa sanktionsavgifter till ett visst belopp. De generella bestämmelserna om tillsyn och efterlevnadskontroll i artiklarna 31–33 reglerar inte närmare, men begränsar inte heller, vilka överträdelser som ska kunna leda till ingripanden. Av skäl 129 framgår att sanktionsavgifter bör kunna påföras för att säkerställa en effektiv efterlevnadskontroll av de skyldigheter som fastställs i direktivet. Direktivet innehåller fler skyldigheter än de som avses i artikel 34.4 och 34.5. Övriga skyldigheter, till exempel skyldigheten att anmäla verksamheten och att anordna utbildning, är centrala delar

av den nya lagen och utgör grundläggande förutsättningar för att uppnå lagens syfte. Mot denna bakgrund bör en tillsynsmyndighet kunna ingripa, även med sanktionsavgift, när en verksamhetsutövare åsidosatt de skyldigheter som beskrivs i avsnitt 6. I enlighet med vad som framgår av avsnitt 6.6.3 föreslås verksamhetsutövare få en viss informationsskyldighet vid betydande cyberhot. Även överträdelser av denna skyldighet, som *Tech Sverige* resonerar kring, bör kunna föranleda ett ingripande i enlighet med utredningens förslag. Detta bör förtydligas i lagen.

I avsnitt 6.3 gör regeringen bedömningen att skyldigheten att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete inte bör lyftas fram som en särskild skyldighet i den nya lagen. Därmed bör det inte heller införas en särskild ingripandemöjlighet i förhållande till den skyldigheten som bland andra *MSB* och *Teracom* föreslår. Tillsynsmyndigheten bör dock kunna ingripa om verksamhetsutövaren har åsidosatt sina skyldigheter enligt sådana rättsakter som har antagits med stöd av NIS 2-direktivet (se avsnitt 7.1).

Naturvårdsverket ifrågasätter om det är möjligt att föreskriva att en tillsynsmyndighet alltid ska ingripa om en verksamhetsutövare har åsidosatt sina skyldigheter, när direktivet i övrigt bland annat föreskriver att medlemsstaterna får tillåta behöriga myndigheter att prioritera tillsyn (se artikel 31.2). I NIS-lagen finns det två olika ingripandemöjligheter, i form av åtgärdsföreläggande och sanktionsavgift. Det är enligt NIS-lagen frivilligt att meddela åtgärdsföreläggande (28 §), men obligatoriskt att ta ut sanktionsavgift vid underlåtenhet att uppfylla vissa krav (29 §). Regeringen instämmer i utredningens uppfattning att systematiken i NIS-lagen med obligatoriskt ingripande bör överföras till den nya lagen. Eftersom flera olika slags ingripandemöjligheter föreslås införas anser regeringen inte att det finns något som talar emot ett obligatoriskt ingripande vid överträdelser (se vidare nästa avsnitt).

Som *Sveriges advokatsamfund* påpekar bör fokus i första hand vara att förhindra att incidenter alls uppstår. Enligt regeringen har flera av ingripandemöjligheterna just detta fokus, exempelvis möjligheten för tillsynsmyndigheterna att förelägga på det sätt som tillsynsmyndigheten finner lämpligt för att verksamhetsutövare ska fullgöra sina skyldigheter enligt lagen (se vidare nästa avsnitt). Ett sådant föreläggande kan exempelvis syfta till att stärka verksamhetsutövarens säkerhetsåtgärder, vilket bidrar till ett skydd mot incidenter.

I avsnitt 10 föreslår regeringen att vissa verksamhetsutövare ska vara skyldiga att föra register över domännamn på visst sätt och att tillgängliggöra uppgifter ur registret. I samma avsnitt föreslår regeringen att tillsynsmyndigheten ska få besluta de förelägganden som behövs för att dessa skyldigheter ska fullgöras.

8.3 Vilka möjligheter till ingripande ska finnas?

Regeringens förslag: Ingripande ska ske genom beslut om föreläggande, ansökan om förbud att inneha ledningsfunktion, beslut om sanktionsavgift eller genom anmärkning.

Tillsynsmyndigheten ska få avstå från ingripande om någon annan tillsynsmyndighet har vidtagit åtgärder mot verksamhetsutövaren med anledning av överträdelsen och dessa åtgärder bedöms tillräckliga.

Utredningens förslag överensstämmer i allt väsentligt med regeringens. Utredningen föreslår att tillsynsmyndigheten även ska få avstå från ingripande om någon annan tillsynsmyndighet har vidtagit åtgärder mot den fysiska personen med anledning av överträdelsen.

Remissinstanserna: *Affärsverket svenska kraftnät* anser att det bör förtydligas vilken tillsynsmyndighet som ska ingripa och vilken myndighet som ska avstå från ingripande när en verksamhetsutövares överträdelser berör flera sektorer. Även *Luleå kommun* anser att regleringen behöver göras tydligare så att tillsynsmyndigheterna inte gör olika bedömningar och utfärdar sanktioner parallellt. *Läkemedelsverket* ställer sig frågande till hur förslaget om att tillsynsmyndigheterna ska få avstå från ingripande ska fungera i praktiken och noterar att det finns ett behov för myndigheterna att kunna kommunicera över myndighetsgränserna om vidtagna åtgärder. *Naturvårdsverket* undrar varför inte en anmärkning klassas som ett ingripande. *Sveriges advokatsamfund* gör gällande att svårigheterna för verksamhetsutövare att förutse hur bestämmelserna kommer att träffa dem bör beaktas vid bedömningen av om ingripande ska ske. *SJ AB* konstaterar att förslaget medför väsentligt mer ingripande sanktioner än vad som gäller enligt NIS-lagen. *Telenor Sverige AB (Telenor)* anser att ordningen med en obligatorisk anmärkning endast bör gälla om det i tillsynen identifieras brister och att ett tillsynsärende, vid mindre brister och ursäktliga tillkortakommanden som rättas omedelbart, bör kunna avslutas utan något ingripande. *Transportstyrelsen* anser att ordet eller i uppräkningen av möjliga sanktioner antyder att tillsynsmyndigheterna inte kan ta ut sanktionsavgift vid sidan av andra ingripandeåtgärder.

Skälen för regeringens förslag

Direktivets krav på möjligheter till efterlevnadskontroll

Enligt artikel 36 i NIS 2-direktivet ska medlemsstaterna bland annat fastställa regler om sanktioner för överträdelse av nationella åtgärder som antagits enligt direktivet och sanktionerna ska vara effektiva, proportionella och avskräckande. Av artiklarna 32 och 33 framgår vilka efterlevnadskontrollåtgärder de behöriga myndigheterna åtminstone ska ha befogenhet att vidta mot väsentliga respektive viktiga entiteter.

Medlemsstaterna ska enligt artiklarna 32.4 och 33.4 säkerställa att de behöriga myndigheterna, när de utövar sina befogenheter med avseende på efterlevnadskontroll gentemot entiteter, åtminstone har befogenhet att utfärda varningar (a), anta bindande instruktioner eller ett föreläggande (b) och ålägga de berörda entiteterna att upphöra med beteenden och att avstå från att upprepa sådana beteenden (c).

Medlemsstaterna ska vidare säkerställa att de behöriga myndigheterna har befogenhet att ålägga de berörda entiteterna att säkerställa att deras riskhanteringsåtgärder för cybersäkerhet överensstämmer med artikel 21 eller att fullgöra de rapporteringsskyldigheter som fastställs i artikel 23, på ett specificerat sätt och inom en angiven tidsperiod (d). De ska också kunna ålägga de berörda entiteterna att informera de fysiska eller juridiska

personer till vilka de tillhandahåller tjänster eller utför verksamheter som potentiellt kan beröras av ett betydande cyberhot om hotets karaktär och om eventuella skyddsåtgärder eller avhjälpande åtgärder som dessa fysiska eller juridiska personer kan vidta som svar på hotet (e) och ålägga de berörda entiteterna att inom en rimlig tidsfrist genomföra de rekommendationer som lämnats till följd av en säkerhetsrevision (f).

De behöriga myndigheterna ska också kunna ålägga de berörda entiteterna att offentliggöra aspekter av överträdelser av direktivet på ett specificerat sätt (artiklarna 32.4 h och 33.4 g) och påföra eller begära att relevanta organ eller domstolar i enlighet med nationell rätt påför administrativa sanktionsavgifter enligt artikel 34 utöver någon av de övriga åtgärder som avses i artikeln (artiklarna 32.4 i och 33.4 h). För väsentliga entiteter ska de behöriga myndigheterna därutöver ha befogenhet att utse en övervakningsansvarig enligt artikel 32.4 g (se vidare avsnitt 8.9).

Ingripandeåtgärder enligt den nya lagen

Bestämmelserna avseende efterlevnadskontrollåtgärder i NIS 2-direktivet bör, som utredningen föreslår, genomföras genom att tillsynsmyndigheterna ges rätt att ingripa mot verksamhetsutövare genom att besluta om föreläggande, ansöka om förbud att inneha ledningsfunktion eller besluta om sanktionsavgift. Om det är tillräckligt bör tillsynsmyndigheten i stället få meddela anmärkning. Även en anmärkning bör alltså, i likhet med vad *Naturvårdsverket* resonerar kring, utgöra en form av ingripande enligt lagen.

Som *SJ AB* konstaterar innebär förslaget att ingripandeåtgärderna, jämfört med NIS-lagen, kommer att vara både fler och mer ingripande. Samtidigt föreslås det, i motsats till NIS-lagen, inte vara obligatoriskt att ta ut en sanktionsavgift vid en överträdelse (se vidare avsnitt 8.7). En tillsynsmyndighet kan i stället välja att ingripa på annat sätt.

Regeringen instämmer i utredningens uppfattning att kraven på effektivitet och proportionalitet i direktivet i förhållande till enskilda verksamhetsutövare är uppfyllda redan genom bland annat 5 § tredje stycket förvaltningslagen. Kravet på att ingripandena ska vara avskräckande uppfylls genom tillsynsmyndigheternas handlingsutrymme i fråga om val, inbegripet utformning, av ingripande. Liksom utredningen anser regeringen att NIS 2-direktivets krav på motivering av beslut och kommunicering i artiklarna 32.8 och 33.5 redan följer av förvaltningslagen. Det behöver inte införas några särskilda bestämmelser i nationell rätt för att tillgodose direktivets krav i dessa avseenden, varken i förhållande till offentliga eller enskilda verksamhetsutövare.

Sveriges advokatsamfund gör gällande att svårigheterna för verksamhetsutövare att förutse hur bestämmelserna kommer att träffa dem bör beaktas vid bedömningen av om ingripande ska ske. Regeringen bedömer att det föreslagna regelverket är tydligt och att det inte behöver tas sådan särskild hänsyn vid bedömningen av om ingripande ska ske. Däremot föreslår regeringen i avsnitt 8.4.1 att det vid valet av ingripande ska tas hänsyn till vad verksamhetsutövaren har gjort för att bland annat förhindra skada och dessutom till om överträdelsen har varit uppsåtlig eller berott på oaktsamhet.

I enlighet med vad som framgår av avsnitt 8.2 bör tillsynsmyndigheten endast ingripa om en verksamhetsutövare har åsidosatt sina skyldigheter. Tillsynsärenden kan, som *Telenor* anför, avslutas utan något ingripande om det visar sig att någon överträdelse inte har skett. Dessutom kan en tillsynsmyndighet välja att enbart ingripa genom att meddela ett föreläggande och, om föreläggandet följs, inte ingripa på något annat sätt. Som *Transportstyrelsen* resonerar kring innebär förslaget också att sanktionsavgift får beslutas även om tillsynsmyndigheten dessförinnan har ingripit genom att meddela föreläggande. Detsamma gäller i förhållande till övriga ingripandeformer förutom anmärkning (se avsnitt 8.8). Regeringen anser inte att detta behöver tydliggöras i lagen.

Eftersom en verksamhetsutövare kan bedriva flera verksamheter som faller under olika tillsynsmyndigheters ansvarsområden finns det en risk för att en överträdelse kan angripas av flera myndigheter parallellt. På motsvarande sätt kan en verksamhetsutövare omfattas av flera länders jurisdiktion. Om någon annan tillsynsmyndighet – svensk eller utländsk – ingriper mot samma överträdelse riskerar agerandet att bryta mot det så kallade dubbelbestraffningsförbudet (se vidare avsnitt 8.7.3). Det bör därför införas en bestämmelse i lagen om att tillsynsmyndigheten får avstå från att ingripa om någon annan myndighet har vidtagit åtgärder mot verksamhetsutövaren med anledning av överträdelsen och tillsynsmyndigheten bedömer att dessa åtgärder är tillräckliga. Bestämmelsen innebär att tillsynsmyndigheten exempelvis kan avstå från ett ingripande om ett sådant skulle riskera att bryta mot dubbelbestraffningsförbudet.

Även om ett förbud att inneha ledningsfunktion, som behandlas i avsnitt 8.6, träffar en fysisk person är det fråga om en åtgärd som vidtas i förhållande till verksamhetsutövaren. Enligt regeringens mening finns det inte anledning att reglera att tillsynsmyndigheten även ska få avstå från ingripande om någon annan tillsynsmyndighet har vidtagit åtgärder mot den fysiska personen med anledning av överträdelsen som utredningen föreslår.

Som *Affärsverket svenska kraftnät, Luleå kommun* och *Läkemedelsverket* resonerar om förutsätter förslaget i denna del samverkan mellan berörda myndigheter. Regeringen konstaterar att det finns många regelverk där olika myndigheter utövar tillsyn utifrån olika perspektiv och även utifrån regelverk med olika syften (se till exempel prop. 2022/23:116 s. 149 f.). Regeringen föreslår i avsnitt 7.1 att det ska regleras i förordning vilka myndigheter som ska vara tillsynsmyndigheter. Det finns enligt regeringens mening ingen anledning att inom ramen för denna lagrådsremiss förtydliga vilken tillsynsmyndighet som ska ingripa och vilken som ska avstå från ingripande i olika sammanhang. Regeringen vill i stället betona myndigheters generella ansvar att samverka med varandra enligt förvaltningslagen och myndighetsförordningen. Regeringen utgår ifrån att samverkan mellan berörda myndigheter kommer att fungera väl när det gäller sådana frågor som de parallella regelverken kan ge upphov till och som behöver hanteras gemensamt.

8.4 Valet av ingripande

8.4.1 Vilka omständigheter ska beaktas vid valet av ingripande?

Regeringens förslag: Vid valet av ingripande ska hänsyn tas till hur allvarlig överträdelsen är, hur länge den har pågått och den skada eller risk för skada som uppstått till följd av överträdelsen.

Vid bedömningen ska särskilt beaktas

1. om verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse,
2. vad verksamhetsutövaren har gjort för att förhindra eller minska skadan,
3. om överträdelsen har varit uppsåtlig eller berott på oaktsamhet, och
4. den ekonomiska fördel som överträdelsen har inneburit för verksamhetsutövaren.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att det särskilt ska anges att omständigheterna även ska beaktas vid utformningen av ingripandeåtgärder. Utredningen föreslår vidare att verksamhetsutövarens samarbete med tillsynsmyndigheten ska anges som en sådan omständighet som ska beaktas särskilt. Utredningen föreslår också att det ska införas en paragraf i lagen om att det ska beaktas som försvårande att verksamhetsutövaren tidigare har begått en överträdelse och i förmildrande riktning om verksamhetsutövaren har följt godkända uppförandekoder eller certifieringsmekanismer.

Remissinstanserna: *Livsmedelsverket* motsätter sig att det särskilt ska beaktas om en överträdelse har begåtts med uppsåt eller av oaktsamhet, då uppsåt är ett komplext juridiskt begrepp som riskerar att skapa oklarheter och försvåra tillsynsmyndigheternas bedömningar. Myndigheten önskar också ett förtydligande av vilka uppförandekoder och certifieringsmekanismer som avses i utredningens förslag och hur dessa ska bedömas som godkända. *Myndigheten för digital förvaltning (Digg)* befarar att bedömningen av risk för skada kan bli svår att göra eftersom det inte rör sig om en faktisk skada. Digg rekommenderar bland annat att förhållandet mellan bedömningen av denna risk och bedömningen av de åtgärder verksamhetsutövaren har vidtagit för att förhindra eller minska skadan förtydligas. *Naturvårdsverket* anser att de omständigheter som ska beaktas är otydliga och bedömer att förvaltningsmyndigheter ofta saknar vana att bedöma uppsåt och oaktsamhet. *Transportstyrelsen* bedömer att det enda som behöver framgå av lagen är under vilka förutsättningar tillsynsmyndigheten ska ta ut sanktionsavgift och vilken storlek sanktionsavgiften ska bestämmas till. Enligt myndigheten kräver övriga ingripandeformer inte att samma omständigheter beaktas, eftersom exempelvis förbud att inneha ledningsfunktion endast kan tillgripas om överträdelsen bedöms som allvarlig. *Trelleborgs kommun* anför att det är av vikt att verksamhetsutövaren får skälig tid på sig att åtgärda identifierade brister innan ett beslut om sanktionsavgift fattas. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: I enlighet med artiklarna 32.7, 33.5 och 34.3 i NIS 2-direktivet ska de behöriga myndigheterna, när de

tillämpar efterlevnadskontrollåtgärder eller fattar beslut om sanktionsavgifter, bland annat ta hänsyn till omständigheterna i varje enskilt fall och som ett minimum ta vederbörlig hänsyn till vissa särskilt angivna omständigheter. Bestämmelserna saknar motsvarighet i NIS-direktivet och NIS-lagen. Vederbörlig hänsyn ska som ett minimum tas till följande:

- överträdelsens allvar och betydelsen av de bestämmelser som har överträtts, med beaktande av att bland annat följande alltid ska anses vara en allvarlig överträdelse:
  - upprepade överträdelser
  - underlåtenhet att underrätta om eller avhjälpa betydande incidenter
  - underlåtenhet att avhjälpa brister enligt bindande instruktioner från behöriga myndigheter
  - hindrande av revisioner eller övervakningsverksamhet som den behöriga myndigheten beordrat efter det att en överträdelse konstaterats
  - tillhandahållande av falsk eller grovt felaktig information i fråga om riskhanteringsåtgärder för cybersäkerhet eller rapporteringsskyldigheter enligt artiklarna 21 och 23 (a)
- överträdelsens varaktighet (b)
- eventuella tidigare relevanta överträdelser från den berörda entitetens sida (c)
- den materiella eller immateriella skada som uppstått, inbegripet finansiella eller ekonomiska förluster, effekter på andra tjänster och det antal användare som berörs (d)
- uppsåt eller oaktsamhet från den som har gjort sig skyldig till överträdelsen (e)
- de åtgärder som entiteten har vidtagit för att förhindra eller begränsa den materiella eller immateriella skadan (f)
- efterlevnad av godkända uppförandekoder eller godkända certifieringsmekanismer (g)
- i vilken utsträckning de fysiska eller juridiska personer som hålls ansvariga samarbetar med de behöriga myndigheterna (h).

Regeringen instämmer i utredningens uppfattning att skyldigheten att ta hänsyn till omständigheterna i varje enskilt fall redan följer av bland annat 23 § förvaltningslagen och att det inte behöver tas in någon särskild reglering om det i den nya lagen. Vidare anser regeringen, likt utredningen, att övriga angivna omständigheter bör anges i lagen med de anpassningar som behövs, i syfte att främja en enhetlig tillämpning hos tillsynsmyndigheterna och åstadkomma en ökad förutsebarhet för verksamhetsutövarna.

Av systematiken i NIS 2-direktivet följer att vissa omständigheter ska föranleda att en överträdelse anses vara allvarlig. Regeringen instämmer i utredningens uppfattning att vissa omständigheter bör beaktas vid valet av ingripande, inbegripet utformningen av ingripandet, samt att dessa omständigheter i det enskilda fallet kan utgöra förmildrande, neutrala eller försvårande omständigheter. Förekomsten av vissa omständigheter bör alltid medföra att överträdelsen är att betrakta som allvarlig (se vidare avsnitt 8.4.2).

Enligt regeringen bör det vid valet av ingripande alltid beaktas hur allvarlig överträdelsen är, hur länge den har pågått och den skada eller risk för skada som uppkommit till följd av den. I bedömningen av överträdelsens allvar bör det ingå att bedöma betydelsen av de bestämmelser som har överträtts och överträdelsens omfattning. Även de särskilda bedömningsgrunder för allvarliga överträdelser som redogörs för i avsnitt 8.4.2 bör vägas in i bedömningen.

Vad gäller den skada som har uppstått, bedömer regeringen i likhet med utredningen, att bedömningsgrunden inte bör vara begränsad till faktisk skada, utan även gälla i förhållande till den risk för skada som överträdelsen kan ha medfört, samt att bedömning bör ta sin utgångspunkt i – men inte vara begränsad till – de aspekter som tas upp i artikel 32.7 d. Regeringen kan inte som *Digg* se att bedömningen av risk för skada skulle bli svår att genomföra. Det finns ett antal regelverk där en motsvarande bedömning ingår som ett led i en myndighets prövning (se till exempel 33 § lagen om granskning av utländska direktinvesteringar och 31 § NIS-lagen).

Av lagen bör det vidare, som utredningen föreslår, framgå att vissa omständigheter ska beaktas särskilt vid bedömningen av överträdelsens allvar, hur länge den har pågått och den skada eller risk för skada som uppstått till följd av densamma. Det bör särskilt beaktas om verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse, vad verksamhetsutövaren har gjort för att förhindra eller minska skadan, om överträdelsen har varit uppsåtlig eller berott på oaktsamhet och den ekonomiska fördel som överträdelsen har inneburit för verksamhetsutövaren. Vad avser omständigheten att verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse så bör det vid bedömningen bland annat vägas in tiden mellan den tidigare och den aktuella överträdelsen och om överträdelserna är likartade.

I bedömningen av vad verksamhetsutövaren har gjort för att förhindra eller minska skadan bör det beaktas vilka verksamma åtgärder som verksamhetsutövaren har vidtagit. Bedömningen av denna omständighet kommer, som Digg resonerar kring, i vissa fall ha ett nära samband med bedömningen av vilken risk för skada som överträdelsen har inneburit, men bedömningen avser vilken faktisk skada som har undvikits eller minimerats genom att verksamhetsutövaren har vidtagit åtgärder. Regeringen bedömer, till skillnad från utredningen, att verksamhetsutövarens samarbete med tillsynsmyndigheten bör räknas som en sådan åtgärd och därmed inte regleras särskilt (jfr till exempel prop. 2022:23:116 s. 205). Inom ramen för samma bedömning bör även beaktas huruvida verksamhetsutövaren har efterlevt godkända uppförandekoder eller certifieringsmekanismer.

Med godkända uppförandekoder och certifieringsmekanismer avses i detta sammanhang, som *Livsmedelsverket* efterfrågar ett förtydligande av, sådana uppförandekoder och certifieringsmekanismer som har tagits fram baserat på arbete inom EU. Som exempel kan nämnas de certifieringsordningar som har antagits eller är under framtagande inom ramen för EU:s cybersäkerhetsakt. Om en överträdelse har skett trots en lojal tillämpning av en uppförandekod eller certifieringsmekanism bör det beaktas i förmildrande riktning.

Den omständigheten att verksamhetsutövaren har agerat uppsåtligt eller av oaktsamhet bör också påverka valet av ingripande. Om någon har överträtt reglerna fullt medveten om överträdelsen bör det beaktas i försvårande riktning. Graden av uppsåt eller oaktsamhet bör också påverka valet av ingripande, inbegripet utformningen av ingripandet. Ju ringare oaktsamheten är, desto starkare skäl kan det finnas att välja en mindre ingripande åtgärd. Om den som har överträtt reglerna har gjort rimliga ansträngningar för att agera korrekt men felbedömt rättsläget är utrymmet också större att välja en mindre ingripande åtgärd. En bedömning av om en överträdelse har varit uppsåtlig eller berott på oaktsamhet, som Livsmedelsverket och *Naturvårdsverket* ställer sig skeptiska till, görs redan av bland annat tillsynsmyndigheter enligt säkerhetsskyddslagen. Enligt regeringen är det lämpligt att även tillsynsmyndigheterna enligt den nya lagen gör denna slags bedömning.

Varken NIS-direktivet eller NIS 2-direktivet reglerar att ekonomisk fördel ska beaktas vid valet av ingripande. Av 31 § NIS-lagen följer dock att bland annat de kostnader som verksamhetsutövaren har undvikit till följd av överträdelsen ska beaktas vid bestämmande av sanktionsavgiftens storlek (jfr även 33 § lagen om granskning av utländska direktinvesteringar). Regeringen instämmer i utredningens uppfattning att denna bedömningsgrund bör överföras till den nya lagen med viss modifiering. Omständigheten bör beaktas vid valet av ingripande – och inte enbart vid bestämmande av en sanktionsutgifts storlek – och ekonomisk fördel bör användas i stället för kostnad. Ekonomisk fördel inbegriper både fastställbara vinster och sådana kostnader som har undvikits till följd av överträdelsen.

Regeringen delar inte Naturvårdsverkets uppfattning att omständigheterna som ska beaktas vid valet av ingripande är otydliga. Förslaget har likheter med regleringar som finns på andra områden, bland annat 18 kap. 3 § försäkringsrörelselagen (2010:2043). Som *Transportstyrelsen* anför föreslås särskilda krav gälla för att ansöka om förbud att inneha ledningsfunktion (se avsnitt 8.6). Regeringen bedömer dock inte att det finns en motstridighet mellan att ha dels en generell reglering om vilka omständigheter som ska beaktas vid valet av ingripande, dels att ställa upp särskilda krav för en viss ingripandeåtgärd.

Regeringen bedömer inte heller att det skulle vara ett alternativ att enbart beakta angivna omständigheter kopplat till överväganden om sanktionsavgift. Omständigheterna är även relevanta att beakta vid till exempel valet mellan att besluta om föreläggande eller meddela en anmärkning. Syftet med bestämmelsen är vidare att tillsynsmyndigheten ska välja den ingripandeåtgärd som den finner lämpligast i det enskilda fallet, oavsett om det rör sig om ett föreläggande, sanktionsavgift eller anmärkning. Om en överträdelse bedöms vara allvarlig, kan tillsynsmyndigheten även i vissa fall ansöka om förbud att inneha ledningsfunktion under vissa förutsättningar.

En första lämplig ingripandeåtgärd kan, beroende på omständigheterna i det enskilda fallet, vara att tillsynsmyndigheten exempelvis beslutar om ett föreläggande att åtgärda identifierade brister, på sätt som *Trelleborgs kommun* förespråkar. Om ett sådant föreläggande följs kan tillsynsmyndigheten sedan bedöma om det föreligger skäl att även ingripa på något annat sätt utifrån ovan angivna omständigheter.

8.4.2 När ska en överträdelse betraktas som allvarlig?

Regeringens förslag: En överträdelse ska betraktas som allvarlig om verksamhetsutövaren

1. har begått upprepade överträdelser,
2. inte har fullgjort sin skyldighet att rapportera eller informera om betydande incidenter,
3. inte har avhjälpt en betydande incident,
4. inte har följt ett föreläggande om att fullgöra vissa skyldigheter enligt lagen,
5. har hindrat en tillsynsåtgärd, eller
6. har lämnat falska eller andra grovt oriktiga uppgifter i fråga om säkerhetsåtgärder eller i samband med incidentrapportering eller fullgörande av informationsskyldighet.

Utredningens förslag överensstämmer i allt väsentligt med regeringens. Vad gäller punkt 2 föreslår utredningen att en överträdelse ska betraktas som allvarlig om verksamhetsutövaren inte har rapporterat en betydande incident. Vad gäller punkt 6 föreslår utredningen att en överträdelse ska betraktas som allvarlig om verksamhetsutövaren har lämnat oriktiga uppgifter.

Remissinstanserna: *Certezza AB* anser att det borde vara mycket ovanligt och svårt att bevisa att ett tillsynsobjekt hindrat säkerhets- eller tillsynsåtgärder, men däremot inte att tillsynsobjektet på olika sätt obstruerat tillsynsåtgärder eller skjutit revisioner framför sig. Bolaget föreslår därför att ordet hindrat ersätts med ”försvårat eller utan giltigt skäl försenat”. *Transportstyrelsen* gör gällande att uttrycket oriktiga uppgifter är mer långtgående än direktivets ”falsk eller grovt felaktig information” och förespråkar en mer direktivnära utformning. Myndigheten anför vidare att det bör framgå att konsekvensen av att en överträdelse betraktas som allvarlig, utöver att den kan ligga till grund för ansökan om förbud att inneha ledningsfunktion, är att sanktionsavgiftens storlek påverkas. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: En överträdelse ska enligt artikel 32.7 a i NIS 2-direktivet, som gäller väsentliga entiteter, alltid anses vara allvarlig i vissa fall. Att artikeln gäller även för viktiga entiteter framgår av artikel 33.5. Som utredningen redogör för anger inte direktivet vad följden av att en överträdelse bedöms som allvarlig ska vara, mer än att överträdelsens allvar ska beaktas vid valet av ingripande.

Enligt artikel 32.7 a ska bland annat följande alltid anses vara en allvarlig överträdelse:

1. upprepade överträdelser,
2. underlåtenhet att underrätta om eller avhjälpa betydande incidenter,
3. underlåtenhet att avhjälpa brister enligt bindande instruktioner från behöriga myndigheter,
4. hindrande av revisioner eller övervakningsverksamhet som den behöriga myndigheten beordrat efter det att en överträdelse konstaterats, och
5. tillhandahållande av falsk eller grovt felaktig information i fråga om riskhanteringsåtgärder för cybersäkerhet eller rapporteringsskyldigheter enligt artiklarna 21 och 23.

Regeringen anser, likt utredningen, att det bör föras in en särskild bestämmelse i den nya lagen om vilka omständigheter som innebär att en överträdelse alltid är att betrakta som allvarlig, med de språkliga anpassningar som utredningen föreslår. Regeringen instämmer i utredningens uppfattning att det förhållandet att en överträdelse bedöms vara allvarlig bör innebära att mer ingripande åtgärder kommer i fråga. Dessutom föreslår regeringen i avsnitt 8.6.1 att en tillsynsmyndighet endast ska få ansöka om förbud att inneha ledningsfunktion vid allvarliga överträdelser. Enligt regeringen är det redan genom förslaget som behandlas i avsnitt 8.4.1 tydligt att överträdelsens allvar ska påverka valet av ingripande. Detta behöver därför inte förtydligas på sätt som *Transportstyrelsen* föreslår.

En överträdelse bör betraktas som allvarlig om verksamhetsutövaren har begått upprepade överträdelser. Om en verksamhetsutövare inte har rapporterat eller informerat om en betydande incident bör överträdelsen också betraktas som allvarlig (se avsnitt 6.6.2 och 6.6.3). Regeringen instämmer i utredningens uppfattning att underlåtenheten i denna del inträder när de tidsramar som anges i avsnitten har överskridits. Likaså bör överträdelsen betraktas som allvarlig om en verksamhetsutövare inte har avhjälpt en betydande incident. Med att avhjälpa en betydande incident avses att så långt som möjligt åtgärda incidenten eller lindra effekterna av den.

Har en verksamhetsutövare inte följt ett föreläggande från en tillsynsmyndighet om att fullgöra de skyldigheter som anges i avsnitt 8.2 bör överträdelsen också anses vara allvarlig. Som utredningen anför bör bedömningen nyanseras om verksamhetsutövaren uppenbart har försökt följa föreläggandet, men inte lyckats fullt ut.

Även sådana ageranden som innebär att verksamhetsutövaren har hindrat tillsynsåtgärder, inbegripet en säkerhetsrevision, bör föranleda att en överträdelse är att betrakta som allvarlig (se vidare avsnitt 7.2). Regeringen anser, likt utredningen, att det bör krävas någon form av passiv eller aktiv obstruktion av åtgärden, till exempel i form av att vägra tillsynsmyndigheten tillträde till verksamhetsutövarens lokaler. Att en verksamhetsutövare har hindrat tillsynsåtgärder bör även anses omfatta att verksamhetsutövaren försvårat eller utan giltigt skäl försenat sådana åtgärder. Enligt regeringen saknas det skäl att ersätta uttrycket hindrat på sätt som *Certezza AB* föreslår.

Slutligen bör även lämnandet av vissa slags oriktiga uppgifter i fråga om säkerhetsåtgärder eller i samband med fullgörande av underrättelseskyldigheter beaktas särskilt i sammanhanget. Utredningen föreslår att direktivets ”falsk eller grovt felaktig information” ska ersättas med ”oriktiga uppgifter”. Regeringen delar dock Transportstyrelsens uppfattning om att genomförandet i denna del bör ligga närmare direktivet för att inte få omotiverat långtgående konsekvenser. En överträdelse bör bland annat betraktas som allvarlig om verksamhetsutövaren har lämnat en falsk uppgift. En överträdelse bör också anses vara allvarlig om det rör sig om att verksamhetsutövaren, oavsett uppsåt eller oaktsamhet, har lämnat en grovt oriktig uppgift. Oriktiga uppgifter bör, som utredningen anger, avse felaktiga och missvisande uppgifter, men även utelämnade uppgifter som borde ha lämnats. Det kan röra sig om en grovt oriktig uppgift exempelvis om en uppgift av central betydelse har utelämnats och avsaknaden av den

har lett till att tillsynsmyndigheten underlåtit att vidta en viss tillsynsåtgärd i förhållande till verksamhetsutövaren. Om verksamhetsutövaren har lämnat en missvisande uppgift av mindre betydelse bör uppgiften inte anses vara grovt oriktig.

Även andra omständigheter än de nu uppräknade kan innebära att en överträdelse är att betrakta som allvarlig och kan därmed beaktas inom ramen för den bedömning som ska göras i enlighet med förslaget som behandlas i avsnitt 8.4.1. Förslaget i denna del innebär dock att ovan angivna omständigheter alltid ska innebära att överträdelsen är allvarlig.

8.5 Förelägganden

Regeringens förslag: Tillsynsmyndigheten ska få besluta de förelägganden som behövs för att verksamhetsutövare ska fullgöra sina skyldigheter att utse företrädare, göra en anmälan, vidta säkerhetsåtgärder, låta ledningen genomgå utbildning, rapportera betydande incidenter eller informera vid betydande incidenter och betydande cyberhot.

Tillsynsmyndigheten ska också få förelägga verksamhetsutövare att offentliggöra information om överträdelser av dessa skyldigheter.

Ett föreläggande ska få förenas med vite. Ett vitesföreläggande ska även få riktas mot staten.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att en tillsynsmyndighet ska få besluta ett särskilt föreläggande med innebörden att verksamhetsutövaren ska informera användare om betydande cyberhot. Utredningen föreslår att det ska införas en bestämmelse i lagen om att tillsynsmyndigheten ska få bestämma att ett föreläggande ska gälla omedelbart.

Remissinstanserna: Ett antal remissinstanser yttrar sig över utredningens förslag om att tillsynsmyndigheterna ska få besluta ett särskilt föreläggande gällande information om betydande cyberhot. *Advokatfirman Kahn Pedersen* är tveksam till om det finns ett behov av att reglera olika slags förelägganden och menar att det i stället bör framgå av förarbetena vilken sorts förelägganden som kan bli aktuella att meddela vid olika överträdelser. *Post- och telestyrelsen (PTS)* och *Tech Sverige* anser att förhållandet mellan skyldigheten att informera om betydande cyberhot, som liknar informationsskyldigheten i 8 kap. 4 § LEK, och den föreslagna rätten att meddela föreläggande måste klargöras.

Säkerhetspolisen anser att den föreslagna möjligheten att förelägga en verksamhetsutövare att offentliggöra information om överträdelser kommer att inbegripa viktiga och komplicerade bedömningar gällande säkerhetsskyddsklassificerade uppgifter samt att det bör framgå av förarbetena att hänsyn behöver tas till lämpligheten av att uppgifterna offentliggörs. Även *Skatteverket* anför att det finns risk att ett offentliggörande leder till att känslig information offentliggörs. Enligt Skatteverket bör det därför förtydligas vilken typ av uppgifter ett offentliggörande bör innehålla och vilket syfte ett offentliggörande har.

Skälen för regeringens förslag

Tillsynsmyndigheten bör kunna besluta om förelägganden

I enlighet med förslaget i avsnitt 7.2.1 ska tillsynsmyndigheten få meddela förelägganden om att den som står under tillsyn ska lämna information och ge tillträde på visst sätt. Som redogörs för i avsnitt 8.3 bör förelägganden även kunna användas vid efterlevnadskontroll i enlighet med artiklarna 32.4 och 33.4 i direktivet. Av dessa artiklar framgår att de behöriga myndigheterna åtminstone ska ha befogenhet att bland annat anta bindande instruktioner eller att meddela föreläggande om att de berörda entiteterna ska avhjälpa konstaterade brister eller överträdelser av direktivet (b) samt att ålägga dem att upphöra med beteenden som utgör en överträdelse av direktivet och att avstå från att upprepa sådana beteenden (c), säkerställa att deras riskhanteringsåtgärder överensstämmer med artikel 21 eller att fullgöra de rapporteringsskyldigheter som fastställs i artikel 23 (d), informera om betydande cyberhot och eventuella skyddsåtgärder eller avhjälpande åtgärder på visst sätt (e) och att inom en rimlig tidsfrist genomföra rekommendationer som lämnats till följd av en säkerhetsrevision (f).

Regeringen anser, i likhet med utredningen, att artiklarna 32.4 b–f och 33.4 b–f bör genomföras i nationell rätt genom att tillsynsmyndigheten får meddela de förelägganden som krävs för att verksamhetsutövare ska fullgöra de skyldigheter som föreslås gälla enligt lagen i enlighet med förslagen i avsnitt 6. För skyldigheterna att föra register över domännamn på visst sätt och att tillgängliggöra uppgifter ur registret föreslår regeringen att tillsynsmyndigheten endast ska få besluta de förelägganden som behövs för att dessa skyldigheter ska fullgöras (se avsnitt 10).

Utredningen föreslår ett särskilt föreläggande med koppling till information om cyberhot och ett antal remissinstanser, däribland *PTS*, har synpunkter på förslaget. I avsnitt 6.6.3 föreslås att det ska införas en skyldighet att vid ett betydande cyberhot informera vissa mottagare av tjänster om skydds- och motåtgärder som mottagarna kan vidta och om det är lämpligt även informera om själva hotet. Enligt regeringen motsvarar skyldigheten det som kan föranleda en ingripandeåtgärd enligt artiklarna 32.4 e och 33.4 e. Det behövs därför, som *Advokatfirman Kahn Pedersen* påpekar, inget särskilt slags föreläggande i denna del. Det kan konstateras att den föreslagna skyldigheten att informera om betydande cyberhot inbegriper en lämplighetsbedömning i fråga om information även ska lämnas om själva hotet. Enligt regeringens bedömning finns det inget hinder mot att tillsynsmyndigheten förelägger verksamhetsutövaren att informera om själva hotet.

Enligt artiklarna 32.4 h och 33.4 g ska medlemsstaterna säkerställa att de behöriga myndigheterna har befogenhet att ålägga de berörda entiteterna att offentliggöra aspekter av överträdelser av direktivet på ett specificerat sätt. Regeringen anser, i likhet med utredningen, att det även bör införas en möjlighet att besluta om sådana förelägganden. *Skatteverket* anser att det bör förtydligas vilket syfte ett offentliggörande har. Vad syftet med ett offentliggörande är utvecklas inte i direktivet. Regeringen bedömer dock att spridningen av berörd informationen i förlängningen kan bidra till att höja cybersäkerhetsnivån i samhället.

Som bland andra *Säkerhetspolisen* anför bör tillsynsmyndigheten vid beslut om förelägganden ta hänsyn till och bedöma lämpligheten av att vissa uppgifter offentliggörs. Regeringen anser, likt utredningen, att det bör ankomma på tillsynsmyndigheterna att närmare besluta på vilket sätt ett offentliggörande ska ske och vilka uppgifter offentliggörandet ska innehålla.

Föreläggandena bör kunna förenas med vite. Ett sådant bör, som framgår av avsnitt 7.2.1, även få riktas mot staten. Allmänna bestämmelser om viten finns, som anges i samma avsnitt, i viteslagen. Dessa bestämmelser bör användas för de förelägganden som beslutas av tillsynsmyndigheterna.

Ett beslut om föreläggande kan gälla omedelbart även utan särskild reglering

De behöriga myndigheterna ska, enligt artikel 32.8 i NIS 2-direktivet, utförligt motivera sina efterlevnadskontrollåtgärder gällande väsentliga entiteter. Innan sådana åtgärder antas ska de behöriga myndigheterna underrätta de berörda entiteterna om sina preliminära slutsatser. De ska också ge dessa entiteter en rimlig tidsfrist för att lämna synpunkter, utom i vederbörligen motiverade fall där omedelbara åtgärder för att förhindra eller reagera på incidenter annars skulle hindras. Artikel 32.8 ska, i enlighet med artikel 33.5, i tillämpliga delar tillämpas på de tillsyns- och efterlevnadskontrollåtgärder som föreskrivs i artikel 33 för viktiga entiteter.

Utredningen föreslår att det ska införas en bestämmelse om att tillsynsmyndigheten ska få bestämma att ett föreläggande ska gälla omedelbart. Mot bakgrund av resonemanget i avsnitt 7.2.1 om vilka möjligheter som förvaltningslagen ger i detta avseende i förhållande till enskilda bedömer regeringen att det inte behöver införas någon sådan bestämmelse som utredningen föreslår.

8.6 Förbud att inneha ledningsfunktion

8.6.1 Förutsättningar för ansökan

Regeringens förslag: Om ett föreläggande om att fullgöra skyldigheterna att utse företrädare, göra en anmälan, vidta säkerhetsåtgärder, låta ledningen genomgå utbildning, rapportera betydande incidenter eller informera vid betydande incidenter och betydande cyberhot inte följs, ska tillsynsmyndigheten få ansöka om förbud att inneha ledningsfunktion för den som är befattningshavare hos en enskild verksamhetsutövare som är väsentlig.

En ansökan ska få göras endast om överträdelsen som ligger till grund för föreläggandet är allvarlig och befattningshavaren uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen.

Utredningens förslag överensstämmer med regeringens. Det framgår inte av utredningens förslag till lagtext att förbudet endast kan riktas mot väsentliga verksamhetsutövare.

Remissinstanserna: *Advokatfirman Kahn Pedersen*, som tillstyrker utredningens förslag, gör gällande att förhållandet mellan kravet i förbuds-

bestämmelsen om att överträdelsen som ligger till grund för föreläggandet ska vara allvarlig och den föreslagna bestämmelsen om att en överträdelse ska betraktas som allvarlig om en verksamhetsutövare inte har följt ett tidigare föreläggande måste förtydligas. *Bolagsverket* bedömer att ett förbud bör innebära att befattningshavaren inte heller får inneha ledningsansvar hos någon annan väsentlig verksamhetsutövare. Det bör enligt Bolagsverket även förtydligas att verksamhetsutövaren, efter att myndigheten har hävt avregistreringen, på nytt måste anmäla till Bolagsverket om personen återfår sitt ledningsansvar. Bolagsverket anser också att gränsdragningen mellan ledningsfunktion och ledningsansvar bör tydliggöras då förbudet enligt förslaget endast omfattar sådant arbete som innebär att personen utövar ledningsansvar och att förbudspersonen således kan vara kvar hos verksamhetsutövaren i andra ledningsfunktioner. *Certezza AB* anser att förbudet inte bör vara begränsat till en person och att det bör förtydligas att det är just befattningen med ledningsansvar som omfattas av förbudet.

En arbetsgrupp inom Cybernoden, *SJ AB* och *Tågföretagen* motsätter sig att förbud endast ska kunna riktas mot enskilda verksamhetsutövare. *Styrelseakademin* och *Svenskt Näringsliv* motsätter sig att förbudet ska kunna träffa samma personkrets som omfattas av utbildningskravet, därmed även styrelsen, eftersom detta utgör en överimplementering av direktivet. *Swedsoft, Tech Sverige* och *Teknikföretagen* påpekar också att utredningens förslag inte följer av direktivet och understryker att en styrelse fattar sina beslut kollektivt.

Skälen för regeringens förslag

Direktivets innehåll

Enligt artikel 32.5 b i NIS 2-direktivet ska medlemsstaterna säkerställa att de behöriga myndigheterna har befogenhet att begära att relevanta organ eller domstolar, i enlighet med nationell rätt, inför ett tillfälligt förbud för varje fysisk person som på nivån för verkställande direktör eller juridiskt ombud har ledningsansvar i den väsentliga entiteten att utöva ledningsfunktioner i den entiteten.

Förbudet ska enligt artikel 32.5 komma i fråga först om vissa andra efterlevnadskontrollåtgärder är ineffektiva och efter att behöriga myndigheter har fastställt en tidsfrist inom vilken en väsentlig entitet ska vidta nödvändiga åtgärder för att avhjälpa bristerna eller uppfylla myndigheternas krav och de begärda åtgärderna inte vidtagits inom den fastställda tidsfristen. Motsvarande reglering finns inte i artikel 33 avseende viktiga verksamhetsutövare.

Förbudet riktar sig, till skillnad från övriga ingripandeåtgärder, mot en fysisk person och inte mot verksamhetsutövaren. Det har ett samband med vad som anges i direktivets artikel 32.6 om att medlemsstaterna ska säkerställa att varje fysisk person som ansvarar för eller agerar som juridiskt ombud för en väsentlig entitet har befogenhet att säkerställa att entiteten efterlever direktivet, på grundval av en befogenhet att företräda entiteten, att fatta beslut på dess vägnar eller att utöva kontroll över entiteten. Enligt samma artikel ska medlemsstaterna säkerställa att dessa fysiska personer kan hållas ansvariga för överträdelser av sitt uppdrag att säkerställa att direktivet efterlevs.

Förbud endast vid allvarliga överträdelser

Förbudsmöjligheten är central för systematiken i NIS 2-direktivet. En sådan ingripandeåtgärd bör därför införas i nationell rätt. Regeringen instämmer i utredningens uppfattning att det är fråga om en mycket ingripande åtgärd som får omedelbara följder för både verksamhetsutövaren och den enskilde befattningshavaren. Därför bör förbud endast komma i fråga om överträdelsen som ligger till grund för föreläggandet är allvarlig. I avsnitt 8.4.1 och 8.4.2 redogör regeringen för vilka omständigheter som ska beaktas vid bedömningen av hur allvarlig en överträdelse är och när en överträdelse alltid ska betraktas som allvarlig. Denna bedömning ligger sedan, som *Advokatfirman Kahn Pedersen* efterfrågar ett förtydligande om, till grund för bedömningen om rekvisiten för att ansöka om ett förbud är uppfyllda. Hur en ansökan ska göras utvecklas i avsnitt 8.6.2.

Endast förbud mot befattningshavare hos enskilda verksamhetsutövare som är väsentliga

Av artikel 32.5 tredje stycket i NIS 2-direktivet framgår att bland annat förbudsmöjligheten inte är tillämplig på sådana offentliga förvaltningsentiteter som omfattas av direktivet. Regeringen instämmer i utredningens uppfattning att förbudsmöjligheten endast bör kunna riktas mot enskilda verksamhetsutövare, och inte mot sådana offentliga verksamhetsutövare som omfattas av lagen, även om inte en offentlig verksamhetsutövare som omfattas av lagen per automatik är en offentlig förvaltningsentitet enligt direktivets definition (se avsnitt 5.3.3). Några remissinstanser, bland andra *Tågföretagen*, anser att detta innebär en omotiverad skillnad. Regeringen menar dock att det är rimligt att förbudet, som i första hand har till syfte att framtvinga vissa åtgärder och inte att utgöra en reaktion på bristfällig ledning, endast gäller i förhållande till enskilda verksamhetsutövare. Utredningen bedömer att förbud endast ska kunna riktas mot befattningshavare hos enskilda verksamhetsutövare som är väsentliga verksamhetsutövare, men detta framgår inte av utredningens förslag till lagtext. Ett förtydligande bör ske i förhållande till utredningens förslag i denna del.

Ett antal remissinstanser yttrar sig över frågan om vilken krets av personer med koppling till den enskilda verksamhetsutövaren som förbudet ska kunna träffa. Det framgår av artikel 32.5 b att förbudet ska kunna träffa varje fysisk person som på nivån för verkställande direktör eller juridiskt ombud har ledningsansvar i den väsentliga entiteten. I artikel 20 anges att viktiga och väsentliga entiteters ledningsorgan har ett visst ansvar för riskhanteringsåtgärder och att de ska kunna ställas till svars för entiteternas överträdelse av artikel 21 som rör riskhanteringsåtgärder (se vidare avsnitt 6.5). Personkretsen i artiklarna 20 och 32.5 b är alltså definierad på olika sätt.

I enlighet med vad regeringen utvecklar i avsnitt 6.5 bör uttrycket ledningsorgan i artikel 20 i ett svenskt sammanhang motsvara ledning. Enligt utredningen kan kretsen som omfattas av artikel 32.5 b uppfattas som snävare än den som omfattas av artikel 20 och formuleringen kan anses innebära att styrelsen inte omfattas av den förstnämnda artikeln. Utredningen föreslår dock att förbudet enligt den nya lagen bör kunna träffa den bredare krets som avses i artikel 20. Detta för att upprätthålla

systematiken som gäller enligt artikel 20 i fråga om att det är verksamhetsutövares ledningsorgan som ska kunna hållas ansvariga för överträdelser av direktivet. Förbudet bör enligt utredningens förslag förutsätta att personen med ledningsansvar ska ha orsakat den allvarliga överträdelsen uppsåtligen eller av grov oaktsamhet.

Utredningen föreslår att personkretsen som kan omfattas av förbudet bör definieras på samma sätt som i 3 § lagen (2014:836) om näringsförbud:

- i kommanditbolag: komplementär,
- i andra handelsbolag: bolagsman,
- i aktiebolag, ömsesidiga försäkringsbolag och ömsesidiga tjänstepensionsbolag: ledamot och suppleant i styrelsen samt verkställande direktör och vice verkställande direktör,
- i sparbanker, ekonomiska föreningar, försäkringsföreningar och tjänstepensionsföreningar: ledamot och suppleant i styrelsen samt verkställande direktör och vice verkställande direktör,
- i europeiska ekonomiska intressegrupperingar med säte i Sverige: företagsledare,
- i europabolag och europakooperativ med säte i Sverige: ledamot och suppleant i förvaltnings-, lednings- eller tillsynsorgan samt verkställande direktör och vice verkställande direktör,
- i utländska filialer som omfattas av lagen (1992:160) om utländska filialer m.m.: verkställande direktör och vice verkställande direktör, och
- i stiftelser som omfattas av 2 kap. 3 § bokföringslagen (1999:1078): ledamot och suppleant i styrelsen samt, när en stiftelse har anknuten förvaltning, sådana befattningshavare hos förvaltaren som anges i detta stycke.

Några remissinstanser, bland andra *Svenskt Näringsliv* och *Tech Sverige*, menar att styrelsen inte bör omfattas av personkretsen som kan träffas av ett förbud. Oavsett om utredningens förslag skulle innebära ett genomförande som går utöver vad som följer av direktivet, som dessa remissinstanser anför, bedömer regeringen att det är ändamålsenligt att samma krets som träffas av 3 § lagen om näringsförbud även kan bli föremål för ett förbud med stöd av den nya lagen. Inte minst för att denna krets ska kunna bli föremål för ingripande på sätt som artikel 20 i direktivet förutsätter. En styrelse fattar visserligen sina beslut kollektivt. Detta innebär dock inget hinder mot att utforma bestämmelsen på det sätt som utredningen föreslår. Som *Certezza AB* anför är förbudsmöjligheten inte begränsad till en person, däremot förutsätter den att den enskilda befattningshavaren uppsåtligen eller av grov oaktsamhet har orsakat den allvarliga överträdelsen.

Vad innebär förbudet i praktiken?

Bolagsverket ber om ett förtydligande i fråga om vad förbudet att inneha ledningsfunktion innebär. Regeringen bedömer, likt *Certezza AB*, att ett förbud bör omfatta befattningen med ledningsansvar. Förbudet får till följd att befattningshavaren blir omedelbart obehörig att inneha ledningsfunktioner inom verksamhetsutövaren under viss tid (se avsnittet nedan). Ett förbud bör inte innebära att personen i fråga inte får utföra andra arbetsuppgifter hos verksamhetsutövaren. Det finns inte heller utrymme för att

inom ramen för detta lagstiftningsärende föreslå en ordning som innebär ett generellt förbud att inneha ledningsfunktion hos andra verksamhetsutövare som *Bolagsverket* förespråkar.

Enligt utredningens förslag till förordning bör Bolagsverket, eller en länsstyrelse som är registreringsmyndighet, efter ett förbudsbeslut avregistrera personen som befattningshavare. Bolagsverket anser att den tillfälliga effekten, som föreslås i avsnitt 8.6.2, uppnås genom att verksamhetsutövaren ansöker om att befattningshavaren ska registreras på nytt efter det att förbudet har upphört under förutsättning att personen ska få tillbaka sitt ledningsansvar. Utredningens förslag till förordning är inte föremål för behandling i denna lagrådsremiss, men regeringen konstaterar att frågan om avregistrering efter ett förbudsbeslut kan regleras på lägre föreskriftsnivå än i lag.

8.6.2 Förfarandet vid en ansökan om förbud

Regeringens förslag: En ansökan om förbud att inneha ledningsfunktion ska göras av tillsynsmyndigheten till allmän förvaltningsdomstol och innehålla uppgift om den person, befattning och verksamhetsutövare som ansökan avser. Ansökan ska också innehålla uppgift om överträdelsen och de omständigheter som behövs för att kännetecknа den samt de bestämmelser som är tillämpliga på överträdelsen.

Ansökan ska lämnas in till förvaltningsrätt inom vars domkrets tillsynsmyndigheten är belägen och målet ska prövas skyndsamt av domstolen.

Ett förbud ska gälla lägst ett år och högst tre år.

Tillsynsmyndigheten ska omedelbart begära att förbudet ska upphävas om den bedömer att det inte längre finns förutsättningar för ett förbud. Den enskilde ska vid ett beslut om förbud upplysas om sin rätt att begära att förbudet ska upphävas.

Om tillsynsmyndigheten eller den enskilde begär det ska domstolen pröva om förbudet ska upphävas. Ett förbud ska upphävas omedelbart om det inte längre finns förutsättningar för det.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår inte att det av ansökan ska framgå vilken befattning som ansökan avser. Utredningen föreslår att det ska regleras dels att ett förbud ska upphävas omedelbart när ett föreläggande har följts, dels att ett beslut om förbud ska upphävas om det inte längre finns förutsättningar för förbudet. Utredningen föreslår att domstolen även ska pröva om ett beslutat förbud ska upphävas om det finns skäl till det på annan grund än att tillsynsmyndigheten eller den enskilde begär det.

Remissinstanserna: Majoriteten av remissinstanserna yttrar sig inte över förslaget. *Förvaltningsrätten i Malmö* tillstyrker förslaget om behörig domstol.

Certezza AB anser att ansökan ska innehålla uppgift om vilken befattning personen som ska träffas av förbudet har. *Naturvårdsverket* anser att det är oklart vilken domstolens uppgift är, vilken lag som ska tillämpas och hur anhängiggörande vid domstolen ska ske.

Styrelseakademin och *Svenskt Näringsliv* anser att förbudsärendena bör hanteras av allmän domstol, som har större vana att bedöma frågor om uppsåt och oaktsamhet och som även hanterar frågor om näringsförbud.

Skälen för regeringens förslag

Frågan om förbud bör avgöras av domstol

Utredningen anser att förbudsbeslut bör meddelas av domstol av rättssäkerhetsskäl. I vissa liknande regelverk förekommer det visserligen att en tillsynsmyndighet får meddela förbud på liknande sätt, men förbudsmöjligheten enligt den nya lagen särskiljer sig genom att det kommer att finnas flera olika tillsynsmyndigheter (jfr lagen om värdepappersmarknaden [2007:528] och lagen [2004:297] om bank- och finansieringsrörelse). På sätt som utredningen redogör för saknas det skäl att frångå utgångspunkten att förbudet ska beslutas av domstol som första instans.

Utredningen bedömer att prövningen av om förbud ska meddelas bör göras av allmän förvaltningsdomstol. *Styrelseakademin* och *Svenskt Näringsliv* anser dock att förbudsärendena bör handläggas i allmän domstol. Regeringen konstaterar att även allmänna förvaltningsdomstolar prövar frågor om uppsåt och oaktsamhet och bedömer, som utredningen och *Förvaltningsrätten i Malmö*, att prövningen bör ske i allmän förvaltningsdomstol.

Som utredningen redogör för bör processen vid domstolen inledas genom att tillsynsmyndigheten lämnar in en ansökan till den domstol inom vars domkrets myndigheten är belägen, det vill säga där myndighetens huvudkontor är beläget. Av ansökan bör de uppgifter som utredningen föreslår framgå. Som *Certezza AB* föreslår bör även den befattning som avses anges i ansökan.

Naturvårdsverket anser att det är oklart vilken domstolens uppgift är. Domstolen ska pröva om det föreligger förutsättningar för att meddela ett förbud. Det krävs enligt regeringen inga övriga förtydliganden i fråga om domstolens prövning eller formerna för anhängiggörandet vid domstolen. Vad som gäller följer direkt av förvaltningslagen och förvaltningsprocesslagen (1971:291).

Tidsbegränsning och förutsättningar för upphävande

Av artikel 32.5 i NIS 2-direktivet följer att förbudet ska vara tillfälligt och endast tillämpas till dess att den berörda entiteten vidtar nödvändiga åtgärder. Förbudet behöver därför dels begränsas i tid, dels upphävas när skäl för ett sådant inte längre föreligger. Regeringen anser, likt utredningen, att förbudet bör tidsbestämmas till mellan ett och tre år samt att det bör upphävas omedelbart när syftet med förbudet har uppnåtts.

Utredningen föreslår att det ska regleras i lagen dels att ett förbud ska upphävas omedelbart när ett föreläggande har följts, dels att ett beslut om förbud ska upphävas om det inte längre finns förutsättningar för förbudet. Utredningen anger att den sistnämnda situationen kan uppstå om verksamhetsutövaren har följt det föreläggande som tillsynsmyndigheten har beslutat. Det bör vara tillräckligt att reglera att ett förbud ska upphävas omedelbart när det inte längre finns förutsättningar för det.

Förutsättningar för ett förbud kan saknas till exempel när det ursprungliga föreläggandet har följts, men även om någon annan bedömning görs i fråga om överträdelsens allvar eller i fråga om befattningshavaren har orsakat överträdelsen uppsåtligen eller av grov oaktsamhet. Tillsynsmyndigheten bör omedelbart begära att ett förbud ska upphävas om den bedömer att det inte längre finns förutsättningar för ett förbud.

Om tillsynsmyndigheten eller den enskilde begär det bör domstolen pröva om ett förbud ska upphävas. Utredningen anser att det även ska regleras att domstolen ska pröva om ett förbud ska upphävas om det annars finns skäl till det. Utredningen anger att sådana skäl kan vara att domstolen får del av en upplysning om att personen i fråga har avlidit. Regeringen anser till skillnad från utredningen inte att det är motiverat att införa en sådan bestämmelse.

Vid ett beslut om förbud bör den enskilda upplysas om sin rätt att begära att förbudet ska upphävas. Förfarandet vid en allmän förvaltningsdomstol är i huvudregel skriftligt, men det finns möjlighet att begära muntlig förhandling enligt 9 § förvaltningsprocesslagen. Mot bakgrund av förbudets tillfälliga art och med hänsyn till syftet med ingripandeåtgärden bör såväl mål om förbud samt mål om upphävande av förbud behandlas med förtur.

8.7 Sanktionsavgifter

8.7.1 När ska en sanktionsavgift få tas ut?

Regeringens förslag: Tillsynsmyndigheten ska få besluta att ta ut en sanktionsavgift av en verksamhetsutövare om verksamhetsutövaren åsidosatt sina skyldigheter att utse företrädare, göra en anmälan, vidta säkerhetsåtgärder, låta ledningen genomgå utbildning, rapportera betydande incidenter eller informera vid betydande incidenter och betydande cyberhot.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Advokatfirman Kahn Pedersen* förordar att det tydliggörs att det är tillsynsmyndigheten som har bevisbördan för att en överträdelse har skett och för de omständigheter som ska beaktas i fråga om sanktionsavgiftens storlek samt att det regleras i lag vilket beviskrav som ska gälla. *Företagarna* understryker vikten av att det ska vara enkelt för verksamhetsutövare att förstå hur de ska agera för att undvika att drabbas av en sanktionsavgift. *Livsmedelsverket* och *Teracom AB* tillstyrker förslaget om att strikt ansvar ska gälla. *Naturvårdsverket* anser att bestämmelserna om sanktionsavgift lämnar ett stort tolkningsutrymme och att de bör ses över för att säkerställa att avgifterna tas ut på ett rättssäkert sätt. *Salems kommun* anser att det behöver tydliggöras om det är kommunstyrelsen eller kommunens nämnder som kommer att träffas av sanktionsavgiften.

Bland andra *Tele2 Sverige AB (Tele2)* och *Transportstyrelsen* tillstyrker utredningens förslag att tillsynsmyndigheterna, till skillnad från vad som gäller enligt NIS-lagen, i varje enskilt fall ska avgöra om sanktionsavgift ska tas ut, snarare än att beslut om sanktionsavgift ska fattas undantagslöst

vid konstaterad överträdelse. *Tech Sverige* anser att beslut om sanktionsavgifter ska fattas med restriktivitet.

Skälen för regeringens förslag

Sanktionsavgifter enligt direktivet

Enligt 34.1 i NIS 2-direktivet ska medlemsstaterna säkerställa att de administrativa sanktionsavgifter som påförs väsentliga och viktiga entiteter för överträdelser av direktivet är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall. Enligt artikel 34.2 ska administrativa sanktionsavgifter påföras utöver någon av de åtgärder som anges i artiklarna 32.4 a–h, 32.5 och 33.4 a–g.

När beslut fattas om huruvida administrativa sanktionsavgifter ska påföras och om avgiftsbeloppet i varje enskilt fall, ska vederbörlig hänsyn i enlighet med artikel 34.3, tas till åtminstone de faktorer som anges i artikel 32.7 (se vidare avsnitt 8.4). Medlemsstaterna ska enligt artikel 34.4 säkerställa att väsentliga entiteter som överträder artikel 21 eller 23, som gäller riskhanteringsåtgärder och rapporteringsskyldighet, i enlighet med i artikel 34.2 och 34.3 påförs administrativa sanktionsavgifter på vissa angivna nivåer.

Tillsynsmyndigheterna ska besluta om avgifterna

I svensk rätt finns sanktionsavgifter på många områden. Sanktionsavgifter är till skillnad från vitessanktionerade åtgärdsförelägganden i huvudsak en tillbakaverkande sanktion som är handlingsdirigerande genom att verka avskräckande. Om en sanktionsavgift riskerar att innebära en kostnad eller förlust som är lika stor som eller större än den besparing som görs genom att regelverket inte följs, skapar avgiften ett incitament att undvika överträdelser. En fördel i sammanhanget är dessutom att sanktionsavgifter kan vara en kännbar sanktion mot en juridisk person som inte kan bli föremål för samtliga straffrättsliga åtgärder. Sanktionsavgifter framstår mot denna bakgrund som en lämplig följd vid överträdelser av den nya lagen.

Det är tillsynsmyndigheterna som genom sin sakkunskap kommer att ha eller kommer att kunna skaffa sig bäst förutsättningar för att bedöma om en överträdelse har skett. Om en tillsynsmyndighet fattar beslut om sanktionsavgift, kan det dessutom antas att handläggningen i regel blir snabbare än om en domstol skulle fatta beslut efter ansökan av myndigheten. Genom regeringens förslag i avsnitt 9 om att ett beslut om sanktionsavgift ska kunna överklagas till domstol tillgodoses också rättssäkerhetsaspekterna för den som blir föremål för en sanktionsavgift och det kommer också att bildas domstolspraxis till vägledning för tillsynsmyndigheternas kommande beslut. Det är sammanfattningsvis lämpligt att det är en tillsynsmyndighet som ska kunna pröva och besluta om sanktionsavgifter som utredningen föreslår.

Systemet bör, som utredningen bedömer, 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.

Regeringen instämmer i utredningens uppfattning att tillsynsmyndigheten bör kunna besluta om sanktionsavgift även om den tidigare har ingripit på något annat sätt (se dock om dubbelbestraffningsförbudet i avsnitt 8.7.3). Beslut om sanktionsavgifter ska enligt *Tech Sverige* fattas med restriktivitet. I enlighet med bland annat 5 § tredje stycket förvaltningslagen ska beslut som tillsynsmyndigheten fattar vara proportionerliga. Regeringen bedömer att det inte finns någon risk för att en tillsynsmyndighet kommer att besluta om sanktionsavgift som förstahandsalternativ i en situation då det hade varit tillräckligt att besluta om en annan åtgärd. Tillsynsmyndigheten bör dock också kunna besluta om sanktionsavgift utan att ha ingripit tidigare om det är motiverat i det enskilda fallet. Som *Företagarna* understryker är det av stor vikt att regelverket är utformat på ett tydligt sätt. Regeringen bedömer, till skillnad från *Naturvårdsverket*, att det inte krävs några förtydliganden i förhållande till utredningens förslag för att uppnå sådan tydlighet.

Salems kommun anser att det behöver tydliggöras om det är kommunstyrelsen eller kommunens nämnder som kommer att träffas av sanktionsavgifter. Kommunen efterfrågar också ett förtydligande av om det är kommunstyrelsen som ska företräda nämnderna i till exempel ett tillsynsärende. Lagen föreslås gälla för kommunen som helhet och med ledning i förhållande till kommuner avses kommunstyrelsen enligt resonemanget i avsnitt 6.5. Det finns ingen anledning att göra något ytterligare förtydligande i fråga om vilken del av kommunerna som ett beslut om sanktionsavgift kommer att riktas till.

Bevisbörda och beviskrav

Regeringen konstaterar, som *Advokatfirman Kahn Pedersen*, att tillsynsmyndigheten kommer att ha bevisbördan för att en överträdelse har skett. När det gäller frågan om vilket beviskrav som gäller konstaterar regeringen att det i förvaltningsprocessen inte finns något för alla situationer gällande beviskrav utan att beviskravet varierar med hänsyn till sakens beskaffenhet (se till exempel HFD 2013 ref. 61). Beviskrav i förvaltningsmål bör dock, för det fall aktuell reglering inte ger någon ledning i frågorna, ses i ljuset av 8 § förvaltningsprocesslagen där det anges att det är domstolens ansvar att varje mål blir så pass utrett som dess beskaffenhet kräver.

Utredningen föreslår inte att det ska regleras i lagen vilket beviskrav som gäller. Någon sådan reglering finns inte heller i till exempel säkerhetsskyddslagen, NIS-lagen eller lagen om granskning av utländska direktinvesteringar. Regeringen bedömer att det inte bör regleras särskilt vilket beviskrav som gäller i aktuella ärenden. Det blir i stället ytterst upp till domstol att vid ett överklagande avgöra huruvida det är utrett att en överträdelse har skett.

8.7.2 Sanktionsavgiftens storlek

Regeringens förslag: För enskilda verksamhetsutövare som är väsentliga ska sanktionsavgiften bestämmas till lägst 5 000 kronor och högst till det högsta av 2 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår eller ett belopp i kronor motsvarande 10 000 000 euro.

För enskilda verksamhetsutövare som är väsentliga ska avgiften bestämmas till lägst 5 000 kronor och högst till det högsta av 1,4 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår eller ett belopp i kronor motsvarande 7 000 000 euro.

För offentliga verksamhetsutövare ska avgiften bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

Utredningens förslag överensstämmer i allt väsentligt med regeringens. Utredningen föreslår att maximibeloppen ska anges enbart i euro när det är fråga om enskilda verksamhetsutövare.

Remissinstanserna: *Advokatfirman Kahn Pedersen* förordar ett tydliggörande av att sanktionsavgifter i den övre halvan av det föreslagna beloppsintervallet endast bör komma i fråga för mycket allvarliga överträdelser. Några remissinstanser, däribland *Chalmers tekniska högskola AB*, *Stockholms universitet* och *Sveriges universitets- och högskoleförbund (SUHF)*, framför att sanktionsbeloppen bör vara desamma för lärosäten oavsett huvudman. *En arbetsgrupp inom Cybernoden* anser att det inte finns stöd i direktivet för en nedsättning av påföljden för offentlig verksamhet och bedömer att det är tveksamt om en sanktionsavgift om högst 10 000 000 kronor kan anses vara effektiv, proportionell och avskräckande. *Drivkraft Sverige* och *Strålsäkerhetsmyndigheten (SSM)* framhåller att sanktionsavgifternas storlek i den nya lagen och säkerhetsskyddslagen bör harmonieras. *MTR* anför att sanktionsavgifter baserade på verksamhetens totala omsättning riskerar att snedvrida konkurrensen mellan branscher och länder och att det därför är viktigt att tillsynsmyndigheterna ges möjlighet att branschanpassa avgifterna. Även *SJ AB* anser att det finns en obalans mellan de ingripandeåtgärder som offentliga och enskilda verksamhetsutövare kan bli föremål för. *Tech Sverige* anser att avgifternas storlek bör samordnas mot de lägre nivåer som gäller på vissa andra områden. *Trafikverket* bedömer att samtliga belopp bör anges i samma valuta och i svenska kronor. *Tågföretagen* anser att sanktionerna måste stå i relation till branschens förväntade lönsamhet för att få ett rättvist sanktionssystem samt att det finns en tydlig obalans mellan offentliga och enskilda verksamhetsutövare i fråga om sanktionsavgifternas storlek som innebär särbehandling.

Skälen för regeringens förslag

Sanktionsavgifternas nivåer enligt direktivet

Av artikel 34.1 i NIS 2-direktivet framgår att medlemsstaterna ska säkerställa att de administrativa sanktionsavgifter som påförs väsentliga och viktiga entiteter för överträdelser av direktivet ska vara effektiva,

proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall. NIS 2-direktivet anger inte något minimibelopp avseende sanktionsavgifter. Av artikel 34.7 i NIS 2-direktivet följer att medlemsstaterna får välja om och i vilken utsträckning sanktionsavgift ska kunna påföras offentliga förvaltningsentiteter.

Avseende maximinivån inför NIS 2-direktivet två olika beräkningsgrunder och belopp beroende på om det rör sig om entiteter som är väsentliga (artikel 34.4) eller viktiga (artikel 34.5). Maximibeloppet ska uppgå till det högsta alternativet av 10 000 000 respektive 7 000 000 euro för väsentlig respektive viktig entitet eller 2,0 respektive 1,4 procent för väsentlig respektive viktig entitet av den totala globala årsomsättningen under föregående räkenskapsår.

Enligt skäl 130 bör, om en administrativ sanktionsavgift påförs en väsentlig eller viktig entitet som är ett företag, företaget i detta sammanhang anses vara ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget. Vidare bör, om en administrativ sanktionsavgift påförs en person som inte är ett företag, den behöriga myndigheten ta hänsyn till den allmänna inkomstnivån i medlemsstaten och personens ekonomiska situation när den överväger lämplig sanktionsavgift. Medlemsstaterna bör fastställa om och i vilken utsträckning myndigheter ska omfattas av administrativa sanktionsavgifter. Föreläggande av en administrativ sanktionsavgift påverkar inte de behöriga myndigheternas tillämpning av andra befogenheter eller andra sanktioner som fastställs i de nationella bestämmelser som införlivar direktivet.

Nivåerna enligt den nya lagen

Skyldigheterna enligt den nya lagen föreslås träffa både offentliga och enskilda verksamhetsutövare och dessutom verksamhetsutövare av olika storlek och som agerar inom olika sektorer. Regleringen om sanktionsavgifter behöver därför utformas på ett sådant sätt att de i varje enskilt fall kan anses vara effektiva, proportionella och avskräckande i enlighet med direktivet.

För väsentliga verksamhetsutövare, som inte är offentliga, föreslår utredningen att sanktionsavgiften ska bestämmas till högst till det högsta av 2 procent av den väsentliga verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår eller 10 000 000 euro. För viktiga verksamhetsutövare föreslår utredningen att avgiften ska bestämmas till högst till det högsta av 1,4 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller 7 000 000 euro. Föreslagna nivåer bör gälla och anges i den nya lagen. Eftersom maximibeloppen följer av direktivet finns det inte utrymme att fastställa ett lägre maximibelopp, som *Tech Sverige* resonerar om. I direktivet anges maximibeloppen i euro och regeringen bedömer, i likhet med utredningen, att det finns skäl att ange vad maximibeloppen är i den valutan. Det bör dock, i linje med vad *Trafikverket* anför, i lagen uttryckas som att maximibeloppet är ett belopp i kronor som motsvarar ett maximibelopp i euro.

Medlemsstaterna får enligt direktivet välja om och i vilken utsträckning sanktionsavgift ska kunna påföras offentliga verksamhetsutövare. Bland andra *Stockholms universitet, SUHF* och *Tågföretagen* är tveksamma till

ordningen som innebär att det görs skillnad på offentliga verksamhetsutövare och enskilda i fråga om sanktionsavgifternas storlek. Regeringen konstaterar dock att det inom ramen för ett antal regleringar görs sådan skillnad (se till exempel 7 kap. 4 § säkerhetsskyddslagen). Inom den privata sektorn kan en överträdelse av regleringen medföra otillbörliga konkurrensfördelar som snedvrider marknaden. Någon sådan ekonomisk vinning, på bekostnad av andra aktörer på marknaden, kan offentliga verksamhetsutövare inte dra. Regeringen bedömer, i likhet med vad som gäller på andra områden och mot denna bakgrund, att det finns skäl att göra skillnad på offentliga och enskilda verksamhetsutövare i aktuellt avseende.

Maximinivå för sanktionsavgifter enligt till exempel NIS-lagen och 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) är 10 000 000 kronor eller i vissa fall lägre. Denna nivå framstår, trots kritiken från *en arbetsgrupp inom Cybernoden*, som lämplig i förhållande till offentliga verksamhetsutövare enligt den nya lagen och ändamålsenlig för att uppnå syftet med regelverket (jfr också prop. 2017:18:205 s. 70 f.).

Drivkraft Sverige och *SSM* framhåller att sanktionsavgifternas storlek enligt den nya lagen och enligt säkerhetsskyddslagen bör harmonieras. Enligt säkerhetsskyddslagen ska en sanktionsavgift bestämmas till lägst 25 000 kronor och högst till 50 000 000 kronor. Sanktionsavgiften för en statlig myndighet, kommun eller region ska dock bestämmas till högt 10 000 000 kronor. Av NIS-direktivet följde inte några beloppsgränser men enligt 30 § NIS-lagen ska en sanktionsavgift bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor. Regeringen instämmer i utredningens uppfattning om att det inte finns skäl att nu förändra miniminivån och den bör därför även fortsättningsvis vara 5 000 kronor för både offentliga och enskilda verksamhetsutövare. Det konstateras att utredningen i sitt slutbetänkande föreslår att maximibeloppet enligt säkerhetsskyddslagen, för andra än statliga myndigheter, kommuner och regioner, ska bestämmas till högst till det högsta av 120 000 000 kronor eller 2 procent av verksamhetsutövarens totala globala årsomsättning under föregående räkenskapsår. Förslaget bereds inom Regeringskansliet.

MTR anför att det är viktigt att tillsynsmyndigheterna ges möjlighet att branschanpassa avgifterna och Tågföretagen anser att sanktioner måste stå i relation till branschens förväntade lönsamhet för att få ett rättvist sanktionssystem. När sanktionsavgiftens storlek bestäms bör, enligt regeringens mening, tillsynsmyndigheten särskilt beakta de omständigheter som följer av avsnitt 8.4. Vilken storlek på sanktionsavgiften som en överträdelse motiverar i det enskilda fallet kommer att avgöras av tillsynsmyndigheten eller, efter överklagande, av en domstol. Belopp i den övre delen av de föreslagna beloppsintervallen bör, som *Advokatfirman Kahn Pedersen* anger, komma i fråga endast för mycket allvarliga överträdelser (jfr till exempel prop. 2022/23:116 s. 129).

8.7.3 Förfarandet vid beslut om sanktionsavgift

Regeringens förslag: En sanktionsavgift ska inte få beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

En sanktionsavgift ska få beslutas endast om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum. Ett beslut om sanktionsavgift ska delges.

En sanktionsavgift ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. Om sanktionsavgiften inte betalas i rätt tid, ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning. Det ska tas in en bestämmelse i lagen som upplyser om att bestämmelser om indrivning finns i lagen om indrivning av statliga fordringar m.m.

Sanktionsavgiften ska tillfalla staten.

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

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att det ska införas en bestämmelse som innebär att ett beslut om sanktionsavgift ska få verkställas enligt utsökningsbalken. Utredningen föreslår också att det ska införas reglering om att en sanktionsavgift inte ska få tas ut om överträdelsen har lett till att verksamhetsutövaren har påförts en sanktionsavgift enligt EU:s dataskyddsförordning. Utredningen föreslår att det ska finnas en särskild bestämmelse om att de omständigheter som behandlas i avsnitt 8.4 ska beaktas vid bestämmandet av avgiftens storlek.

Remissinstanserna: *Hi3G Access AB (Tre)* och *Post- och telestyrelsen (PTS)* föreslår att förbudet att påföra flera sanktionsavgifter för samma överträdelse ska gälla även i förhållande till LEK. Tre föreslår att motsvarande bestämmelser ska föras in i bland annat den lagen. *Livsmedelsverket* ställer sig tveksamt till om det är nödvändigt att ange att det är ett hinder mot att ta ut sanktionsavgift att samma överträdelse har lett till sanktionsavgift enligt EU:s dataskyddsförordning med tanke på de bestämmelser som finns gällande dubbel bestraffning. *Tech Sverige* anför att det måste säkerställas att sanktionsavgifter inte kan tas ut flera gånger enligt olika regelverk för samma överträdelse. Remissinstanserna yttrar sig inte särskilt över övriga förslag.

Skälen för regeringens förslag

Rätten att yttra sig och om delgivning

Den som riskerar att påföras en sanktionsavgift bör ges tillfälle att yttra sig innan tillsynsmyndigheten fattar beslut om en sådan avgift. Verksamhetsutövaren ges därigenom möjlighet att till exempel påtala eventuella felaktigheter och omständigheter som kan utgöra skäl för att helt eller delvis efterge avgiften.

På grund av sanktionsavgiftens ingripande natur bör det finnas en bortre tidsgräns för när en sanktionsavgift ska få beslutas. Regeringen anser att en sanktionsavgift bör få beslutas endast om den som anspråket riktas mot

har getts tillfälle att yttra sig inom två år från överträdelsen. Om kommunikation enligt 25 § förvaltningslagen inte har skett med den som avgiften ska tas ut av inom denna tid, får en sanktionsavgift därmed inte tas ut. Det är tillsynsmyndighetens ansvar att kontrollera att kommunikation har skett.

Ett beslut om en sanktionsavgift är en särskilt ingripande åtgärd. Sådana beslut bör därför delges den avgiftsskyldige enligt delgivningslagen (2010:1932).

Betalning, indrivning och preskription

En sanktionsavgift bör tillfalla staten. Det bör också föreskrivas att avgiften ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. Om sanktionsavgiften inte betalas i tid, bör myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

Utredningen föreslår att det ska införas en bestämmelse som innebär att ett beslut om sanktionsavgift ska få verkställas enligt utsökningsbalken. Genom en lagändring som trädde i kraft den 1 september 2022 får de aktuella besluten med stöd av 3 kap. 1 § första stycket 6 a utsökningsbalken verkställas enligt samma balk även utan en sådan bestämmelse som utredningen föreslår (prop. 2021/22:206). Utredningens förslag i denna del bör därför inte genomföras.

Som utredningen bedömer bör möjligheten att kräva in en beslutad sanktionsavgift falla bort i den utsträckning som verkställighet inte har skett inom fem år från det att beslutet fick laga kraft. Kravet att ett beslut om sanktionsavgift ska delges innebär att beslutet får laga kraft tre veckor efter det att den avgiftsskyldige har delgetts beslutet.

Dubbelbestraffningsförbudet och hinder mot beslut om sanktionsavgift

Enligt Europakonventionen och Europeiska unionens stadga om de grundläggande rättigheterna får ingen lagföras eller straffas på nytt i en brottmålsrättegång i samma stat för ett brott för vilket han redan blivit frikänd eller dömd i enlighet med lagen och rättegångsordningen i denna stat (dubbelbestraffningsförbudet).

Som har konstaterats i flera lagstiftningsärenden får straff, i den mening som avses i Europakonventionen, anses omfatta vite. Om ett vite har dömts ut, bör det därför inte vara möjligt att besluta om en sanktion, varken administrativ eller straffrättslig, för samma sak. Den avgörande tidpunkten för när sådant hinder uppkommer bör vara när det inleds en domstolsprocess angående frågan om att döma ut vite. Ett föreläggande om vite bör därför inte hindra ett senare ingripande med sanktionsavgift så länge som en myndighet inte har ansökt om utdömande av vitet. När tillsynsmyndigheten har ansökt om att vitet ska dömas ut bör myndigheten dock vara förhindrad att besluta om en sanktionsavgift för en överträdelse som omfattas av vitesföreläggandet. En bestämmelse om detta bör tas in i den nya lagen.

I artikel 35 i NIS 2-direktivet finns reglering om överträdelser som innebär personuppgiftsincidenter. Enligt artikel 35.1 finns en skyldighet för behöriga myndigheter att under vissa förhållanden och utan onödigt

dröjsmål informera tillsynsmyndigheter enligt EU:s dataskyddsförordning om överträdelser som kan innebära en personuppgiftsincident. I artikel 35.2 anges att de behöriga myndigheterna inte ska ta ut en sanktionsavgift om en sådan har tagits ut av en tillsynsmyndighet enligt EU:s dataskyddsförordning för en sådan överträdelse som avses i artikel 35.1 och som följer av samma beteende som den administrativa sanktionsavgiften avsåg enligt dataskyddsförordningen.

Utredningen föreslår att det ska införas en bestämmelse i den nya lagen om att en sanktionsavgift inte ska få tas ut om överträdelsen har lett till att verksamhetsutövaren har påförts en sanktionsavgift enligt EU:s dataskyddsförordning. Det behöver dock, som *Livsmedelsverket* nämner, inte regleras särskilt att en sanktionsavgift inte får tas ut av verksamhetsutövaren om en sådan har tagits ut enligt ett annat regelverk för samma överträdelse. Detta gäller oavsett vilket regelverk som det rör sig om eftersom det följer av dubbelbestraffningsförbudet. Mot denna bakgrund bör det inte införas en sådan bestämmelse som utredningen föreslår och inte heller sådana som föreslås av *PTS* och *Tre*. *Tech Sverige* anför att det måste säkerställas att sanktionsavgifter inte kan tas ut flera gånger enligt olika regelverk för samma överträdelse. Detta får säkerställas genom samverkan och i rättstillämpningen.

8.8 Anmärkning

Regeringens förslag: Om tillsynsmyndigheten inte finner skäl att ingripa mot en överträdelse på något annat sätt, ska den meddela verksamhetsutövaren en anmärkning.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Naturvårdsverket* anser att det är oklart vad som avses med en anmärkning. *Telenor Sverige AB (Telenor)* lyfter fram att en anmärkning kan få negativa effekter för en verksamhetsutövare och anser att det bör tydliggöras att det inte är obligatoriskt att meddela en anmärkning om inget annat ingripande görs. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: Enligt artiklarna 32.4 a och 33.4 a i NIS 2-direktivet ska medlemsstaterna säkerställa att deras behöriga myndigheter, när de utövar sina befogenheter med avseende på efterlevnadskontroll, åtminstone har befogenhet att utfärda varningar om berörda entiteters överträdelser av direktivet.

Det saknas bestämmelser om varningar i NIS-lagen. Utredningen anger att en ingripandeåtgärd i form av en varning kan vara av värde exempelvis när en överträdelse inte bedöms vara av sådan art eller svårighetsgrad att något annan slags ingripande bör komma i fråga. Varning som ingripande förekommer, som utredningen anger, inom andra delar av svensk rätt, ofta med den alternativa möjligheten att meddela en anmärkning (se exempelvis 15 kap. 1 § andra stycket lagen om bank- och finansieringsrörelse och 25 kap. 1 § lagen om värdepappersmarknaden). *Naturvårdsverket* anser att det är oklart vad som avses med en anmärkning. Bestämmelser om anmärkningar fanns dock till exempel i lagen (2005:405) om försäkringsförmedling och finns i lagen (2018:1219) om

försäkringsdistribution. Regeringen anser, liksom utredningen, att regleringen om varning i NIS 2-direktivet har likheter med hur anmärkning används inom nationell rätt och att uttrycket anmärkning bör användas i den nya lagen. Åtgärden bör kunna riktas mot såväl offentliga som enskilda verksamhetsutövare.

Telenor anser att det bör tydliggöras att det inte är obligatoriskt att meddela en anmärkning om inget annat ingripande görs. En anmärkning bör meddelas om något annat ingripande inte görs, givet att tillsynsmyndigheten inte väljer att helt avstå från ett ingripande (jfr avsnitt 8.3). En överträdelse av de skyldigheter som anges i avsnitt 8.2 bör i princip alltid leda till ett ingripande, men valet av åtgärd avgörs av hur allvarlig överträdelsen är. Anmärkning utgör den lindrigaste åtgärden.

8.9 Ingen reglering om övervakningsansvariga

Regeringens bedömning: Det behöver inte införas någon särskild reglering för att en tillsynsmyndighet ska kunna utse en övervakningsansvarig.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Länsstyrelsen i Stockholms län* anför att det är otydligt vad den övervakningsansvariges uppgifter innebär i praktiken och att detta bör förtydligas. *Sveriges advokatsamfund* anför att direktivet kan tolkas som att den övervakningsansvarige ska finnas hos verksamhetsutövaren i stället för hos tillsynsmyndigheten och att utredningen inte har klarlagt vilka krav som bör ställas på en övervakningsansvarig, exempelvis i fråga om certifiering. Övriga remissinstanser yttrar sig inte särskilt över bedömningen.

Skälen för regeringens bedömning: Enligt artikel 32.4 g i NIS 2-direktivet ska medlemsstaterna säkerställa att de behöriga myndigheterna, när de utövar sina befogenheter med avseende på efterlevnadskontroll gentemot väsentliga entiteter, åtminstone har befogenhet att utse en övervakningsansvarig med väldefinierade uppgifter för en fastställd tidsperiod för att övervaka att de berörda entiteterna efterlever artiklarna 21 och 23 som handlar om riskhanteringsåtgärder och rapporteringsskyldighet.

Regeringen kan, utifrån hur artikel 32.4 g har formulerats, inte se att den skulle ha den innebörden som *Sveriges advokatsamfund* lyfter fram som ett alternativ. Regeringen instämmer i utredningens uppfattning att det inte krävs någon särskild reglering för att tillsynsmyndigheten ska kunna utse en sådan övervakningsansvarig som artikeln avser. Vilka särskilda uppgifter den ansvarige ska ha kopplat till tillsynen får avgöras av tillsynsmyndigheten. Detta behöver inte, som *Länsstyrelsen i Stockholms län* hävdar, förtydligas i denna lagrådsremiss.

8.10 Ingen särskild reglering om tillfälligt upphävande av auktorisation eller certifiering

Regeringens bedömning: Det bör inte införas någon särskild reglering om möjlighet till tillfälligt upphävande av en väsentlig verksamhetsutövares auktorisation eller certifiering.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Advokatfirman Kahn Pedersen* delar utredningens uppfattning att ett tillfälligt upphävande av auktorisation eller certifiering är en mycket långtgående sanktion, men anser att det kan ifrågasättas om direktivets krav är uppfyllt i detta avseende. *Försvarets materielverk (FMV)* gör samma bedömning som utredningen, men föreslår att tillsynsmyndigheten ska kunna uppmärksamma ett certifieringsorgan och/eller den nationella myndigheten för cybersäkerhetscertifiering på förhållanden som kan innebära att förutsättningarna för ett giltigt certifikat eller bemyndigande inte längre är uppfyllda. Enligt *Transportstyrelsen* borde utredningen åtminstone ha övervägt att införa certifikat för verksamhet som uppfyller kraven enligt NIS 2-direktivet och som då även hade kunnat upphävas tillfälligt under vissa omständigheter. Övriga remissinstanser yttrar sig inte särskilt över bedömningen.

Skälen för regeringens bedömning: Om efterlevnadskontrollåtgärder som antas enligt artikel 32.4 a–d och f avseende väsentliga entiteter är ineffektiva ska medlemsstaterna enligt artikel 32.5 i NIS 2-direktivet säkerställa att deras behöriga myndigheter har befogenhet att fastställa en tidsfrist inom vilken en väsentlig entitet ska vidta nödvändiga åtgärder för att avhjälpa bristerna eller uppfylla dessa myndigheters krav. Om de begärda åtgärderna inte vidtas inom den fastställda tidsfristen ska medlemsstaterna säkerställa att de behöriga myndigheterna har befogenhet att tillfälligt upphäva eller begära att ett certifierings- eller auktorisationsorgan, eller en domstol, i enlighet med nationell rätt, tillfälligt upphäver en certifiering eller auktorisation för en del av eller alla relevanta tjänster som tillhandahålls eller verksamheter som utövas av den väsentliga entiteten. Det sistnämnda följer av artikel 32.5 a i direktivet.

Enligt skäl 133 bör bland annat tillfälliga upphävanden, med tanke på deras stränghet och påverkan på entiteternas verksamheter och i sista hand på användarna, endast tillämpas proportionellt mot överträdelsens allvarlighetsgrad och med beaktande av omständigheterna i varje enskilt fall, inbegripet om överträdelsen var avsiktlig eller berodde på försumlighet, samt åtgärder som vidtagits för att förhindra eller begränsa de materiella eller immateriella skadorna.

I skälet anges vidare att bland annat tillfälliga upphävanden endast bör tillämpas som sista utväg, det vill säga först efter det att de andra relevanta åtgärder för efterlevnadskontroll som fastställs i direktivet har uttömts, och endast fram till dess att den berörda entiteten vidtar nödvändiga åtgärder för att avhjälpa de brister eller uppfylla de krav från den behöriga myndigheten för vilka de tillfälliga upphävandena tillämpades. Införandet av bland annat tillfälliga upphävanden bör vidare omfattas av lämpliga rättssäkerhetsgarantier i enlighet med de allmänna principerna i unions-

rätten och stadgan, inbegripet rätten till ett effektivt rättsmedel och till en opartisk domstol, oskuldspresumtion och rätten till försvar.

Det framgår inte av artikel 32.5 a vilka certifieringar eller auktorisationer som avses. Enligt utredningen kan åtminstone två tolkningar göras i detta avseende. Enligt en tolkning kan det anses röra sig om möjligheten att upphäva ett tillstånd att bedriva verksamhet som faller in under direktivets tillämpningsområde. Utredningen bedömer att det inte bör införas något generellt tillståndskrav för att bedriva sådan verksamhet som lagen avser och därmed inte heller någon möjlighet att tillfälligt upphäva ett sådant.

Utredningen anger att artikeln också till exempel kan anses ta sikte på certifieringar och auktorisationer som kan vara av betydelse för att uppnå en hög gemensam cybersäkerhetsnivå inom EU. Det bör då enligt utredningen röra sig om certifiering kopplad till lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering enligt vilken Post- och telestyrelsen (PTS) får meddela föreskrifter som kan innebära till exempel krav på certifiering och cybersäkerhetscertifikat som utfärdas av FMV med stöd av lagen (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

Utredningen redogör för skillnaderna mellan vilka möjligheter som nämnda regelverk innebär när det gäller upphävande av certifieringar jämfört med vad som krävs enligt artikel 32.5 i NIS 2-direktivet. Utredningen bedömer att regelverkens systematik inte motsvarar vad som krävs enligt artikeln men anser samtidigt att kopplingen mellan regelverken och NIS 2-direktivet inte är tillräcklig för att föreslå ändringar. Slutligen anger utredningen att den inte har kunnat identifiera några andra certifieringar eller auktorisationer som skulle kunna komma i fråga att angripa med aktuell slags sanktion. Mot denna bakgrund saknas det enligt utredningen tillräckligt underlag för att föreslå att sanktionen ska genomföras i svensk rätt.

Advokatfirman Kahn Pedersen ifrågasätter om de krav som direktivet ställer upp i artikel 32.5 är uppfyllda. Regeringen instämmer i utredningens uppfattning att NIS 2-direktivet inte kan anses ställa krav på att en verksamhetsutövare ska beviljas tillstånd för att få bedriva den verksamhet som gör att de träffas av direktivet. Det bör därför, även med beaktande av *Transportstyrelsens* synpunkter, inte införas något sådant krav i den nya lagen och därmed inte heller någon möjlighet att tillfälligt upphäva ett sådant tillstånd.

När det gäller certifieringar som meddelas inom de ramverk där PTS respektive FMV är ansvariga myndigheter, och som nämns ovan, konstaterar regeringen att det finns möjligheter att upphäva sådana med stöd av befintlig reglering. Visserligen kan certifieringar som meddelas inom de ramverk där PTS är ansvarig myndighet endast upphävas permanent, men regeringen konstaterar att detta innebär en strängare reglering än vad direktivet, som är ett minimidirektiv, kräver.

Certifieringarna kan inte, utan en ändring av regleringen, upphävas av en tillsynsmyndighet enligt den nya lagen med hänvisning till denna funktion. Som *FMV* resonerar om i relation till cybersäkerhetscertifikat kan dock en tillsynsmyndighet uppmärksamma ansvarig myndighet på åtgärder som bör föranleda en återkallelse. Myndigheterna har därmed sådan rätt att begära ett upphävande som nämns i artikeln. Det konstateras,

trots att förslaget inte är föremål för behandling i denna lagrådsremiss, att PTS föreslås pekas ut som tillsynsmyndighet i förordning av utredningen.

Det bör beaktas att artikel 32.5 endast tar sikte på en situation då övriga ingripandeåtgärder är otillräckliga och enbart om verksamhetsutövaren inte vidtar begärda åtgärder inom en fastställd tidsfrist. Regeringen bedömer att den senare situationen endast bör uppstå i mycket sällsynta fall givet hur övriga ingripandeåtgärder föreslås utformas. Det finns dessutom förutsättningar för att upphäva de certifieringar som har meddelats inom de ramverk där PTS respektive FMV är ansvariga myndigheter. Regeringen bedömer, i likhet med utredningen, att det inte finns andra certifieringar eller auktorisationer som bör komma i fråga att angripa med aktuell slags sanktion. Regeringen kan därmed inte se att det behöver införas någon särskild reglering om möjlighet att tillfälligt upphäva en väsentlig verksamhetsutövares auktorisation eller certifiering som har meddelats med stöd av något annat regelverk. Det behöver därför inte införas någon särskild reglering för att genomföra artikel 32.5 i nationell rätt.

9 Överklagande

Regeringens förslag: Tillsynsmyndighetens beslut enligt lagen ska få överklagas till allmän förvaltningsdomstol.

Tillsynsmyndigheten ska vid ett överklagande vara motpart i domstolen.

Det ska krävas prövningstillstånd vid överklagande till kammarrätten.

Utredningens förslag överensstämmer i allt väsentligt med regeringens. Utredningen föreslår att även tillsynsmyndighetens beslut enligt anslutande föreskrifter ska få överklagas till allmän förvaltningsdomstol.

Remissinstanserna: *Förvaltningsrätten i Malmö* tillstyrker förslaget. *Kammarrätten i Stockholm* påpekar att det vid överklagande av beslut enligt LEK är Kammarrätten i Stockholm som är sista instans, men att utredningens förslag innebär att beslut kommer att kunna överklagas till Högsta förvaltningsdomstolen. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag

Rätten att överklaga beslut

Enligt 40 § förvaltningslagen överklagas beslut till allmän förvaltningsdomstol och prövningstillstånd krävs vid överklagande till kammarrätten. Enligt 41 § samma lag får ett beslut överklagas om det kan antas påverka någons situation på ett inte obetydligt 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 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.

Artikel 6 i Europakonventionen ställer 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.

Överklagandemöjligheter enligt den nya lagen

En tillsynsmyndighets beslut enligt lagen 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 NIS-lagen.

Rätten till överklagande bör gälla för både offentliga och enskilda verksamhetsutövare. Tillsynsmyndigheten bör i båda fallen vara motpart till klaganden och detta bör anges i den nya lagen eftersom det av 7 a § förvaltningsprocesslagen endast regleras vem som är motpart vid överklagande av enskilda.

Förvaltningsrättens avgörande bör kunna överklagas till behörig kammarrätt. Prövningstillstånd bör krävas vid sådant överklagande. Att domstolens beslut om förbud att inneha ledningsfunktion går att överklaga följer av 33 § förvaltningsprocesslagen och behöver inte anges särskilt i lagen. Kravet på prövningstillstånd bör inte omfatta överklagande av sådana beslut.

Regeringen föreslås i avsnitt 5.3.2 och 5.3.4, om det finns särskilda skäl, få fatta beslut om undantag i enskilda fall från skyldigheterna enligt lagen för vissa partnerföretag och anknutna företag och enskilda utbildningsanordnare med tillstånd att utfärda examina. Regeringens beslut kan bli föremål för rättsprövning enligt lagen (2006:304) om rättsprövning av vissa regeringsbeslut, om beslutet innefattar en prövning av enskildas civila rättigheter och skyldigheter enligt artikel 6 i Europakonventionen. Därigenom tillgodoses de krav på domstolsprövning som följer av artikel 6 i konventionen.

I avsnitt 11 föreslår regeringen bland annat att bestämmelser i LEK om skyldigheter för vissa aktörer ska upphävas. Som *Kammarrätten i Stockholm* påpekar innebär förslaget att dessa beslut enligt den nya lagen kommer att kunna överklagas till Högsta förvaltningsdomstolen.

10 Register för uppgifter om domännamnsregistrering

Regeringens förslag: En registreringsenhet för toppdomäner eller en verksamhetsutövare som erbjuder domännamnsregistreringstjänster som omfattas av lagen, men inte av lagen om nationella toppdomäner för Sverige på internet (toppdomänlagen), ska föra ett register över tilldelade domännamn under toppdomänen och löpande upprätta säkerhetskopior av registeruppgifterna.

Registret ska innehålla

1. domännamnet,
2. namnet på domännamnsinnehavaren och dennes telefonnummer och e-postadress,
3. namnet på den som tekniskt administrerar domännamnet och dennes telefonnummer och e-postadress, och
4. registreringsdatum.

Uttrycket registreringsenhet för toppdomäner ska i lagen avse en verksamhetsutövare som har delegerats en specifik toppdomän och som ansvarar för administrationen av den, dock inte om toppdomänen endast används för registreringsenhetens eget bruk.

Uppgifter ur registret ska kunna hämtas utan avgift via internet. Personuppgifter ska endast få göras tillgängliga på internet om den registrerade har samtyckt till det. Verksamhetsutövaren ska vara personuppgiftsansvarig för behandling av personuppgifter i registret.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om registret.

Den som är domänadministratör enligt toppdomänlagen ska också föra in registreringsdatum i det register som förs enligt den lagen. Uppgift om postadress ska dock inte längre föras in i registret.

Uppgifter ur registren ska på begäran lämnas ut skyndsamt och senast 72 timmar från mottagandet av begäran till den som gör en lagligen grundad och motiverad begäran.

Tillsynsmyndigheten ska få besluta de förelägganden som behövs för att verksamhetsutövare ska fullgöra skyldigheterna att föra register över domännamn och tillhandahålla uppgifter enligt den nya lagen eller föreskrifter som har meddelats i anslutning till lagen. Ett föreläggande får förenas med vite. Ett vitesföreläggande ska även få riktas mot staten.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen lämnar förslag som innebär att skyldigheten att föra register i enlighet med NIS 2-direktivet ska regleras enbart i lagen (2006:24) om nationella toppdomäner för Sverige på internet (toppdomänlagen). Utredningen föreslår att uttrycket domänadministratör i toppdomänlagen ska användas för att beteckna alla som omfattas av skyldigheten att föra register i stället för uttrycket registreringsenhet för toppdomäner och föreslår en annan definition av uttrycket än regeringen. Utredningen föreslår inte att verksamhetsutövare som erbjuder domännamnsregistreringstjänster ska omfattas av skyldigheten att föra register. Utredningen lämnar inget förslag om en bortre tidsgräns för utlämnande av uppgifter. Utredningen föreslår inget bemyndigande i den nya lagen. Utredningen

föreslår att uttrycket domännamnsregistreringstjänst ska definieras som registrar eller annan verksamhetsutövare som verkar som ombud eller återförsäljare av domännamn. Utredningen föreslår att registeruppgifter ska lämnas ut på begäran till myndigheter och andra med offentligrättsliga uppgifter inom EES. Utredningen föreslår inte att begäran ska vara lagligen grundad och motiverad. Utredningen föreslår inte att uppgift om postadress ska utgå i uppräkningen av uppgifter som ska finnas i registret som ska föras enligt toppdomänlagen. Utredningen föreslår också vissa följdändringar i toppdomänlagen.

Remissinstanserna: Majoriteten av remissinstanserna tillstyrker eller har inga synpunkter på förslaget. Bland andra *Post- och telestyrelsen (PTS)* påtalar att utredningens förslag till definition av ”domänadministratör” skiljer sig åt från definitionen av ”registreringsenhet för toppdomäner” i NIS 2-direktivet. PTS och *Stiftelsen för internetinfrastruktur (Internetstiftelsen)* anser att kravet på huvudsakligt etableringsställe bör knytas till domänadministratören i stället för till toppdomänen. Internetstiftelsen anser också att utredningens förslag innebär att det finns risk för överlappande skyldigheter. Därutöver anmärker Internetstiftelsen att en skillnad mellan registreringsskyldigheten i toppdomänlagen och artikel 28 i direktivet är att artikeln inte kräver insamling av postadress. Internetstiftelsen, som anlägger ett integritets- och dataminimeringsperspektiv, föreslår att postadress utgår i toppdomänlagen eftersom det skulle bidra till likvärdig konkurrens på den europeiska marknaden. Både Internetstiftelsen och PTS anser att även entiteter som erbjuder domännamnsregistreringstjänster bör omfattas av regleringen.

Internetstiftelsen bedömer att uttrycket legitima åtkomstsökande har getts en för vid och oprecis definition. Det bör enligt Internetstiftelsen bland annat framgå tydligt att en begäran från legitima åtkomstsökande ska vara lagligen motiverad för varje specifik domäns registreringsdata som förfrågan avser och följa gällande dataskyddsregler. Internetstiftelsen delar utredningens uppfattning att rätten att begära ut uppgifter inte bör utsträckas till privatpersoner. *Rättighetsalliansen* menar att aktörer som inte utgör myndigheter eller som inte har offentligrättsliga uppgifter inom EES bör omfattas av möjligheten att begära ut uppgifter ur registret när exempelvis immaterialrättsliga intrång har förekommit. Bland andra *Svenskt Näringsliv* avstyrker den från direktivet avvikande begränsningen som innebär att endast myndigheter och andra med offentligrättsliga uppgifter anses vara legitima åtkomstsökande.

Integritetsskyddsmyndigheten (IMY) yttrar sig om personuppgiftsbehandlingen. IMY ser positivt på att uppgiftsskyldigheten tydliggörs i lag eftersom, som utredningen påpekar, dataskyddsregleringen gäller vid hanteringen. Det bör dock, enligt myndigheten, övervägas att närmare beskriva den behandling som kan bli aktuell och konsekvenserna av den för de registrerade. Det bör exempelvis, enligt myndigheten, övervägas att lämna anvisningar till stöd för den närmare regleringen i föreskrifter om uppgiftsskyldigheten. I dessa bör det tydliggöras att EU-domstolen har betonat att när ett utlämnande av personuppgifter inte direkt grundar sig på den rättsliga bestämmelse som utgör stöd för utlämnandet, utan följer av en begäran från den behöriga myndigheten, måste det särskilda ändamålet med insamlingen av personuppgifterna – mot bakgrund av den aktuella uppgiften av allmänt intresse eller den aktuella myndighetsutöv-

ningen – framgå av begäran, så att den som begäran riktar sig till ska kunna försäkra sig om att överföringen av uppgifterna är laglig och för att lagenligheten ska kunna kontrolleras av domstolarna.

Skälen för regeringens förslag

Regleringen i NIS 2-direktivet

Att upprätthålla korrekta och fullständiga databaser med registreringsuppgifter för domännamn, så kallade WHOIS-data, och ge laglig åtkomst till sådana uppgifter är enligt NIS 2-direktivet avgörande för att säkerställa domännamnssystemets säkerhet, stabilitet och resiliens, vilket i sin tur bidrar till en hög gemensam nivå av cybersäkerhet i hela unionen (skäl 109). För detta specifika ändamål bör enligt direktivet registreringsenheter för toppdomäner och de entiteter som erbjuder domännamnsregistreringstjänster vara skyldiga att behandla vissa uppgifter som är nödvändiga för detta.

I artikel 28.1 och 28.2 i NIS 2-direktivet anges att medlemsstaterna ska ålägga registreringsenheter för toppdomäner och ”enheter” som tillhandahåller domännamnsregistreringstjänster att samla in och upprätthålla korrekta och fullständiga registreringsuppgifter för domännamn i en särskild databas. I den engelska och franska versionen av direktivet används uttryck som på svenska motsvarar ”entiteter” i stället för ”enheter”. Enheter i artikeln bör därmed ta sikte på entiteter som i avsnitt 5.3.1 föreslås benämnas verksamhetsutövare i den nya lagen.

Databasen med registreringsuppgifter för domännamn ska enligt artikel 28.2 innehålla information om domännamn, registreringsdatum, registrantens namn, e-postadress och telefonnummer samt e-postadress och telefonnummer till den kontaktpunkt som administrerar domännamnet om dessa inte är desamma som för registranten. Vidare ska medlemsstaterna enligt artikel 28.4 ålägga registreringsenheter för toppdomäner och entiteter som tillhandahåller domännamnsregistreringstjänster att utan onödigt dröjsmål efter registreringen offentliggöra registreringsuppgifter som inte är personuppgifter. Enligt artikel 28.5 ska medlemsstaterna ålägga registreringsenheterna och entiteterna att ge åtkomst till specifika registreringsuppgifter på lagliga och vederbörligen motiverade begäranden från legitima åtkomstsökande, i enlighet med unionens dataskyddslagstiftning. Svar på en sådan begäran ska lämnas skyndsamt och under alla omständigheter inom 72 timmar.

Legitima åtkomstsökande bör enligt skäl 110 tolkas som varje fysisk eller juridisk person som gör en begäran i enlighet med unionsrätten eller nationell rätt, vilket kan inbegripa myndigheter som är behöriga enligt direktivet och sådana som enligt unionsrätten eller nationell rätt är behöriga i fråga om förebyggande, utredning, upptäckt eller lagföring av brott, samt ”Cert” eller CSIRT-enheter.

”Registreringsenhet för toppdomäner” och ”entitet som erbjuder domännamnsregistreringstjänster” definieras i artikel 6.21 och 6.22. Enligt artikel 26.1 b ska sådana aktörer omfattas av jurisdiktionen i den medlemsstat där de har sitt huvudsakliga etableringsställe i unionen i enlighet med artikel 26.2 eller där de har en företrädare enligt artikel 26.3 (se vidare avsnitt 5.3.2).

Med ”registreringsenhet för toppdomäner” avses enligt direktivet en enhet som har delegerats en specifik toppdomän och som ansvarar för administrationen av toppdomänen, inbegripet registreringen av domännamn under toppdomänen och den tekniska driften av toppdomänen, inbegripet drift av dess namnservrar, underhåll av dess databaser och distribution av zonfiler för toppdomänen mellan namnservrar, oberoende av huruvida någon aspekt av denna drift utförs av enheten själv eller har utkontrakterats, dock inte situationer där toppdomäner används av en registreringsenhet endast för dess eget bruk. I den engelska språkversionen av direktivet är motsvarande uttryck ”top-level domain name registry”.

Med entitet som erbjuder domännamnsregistreringstjänster avses, enligt den svenska språkversionen av direktivet, en registrar som verkar på uppdrag av en ”regeringsenhet” eller ett ombud för en registreringsenhet, såsom återförsäljare och leverantörer av integritetsregistreringstjänster och proxyregistreringstjänster. I den engelska och franska språkversionen anger man dock närmast att det ska handla om en registrar eller ett ombud som agerar för en registrars räkning.

Toppdomänlagen

Toppdomänlagen gäller teknisk drift av nationella toppdomäner för Sverige på internet samt tilldelning och registrering av domännamn under dessa toppdomäner (1 §). I 6 § toppdomänlagen föreskrivs en skyldighet för domänadministratörer att föra register över tilldelade domännamn under toppdomänen och löpande upprätta säkerhetskopior av registeruppgifterna. Av paragrafens andra stycke framgår vilka uppgifter registret ska innehålla och i tredje stycket anges att uppgifterna i registret ska kunna hämtas utan avgift via internet. Med domänadministratör avses enligt 2 § den som ansvarar för administration av en nationell toppdomän för Sverige.

Syftet med toppdomänlagen är huvudsakligen att säkerställa att administrationen av den nationella toppdomänen utförs på ett säkert och effektivt sätt (se prop. 2004/04:175 s. 240 f.). Lagen ställer därför vissa krav på domänadministratörer som ansvarar för administrationen av en nationell toppdomän för Sverige. Enligt lagen får regeringen, under vissa förutsättningar, meddela föreskrifter om administrationen av en nationell toppdomän för Sverige vid bland annat krig eller krigsfara.

Sverige har endast en nationell toppdomän, .se-domänen, vilken hanteras av Internetstiftelsen. Internetstiftelsen hanterar även administration av toppdomänen .nu men har inte delegerats denna toppdomän. Sistnämnda domän har i stället delegerats den amerikanska stiftelsen IUSN Foundation. Internetstiftelsens administration av toppdomänen .nu omfattas inte av toppdomänlagens tillämpningsområde eftersom den inte är en nationell toppdomän för Sverige. Enligt definitionen i 2 § toppdomänlagen omfattar administration teknisk drift av en toppdomän samt tilldelning och registrering av domännamn under denna.

Av 3 § förordningen (2006:25) om nationella toppdomäner för Sverige på internet följer att PTS får meddela föreskrifter om bland annat register enligt toppdomänlagen.

Vilka som bör omfattas av skyldigheten att föra register och var skyldigheten bör regleras

Utredningen föreslår att skyldigheten enligt NIS 2-direktivet att föra register ska införas genom ändringar i toppdomänlagen, där en liknande skyldighet redan finns, men att endast de som i direktivet benämns som registreringsenheter för toppdomäner ska omfattas av skyldigheten. Vidare föreslår utredningen en ändring av definitionen av domänadministratör i toppdomänlagen. Utredningen föreslår inte att skyldigheten att föra register ska omfatta dem som i direktivet benämns som entiteter som erbjuder domännamnsregistreringstjänster. Regeringen anser, likt *Internetstiftelsen* och *PTS*, att utredningens förslag inte genomför direktivet fullt ut.

Som anges i avsnitt 5.3.2 bör den nya lagen bland annat omfatta registreringsenheter för toppdomäner och verksamhetsutövare som erbjuder domännamnsregistreringstjänster. För att omfattas av lagen krävs att sådana verksamhetsutövare har sitt huvudsakliga etableringsställe i Sverige eller en företrädare som är etablerad här. Vad som avses med huvudsakligt etableringsställe behandlas i avsnitt 5.3.2. Om verksamhetsutövaren tillhandahåller tjänster i Sverige, men inte är etablerad inom EES och inte heller har utsett någon företrädare inom EES, föreslås denne vara skyldig att utse en företrädare med etablering i Sverige eller i något annat land inom EES där tjänsterna erbjuds (se avsnitt 6.1).

Regeringen anser, till skillnad från utredningen, att det enligt direktivet krävs att både registreringsenheter för toppdomäner och verksamhetsutövare som erbjuder domännamnsregistreringstjänster omfattas av skyldigheten att föra register. Enligt regeringen bör de som omfattas av skyldigheten enligt den svenska regleringen motsvara dem som avses i direktivet.

Det bör i den nya lagen införas en definition av registreringsenhet för toppdomäner som i sak följer definitionen i artikel 6.21 i direktivet. Med uttrycket registreringsenhet för toppdomäner bör i den nya lagen avses en verksamhetsutövare som har delegerats en specifik toppdomän och som ansvarar för administrationen av den, dock inte om toppdomänen endast används för registreringsenhetens eget bruk. Regeringen anser således, till skillnad från vad utredningen redogör för, att en registreringsenhet både ska ha delegerats en toppdomän och ska ansvara för administrationen av den. Av definitionen i direktivet framgår att administration inbegriper registrering av domännamn under toppdomänen och den tekniska driften av toppdomänen samt att teknisk drift avser drift av toppdomänens namnservrar, underhåll av toppdomänens databaser och distribution av zonfiler för toppdomänen mellan namnservrar, oberoende av huruvida driften utförs av registreringsenheten själv eller om den har utkontrakterats. Även i svenska sammanhang används begreppet registry för den här typen av verksamhetsutövare.

En verksamhetsutövare som erbjuder domännamnsregistreringstjänster har avtalat med en registreringsenhet för toppdomäner att sälja domännamn under den toppdomänen. I svenska sammanhang används även begreppet registrar för den här typen av verksamhetsutövare. Utredningen föreslår att domännamnsregistreringstjänst ska definieras som registrar eller annan verksamhetsutövare som verkar som ombud eller återförsäljare av domännamn. Regeringen konstaterar att utredningens förslag till

definition, till skillnad från den som finns i artikel 6.22 i direktivet, innebär att tjänsten definieras utifrån vem som tillhandahåller den och att kretsen inte innehåller någon egentlig begränsning eftersom även ett ombud för en registrar nämns. Eftersom utredningens föreslagna definition inte ger någon närmare ledning i fråga om vilken tjänst som avses bör den inte införas i lagen. När uttrycket verksamhetsutövare som erbjuder domännamnsregistreringstjänst används i lagen bör det, i linje med vad som kommer till uttryck i direktivet, dock avse en registrar som verkar på uppdrag av en registreringsenhet för toppdomäner eller ett ombud för en sådan registreringsenhet, såsom återförsäljare och leverantör av integritetsregistreringstjänster och proxyregistreringstjänster.

Även den som är domänadministratör enligt toppdomänlagen omfattas av NIS 2-direktivets krav på att föra register. Med hänsyn till toppdomänlagens syfte, att säkerställa säker och effektiv administration av just nationella toppdomäner för Sverige, bedömer regeringen att det inte är lämpligt att genomföra direktivet genom enbart ändringar i toppdomänlagen som utredningen föreslår. Skyldigheten att föra register för andra än domänadministratörer enligt toppdomänlagen bör i stället regleras i den nya lagen. För den som är domänadministratör enligt toppdomänlagen bör skyldigheten att föra register även i fortsättningen följa av toppdomänlagen, med de ändringar som framgår nedan avseende bland annat vilka uppgifter som ska registreras. Det bör i den nya lagen tydliggöras att skyldigheten att föra register inte gäller för den som är domänadministratör enligt toppdomänlagen och att en sådan domänadministratör i stället omfattas av skyldigheten att föra register enligt toppdomänlagen.

Registrens innehåll och insamling av uppgifter

Vilka uppgifter som ett register enligt NIS 2-direktivet ska innehålla framgår av artikel 28.2. Det saknas skäl att frångå uppräkningen i direktivet när det gäller innehållet i registret enligt den nya lagen. Vad avser registret enligt toppdomänlagen, instämmer regeringen i utredningens uppfattning att innehållet i registret i allt väsentligt överensstämmer med uppräkningen i direktivet, med undantag för att direktivet även kräver att uppgift om registreringsdatum ska finnas i registret. Bestämmelsen i toppdomänlagen bör därför kompletteras med ett krav på att registret även ska innehålla uppgift om registreringsdatum. Som *Internetstiftelsen* anger finns det skäl att ta bort kravet i toppdomänlagen på att postadress ska registreras. Skyldigheten kommer att gälla för såväl de domänadministratörer som, både vid lagens ikraftträdande och därefter, för register enligt toppdomänlagen som för de verksamhetsutövare som ska föra register enligt den nya lagen. Registren ska innehålla registreringsdatum för samtliga registrerade domännamn.

Enligt artikel 28.6 i NIS 2-direktivet får fullgörandet av skyldigheterna enligt artikel 28.1–28.5 inte leda till dubblerad insamling av registreringsuppgifter för domännamn. Medlemsstaterna ska ålägga registreringsenheter för toppdomäner och entiteter som tillhandahåller domännamnsregistreringstjänster att samarbeta med varandra i detta syfte. Registreringsenheter för toppdomäner och verksamhetsutövare som tillhandahåller domännamnsregistreringstjänster har ett intresse av att samordna sig

gällande insamlingen av uppgifter och det bör, med hänsyn till deras förhållande till varandra, finnas naturliga förutsättningar för ett sådant samarbete. Skyldigheten att samarbeta i syfte att undvika dubblerad insamling av uppgifter behöver därför inte regleras särskilt.

I artikel 28.3 i NIS 2-direktivet anges att medlemsstaterna ska ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att ha strategier och förfaranden, inbegripet kontrollförfaranden, för att säkerställa att de databaser som avses i artikel 28.1 innehåller korrekt och fullständig information. Medlemsstaterna ska föreskriva att sådana strategier och förfaranden offentliggörs. Skyldigheten att samla in och offentliggöra uppgifterna i registret innebär även en skyldighet att tillse att uppgifterna är korrekta och fullständiga. Registreringsenheter för toppdomäner och verksamhetsutövare som tillhandahåller domännamnsregistreringstjänster har därför en skyldighet att ha strategier och förfaranden för att säkerställa detta och denna skyldighet behöver inte regleras särskilt. För att säkerställa tillgången till uppgifterna i registret bör det dock föreskrivas en skyldighet att löpande upprätta säkerhetskopior av registeruppgifterna.

Skyldighet att ge tillgång till uppgifter i registren

Vad gäller skyldigheten att ge tillgång till registeruppgifter är utredningens uppfattning att legitima åtkomstsökande, som nämns i artikel 28.5 i NIS 2-direktivet, bör anses omfatta myndigheter och andra aktörer med offentligrättsliga uppgifter inom EES. Utredningen föreslår att den närmare definitionen av personer med offentligrättsliga uppgifter ska följa av föreskrifter på lägre normgivningsnivå. Utredningen anger att det finns en möjlighet för PTS att meddela sådana föreskrifter med stöd av toppdomänlagen. Utredningen anser vidare att det inte krävs något förtydligande i lag rörande vilka aktörer som omfattas av uttrycket andra med offentligrättsliga uppgifter.

Rättighetsalliansen för fram att det finns anledning att utvidga kretsen av legitima åtkomstsökande. Av skäl 110 i direktivet framgår att legitima åtkomstsökande ska tolkas som varje fysisk eller juridisk person som gör en begäran i enlighet med unionsrätten eller nationell rätt. Mot den bakgrunden anser regeringen att den av utredningen föreslagna kretsen riskerar att vara för snäv för att uppfylla syftet med bestämmelserna om tillgång till uppgifter i registret. Även andra aktörer än myndigheter och andra med offentligrättsliga uppgifter inom EES bör därför anses vara legitima åtkomstsökande. Till skillnad från *Internetstiftelsen* anser regeringen att rätten att begära ut uppgifter även bör tillkomma privatpersoner. Rätten att få del av uppgifter bör däremot endast avse sådana legitima krav som kan framställas med stöd av unionsrätten eller nationell rätt. En sökande bör alltså ha lagstöd eller en lagligen grundad rätt att få ta del av uppgifter för att begäran ska kunna beviljas. I likhet med vad Internetstiftelsen påpekar, och med hänsyn till att kretsen utvidgas, bör det förtydligas i lagtexten att en begäran måste vara lagligen grundad och motiverad. En begäran kan vara grundad på en bestämmelse som ger rätt att få del av uppgifter eller ett beslut meddelat av domstol, som ett editionsbeslut meddelat i en civilrättslig tvist mellan enskilda parter. Att begäran ska vara lagligen grundad innebär, vilket Internet-

stiftelsen framhåller, att den ska vara förenlig med gällande dataskydds-lagstiftning. Det är åtkomstsökanden som måste visa stöd för sin begäran i förhållande till varje specifik domäns registreringsdata. Utifrån ansökan får verksamhetsutövaren som för register göra en bedömning i det enskilda fallet.

En begäran om registeruppgifter från en legitim åtkomstsökande ska besvaras skyndsamt. Med skyndsamt avses att begäran ska besvaras utan onödigt dröjsmål. Regeringen instämmer i utredningens bedömning att frågan om hur som uppgiftsskyldigheten ska fullgöras bör regleras på annan föreskriftsnivå än i lag. Det bör dock framgå av lagen att 72 timmar gäller som en bortre tidsgräns för svar. Regeringen eller den myndighet som regeringen bestämmer bör, i enlighet med vad som gäller enligt toppdomänlagen, få meddela föreskrifter om registret enligt den nya lagen och bland annat de närmare kraven på hur en begäran om uppgifter ska utformas. Med stöd av föreslagen föreskriftsrätt bör regeringen eller den myndighet som regeringen bestämmer också bland annat kunna meddela närmare reglering gällande strategier och förfaranden för korrekt och fullständig information i och för utlämnande av uppgifter ur registret (se artikel 28.3 och 28.4 i NIS 2-direktivet).

Det bör, med hänvisning till artikel 28.5, framgå att personuppgifter endast ska få göras tillgängliga på internet om den registrerade har samtyckt till det. Verksamhetsutövaren som för register enligt den nya lagen ska vara personuppgiftsansvarig för behandling av personuppgifter i registret. Denna ordning överensstämmer också med regleringen i toppdomänlagen.

Skyldigheten för domänadministratörer enligt toppdomänlagen att lämna ut uppgifter ur registret enligt den lagen och inom vilken tid utlämnandet ska ske bör regleras i toppdomänlagen på samma sätt som i den nya lagen.

Personuppgiftsbehandlingen

IMY bedömer att det finns anledning att närmare beskriva den personuppgiftsbehandling som kan bli aktuell med stöd av uppgiftsskyldigheten och konsekvenserna av den för de registrerade. Det bör också exempelvis, enligt myndigheten, göras uttalanden som ger ledning i framtagandet av föreskrifter.

Vilka slags personuppgifter som registren enligt den nya lagen och toppdomänlagen föreslås innehålla, vilka aktörer som kommer att behandla dessa i registret och vad som är ändamålet med behandlingen redovisas ovan. Som utvecklas i avsnitt 12 fastslås, i artikel 2.14 i NIS 2-direktivet, att bland annat entiteter ska behandla personuppgifter i den utsträckning som krävs för tillämpningen av direktivet och i enlighet med EU:s dataskyddsförordning. I synnerhet ska sådan behandling, enligt samma artikel, baseras på artikel 6 i EU:s dataskyddsförordning. Den rättsliga grunden för den personuppgiftsbehandling som sker hos verksamhetsutövaren är att behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som följer av lag i enlighet med artikel 6.1 c i EU:s dataskyddsförordning och 2 kap. 1 § dataskyddslagen.

Uppgifterna föreslås kunna hämtas via internet men personuppgifter ska enligt förslaget få göras tillgängliga på internet endast om den registrerade

har samtyckt till det (jfr 6.1 a i EU:s dataskyddsförordning). Uppgifter ur registren föreslås på begäran också lämnas ut till den som gör en lagligen grundad och motiverad begäran. Med stöd av föreslagen föreskriftsrätt bör regeringen eller den myndighet som regeringen bestämmer bland annat kunna meddela närmare reglering gällande utlämnande av uppgifter ur registret. Som IMY nämner finns det avgöranden från EU-domstolen som bör beaktas vid framtagandet av föreskrifter (se till exempel EU-domstolens dom den 24 februari 2022, Valsts ieņēmumu dienests, C-175/20, EU:C:2022:124). Eftersom frågan om föreskrifternas utformning inte är föremål för denna lagrådsremiss anser regeringen dock inte att det bör göras sådana förtydliganden som IMY efterfrågar. Den som tar del av uppgifterna ur registret ansvarar för att det finns stöd för dennes personuppgiftsbehandling utifrån EU:s dataskyddsförordning och dataskyddslagen. Detta får avgöras av den personuppgiftsansvarige i varje enskilt fall utifrån befintlig reglering.

Tillsynsmyndigheten bör kunna besluta om förelägganden

Enligt 12 § toppdomänlagen får tillsynsmyndigheten meddela de förelägganden som behövs för efterlevnad av lagen eller föreskrifter som meddelats med stöd av lagen. Ett beslut om föreläggande får förenas med vite. Utredningens förslag om att skyldigheten att föra register över domännamn enligt NIS 2-direktivet helt ska regleras i toppdomänlagen innebär därmed att tillsynsmyndigheten skulle kunna besluta om förelägganden vid äventyr av vite om skyldigheten att föra register inte uppfylls, men inte ingripa på något annat sätt.

Regeringens förslag innebär att skyldigheten att föra register regleras i toppdomänlagen för den som omfattas av den lagen och i den nya lagen för den som i annat fall är en registreringsenhet för toppdomäner eller en verksamhetsutövare som erbjuder domännamnsregistreringstjänster enligt den nya lagen. Enligt regeringen bör tillsynsmyndighetens möjlighet att ingripa mot en verksamhetsutövare som inte uppfyller skyldigheten att föra register vara densamma enligt toppdomänlagen och den nya lagen.

Som redogörs för i avsnitt 8 sker ingripande i övrigt enligt den nya lagen genom beslut om föreläggande, ansökan om förbud att inneha ledningsfunktion, beslut om sanktionsavgift eller genom anmärkning. I vissa fall får tillsynsmyndigheten avstå från ingripande. Eftersom skyldigheten att föra register endast träffar vissa utpekade verksamhetsutövare och skyldigheten dessutom inte är nära kopplad till direktivets centrala skyldigheter rörande incidentrapportering och säkerhetsåtgärder, anser regeringen att det är tillräckligt att tillsynsmyndigheten kan ingripa mot överträdelser av skyldigheten att föra register, inklusive skyldigheten att tillgängliggöra uppgifterna, med föreläggande vid äventyr av vite. Det bör därför införas en bestämmelse i den nya lagen om att tillsynsmyndigheten får besluta de förelägganden som behövs för att verksamhetsutövare ska fullgöra skyldigheten. Ett föreläggande bör få förenas med vite. Ett sådant bör, som framgår av resonemanget i avsnitt 7.2.1 även få riktas mot staten.

11 Ändringar i lagen om elektronisk kommunikation (LEK)

Regeringens förslag: Bestämmelserna i lagen om elektronisk kommunikation om skyldighet för den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst att vidta åtgärder för att hantera risker som hotar säkerheten i nät och tjänster, låta utföra säkerhetsgranskning samt rapportera och informera om vissa säkerhetsincidenter ska upphävas.

Det ska tas in en upplysningsbestämmelse i den lagen om att det finns bestämmelser i den nya lagen om säkerhetsåtgärder, säkerhetsrevision, incidentrapportering och informationsskyldighet.

Nödvändiga följdändringar ska också genomföras i lagen.

Utredningens förslag överensstämmer i allt väsentligt med regeringens. Utredningen föreslår inte att det ska införas en upplysningsbestämmelse i LEK.

Remissinstanserna: *Hi3G Access AB (Tre)* poängterar att det är viktigt att föreskrifter med koppling till den nya lagen utformas i överensstämmelse med de bestämmelser som gäller i dag för telekomsektorn och som reglerar både informations- och driftsäkerhet. Tre har också synpunkter på utredningens förslag till förordning och bland annat frågan om vilken myndighet som ska ges föreskriftsrätt. *Post- och telestyrelsen (PTS)* väcker bland annat frågan om NIS 2-direktivet delvis skulle kunna genomföras genom att ha kvar bestämmelserna i LEK. *Skatteverket* anser att PTS bör få ansvaret för tillsyn över digitala tjänster och att bestämmelser om det bör föras in i LEK. *Stokab AB* anför att det finns grundläggande skillnader mellan den nya lagen och LEK och anser att gränsdragningen mellan regelverken måste utredas ytterligare. *Tech Sverige* anser att PTS möjlighet att meddela undantag från skyldigheten att vidta säkerhetsåtgärder och att rapportera incidenter enligt LEK bör kvarstå. Organisationen anser att förslaget kommer att leda till svåra och kostsamma tolkningar i fråga om vilken tillsynsmyndighet som berörs. *Telenor Sverige AB (Telenor)* bedömer att kravet på säkerhetsarbete och säkerhetsåtgärder för telekomsektorn med fördel hade kunnat finnas kvar i LEK och att PTS skulle kunna ges föreskriftsrätt och tillsynsansvar för samtliga krav som gäller för sektorn. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag

Den europeiska kodexen för elektronisk kommunikation

Kodexen, som nämns i avsnitt 6.4, är genomförd i svensk rätt huvudsakligen genom LEK. Genom artikel 43 i NIS 2-direktivet upphävs artiklarna 40 och 41 i kodexen med verkan från och med den 18 oktober 2024 (se även skäl 92).

Av artikel 40.1 i kodexen följde bland annat ett krav på att den som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster skulle vidta ändamåls-

enliga och proportionella tekniska och organisatoriska åtgärder för att på ett lämpligt sätt hantera risker som hotar säkerheten i nät och tjänster.

Av artikel 41.2 b i kodexen följde att tillsynsmyndigheten kunde kräva att tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster på egen bekostnad skulle låta ett kvalificerat oberoende organ eller en behörig myndighet utföra en säkerhetsgranskning och göra resultatet tillgängligt för den behöriga myndigheten.

Artiklarna 40 och 41 ligger till grund för bestämmelserna i 8 kap. 1–4 §§ LEK. Som utredningen redogör för närmare innebär nämnda bestämmelser i LEK att berörda aktörer ska vidta åtgärder för att hantera risker som hotar säkerheten i nät och tjänster, låta utföra säkerhetsgranskning samt rapportera säkerhetsincidenter som har haft en betydande påverkan på nät och tjänster och informera allmänheten eller vissa användare om säkerhetsincidenter.

Bestämmelserna i LEK bör upphävas

Utredningen bedömer att den krets som träffas av 8 kap. 1–4 §§ LEK kommer att träffas av den föreslagna lagen. Vidare är det utredningens bedömning att de ingripanden, sanktioner och tillsynsbefogenheter som i aktuella delar följer av LEK motsvaras av utredningens förslag till ny lag. Utredningen föreslår därför att 8 kap. 1–4 §§ LEK ska upphävas och lämnar också förslag om följdändringar, men anger samtidigt att det finns utrymme för närmare överväganden kopplat till ett antal frågor (se vidare nedan).

PTS och *Telenor* väcker frågan om NIS 2-direktivet i aktuell del i stället skulle kunna genomföras genom att ha kvar bestämmelserna i LEK. Enligt PTS finns det vissa fördelar med att behålla bestämmelserna i LEK och att låta regelverket för telekomsektorn vara fortsatt samlat i en lag som på ett tydligt sätt pekar ut myndigheten som ansvarig för tillsyn, främjande och reglering genom myndighetsföreskrifter. Denna ordning skulle enligt myndigheten troligtvis innebära en minskad administrativ börda för både sektorn och PTS.

Stokab AB anser i sin tur att gränsdragningen mellan den föreslagna lagen och LEK måste analyseras ytterligare. Stokab AB anger att en fundamental skillnad mellan de aktuella regelverken är att NIS 2-direktivet ställer krav på säkerhet i nätverks- och informationssystem, medan den sektorsspecifika lagstiftningen i LEK tar sikte på tillhandahållandet av allmänna elektroniska kommunikationsnät och kommunikationstjänster som helhet. När det gäller allmänna elektroniska kommunikationsnät är exempelvis den fysiska säkerheten i nätet enligt bolaget avgörande för skydd mot incidenter. Stokab AB anför att en kabelskada kan få mycket stora konsekvenser på tillhandahållandet av tjänsten, men att en sådan skada inte kan undvikas genom att vidta åtgärder för att skydda nätverks- och informationssystem. Kravet på fysisk säkerhet är en del av LEK, men det är enligt Stokab AB:s uppfattning inte självklart att motsvarande gäller enligt den nya lagen.

De bestämmelser som är aktuella att upphäva i LEK har införts för att genomföra bestämmelser i kodexen som har upphävts. Bestämmelser om säkerhetsåtgärder, säkerhetsrevision, incidentrapportering och informat-

ionsskyldighet som föreslås i denna lagrådsremiss, och som i stort motsvarar 8 kap. 1–4 §§ LEK, måste införas i nationell rätt med anledning av NIS 2-direktivets krav. Regeringen kan, mot denna bakgrund, inte se att det krävs någon ytterligare analys av skillnaderna mellan regelverken och gränsdragningen mellan den föreslagna lagen och LEK.

För det fall direktivet delvis skulle genomföras genom bestämmelser i LEK, som PTS och Telenor nämner som ett alternativ, skulle bestämmelserna i LEK behöva justeras för att motsvara bestämmelserna i den nya lagen. Den nya lagen skulle gälla för alla andra verksamhetsutövare som inte tillhör telekomsektorn. Regeringen bedömer att det som utgångspunkt finns ett stort värde i att låta regleringen som genomför NIS 2-direktivet och som gäller för samtliga som träffas av direktivet vara samlad i en lag. *Tech Sverige* hävdar att förslaget kommer att leda till tolkningsproblem i fråga om vilken tillsynsmyndighet som berörs. Det kan konstateras att utredningen föreslår att PTS, som utövar tillsyn enligt LEK, även ska pekas ut som tillsynsmyndighet enligt den nya lagen över bland annat sektorn digital infrastruktur.

Regeringen bedömer, mot denna bakgrund, att bestämmelserna i 8 kap. 1–4 §§ LEK bör upphävas i enlighet med utredningens förslag. Detta ställningstagande innebär att bestämmelser om tillsynsansvar inte bör föras in i LEK som *Skatteverket* föreslår. Nödvändiga följdändringar bör göras i LEK. Förutom de ändringar som utredningen föreslår bör även definitionen av uttrycken säkerhetsincident och säkerhet i nät och tjänster utgå. Det bör också göras vissa andra redaktionella ändringar.

I LEK finns det ett antal bestämmelser som behandlar lagens förhållande till annan reglering. Regeringen anser, vilket även utredningen resonerar om som ett alternativ, att det bör föras in en upplysningsbestämmelse i LEK om att det i den nya föreslagna lagen finns bestämmelser som innebär krav på bland annat säkerhetsåtgärder.

Ingen portalparagraf och ingen ytterligare uppgiftsskyldighet

Enligt 1 kap. 1 § tredje stycket LEK ska, vid tillämpningen av den lagen, särskilt beaktas Sveriges säkerhet liksom elektroniska kommunikationers betydelse för yttrandefrihet och informationsfrihet. Utredningen pekar på att det finns skäl att överväga om det bör införas en motsvarighet till den portalbestämmelsen i den nya lagen. Portalbestämmelsen kan, enligt utredningen, påverka hur andra materiella bestämmelser som 8 kap. 1–4 §§ LEK ska tillämpas, men det är enligt utredningen oklart i vilken utsträckning.

I förarbetena som avser 1 kap. 1 § tredje stycket LEK anges att det i lagen har införts en särskild reglering för att kunna skydda Sveriges säkerhet vid radioanvändning. Det anges vidare att det även inom andra områden enligt LEK, vid intresseavvägningar, kan finnas behov av att ta särskild hänsyn till intresset av att värna Sveriges säkerhet (se prop. 2019/20:15 s. 27). Lagen ansågs därför behöva ge tydligt stöd för att beakta säkerhetsintressen vid tillämpningen. Vilka omständigheter som bör beaktas vid tillämpningen av den nya lagen bör dock, enligt regeringens mening, anges specifikt i varje enskild bestämmelse. Det bör därför inte införas någon bestämmelse motsvarande 1 kap. 1 § tredje stycket LEK i den nya lagen.

Enligt 11 kap. 3 § första stycket LEK får tillsynsmyndigheten förelägga den som bedriver verksamhet som omfattas av lagen att tillhandahålla myndigheten de upplysningar eller handlingar som behövs för tillsynen. Om de uppgifter som kan lämnas inte är tillräckliga, får tillsynsmyndigheten enligt andra stycket förelägga andra företag som bedriver verksamhet inom sektorn för elektronisk kommunikation eller nära anknutna sektorer att tillhandahålla sådana upplysningar eller handlingar. Föreläggandena får förenas med vite.

Utredningen anger att det bör analyseras om det finns behov av en möjlighet att enligt den nya lagen utfärda förelägganden motsvarande den som finns enligt 11 kap. 3 § andra stycket LEK. Möjligheten att begära in information även från andra företag enligt LEK är en följd av artikel 20.1 andra stycket i kodexen där det anges att sådan information får efterfrågas. Någon motsvarande bestämmelse finns inte i NIS 2-direktivet och bör inte heller gälla enligt den nya lagen.

Föreskriftsrätt och frågor som bör regleras på annan föreskriftsnivå

Enligt 8 kap. 1 § tredje stycket LEK får regeringen eller den myndighet som regeringen bestämmer meddela ytterligare föreskrifter om säkerhetsåtgärder och föreskrifter om undantag från skyldigheten att vidta sådana åtgärder. I 8 kap. 3 § tredje stycket LEK ges vidare regeringen eller den myndighet som regeringen bestämmer rätt att meddela ytterligare föreskrifter om rapportering av säkerhetsincidenter och föreskrifter om undantag från rapporteringsskyldigheten. PTS har föreskriftsrätt enligt förordningen om elektronisk kommunikation.

Utredningen föreslår att PTS, i egenskap av tillsynsmyndighet, endast ska få föreskriftsrätt avseende säkerhetsåtgärder och anser att det i den fortsatta lagstiftningsprocessen bör utredas vilka konsekvenser det medför. Det är enligt *PTS* och *Tech Sverige* viktigt att PTS även fortsättningsvis har motsvarande möjlighet att meddela föreskrifter om undantag motsvarande det som gäller enligt LEK. PTS anser att det garanterar att en proportionalitetsbedömning av åtgärden alltid kan göras i varje enskilt fall.

Regeringen har svårt att se att NIS 2-direktivets krav kan anses vara uppfyllda om en verksamhetsutövare helt undantas från skyldigheten att vidta säkerhetsåtgärder och rapportera incidenter (se avsnitt 6.4 och 6.6). Utformningen av bestämmelserna om säkerhetsåtgärder och incidentrapportering och bland annat 5 § tredje stycket förvaltningslagen innebär tillräcklig garanti för att vidtagna åtgärder är proportionerliga. Någon motsvarande bestämmelse som finns i LEK bör därför inte införas i den nya lagen i enlighet med PTS förslag.

Det finns, trots synpunkter från till exempel *Tre*, inte anledning att inom ramen för denna lagrådsremiss närmare beröra utredningens förslag föreskrifter på annan normgivningsnivå än lag. Regeringen kommer att beakta synpunkterna från remissinstanserna inom ramen för förordningsarbetet.

12 Sekretess och personuppgiftsbehandling

Regeringens förslag: Det ska föras in en ny bestämmelse i offentlighets- och sekretesslagen om att sekretess ska gälla för uppgift i en incidentrapport som lämnas enligt den nya lagen och för uppgift om vilka åtgärder som en verksamhetsutövare har vidtagit till följd av incidenten, om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens framtida verksamhet skadas eller syftet med vidtagen åtgärd motverkas. Sekretessen ska gälla i högst fyrtio år. Rätten att meddela och offentliggöra uppgifter ska inte ha företräde framför den tystnadsplikt som följer av sekretessen.

Det ska också föras in en ny bestämmelse i offentlighets- och sekretesslagen om att sekretessen i det internationella samarbetet inte ska hindra att Myndigheten för samhällsskydd och beredskap (MSB) i egenskap av gemensam kontaktpunkt, enhet för hantering av it-säkerhetsincidenter eller cyberkrishanteringsmyndighet enligt NIS 2-direktivet lämnar en uppgift till en tillsynsmyndighet enligt den nya lagen, om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag enligt den nya lagen. Sekretessen ska inte heller hindra att en tillsynsmyndighet lämnar en uppgift till MSB, om uppgiften behövs för att MSB ska kunna fullgöra sitt uppdrag som gemensam kontaktpunkt, enhet för hantering av it-säkerhetsincidenter eller cyberkrishanteringsmyndighet enligt direktivet. En uppgift som omfattas av sekretessen i det internationella samarbetet ska få lämnas endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

Det ska föras in en bestämmelse i den nya lagen som upplyser om att den myndighet som regeringen bestämmer ska vara gemensam kontaktpunkt, enhet för hantering av it-säkerhetsincidenter och cyberkrishanteringsmyndighet enligt NIS 2-direktivet.

Regeringens bedömning: Någon ytterligare reglering, utöver den som föreslås gälla för domännamnsregistreringsuppgifter, behöver inte införas för den personuppgiftsbehandling som kan komma att ske med anledning av den nya lagen.

Utredningens förslag i slutbetänkandet överensstämmer delvis med regeringens. I utredningens förslag anges att den nya sekretessbestämmelsen ska gälla utöver sekretessen i 18 kap. 8 § OSL. Utredningen föreslår att sekretessen ska gälla om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens verksamhet skadas eller de åtgärder som vidtagits motverkas. Utredningen föreslår att sekretessen i det internationella samarbetet enligt 15 kap. 1 a § OSL inte ska hindra att MSB lämnar en uppgift som avses där till tillsynsmyndigheten enligt den nya lagen, om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag. Utredningen föreslår att detsamma ska gälla när en tillsynsmyndighet lämnar sådana uppgifter till MSB. Utredningen föreslår ingen upplysningsbestämmelse i den nya lagen. Utredningen gör ingen bedömning i fråga om personuppgiftsbehandling kopplat till genomförandet av NIS 2-direktivet.

Remissinstanserna: Ett antal remissinstanser väcker frågor gällande sekretess med anledning av förslagen i delbetänkandet. Bland andra *Energiföretagen Sverige*, *Statens veterinärmedicinska anstalt*, *Svenskt Näringsliv*, *Sveriges advokatsamfund*, *Swedish Medtech* och *Tech Sverige* lyfter behovet av ett starkt sekretesskydd för de uppgifter som lämnas i anmälningar och i samband med tillsyn och incidentrapporter.

Enligt Sveriges advokatsamfund bör 18 kap. 8 § OSL ändras på så sätt att ett omvänt skaderekvisit gäller i stället för ett rakt. Även *Finansiell ID-Teknik BID AB* och *Hi3G Access AB (Tre)* betonar vikten av en reglering som gäller med ett omvänt skaderekvisit. Tre poängterar också att den föreslagna informationsskyldigheten kan innebära personuppgiftsbehandling för verksamhetsutövarna och behandling av lokaliseringsuppgifter samt att sistnämnda slags uppgifter är mycket känsliga. *Region Stockholm* bedömer att informationslämnande som rör själva incidenten skulle kunna stå i konflikt med till exempel förundersökningssekretess och förespråkar därför att utredningens förslag om att CSIRT-enheten ska kunna begära ytterligare information av verksamhetsutövaren i samband med en incidentanmälan ses över. *Strålsäkerhetsmyndigheten (SSM)* anser att ett antal frågor behöver utredas på området. SSM anser att det bör utredas om det finns behov av bestämmelser i den nya lagen avseende uppgiftsskyldighet myndigheter emellan samt mellan myndigheter och enskilda verksamhetsutövare. Det bör även enligt myndigheten utredas huruvida det finns behov av en bestämmelse om tystnadsplikt i den nya lagen, likt den som finns i säkerhetsskyddslagen. SSM anför att en utredning också bör se över förutsättningarna för utbyte av uppgifter som omfattas av sekretess med myndigheter och verksamhetsutövare utomlands. Utöver nämnda utredningsbehov finns det, enligt SSM, även behov av att utreda frågor om sekretess och sekretessbrytande bestämmelser vad avser uppgifter om cybersäkerhetsbrister, incidenter, hotinformation, hotaktörsinformation samt behov av att agera med risk att röja källor, säkerhetsförmågor och kännedom om aktuella sårbarheter. *Växjö kommun* ser en risk med att skicka incidentrapporter till CSIRT-enheten då dessa kan innehålla både personuppgifter och data som omfattas av sekretess.

Ett antal remissinstanser yttrar sig om förslagen som gäller offentlighet och sekretess i slutbetänkandet i förhållande till NIS 2-direktivets genomförande. *Pensionsmyndigheten* ställer sig bakom de överväganden som utredningen gör i fråga om behovet av nya sekretessbestämmelser. Bland andra *Försvarets radioanstalt (FRA)*, *Länsstyrelsen i Stockholms län*, *Post- och telestyrelsen (PTS)*, *Stiftelsen för internetinfrastruktur (Internetstiftelsen)* och Tech Sverige instämmer i uppfattningen att en ny sekretessbestämmelse bör införas för att skydda uppgifter i incidentrapporterna. Internetstiftelsen noterar att skyddet endast avser uppgift i incidentrapporter och lyfter frågan om skyddet även avser vem som har lämnat rapporten.

Affärsverket svenska kraftnät föreslår att den nya sekretessbestämmelsen utvidgas till att också omfatta anmälningar om säkerhetshotande händelser enligt säkerhetsskyddsförordningen. *Integritetsskyddsmyndigheten (IMY)* anser att förslaget bör utvidgas till att även omfatta personuppgiftsincidentanmälningar eftersom samma uppgifter om en incident annars kommer att få olika starkt skydd beroende av om de lämnas till IMY i form av en personuppgiftsincidentanmälan eller till en tillsyns-

myndighet enligt den nya lagen. *Svensk Dagligvaruhandel* och *Svensk Handel* anser att de föreslagna ändringarna även bör omfatta tillsynsmyndigheternas rapporter.

Domstolsverket ifrågasätter bedömningen att befintliga sekretessbestämmelser ger ett tillräckligt skydd för förteckningar över verksamhetsutövare och förordar att frågan utreds vidare. *Länsstyrelsen i Västra Götalands län* anser att det finns risk för att praxis kan komma att förändras vad avser tillämpningen av 18 kap. 8 och 13 §§ OSL och menar därför att det finns ett behov av att säkerställa att uppgifter i riskanalyser, riskbedömningar och förteckningar över verksamhetsutövare fortsatt ska omfattas av sekretess genom att förtydligande görs i lag. *Länsstyrelsen i Kalmar län* betonar vikten av att förteckningarna över verksamhetsutövare är sekretessbelagda enligt 18 kap. 8 § OSL.

Svenska Journalistförbundet (Journalistförbundet) och *Svenska Tidningsutgivareföreningen (TU)* avstyrker förslaget om sekretess för uppgifter i incidentrapporter. Enligt Journalistförbundet och TU riskerar förslaget att få en effekt motsvarande absolut sekretess. Om regeringen går vidare med förslaget anser Journalistförbundet och TU att bestämmelsen bör ha ett rakt skaderekvisit för att möjliggöra såväl insyn som skydd för uppgifter. Vad avser förslaget kopplat till meddelarfriheten anser Journalistförbundet och TU att skälen för att inskränka denna inte är tillräckliga. Journalistförbundet noterar även att meddelarfriheten inte är inskränkt avseende incidentrapporter enligt 18 kap. 8 a § OSL.

Livsmedelsverket ställer sig tveksamt till om utredningens förslag om sekretesskydd är tillräckligt i fråga om uppgifter som kan framkomma vid tillsyn och utredning eftersom 30 kap. 23 § OSL endast avser uppgifter som rör affärs- och driftförhållanden och där det kan antas att den enskilde lider skada om uppgiften röjs. Myndigheten anser därför att det behövs en bestämmelse, likt den som föreslås för uppgifter i incidentrapporter och för uppgift om åtgärder, även för uppgifter om tillsyn och utredning.

Transportstyrelsen anser att det är angeläget att beslut vid tillsyn ska kunna beläggas med sekretess eftersom det i besluten bland annat hänvisas till brister som kan vara av sådan art att de bör kunna omfattas av sekretessen enligt 30 kap. 23 § OSL. Transportstyrelsen anser vidare att tillsynsmyndigheterna behöver kunna dela information mellan sig, både om vilka tillsynsobjekt som faller inom respektive myndighets tillsynsområde och om utfallet vid en tillsyn. Enligt Transportstyrelsen är det tveksamt om generalklausulen i 10 kap. 27 § OSL täcker det behov av informationsdelning som finns och myndigheten menar att det bör övervägas om möjligheterna till utbyte av sekretessbelagda uppgifter mellan tillsynsmyndigheterna kan utökas. Transportstyrelsen anser även att möjligheterna att kunna sekretessbelägga identiteten på tillsynsobjekten i de beslut som fattas bör utredas vidare.

Finansinspektionen instämmer inte i utredningens uppfattning att uppgifter som är sekretessbelagda enligt 15 kap. 1 a § OSL, och som lämnas från en svensk myndighet till en annan, kommer att ha samma sekretesskydd hos den mottagande myndigheten som hos myndigheten som har lämnat uppgifterna vidare. Enligt Finansinspektionen bör det i det fortsatta lagstiftningsarbetet analyseras om sådana uppgifter som kommer att behöva utbytas mellan svenska myndigheter redan ges ett tillräckligt sekretesskydd med stöd av andra bestämmelser i OSL eller om

sekretesskyddet behöver regleras särskilt. Även *Skatteverket* ifrågasätter slutsatsen att sekretessen följer med en uppgift som lämnas vidare och anser att räckvidden av 15 kap. 1 a § OSL bör förtydligas.

Göteborgs kommun efterfrågar ett förtydligande i fråga om hur informationsdelning inom en kommun ska kunna ske, då en kommun ur ett sekretessperspektiv består av flera olika självständiga myndigheter.

Skälen för regeringens förslag och bedömning

Krav på konfidentialitet i direktivet

Enligt artikel 2.11 i NIS 2-direktivet ska de skyldigheter som fastställs i direktivet inte medföra tillhandahållande av information vars utlämnande strider mot väsentliga intressen i fråga om medlemsstaternas nationella säkerhet, allmänna säkerhet eller försvar. Utan att det påverkar tillämpningen av artikel 346 i EUF-fördraget ska vidare, enligt artikel 2.13 i direktivet, information som är konfidentiell enligt unionsbestämmelser eller nationella bestämmelser, såsom bestämmelser om affärshemligheter, utbytas med kommissionen och andra berörda myndigheter i enlighet med direktivet endast när ett sådant utbyte är nödvändigt för att tillämpa direktivet. Den information som utbyts ska begränsas till vad som är relevant och proportionellt för ändamålet med utbytet. Vid utbytet ska informationens konfidentialitet bevaras och berörda entiteters säkerhets- och affärsintressen skyddas.

Enligt artikel 23.6 i NIS 2-direktivet ska, när så är lämpligt och särskilt om en betydande incident berör två eller flera medlemsstater, CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten utan onödigt dröjsmål informera andra berörda medlemsstater och Enisa om den betydande incidenten. Sådan information ska åtminstone inbegripa den typ av information som har mottagits i enlighet med artikel 23.4, det vill säga inom ramen för entiteternas rapporteringsskyldighet. Därvid ska CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten, i enlighet med unionsrätten eller nationell rätt, bevara entitetens säkerhets- och affärsintressen samt den tillhandahållna informationens konfidentialitet.

Enligt artikel 23.4 i NIS 2-direktivet ska medlemsstaterna, när det gäller det underrättelseförfarande som avses i artikel 23.1, säkerställa att de berörda entiteterna till CSIRT-enheten eller, i tillämpliga fall, den behöriga myndigheten lämnar viss information. Det rör sig bland annat om att i en slutrapport lämna en detaljerad beskrivning av incidenten samt uppgifter om den typ av hot som sannolikt har utlöst incidenten och om tillämpade och pågående begränsande åtgärder.

I artikel 30 i NIS 2-direktivet, som gäller frivillig underrättelse om relevant information, anges att de frivilliga underrättelserna ska behandlas i enlighet med det förfarande som anges i artikel 23. Det anges vidare att CSIRT-enheterna och i tillämpliga fall de behöriga myndigheterna vid behov ska informera de gemensamma kontaktpunkterna om sådana underrättelser och samtidigt säkerställa att informationen från den underrättande entiteten förblir konfidentiell och skyddas på lämpligt sätt.

Relevanta sekretessbestämmelser

Enligt 2 kap. 2 § tryckfrihetsförordningen får rätten att ta del av allmänna handlingar begränsas endast om det är påkallat med hänsyn till vissa angivna intressen, till exempel rikets säkerhet eller dess förhållande till annan stat eller mellanfolklig organisation, myndigheters verksamhet för inspektion, kontroll eller annan tillsyn, intresset av att förebygga eller beivra brott eller skyddet för enskildas personliga eller ekonomiska förhållanden. En sådan begränsning ska anges noga i en bestämmelse i en särskild lag eller, om det i ett visst fall anses lämpligare, i en annan lag som den särskilda lagen hänvisar till. Efter bemyndigande i en sådan bestämmelse får regeringen genom förordning meddela närmare föreskrifter om bestämmelsens tillämplighet. Den särskilda lagen är OSL och regeringen har meddelat närmare föreskrifter i offentlighets- och sekretessförordningen (2009:641) (OSF). Av 3 kap. 1 § OSL framgår att det med sekretess avses ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt.

I 15 kap. 1 § OSL regleras den så kallade utrikessekretessen. Sekretess gäller enligt paragrafen för uppgift som rör Sveriges förbindelser med en annan stat eller i övrigt rör bland annat en annan stat, mellanfolklig organisation eller myndighet, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs. Skadebegreppet, det vill säga att ett röjande skulle störa Sveriges mellanfolkliga förbindelser eller på annat sätt skada landet, ska inte ges en vid innebörd.

I 15 kap. 1 a § OSL finns bestämmelser om sekretess i det internationella samarbetet. Av första stycket framgår att sekretess gäller 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 enligt andra stycket 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 första stycket. Paragrafen är alltså tillämplig på uppgifter som har tagits emot eller hämtats in som en direkt följd av en EU-rättsakt.

Förundersökningssekretess gäller enligt 18 kap. 1 § OSL bland annat för en uppgift som hänför sig till förundersökning i brottmål, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs. Sekretess gäller, under motsvarande förutsättningar, för en uppgift som hänför sig till bland annat annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av till exempel en åklagarmyndighet eller Polismyndigheten. Förundersökningssekretess gäller oavsett hos vilken myndighet uppgiften finns.

I 18 kap. 8 § OSL regleras sekretess för säkerhets- eller bevakningsåtgärd. Sekretessen gäller enligt paragrafens tredje punkt bland annat för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om

uppgiften röjs och åtgärden avser telekommunikation eller system för automatiserad behandling av information.

Med ordet telekommunikation avses i paragrafen överföring av meddelande med tråd, radio eller en liknande metod. Med uttrycket 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. Sekretessen avser bland annat att skydda funktioner för användning av lösenord, loggning och kryptering, installation och konfigurering av brandväggar och antivirusprogram samt administrativa rutiner för till exempel utdelning av lösenord eller bevakning av loggar och larm.

Beskrivningar av hur ett program fungerar i stora drag och vilka typer av uppgifter som bearbetas i ett program bör alltid kunna lämnas utan att uppgifter som omfattas av bestämmelsen behöver röjas (se prop. 2003/04:93 s. 88). Vidare kan till exempel inte kostnader för införskaffande och installation av ett datorsystem hemlighållas med stöd av bestämmelsen, även om uppgifter i en faktura om vilken typ och/eller version av system som har införskaffats kan komma att hemlighållas.

Av 18 kap. 13 § OSL framgår att sekretess gäller 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 förebygga och hantera fredstida kriser motverkas om uppgiften röjs.

Övriga relevanta bestämmelser i OSL

I 8 kap. 3 § OSL finns bestämmelser som reglerar när uppgifter som omfattas av sekretess får röjas för utländska myndigheter och mellanfolkliga organisationer. En uppgift för vilken sekretess gäller enligt OSL får enligt paragrafen inte röjas för en utländsk myndighet eller en mellanfolklig organisation, om inte utlämnande sker i enlighet med särskild föreskrift i lag eller förordning, eller uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen.

Av den sekretessbrytande bestämmelsen i 10 kap. 2 § OSL framgår att sekretess inte hindrar att en uppgift lämnas till en enskild eller en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet.

Enligt 10 kap. 17 § OSL hindrar sekretess inte att en uppgift lämnas till en myndighet, om uppgiften behövs där för tillsyn över eller revision hos den myndighet där uppgiften förekommer. Om en myndighet i verksamhet som avser tillsyn eller revision, får en sekretessreglerad uppgift från en annan myndighet, blir sekretessbestämmelsen tillämplig på uppgiften även hos den mottagande myndigheten enligt 11 kap. 1 § OSL.

Utlämnande av sekretessbelagda uppgifter kan ske med stöd av generalklausulen i 10 kap. 27 § OSL. En sekretessbelagd uppgift får enligt generalklausulen lämnas till en myndighet, om det är uppenbart att

intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

Enligt 10 kap. 28 § OSL hindrar sekretess inte att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning. För att bestämmelsen ska vara tillämplig krävs att uppgiftsskyldigheten har viss konkretion. Uppgiftsskyldigheten kan antingen ta sikte på utlämnande av uppgifter av ett speciellt slag, gälla en viss myndighets rätt att få del av uppgifter i allmänhet eller avse skyldighet för en viss myndighet att lämna andra myndigheter information (se prop. 1979/80:2 Del A s. 322)

Om sekretess gäller enligt 15 kap. 1 a § första eller andra stycket, får de sekretessbrytande bestämmelserna i bland annat 10 kap. 17, 27 och 28 §§ första stycket inte tillämpas. Detta följer av 15 kap. 1 a § tredje stycket.

En ny sekretessbestämmelse kopplad till incidentrapporteringen

Den befintliga sekretessbestämmelse som främst har varit av intresse för utredningen vid bedömningen av behovet av en ändrad sekretessreglering är 18 kap. 8 § 3 OSL. Bestämmelsen rör sekretess för uppgifter som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärder som avser telekommunikation eller system för automatiserad behandling av information. Utifrån bestämmelsens lydelse och den rättspraxis som finns bedömer utredningen att det är osäkert om sådant som identiteten på ingivaren av en incidentrapport och de åtgärder som kan behöva vidtas till följd av incidenten kan ges ett tillräckligt sekretesskydd. Regeringen gör samma bedömning. Därtill noterar regeringen, i likhet med utredningen, att en uppgift om vem som är ingivare av en incidentrapport i vissa fall kan vara mycket känslig. En sådan uppgift kan, enskilt eller tillsammans med andra uppgifter i en incidentrapport, ge en antagonistisk aktör information om huruvida ett angrepp har lyckats eller har upptäckts och om ingivarens it-system är sårbart för attacker (jfr prop. 2017/18:105 s. 129). Regeringen delar också utredningens uppfattning att en uppgift om att inga åtgärder har vidtagits kan ge en antagonistisk aktör en god bild om kvarvarande sårbarheter i ett system.

Som utredningen noterar saknas det i dag ett ändamålsenligt sekretesskydd för uppgifter med koppling till en incidentrapport, både med beaktande av 18 kap. 8 § 3 OSL och övrig sekretessreglering. När en ny sekretessbestämmelse övervägs ska det alltid göras en avvägning mellan sekretessintresset och insynsintresset (se prop. 1979/80:2 Del A s. 75 f.). Utredningen anför att insynsintresset avseende viss verksamhet som har betydelse för viktiga samhällsfunktioner kan anses vara betydande, men att sådana uppgifter som föreslås skyddas genom den nya sekretessbestämmelsen har ett relativt lågt informationsvärde hos allmänheten.

Regeringen har förståelse för *TU:s* synpunkt att den föreslagna bestämmelsen kan innebära att motiverad insyn försvåras i de fall det har skett en incident. Som utredningen resonerar kring bygger ett regelverk som innebär krav på incidentrapportering emellertid på att de aktörer som ska genomföra rapportering har en hög tilltro till systemet och att deras känsliga uppgifter ges ett fullgott skydd hos mottagaren. I annat fall kan rapporter utebli och känsliga uppgifter utelämnas. En sådan utveckling riskerar att motverka ändamålet med rapporteringen, vilket i slutändan kan

leda till att samhället blir mer sårbart. De incidentrapporter som föreslås lämnas kan därtill innefatta uppgifter som vid en första anblick kan framstå som harmlösa, men där det samtidigt kan få stora konsekvenser om uppgifterna röjs. Det kan till exempel röra sig om uppgifter som lämnas i ett tidigt skede i samband med ett it-angrepp där omfattningen av angreppet ännu inte är klarlagt eller uppgifter som ger en antagonistisk aktör en bild av de sårbarheter som finns.

Mot bakgrund av den betydelse som behovet av tilltro till systemet och möjligheten att ge skydd åt känsliga uppgifter har för rapporteringen och med hänsyn till de negativa effekter som ett röjande av uppgifterna kan få anser regeringen att det finns behov av ett erforderligt skydd för den aktuella sortens uppgifter. 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 NIS 2-direktivet, får enligt regeringen anses väga tyngre än det motstående intresset av insyn i myndigheternas verksamhet. Det bör därför, till skillnad från vad *Journalistförbundet* och TU anser, men i likhet med vad utredningen och ett antal remissinstanser föreslår, införas en ny sekretessbestämmelse som ger skydd för uppgifter i en incidentrapport och uppgifter om åtgärder som har vidtagits till följd av aktuella incidenter. Detta framstår enligt regeringen som ett bättre alternativ än att ändra 18 kap. 8 § OSL i enlighet med förslaget från *Sveriges advokatsamfund*.

Det finns inget utrymme för att inom ramen för denna lagrådsremiss föreslå sådana ändringar kopplade till säkerhetsskyddsförordningen och personuppgiftsincidentanmälningar som *Affärsverket svenska kraftnät* och *IMY* föreslår. Detta gäller även i förhållande till de förslag på ändrat regelverk som *Svensk Dagligvaruhandel* och *Svensk Handel* lämnar. Med anledning av vad *Länsstyrelsen i Västra Götalands län* anför vill regeringen framhålla att det inte har framkommit något behov av att göra ändringar i 18 kap. 8 och 13 §§. Regeringen ser inte att förslaget i denna lagrådsremiss skulle riskera att påverka hur dessa paragrafer tillämpas.

Sekretessbestämmelsens utformning och placering

En sekretessbestämmelse består i regel av tre huvudsakliga rekvisit, det vill säga förutsättningar för bestämmelsens tillämplighet. Dessa tre rekvisit anger sekretessens föremål, sekretessens räckvidd och sekretessens styrka. Sekretessens föremål är den information som kan hemlighållas och kommer till uttryck i sekretessregleringen genom att ordet uppgift används tillsammans med en mer eller mindre långtgående precisering av uppgiftens art, till exempel uppgift om enskilds personliga förhållanden. En sekretessbestämmelses räckvidd bestäms normalt genom att det i bestämmelsen preciseras att sekretessen för de angivna uppgifterna endast gäller i en viss typ av ärende, i en viss typ av verksamhet eller hos en viss myndighet. Några få sekretessbestämmelser gäller utan att räckvidden är begränsad. En uppgift kan då hemlighållas oavsett i vilket ärende, i vilken verksamhet eller hos vilken myndighet den förekommer. Som exempel på en sådan bestämmelse kan nämnas utrikessekretessen i 15 kap. 1 § OSL.

Den brist som har uppmärksammats i den nuvarande sekretessregleringen är att uppgifter som kan förekomma i incidentrapporter och uppgifter om vilka åtgärder som har vidtagits till följd av incidenter inte alltid kommer att kunna skyddas. Sekretessens föremål bör därför lämpligen begränsas till sådana uppgifter. Föremålet för sekretessen enligt den föreslagna bestämmelsen kan även omfatta vem som har lämnat in en sådan rapport, något som *Internetstiftelsen* efterfrågar ett förtydligande av. Vidare innebär förslaget att sekretess kan gälla för uppgifter som har lämnats vid de olika delarna av en incidentrapportering, det vill säga upplysning, incidentanmälan, delrapport, lägesrapport och slutrapport (se avsnitt 6.6). Sekretessen enligt den nya bestämmelsen kommer däremot inte att gälla för uppgifter som lämnas inom ramen för en frivillig underrättelse. Eftersom sekretessregleringen enbart gäller för uppgifter i incidentrapporter och om uppgifter som avser efterföljande åtgärder och då sekretessen dessutom är begränsad till att avse den incidentrapportering som ska ske enligt den nya lagen kommer den att tillämpas inom ett väl avgränsat område. Mot den bakgrunden saknas det skäl att, som *Journalistförbundet* lyfter, begränsa tillämpningsområdet ytterligare.

Sekretessens styrka bestäms i regel med hjälp av så kallade skaderekvisit. Man skiljer på raka och omvända skaderekvisit. Vid raka skaderekvisit är utgångspunkten att uppgifterna är offentliga och att sekretess gäller endast om det kan antas att en viss skada uppkommer om uppgiften röjs. Det omvända skaderekvisitet har den omvända utgångspunkten, vilket innebär sekretess som huvudregel. Vid ett omvänt skaderekvisit gäller sekretess om det inte står klart att uppgiften kan röjas utan att viss skada uppstår. En del bestämmelser innehåller ett kvalificerat rakt skaderekvisit, vilket innebär att det krävs särskilt mycket för att sekretessen ska gälla. Sekretessen enligt en bestämmelse kan även vara absolut. I ett sådant fall ska de uppgifter som omfattas av bestämmelsen hemlighållas utan någon skadeprövning om uppgifterna begärs ut.

Ett antal remissinstanser, bland andra *Sveriges advokatsamfund,* instämmer i utredningens uppfattning att ett omvänt skaderekvisit bör gälla enligt den nya sekretessbestämmelsen. Journalistförbundet och *TU* anser i stället att bestämmelsen bör ha ett rakt skaderekvisit och att förslaget om ett omvänt skaderekvisit riskerar att få en effekt motsvarande absolut sekretess.

Avgörande vid prövningar kopplat till en bestämmelse med ett rakt skaderekvisit är om uppgiften är av den arten att ett utlämnande typiskt sett kan vara ägnat att medföra skada för det intresse som ska skyddas genom bestämmelsen. Om uppgiften är sådan att den genomsnittligt sett måste betraktas som harmlös ska den alltså normalt anses falla utanför sekretessens tillämpningsområde. Om uppgiften typiskt sett måste betraktas som känslig omfattas den däremot normalt av sekretess. Genom att avgörande betydelse som regel tillerkänns arten av den uppgift som efterfrågas innebär det att det vid en bedömning enligt ett rakt skaderekvisit sällan krävs att myndigheten efterforskar vem som begär att få ta del av uppgiften eller vilket syfte den enskilde har med sin begäran (se prop. 1979/80:2 Del A s. 80 f., prop. 2008/09:150 s. 348 f. och 2 kap. 18 § tryckfrihetsförordningen).

En sekretessbestämmelse ska inte göras starkare än vad som är oundgängligen nödvändigt för att skydda det intresse som har föranlett

bestämmelsen och sekretesskyddet får inte utformas så att handlingsoffentligheten inskränks mer än vad syftet med sekretessen kräver (se prop. 2011/12:160 s. 58 f.). Behovet av en, i förhållande till 18 kap. 8 § OSL, skärpt sekretess måste också bland annat vägas mot att det kan finnas ett intresse av insyn när det gäller incidenter som har drabbat en offentlig verksamhetsutövare. Som utredningen anger kan utformningen av skaderekvisitet emellertid ha stor betydelse för en verksamhetsutövares tilltro till regelverket. Intresset av insyn bör därmed, som utredningen bedömer, få stå tillbaka med hänsyn till den skada som kan uppstå om känsliga uppgifter offentliggörs.

Det bör också beaktas att det kan vara svårt att i ett tidigt skede bedöma om uppgifter i incidentrapporter är känsliga, vilket innebär att känsliga uppgifter inledningsvis riskerar att uppfattas som harmlösa. Genom att införa ett omvänt skaderekvisit måste myndigheten i varje enskilt fall förvissa sig om att ett utlämnade inte leder till men för den som uppgifterna rör. I praktiken innebär detta att en uppgift som omfattas av en sådan sekretessbestämmelse många gånger inte kan lämnas ut utan kännedom om mottagarens identitet och om dennes avsikter med uppgifterna (se prop. 1979/80:2 Del A s. 82). Ett omvänt skaderekvisit innebär dock inte att rätten att ta del av information i ärenden som rör incidentrapportering saknas, vilket Journalistförbundet och TU uttrycker oro för, utan uppgifter kan i det enskilda fallet komma att lämnas ut efter en sekretessprövning.

Som utredningen konstaterar kommer uppgifter i en incidentrapport, eller om vilka åtgärder som har vidtagits, i många fall ändå kunna lämnas ut relativt tidigt efter en incident när åtgärder för att minska incidentens effekt har vidtagits. Exempel på sådana åtgärder är så kallade patchningar, som innebär att en sårbarhet minskas eller försvinner. Intresset av insyn tillgodoses dessutom i viss mån av förslaget om att en tillsynsmyndighet ska kunna förelägga en verksamhetsutövare att i vissa fall lämna information rörande incidenter (se avsnitt 6.6 och 8.5). Sammanfattningsvis bör den nya sekretessbestämmelsen, som utredningen och till exempel Sveriges advokatsamfund föreslår, innefatta ett omvänt skaderekvisit.

Utredningen föreslår att det ska anges i paragrafen att sekretess gäller om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens verksamhet skadas eller de åtgärder som har vidtagits motverkas. Utredningen föreslår vidare att den nya sekretessbestämmelsen ska placeras i 18 kap. OSL och att det även ska anges att sekretessen gäller utöver 18 kap. 8 §.

Sekretessen bör, i enlighet med utredningens förslag, gälla i fyrtio år, vilket är samma sekretesstid som gäller för incidentrapporter i bland annat domstolar enligt 18 kap. 8 a § OSL och för utrikessekretessen och sekretessen i det internationella samarbetet enligt 15 kap. 1 och 1 a §§.

I 18 kap. OSL regleras sekretess till skydd främst för intresset av att förebygga eller beivra brott. Det är lämpligt att placera den föreslagna paragrafen i nära anslutning till 18 kap. 8 § OSL eftersom den kompletterar nämnda paragraf och har i huvudsak samma skyddsintresse. Paragrafen bör dock omformuleras i förhållande till utredningens förslag för att förtydliga att det framför allt är fråga om sådana begränsningar som krävs med hänsyn till intresset av att förebygga och beivra brott. Det bör därför anges 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.

Regeringen anser vidare, till skillnad från utredningen, att det inte behöver anges att sekretessen enligt den nya paragrafen gäller utöver 18 kap. 8 § OSL. Motsvarande formulering finns visserligen i 18 kap. 8 a § OSL men har sin grund i att det vid införandet av den paragrafen fanns ett behov av att tydliggöra att en uppgift som omfattas av sekretess enligt 8 § inte samtidigt kan omfattas av sekretess enligt 8 a § (se prop. 2018/19:81 s. 77 och 154 f.). Motsvarande behov finns inte i detta sammanhang. Uppgifter som avses i den nya sekretessbestämmelsen kan även omfattas av tillämpningsområdet för 18 kap. 8 § OSL. I förekommande fall får konkurrensfrågor hanteras enligt bestämmelsen i 7 kap. 3 § OSL.

Rätten att meddela och offentliggöra uppgifter bör begränsas

Sekretess innebär ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av allmän handling eller på något annat sätt. Bestämmelserna om sekretess innefattar alltså såväl handlingssekretess som tystnadsplikt. Den rätt att meddela och offentliggöra uppgifter som följer av tryckfrihetsförordningen och yttrandefrihetsgrundlagen har som huvudregel företräde framför tystnadsplikten. Utredningen bedömer dock att rätten att meddela och offentliggöra uppgifter inte bör ha företräde framför den tystnadsplikt som följer av den föreslagna bestämmelsen.

Stor återhållsamhet bör iakttas vid prövningen av om det bör göras undantag från rätten att meddela och offentliggöra uppgifter. Redan den omständigheten att en sekretessbestämmelse är försedd med ett omvänt skaderekvisit talar dock i viss utsträckning för att den tystnadsplikt som följer av bestämmelsen bör ha företräde framför rätten att meddela och offentliggöra uppgifter (jfr prop. 1979/80:2 Del A s. 111). Det finns också, som utredningen anför och bland annat med beaktande av att rätten till insyn tillgodoses på vissa andra sätt, skäl att göra undantag för den aktuella typen av uppgifter. Till skillnad från *Journalistförbundet* och *TU* anser regeringen därför att rätten att meddela och offentliggöra uppgifter inte bör ha företräde framför den tystnadsplikt som följer av den föreslagna bestämmelsen. Det kan noteras att samma sak gäller i förhållande till 18 kap. 8 § OSL enligt 18 kap. 19 § samma lag. Av sistnämnda paragraf 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 läggas till i uppräkningen i enlighet med utredningens förslag.

Sekretessen i det internationella samarbetet bör inte hindra informationsutbyte

Enligt 8 kap. 1 § OSL får uppgifter som omfattas av sekretess inte röjas för enskilda eller för andra myndigheter, om inte annat anges i OSL eller i lag eller förordning som OSL hänvisar till. En sekretessbrytande bestämmelse är enligt 3 kap. 1 § OSL en bestämmelse som innebär att en sekretessbelagd uppgift får lämnas ut under vissa förutsättningar. För att en sekretessbrytande bestämmelse ska kunna tillämpas måste alltså rättstillämparen i en första prövning komma fram till att uppgifterna är

sekretessbelagda, det vill säga att det i det enskilda fallet finns ett förbud mot att röja uppgifterna. Det är inte tillräckligt att uppgifterna är sekretessreglerade.

Utredningen anger att MSB liksom tillsynsmyndigheterna enligt den nya lagen ömsesidigt behöver kunna utbyta sådana uppgifter som härrör från andra EU-medlemsstater och EU:s institutioner oberoende av vilken myndighet som har fått uppgiften. Det rör sig enligt utredningen till exempel om uppgifter i incidentrapporter och uppgifter som delges i samverkan med andra medlemsstaters tillsynsmyndigheter enligt NIS 2-direktivet.

MSB har i ett regeringsuppdrag som beslutades den 27 februari 2025 pekats ut som bland annat gemensam kontaktpunkt, CSIRT-enhet och cyberkrishanteringsmyndighet (Fö2025/00387). Regeringen konstaterar att den myndighet som är gemensam kontaktpunkt, CSIRT-enhet och cyberkrishanteringsmyndighet enligt NIS 2-direktivet kan få del av uppgifter med stöd av direktivet som den bör kunna vidarebefordra till tillsynsmyndigheterna enligt lagen (se till exempel artikel 23.6). Tillsynsmyndigheterna kan också få del av uppgifter med stöd av direktivet som bör kunna vidarebefordras till den myndighet som är gemensam kontaktpunkt, CSIRT-enhet och cyberkrishanterings-myndighet.

NIS 2-direktivet räknas som en sådan bindande EU-rättsakt som nämns i 15 kap. 1 a § OSL. Regeringen bedömer, i likhet med utredningen, att uppgifterna som bör kunna utbytas i stor utsträckning kommer att omfattas av sekretess enligt 15 kap. 1 a § OSL. Av det skälet behövs en sekretessbrytande bestämmelse som möjliggör uppgiftslämnande som krävs enligt direktivet från den myndighet som tar emot uppgifterna inom ramen för samverkan enligt NIS 2-direktivet. Sekretessen bör inte brytas för andra uppgifter än sådana som den mottagande myndigheten behöver ha tillgång till. Tillämpningsområdet bör därför avgränsas så att det endast omfattar uppgifter som behöver utbytas för att den mottagande myndigheten ska kunna fullgöra sitt uppdrag. Det bör föras in en bestämmelse i den nya lagen som upplyser om att den myndighet som regeringen bestämmer ska vara gemensam kontaktpunkt, enhet för hantering av it-säkerhetsincidenter och cyberkrishanteringsmyndighet enligt direktivet. Uttrycket CSIRT-enheten bör inte användas i den nya lagen (jfr prop. 2017/18:205 s. 48).

Något som i viss mån talar mot att införa en uppgiftsskyldighet är att en sådan kan ge mindre utrymme för att beakta omständigheter som i det enskilda fallet innebär att en uppgift inte bör lämnas ut. De uppgifter som skyddas med stöd av 15 kap. 1 a § OSL kan dessutom vara av mycket känslig natur. Mot denna bakgrund anser regeringen att det bör finnas utrymme för berörda myndigheter att bedöma om uppgifter bör lämnas eller inte i det enskilda fallet och vilka uppgifter som är lämpliga att lämna. En uppgift bör därför få lämnas endast om intresset av att den lämnas har företräde framför det intresse som sekretessen ska skydda. Intresse-avvägningen ska göras oavsett om en uppgift lämnas ut på eget initiativ eller på begäran av en annan myndighet med stöd av 6 kap. 5 § OSL. Vid bedömningen av hur starkt intresset för ett utlämnande är kan hänsyn tas till flera olika faktorer. Exempelvis kan sekretesskyddet hos den mottagande myndigheten vägas in i bedömningen.

Utredningen bedömer att 15 kap. 1 a § OSL innebär att sekretess även kommer att gälla hos den myndighet som får del av uppgifterna efter vidarebefordran. Slutsatsen om att den internationella sekretessen även gäller hos den myndighet som får del av uppgifterna efter vidarebefordran ifrågasätts av såväl *Finansinspektionen* som *Skatteverket*. I förarbetena till 15 kap. 1 a § OSL anges att den aktuella bestämmelsen om sekretess i det internationella samarbetet enbart gäller hos den myndighet som fått uppgiften från ett utländskt organ eller har inhämtat den (se prop. 2012/13:192 s. 30). Det behöver därför inte införas en sådan bestämmelse som utredningen föreslår för att möjliggöra sekretessgenombrott för en myndighet som efter vidarebefordran har fått del av uppgifter som omfattas av sekretess i det internationella samarbetet.

Informationsutbytet mellan verksamhetsutövare och tillsynsmyndigheter i övrigt

SSM uttrycker i sitt remissvar att det bör utredas om det finns behov av att införa bestämmelser i den nya lagen som innebär uppgiftsskyldighet mellan myndigheter och enskilda verksamhetsutövare. *Region Stockholm* bedömer att information om själva incidenten kan omfattas av till exempel förundersökningssekretess och förespråkar därför att utredningens förslag om att CSIRT-enheten ska kunna begära ytterligare information av verksamhetsutövaren ses över.

I avsnitt 7.2.1 föreslås en uppgiftsskyldighet för verksamhetsutövare i förhållande till tillsynsmyndigheten. I avsnitt 6.6 föreslås vidare uppgiftsskyldighet inom ramen för skyldigheterna att genomföra incidentrapportering. Införandet av dessa uppgiftsskyldigheter innebär att en uppgift, trots att den omfattas av sekretess hos en offentlig verksamhetsutövare, kan lämnas till en annan myndighet enligt 10 kap. 28 § första stycket OSL. En verksamhetsutövare som omfattas av tillämpningsområdet för OSL har vidare en möjlighet att lämna ut uppgifter med stöd av 10 kap. 17 § samma lag, om uppgiftslämnandet sker inom ramen för tillsyn eller revision. Därtill hindrar sekretess inte 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 enligt 10 kap. 2 § OSL. Om nämnda bestämmelser inte kan användas, kan frågan om utlämnande av sekretessbelagda uppgifter även prövas utifrån generalklausulen i 10 kap. 27 § OSL. Mot denna bakgrund bedömer regeringen att det inte krävs någon ytterligare sekretessbrytande bestämmelse för att möjliggöra informationsutbyte mellan offentliga verksamhetsutövare och andra myndigheter.

Det bör vidare noteras att om en myndighet i verksamhet som avser tillsyn eller revision, får en sekretessreglerad uppgift från en annan myndighet, blir sekretessbestämmelsen tillämplig på uppgiften även hos den mottagande myndigheten enligt 11 kap. 1 § OSL. Som utredningen anför kan också bestämmelsen om utrikessekretess i 15 kap. 1 § OSL aktualiseras för uppgifter som har tagits emot från EU-kommissionen och andra medlemsstater. Vilket sekretesskydd som uppgifterna får hos den mottagande myndigheten får dock avgöras i varje enskilt fall utifrån den sekretess som gäller hos berörd myndighet.

Det har inte framkommit något behov av att införa en sådan tystnadsplikt som SSM nämner. Någon sådan översyn som myndigheten föreslår finns det inte heller utrymme för att göra inom ramen för denna lagrådsremiss. Huruvida det finns förutsättningar för informationsdelning mellan olika kommunala nämnder med anledning av det regelverk som föreslås i denna lagrådsremiss, något som *Göteborgs kommun* efterfrågar ett förtydligande av, får avgöras i varje enskilt fall med beaktande av tillämplig sekretessreglering. Med anledning av vad Region Stockholm framför om förundersökningssekretess vill regeringen framhålla att uttrycket ytterligare information föreslås ersättas med ”relevanta statusuppdateringar” för att förtydliga vad för slags uppgifter som uppgiftsskyldigheten tar sikte på när det gäller sådana delrapporter som verksamhetsutövare kan behöva lämna (se avsnitt 6.6.2). I fråga om exempelvis förundersökningssekretess hos offentliga verksamhetsutövare noteras att tillämpningsområdet för de sekretessbrytande bestämmelserna i 10 kap. OSL inte är begränsat på samma sätt som är fallet när det är fråga om 15 kap. 1 a § OSL.

Informationsutbyte i övrigt kopplat till tillsynsmyndigheterna

SSM anser att det bör utredas om det finns behov av någon bestämmelse i den nya lagen avseende uppgiftsskyldighet myndigheter emellan. *Transportstyrelsen* anser att det bör övervägas om möjligheterna till utbyte av sekretessbelagda uppgifter mellan tillsynsmyndigheterna kan utökas. Det är inte uteslutet att en tillsynsmyndighet även kan behöva dela med sig av andra uppgifter än sådana uppgifter som omfattas av sekretess i det internationella samarbetet till en annan tillsynsmyndighet. Som konstaterats ovan hindrar inte sekretess att en uppgift lämnas till en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Detta framgår av 10 kap. 2 § OSL. Bestämmelsen ska användas med restriktivitet. Regeringen anser dock att en tillsynsmyndighet i vissa fall bör kunna tillämpa paragrafen för utlämnande av uppgifter till en annan tillsynsmyndighet. Informationsutbyte får ske utifrån tillämpliga bestämmelser och huruvida förutsättningar finns för sådant utbyte med stöd av 10 kap. 2 § OSL, generalklausulen i 10 kap. 27 § OSL eller någon annan bestämmelse, får avgöras i varje enskilt fall.

Direktivet kräver, som utredningen nämner, att det finns möjlighet att lämna ut uppgifter som omfattas av sekretess till utländska myndigheter och EU-kommissionen. Som utredningen konstaterar, och lämnar förslag på, kan möjligheten till ett sådant utlämnande regleras i förordning enligt 8 kap. 3 § OSL. Förordningsförslagen är inte föremål för behandling i denna lagrådsremiss.

Övriga författningsförslag från utredningen

Utredningen föreslår att det ska regleras i OSF att sekretess även gäller för diarium, ett förslag som enligt Journalistförbundet och TU är för långtgående. Ett antal remissinstanser betonar vikten av att skydda enskildas affärs- och driftförhållanden i utredning och tillsyn enligt den nya lagen. *Livsmedelsverket* ställer sig till exempel tveksamt till om det finns ett tillräckligt sekretesskydd för uppgifter som kan framkomma vid

tillsyn och anser att det behövs en bestämmelse, likt den som föreslås för uppgifter i incidentrapporter och för uppgift om åtgärder, även för uppgifter om tillsyn och utredning. Utredningen lämnar ett förslag till ändring av bilagan till OSF i detta syfte, men med begränsningen att sekretessen inte ska gälla för beslut. Transportstyrelsen anser att det är angeläget att beslut vid tillsyn ska kunna beläggas med sekretess eftersom det i besluten bland annat hänvisas till brister som kan vara av sådan art att de bör kunna omfattas av sekretess enligt 30 kap. 23 § OSL. Enligt Transportstyrelsen bör även möjligheterna att sekretessbelägga identiteten på tillsynsobjekten i de beslut som fattas utredas vidare.

Enligt 30 kap. 23 § OSL och 9 § OSF gäller sekretess, i den utsträckning som anges i bilagan till förordningen, i en statlig myndighets verksamhet som består i utredning, planering, prisreglering, tillståndsgivning, tillsyn eller stödverksamhet med avseende på produktion, handel, transportverksamhet eller näringslivet i övrigt för bland annat uppgift om en enskilds affärs- eller driftförhållanden, uppfinningar eller forskningsresultat, om det kan antas att den enskilde lider skada om uppgiften röjs. I bilagan till OSF anges dels vad aktuell verksamhet består i, dels vilka särskilda begränsningar i sekretessen som gäller. Varken förslaget om förordningsändringar avseende sekretess hos tillsynsmyndigheterna eller förslaget om sekretess för diarium är dock föremål för denna lagrådsremiss.

Regeringen bedömer, som utredningen men till skillnad från *Domstolsverket* och *Länsstyrelsen i Kalmar län*, att 18 kap. 8 och 13 §§ OSL utgör tillräckligt skydd för förteckningar avseende verksamhetsutövare och uppgifter i riskanalyser och riskbedömningar som ska göras enligt den nya lagen.

SSM anför att en utredning bör se över förutsättningarna för utbyte av uppgifter som omfattas av sekretess med myndigheter och verksamhetsutövare utomlands. Utöver nämnda utredningsbehov finns det, enligt SSM, även behov av att utreda flera andra frågor om sekretess och sekretessbrytande bestämmelser. Det finns inte utrymme för att inom ramen för denna lagrådsremiss ge något ytterligare utredningsuppdrag och det har inte heller framkommit behov av andra ändringar än de ändringar som föreslås i övrigt. Det kan dock noteras att regeringen den 14 november 2024 har gett en särskild utredare i uppdrag att analysera hur en överföring av arbetsuppgifter med koppling till cyber- och informationssäkerhet kan genomföras från MSB till FRA (dir. 2024:111). Utredaren ska bland annat ta ställning till om det finns förutsättningar för att genomföra visst nödvändigt informationsutbyte. Uppdraget ska redovisas senast den 1 juli 2025.

Inget behov av ytterligare reglering för personuppgiftsbehandlingen

I NIS 2-direktivet anges att unionens dataskyddslagstiftning och integritetslagstiftning är tillämplig på all behandling av personuppgifter inom ramen för direktivet (skäl 14). Det anges vidare att direktivet i synnerhet inte påverkar tillämpningen av EU:s dataskyddsförordning. Detsamma anges gälla i förhållande till dataskyddsdirektivet, det vill säga 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.

I artikel 2.14 i NIS 2-direktivet fastslås också att entiteter, behöriga myndigheter, gemensamma kontaktpunkter och CSIRT-enheter ska behandla personuppgifter i den utsträckning som krävs för tillämpningen av direktivet och i enlighet med EU:s dataskyddsförordning. I synnerhet ska sådan behandling, enligt samma artikel, baseras på artikel 6 i EU:s dataskyddsförordning. Behandlingen av personuppgifter enligt NIS 2-direktivet ska vidare, av tillhandahållare av allmänna elektroniska kommunikationsnät eller tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster, utföras i enlighet med unionens dataskydds- och integritetslagstiftning, särskilt 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).

I avsnitt 10, som behandlar frågan om register för domännamnsregistreringsuppgifter, föreslås att personuppgifter endast ska få göras tillgängliga på internet om den registrerade har samtyckt till det. Verksamhetsutövaren som för register ska vara personuppgiftsansvarig för behandling av personuppgifter i registret. Fråga är om det i lagen i övrigt bör införas några bestämmelser om personuppgiftsbehandling.

Den myndighet som tar emot incidentrapporter kan få del av uppgifter om bland annat affärs- och driftförhållanden, och sådana uppgifter kan utgöra personuppgifter. Regeringen konstaterar också att myndigheten i viss utsträckning, i enlighet med utredningens förslag till förordning, kan komma att vidarebefordra personuppgifter till andra myndigheter. Vid handläggningen av ett ärende enligt den nya lagen kommer därmed personuppgifter av olika slag att behandlas av olika myndigheter med ansvar enligt regelverket. Behandlingen kommer att utföras som en följd av de arbetsuppgifter som myndigheten som tar emot rapporterna och tillsynsmyndigheterna får genom det samlade regelverket.

Behandling av personuppgifter kommer också, som *Tre* och *Växjö kommun* anger, att behöva utföras av verksamhetsutövarna, bland annat till följd av att de kommer att vara skyldiga att lämna uppgifter med anledning av den anmälnings-, rapporterings- och informationsskyldighet som föreslås i avsnitt 6.2 och 6.6 och i samband med tillsyn i enlighet med förslagen i avsnitt 7. Vad som krävs för att fullgöra informationsskyldigheten, som Tre resonerar kring, behandlas i avsnitt 6.6.

Den rättsliga grunden för den personuppgiftsbehandling som aktualiseras hos berörda myndigheter med särskilt ansvar enligt regelverket är att behandlingen är nödvändig för att utföra en uppgift av allmänt intresse som följer av föreslagen lag eller annan författning eller som ett led i myndighetsutövning enligt lagen eller annan författning på det sätt som anges i artikel 6.1 e i EU:s dataskyddsförordning. Eventuell behandling av personnummer och samordningsnummer hos de berörda myndigheterna är klart motiverad med hänsyn till ändamålet med behandlingen och vikten av en säker identifiering i enlighet med 3 kap. 10 § dataskyddslagen.

Den rättsliga grunden för den personuppgiftsbehandling som sker hos verksamhetsutövarna är att behandlingen är nödvändig för att fullgöra en

rättslig förpliktelse som följer av lag i enlighet med artikel 6.1 c i EU:s dataskyddsförordning och 2 kap. 1 § dataskyddslagen.

Sammanfattningsvis bedömer regeringen att EU:s dataskyddsförordning och dataskyddslagen ger stöd för den personuppgiftsbehandling som regelverket innebär. Det behöver inte införas någon ytterligare reglering för att behandlingen ska vara tillåten.

13 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag: Den nya lagen och övriga lagändringar ska träda i kraft den 15 januari 2026. Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster ska då upphöra att gälla.

För överträdelser som regleras i den nya lagen, men som har skett före ikraftträdandet av den lagen, ska lagen om informationssäkerhet för samhällsviktiga och digitala tjänster respektive lagen om elektronisk kommunikation fortfarande gälla.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår att den nya lagen och övriga lagändringar ska träda i kraft den 1 januari 2025. Utredningen lämnar inget förslag i fråga om att LEK ska gälla för vissa överträdelser som har skett före ikraftträdandet.

Remissinstanserna: Ett antal remissinstanser, bland andra *Företagarna*, *Hi3G Access AB*, *Lantbrukarnas riksförbund* och *Luftfartsverket*, påpekar att det av utredningen föreslagna ikraftträdandet ger berörda aktörer en mycket kort tid att anpassa sig efter de krav som den nya lagen innebär. *Försäkringskassan* bedömer att det krävs minst ett år för att säkerställa att samtliga krav uppfylls från det att föreskrifter har meddelats av berörda myndigheter. Myndigheten anser att sanktionsbestämmelserna inte bör tillämpas förrän verksamhetsutövarna har getts skälig tid att implementera åtgärderna. *Teknikföretagen* och *Teracom* föreslår att regeringen ska överväga att instruera tillsynsmyndigheterna att tillämpa ”grace periods” med innebörden att myndigheterna inledningsvis ska fokusera på att ge stöd i tillämpningen och vara restriktiva med att besluta om sanktioner. *Statens servicecenter* efterfrågar en övergångsbestämmelse eller ett förtydligande på annat sätt om vilka säkerhetsåtgärder en verksamhetsutövare är skyldig att vidta i förhållande till redan befintliga leverantörer. *Sveriges advokatsamfund* gör gällande att sanktionsbestämmelserna inte bör tillämpas före det att tillsynsmyndigheterna har klargjort vilka verksamheter som omfattas av verksamhetsdefinitionerna och berörda verksamhetsutövare fått erforderlig tid att anpassa sin verksamhet till den nya lagens krav. *Telenor Sverige AB* bedömer att en mer rimlig tid för lagen att träda i kraft är den 1 juli 2025, alternativt att lagen träder i kraft tidigare men att den tillämpas på relevanta verksamhetsutövare från den 1 juli 2025 samt att tidigare gällande bestämmelser övergångsvis gäller fram till dess.

En arbetsgrupp inom Cybernoden anser att det krävs ett förtydligande i fråga om en EU-rättslig direkt effekt trätt i kraft den 18 oktober 2024, när direktivet började tillämpas, och i fråga om vad som gäller rättsligt för aktörer som inte omfattas av den nya lagen men som måste uppfylla lagens krav i förhållande till verksamhetsutövare som gör det.

Skälen för regeringens förslag: Av artikel 41 i NIS 2-direktivet följer att medlemsstaterna senast den 17 oktober 2024 ska anta och offentliggöra de bestämmelser som är nödvändiga för att följa direktivet. Bestämmelserna ska tillämpas från och med den 18 oktober 2024.

Den nya lagen bör träda i kraft så snart som möjligt. Lagens tillämpningsområde föreslås dock avgränsas närmare inom ramen för föreskrifter på en lägre normgivningsnivå och dessa föreskrifter måste ha utfärdats innan lagen kan tillämpas fullt ut. Tillsynsmyndigheterna och berörda verksamhetsutövare måste också, som till exempel *Teracom* resonerar kring, ges möjlighet att anpassa sin verksamhet i den utsträckning som krävs för att de ska kunna fullgöra sina uppgifter respektive skyldigheter enligt den nya lagen. Det finns inte anledning att låta vissa delar av lagen träda i kraft senare än andra. Det finns inte heller någon möjlighet för regeringen att ge tillsynsmyndigheterna sådana instruktioner som exempelvis *Teknikföretagen* nämner. Som utvecklas i avsnitt 14.2 avser regeringen också att återkomma i budgetpropositionen för 2026 om hur kommunernas och regionernas ökade kostnader ska hanteras. Med hänsyn till detta och vid en samlad bedömning anser regeringen att lagen i sin helhet bör träda i kraft den 15 januari 2026. Även övriga lagändringar bör träda i kraft detta datum. NIS-lagen bör upphöra att gälla samma datum.

NIS 2-direktivet innehåller inga övergångsbestämmelser. Genom den nya lagen införs bland annat nya och strängare sanktioner än vad som gäller enligt NIS-lagen. Dessa bestämmelser kan inte ges retroaktiv effekt. I enlighet med utredningens förslag bör NIS-lagen gälla för överträdelser som har skett före ikraftträdandet, det vill säga före den 15 januari 2026. På samma sätt bör LEK gälla för överträdelser enligt den lagen som har skett före ikraftträdandet av den nya lagen. Regeringen instämmer i utredningens uppfattning om att det saknas behov av ytterligare övergångsbestämmelser.

En arbetsgrupp inom Cybernoden och *Statens servicecenter* resonerar bland annat kring vad som gäller i förhållande till redan ingångna avtal. Arbetsgruppen efterfrågar också ett förtydligande i fråga om NIS 2-direktivet har så kallad direkt effekt. Principen om direkt effekt innebär att enskilda kan åberopa unionsrättsliga bestämmelser inför nationella domstolar och myndigheter, under förutsättning att de är tillräckligt klara, precisa och ovillkorliga. Detta innebär att EU-rätten inte bara ger upphov till skyldigheter för medlemsstaterna utan även till rättigheter för enskilda personer. Sådan direkt effekt kallas vertikal direkt effekt. Så kallad horisontell direkt effekt kan inte tillämpas med stöd av ett direktiv eftersom ett direktiv enligt unionsrätten inte i sig kan medföra skyldigheter för en enskild (se till exempel EU-domstolens dom den 11 april 2024, Gabel Industria Tessile och Canavesi, C-316/22, EU:C:2024:301, punkterna 23–25). NIS 2-direktivet innebär därmed inga skyldigheter för dem som omfattas av den nya lagen förrän regelverket har trätt i kraft. I fråga om vad som gäller om en verksamhetsutövares skyldighet att vidta åtgärder i

förhållande till befintliga leverantörer och leveranser konstaterar regeringen att det är en huvudprincip i svensk rätt att civilrättslig lagstiftning inte ska ges retroaktiv effekt. Frågan behandlas dock i avsnitt 6.4.

14 Konsekvenser av förslagen

14.1 Konsekvenser för cybersäkerheten och samhällsekonomin

Regeringens bedömning: Förslagen innebär att cybersäkerheten i samhället stärks och de samhällsekonomiska effekterna av förslagen är godtagbara.

Utredningens bedömning överensstämmer i stort med regeringens. Utredningen gör ingen bedömning när det gäller inverkan på samhällsekonomin.

Remissinstanserna: Majoriteten av remissinstanserna välkomnar en ny cybersäkerhetslagstiftning och ser positivt på att samhället på bred front ska arbeta systematiskt och riskbaserat för att höja cybersäkerhetsnivån i Sverige och inom EU. *Region Sörmland* framhåller att samhällsviktiga funktioner genom förslagen ökar sin motståndskraft mot cyberangrepp. *Östersunds kommun* anför att direktivet kommer att ge synergieffekter och förenkla för alla berörda och i slutändan för den enskilda medborgaren.

Ett fåtal remissinstanser kommenterar de samhällsekonomiska effekterna av förslagen. *Energiföretagen Sverige* påpekar att vissa administrativa pålagor, som att rapportera incidenter på verksamhetsnivå i stället för koncernnivå, riskerar att hindra snabb krishantering av cyberangrepp, vilket inte kommer att bidra till ekonomisk effektivitet i enlighet med direktivets syfte. *Kemikalieinspektionen* anser att det är rimligt att sätta av resurser för att säkerställa en högre cybersäkerhetsnivå än i dag. *Luftfartsverket (LFV)* bedömer att ett systematiskt och riskbaserat informationssäkerhetsarbete och ett proaktivt it-säkerhetsarbete långsiktigt medför minskade kostnader. *Region Skåne* bedömer, till skillnad från utredningen, inte att färre incidenter, till följd av de ökade kraven och den på sikt förmodade förbättrade säkerheten, ger lägre kostnader.

Skälen för regeringens bedömning: Det försämrade säkerhetspolitiska omvärldsläget med hot och krigföring inom cyberdomänen kräver en avsevärt högre nivå av motståndskraft i Sverige och inom EU. Det krävs, som anges i avsnitt 5.1, en ny lag för att hantera de risker som hotar säkerheten i nätverks- och informationssystem och för att genomföra NIS 2-direktivet i nationell rätt. Den nya lagen säkerställer att verksamhetsutövare som tillhandahåller för samhället grundläggande tjänster vidtar säkerhetsåtgärder och bland annat rapporterar incidenter i syfte att öka den övergripande förmågan i samhället att förebygga, hantera och återhämta sig från cyberattacker och andra it-incidenter. Förslagen innebär att cybersäkerheten i samhället stärks.

Ett antal remissinstanser yttrar sig gällande de samhällsekonomiska effekterna av förslagen. Det kan konstateras att den föreslagna lagen är en

förutsättning för att genomföra NIS 2-direktivet i svensk rätt. EU-kommissionen har i sin konsekvensbedömning uppskattat att införandet av bestämmelserna i NIS 2-direktivet kan leda till en minskning av kostnaderna för cyberincidenter med 11,3 miljarder euro inom unionen. Detta framgår av Förslag till Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148, COM(2020) 823 final.

Regeringen bedömer, i likhet med EU-kommissionen och till skillnad från *Region Skåne*, att en konsekvent nivå av cyberresiliens hos centrala verksamhetsutövare kan leda till kostnadsbesparingar för verksamhetsutövarna på längre sikt även om det på kort sikt kan uppstå kostnader för att möta kraven. Vidare kan höjda cybersäkerhetsnivåer bidra till att minska negativa konsekvenser av cybersäkerhetsincidenter, vilket i sin tur kan ha en positiv inverkan på tillväxt och investeringar och därmed samhällsekonomin i stort. De samhällsekonomiska effekterna är oavsett godtagbara givet bakgrunden och syftet med regelverket.

14.2 Ekonomiska konsekvenser för den offentliga sektorn

Regeringens bedömning: Förslagen innebär ökade kostnader för tillsynsmyndigheterna. De ökade kostnaderna för dessa myndigheter finansieras genom medel som tillfördes i budgetpropositionen för 2025. Kostnaderna kan också komma att finansieras genom avgifter när det gäller tillsyn över viss del av sektorn digital infrastruktur.

Förslagen leder till ökade kostnader för kommuner och regioner. Regeringen avser att återkomma i budgetpropositionen för 2026 om finansieringen av dessa kostnader.

Förslagen innebär ökade kostnader för allmänna förvaltningsdomstolar. Kostnaderna ryms inom domstolarnas befintliga anslagsramar. De kostnadsökningar som förslagen medför för övriga statliga myndigheter kan också hanteras inom befintliga ekonomiska ramar.

Utredningens bedömning överensstämmer delvis med regeringens. Utredningen bedömer att tillsynen ska finansieras enbart genom ökade anslag. Utredningen bedömer att det inte krävs någon finansiering för kommuner och regioner. Utredningen gör ingen bedömning i fråga om konsekvenser för allmänna förvaltningsdomstolar.

Remissinstanserna: Ett stort antal remissinstanser, däribland *Livsmedelsverket, Myndigheten för samhällsskydd och beredskap (MSB), Länsstyrelsen i Stockholms län, SJ AB, Skatteverket, Tillväxtverket* och ett antal regioner, anser att behövs kompletterande analyser av vilka ekonomiska konsekvenser som förslagen innebär för den offentliga sektorn och att tillräckliga resurser för implementering av NIS 2-direktivet behöver säkerställas.

Ett antal myndigheter som utredningen föreslår ska pekas ut som tillsynsmyndigheter, bland andra *Finansinspektionen*, Livsmedelsverket, *Läkemedelsverket, Post- och telestyrelsen (PTS)* och *Statens energimyndighet*, gör en annan bedömning än utredningen i fråga om vilka kostnader

som förslagen innebär för dem. Ett antal länsstyrelser bedömer, till skillnad från utredningen, att kostnaderna inte kan finansieras inom deras befintliga ekonomiska ramar. *Transportstyrelsen* bedömer att utredningens förslag i fråga om myndighetens anslag skulle innebära en försämring av dess möjlighet att utöva tillsyn.

Domstolsverket konstaterar att domstolarna inte nämns i utredningens konsekvensanalys och efterfrågar kompletterande analys. *Förvaltningsrätterna i Malmö* och *Stockholm* och *Kammarrätten i Stockholm* anser att kostnaderna för domstolarna behöver analyseras och att domstolarna bör få ytterligare resurser.

Flera andra statliga myndigheter, bland andra *Bolagsverket, Försvarshögskolan, Försäkringskassan* och *Säkerhetspolisen,* framhåller att förslagen aktualiserar behov av ökade resurser för offentliga verksamhetsutövare. Bolagsverket bedömer också bland annat att förslagen innebär att ett nytt it-stöd behöver finnas på myndigheten. Säkerhetspolisen förutser exempelvis att förslagen riskerar att leda till flera komplicerade gränsdragningar i förhållande till verksamhet som omfattas av säkerhetsskyddslagen och att frågor till tillsynsmyndigheterna enligt säkerhetsskyddslagen kommer att öka. *Jordbruksverket*, *Kemikalieinspektionen* och *länsstyrelserna i Norrbottens* och *Västra Götalands län* bedömer att förslagen kommer att leda till konkurrens om cybersäkerhetskompetens och att detta riskerar att driva upp lönekostnaderna. *Patent- och registreringsverket (PRV)* menar att ett mer omfattande och riktat stöd till myndigheten från bland annat MSB till viss del skulle kunna påverka behovet av rekrytering och resurspåverkan. *Kronofogdemyndigheten* bedömer att myndighetens kostnader ryms inom befintlig anslagsram, men tillägger att finansiering behöver säkerställas om kommande föreskrifter blir kostnadsdrivande. En majoritet av lärosätena uttrycker att de ställer sig bakom remissyttrandet från *Sveriges universitets- och högskoleförbund* (*SUHF*) och bedömer därmed att utredningens förslag kommer att leda till betydande kostnadsökningar och en ökad administrativ börda vid universitet och högskolor.

Sveriges Kommuner och Regioner (SKR) anser att kostnadseffekterna av förslagen bör finansieras av staten i enlighet med finansieringsprincipen. Ett stort antal kommuner, däribland *Linköpings kommun*, *Malmö kommun*, *Stockholms kommun* och *Östhammars kommun*, framhåller att kommunerna behöver tilldelas ökade resurser. *Karlstads kommun* bedömer även att det kan blir svårt för mindre kommuner att hitta kompetens inom cybersäkerhet. *Region Gotland* bedömer att det föreslagna utbildningskravet kommer att bli kostnadsdrivande och att utredningens ekonomiska analys är otillräcklig. Även *Region Skåne, Region Stockholm* och *Region Sörmland* bedömer att regionerna behöver få ersättning för att uppfylla de skärpta krav som följer av den nya lagen.

Skälen för regeringens bedömning

Konsekvenser för tillsynsmyndigheterna

Utredningen föreslår att Finansinspektionen, Inspektionen för vård- och omsorg (IVO), Livsmedelsverket, Läkemedelsverket, PTS, Statens energimyndighet, Transportstyrelsen samt länsstyrelserna i Norrbottens, Skåne, Stockholms och Västra Götalands län ska utses till tillsynsmyndig-

heter genom utpekande i förordning. Tillsynsmyndigheternas ska bland annat utöva tillsyn över att verksamhetsutövarna uppfyller sina skyldigheter att vidta säkerhetsåtgärder. Utredningen föreslår att PTS ska pekas ut som tillsynsmyndighet för bland annat sektorn digital infrastruktur.

Vad gäller de ekonomiska konsekvenserna för tillsynsmyndigheterna bedömer utredningen att det för närvarande inte är möjligt att dra tillförlitliga slutsatser om de löpande kostnaderna för tillsynsmyndigheterna under en treårsperiod och att det krävs kompletterande analyser. Utredningen anser därför att de föreslagna tillsynsmyndigheterna, förutom Finansinspektionen, bör få en skönsmässig ökning av anslag och att regeringen bör ge Statskontoret i uppdrag att göra en kartläggning av kostnaderna för tillsynsverksamheten.

Regeringen gav den 24 oktober 2024 Statskontoret i uppdrag att utreda de ekonomiska konsekvenserna för tillsynsmyndigheternas verksamhet till följd av NIS 2-direktivet (Fö2024/01753). Uppdraget redovisades den 11 april 2025 i rapporten Tillsynsmyndigheternas kostnader till följd av NIS 2-direktivet (2025:8). Av rapporten framgår bland annat att myndigheterna uppskattar initiala kostnaderna till över 150 000 000 kronor för samtliga tillsynsmyndigheter och löpande kostnader till mer än 185 000 000 kronor totalt per år. De initiala uppskattade kostnaderna varierar kraftigt mellan tillsynsmyndigheterna. Statskontoret framhåller att beräkningarna i rapporten bygger på uppskattningar från myndigheterna och att de uppskattade kostnaderna är mycket preliminära.

Ett flertal av de myndigheter som föreslås utses till tillsynsmyndigheter av utredningen har synpunkter på utredningens konsekvensanalys. *Länsstyrelserna i Norrbottens* och *Västra Götalands län* pekar till exempel på att bristen på kompetens inom cybersäkerhetsområdet kommer att innebära en ökning av lönekostnaderna för personal hos tillsynsmyndigheterna. Regeringen delar remissinstansernas uppfattning att det finns kompetensförsörjningsbehov inom cybersäkerhetsområdet.

I avsnitt 7.1 föreslår regeringen att tillsynsmyndigheterna ska pekas ut i förordning och vilka sektorer som tillsynsmyndigheterna ska ansvara för föreslås inte heller regleras i lag. Samtliga myndigheter som utredningen föreslår ska pekas ut som tillsynsmyndigheter, förutom Finansinspektionen, fick av regeringen i budgetpropositionen för 2025 ökade anslag med sammanlagt 28 000 000 kronor. Detta med anledning av deras utökade ansvar i samband med NIS 2-direktivet och den kommande nationella lagstiftningen. I avsnitt 7.3 föreslås vidare att det ska införas en bestämmelse i lagen som ger tillsynsmyndigheten för en viss del av sektorn digital infrastruktur rätt att ta ut avgifter för sin tillsyn. PTS har i dag, som utvecklas i avsnittet, motsvarande möjlighet att ta ut avgifter enligt LEK. Förslaget om avgiftsrätt innebär att PTS, i det fall det rör sig om tillsyn inom sektorn som i dag omfattas av LEK, inte kommer att påverkas finansiellt av förslagen i denna lagrådsremiss. Genom fortsatt avgiftsfinansiering skulle myndigheten ges finansiella förutsättningar för att säkerställa att NIS 2-direktivets och lagens krav följs när det gäller en viss del av sektorn digital infrastruktur. Avgiftsrätten gäller inte för tillsyn av andra verksamhetsutövare än verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster i Sverige. För övrig tillsyn kommer tillsynsmyndigheten inte kunna ta ut avgifter. De ökade kostnaderna för

tillsynsmyndigheterna finansieras sammanfattningsvis genom medel som tillfördes i budgetpropositionen för 2025 och genom avgiftsrätt i viss del.

Konsekvenser för övriga statliga myndigheter

Förslagen innebär även skyldigheter och nya uppgifter för vissa andra statliga myndigheter än tillsynsmyndigheterna. Förslagen i denna lagrådsremiss innebär förvisso att de statliga myndigheter som omfattas av lagen behöver vidta vissa åtgärder med koppling till deras cybersäkerhet som kan vara kostnadsdrivande. Samtidigt är åtgärderna i stor utsträckning förenliga med relevanta europeiska och internationella standarder på området.

Regleringen i NIS 2-direktivet utgör en grundplatta av säkerhetsåtgärder som det i hög utsträckning råder samsyn om bör vidtas inom cybersäkerhetsområdet. Många aktörer arbetar redan aktivt utifrån dessa åtgärder för att förhindra cybersäkerhetsincidenter, medan andra behöver genomföra vissa förändringar för att nå upp till de krav som föreslås gälla i denna lagrådsremiss. Åtgärderna kommer att leda till högre motståndskraft mot cybersäkerhetsincidenter och effekterna kommer enligt regeringens bedömning sannolikt att uppväga eventuella kostnader.

Regeringens sammantagna bedömning är att kostnaderna för berörda myndigheter inte bör vara så stora att de inte kan hanteras inom givna budgetramar och att det inte krävs någon ytterligare analys som en stor andel remissinstanser och till exempel *SJ AB* efterfrågar. De konsekvenser som *Bolagsverket* beskriver kopplat till utvecklingskostnader för avregistrering, som är en del av utredningens förordningsförslag och inte föremål för denna lagrådsremiss, bör inte heller vara av sådan omfattning att de inte ryms inom given budgetram. Det krävs inte heller ytterligare finansiering med anledning av det som exempelvis *Säkerhetspolisen* framhåller.

Flera myndigheter, bland andra *Jordbruksverket* och *Kemikalieinspektionen*, lyfter att det kommer att bli stor konkurrens om personal med cybersäkerhetskompetens. Regeringen instämmer i att kompetensbrist kan bli en utmaning för alla som berörs av det nya regelverket. Riktat stöd från andra myndigheter kan dock bidra till att minska behovet av rekrytering och regeringen har därför ökat anslaget för ett antal myndigheter.

Konsekvenser för kommuner och regioner

Den kommunala finansieringsprincipen innebär att kommuner och regioner ska kompenseras för statligt beslutade åtgärder som direkt tar sikte på den kommunala verksamheten. Principen gäller när riksdagen, regeringen eller en myndighet fattar bindande beslut om ändrade regler för verksamhet.

Förslagen innebär att kommuner och regioner, liksom andra verksamhetsutövare, bland annat ska vidta säkerhetsåtgärder och i vissa fall rapportera incidenter. Utredningen bedömer att förslagen är sådana att kommuner och regioner kan behöva avsätta ytterligare resurser för cybersäkerhetsarbetet. Samtidigt kommer detta arbete också, enligt utredningen, att leda till minskad förekomst av incidenter och därmed minskade kostnader för hantering av sådana. *Stockholms kommun*

invänder dock mot denna argumentation och menar att de högre kraven innebär att fler incidenter identifieras och behöver hanteras samt att fler organisatoriska och tekniska åtgärder kommer att krävas. *Östersunds kommun* påpekar vidare att förslagen kommer att innebära en högre grad av rapporteringsskyldigheter och större risker för kostnader i form av sanktionsavgifter.

Regeringen invänder inte mot utredningens uppfattning om att effekten av kraven i den nya lagen i förlängningen kan innebära kostnadsbesparingar för verksamhetsutövarna. Att kunna förebygga incidenter, upptäcka dem i tid och hantera dem på ett effektivt sätt kan i slutändan innebära att både verksamhetsutövaren lider mindre skada och att det inte uppstår spridningseffekter till andra. I fråga om sanktionsavgifter, som Östersunds kommun lyfter fram, är det rimligt att utgå från att tillsynsmyndigheternas beslut om sådana kommer att överklagas till allmän förvaltningsdomstol i relativt stor utsträckning, bland annat eftersom avgifterna kan vara ekonomiskt kännbara. Sannolikt kommer det dock inte bli fråga om särskilt många beslut om sanktionsavgifter riktade mot kommunerna och regionerna.

Ett antal remissinstanser framhåller att mindre kommuner har särskilda utmaningar att hitta den kompetens som krävs för att genomföra de åtgärder som kommer att krävas enligt förslagen och därför kan behöva upphandla sådana tjänster. Även en majoritet av regionerna understryker att förslagen är kostnadsdrivande och pekar på problematiken med kompetensförsörjning. Liksom för berörda statliga myndigheter bedömer regeringen att det finns möjligheter för kommuner och regioner att samverka kring både upphandlingar av stödtjänster och kring kompetensförsörjning för att effektivisera arbetet och minska kostnaderna. Att kraven kommer att se lika ut för alla kommuner och regioner är något som får anses vara fördelaktigt i sammanhanget.

Kostnaderna för kommuner och dåvarande landsting ansågs i samband med genomförandet av NIS-direktivet vara begränsade (se prop. 2017/18:205 s. 89). Förslagen i denna lagrådsremiss är visserligen i viss mån överensstämmande med vad som gäller enligt europeiska och internationella standarder inom cybersäkerhetsområdet och många aktörer vidtar redan aktuell slags åtgärder att förhindra cybersäkerhetsincidenter. Förslagen leder dock till ökade kostnader för kommuner och regioner som kräver finansiering enligt den kommunala finansieringsprincipen. Regeringen avser att återkomma i budgetpropositionen för 2026 om finansieringen av dessa kostnader.

Konsekvenser för allmänna förvaltningsdomstolar

Till exempel *Förvaltningsrätten i Malmö* anser att kostnaderna för domstolarna behöver analyseras och att domstolarna bör få ytterligare resurser. Förslagen innebär att fler överklagbara beslut kan komma att fattas av de myndigheter som ska utöva tillsyn och att en ny måltyp som ska hanteras med förtur införs för de allmänna förvaltningsdomstolarna. Regeringen föreslår nya former av ingripanden jämfört med NIS-lagen. Förslagen kan påverka måltillströmningen. Det är dock svårt att bedöma eventuella merkostnader för domstolarna eftersom det är osäkert hur stor måltillströmingen kommer att bli. Sedan NIS-lagen infördes har endast ett

fåtal beslut med stöd av den lagen blivit föremål för domstolsprövning, vilket kan vara en indikation på att inte heller förslagen i denna lagrådsremiss kommer att leda till en stor ökning av ärenden hos domstolarna. Vidare är beslutet om förbud att inneha ledningsfunktion ett ingripande som föreslås bli aktuellt endast om överträdelsen som ligger till grund för föreläggandet är allvarlig och om befattningshavaren i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen (se vidare avsnitt 8.6). Sådana beslut bör därmed endast fattas i ett mycket begränsat antal fall och överklaganden blir således något som kommer att tillhöra ovanligheterna. Beslut av regeringen som innefattar en prövning av en enskilds civila rättigheter eller skyldigheter kan bli föremål för rättsprövning av Högsta förvaltningsdomstolen enligt lagen om rättsprövning av vissa regeringsbeslut. Antalet beslut om undantag från skyldigheterna enligt lagen, med stöd av förslagen i avsnitt 5.3.2 och 5.3.4, och därmed eventuella mål om rättsprövningar hos Högsta förvaltningsdomstolen, förväntas bli lågt. Regeringens sammantagna bedömning är därmed att eventuella merkostnader för domstolarna kan hanteras inom befintliga anslag.

14.3 Konsekvenser för enskilda

Regeringens bedömning: Förslagen kan innebära ökade kostnader och kommer att innebära administrativa bördor för enskilda verksamhetsutövare.

Förslagen är förenliga med näringsfriheten.

Förslaget om register för domännamnsregistreringsuppgifter innebär en godtagbar risk för ökat integritetsintrång.

En utvärdering av konsekvenserna för företagen bör ske tre år efter ikraftträdandet av den nya lagen.

Utredningens bedömning i fråga om ekonomiska konsekvenser överensstämmer med regeringens. Utredningen gör ingen särskild bedömning i förhållande till näringsfriheten och den personliga integriteten. Utredningen gör inte heller någon särskild bedömning av om en utvärdering ska ske.

Remissinstanserna: *Stiftelsen för internetinfrastruktur (Internetstiftelsen)* lyfter att regleringen om domännamnsregistrering riskerar att slå oproportionerligt mot mindre aktörer på marknaden och att regleringen i förlängningen riskerar att försvåra för en effektiv konkurrens.

Flera remissinstanser, däribland *Energiföretagen Sverige* och *Svenskt Näringsliv*, framhåller att konsekvenserna av förslagen är beskrivna på ett bristfälligt sätt och efterfrågar en mer gedigen konsekvensanalys vad gäller företagens merkostnader och förslagens inverkan på konkurrensförhållandena. *Orange Cyberdefense* framför att det är viktigt att konkurrensen på marknaden för oberoende säkerhetsgranskningar inte snedvrids. *Regelrådet* finner att konsekvensutredningen inte uppfyller kraven i 6 och 7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning då det inte finns någon information om vilka företag som berörs och hur de påverkas av regleringen. *Tech Sverige* och *Teknikföretagen* ansluter sig till Regelrådets remissvar. *Svensk Handel*

anser att det krävs en tydligare analys av förslagens lämplighet och proportionalitet eftersom utredningen lämnar förslag som innebär strängare krav än direktivet. *SJ AB* och *Tågföretagen* bedömer att kraven kommer att medföra betydande merkostnader snarare än besparingar mot bakgrund av antalet större incidenter som registrerades i SJ AB:s och Tågföretagens medlemmars verksamhet under 2023. *Swedac* bedömer att utredningens förslag gällande tillsynsmyndigheter och föreskriftsrätt kommer att resultera i en komplex struktur både vad gäller tillsynsverksamheten och regelbördan för inblandade aktörer.

Skälen för regeringens bedömning

Konsekvensanalys i andra sammanhang

EU-kommissionen har uppskattat att utgifterna för de företag som omfattas av NIS 2-regelverket kommer att öka med högst 22 procent under de första åren efter införandet av de nya reglerna (se Förslag till Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148, COM[2020]823 final). För företag som omfattas av NIS-direktivet uppskattas utgifterna öka med 12 procent. Samtidigt understryker kommissionen att det också kan bli fråga om besparingar för berörda företag med hänvisning till att kostnaderna för att hantera cybersäkerhetsincidenter kommer att minska. EU-kommissionen uppskattar att sådana besparingar kommer att motsvara ca 118 000 000 000 euro under en tioårsperiod. EU-kommissionen uppskattar vidare att utgifterna för cybersäkerhet kommer att uppgå till i genomsnitt 0,52 procent av den årliga omsättningen inom de olika sektorerna (se följedokument till Förslag till Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148, SWD[2020] 345 final).

I propositionen som avser genomförandet av NIS 2-direktivet i Finland anges att it-kostnader i genomsnitt uppgår till ca 4–5 procent av ett företags omsättning. Beroende på aktörens storlek, cybermognad och vilken sektor företaget omfattas av, bedöms variationsintervallet uppgå till 1,5–5 procent. Inom livsmedelssektorn bedöms exempelvis kostnaderna för cybersäkerhet uppgå till i genomsnitt 0,28 procent av den årliga omsättningen och inom tillverkningssektorn till 0,69 procent av den årliga omsättningen (se RP 57/2024 rd, s. 88). Kostnaderna för hanteringen av cybersäkerhetsrisker för ett företag som omfattas av tillämpningsområdet för den finländska cybersäkerhetslagen uppskattas uppgå till ca 0,2–0,8 procent av den årliga omsättningen med den miniminivå som den finska lagen kräver, om man jämför med en nivå där företaget inte tidigare vidtagit några åtgärder för att hantera sådana risker. Det betonas att bedömningarna är förenade med betydande osäkerhet när det gäller skillnaderna mellan olika företag.

I samband med beredningen av den finska propositionen genomfördes en utredning om de kostnader som skyldigheten enligt artikel 21 i NIS 2-direktivet, som gäller riskhanteringsåtgärder, kommer att innebära för de finländska företagen. Syftet med utredningen var att bedöma kostnaderna inom sektorerna livsmedel och tillverkning, eftersom företagen som ingår i dessa sektorer inte omfattades av tillämpningsområdet för NIS-direktivet

och ett betydande antal företag inom sektorerna kommer att omfattas av tillämpningsområdet för den regleringen som genomför NIS 2-direktivet i Finland. Genom utredningen försökte man klarlägga antalet årsarbetskrafter som fullgörandet av skyldigheterna att vidta riskhanteringsåtgärder i enlighet med NIS 2-direktivet ger upphov till samt andra kostnader som uppkommer i form av engångskostnader och löpande kostnader under ett år. Totalt 20 företag deltog i en enkätstudie och resultatet baseras på företagens uppskattningar.

Enligt utredningen innebär skyldigheterna för företagen inom livsmedels- och tillverkningssektorn en engångskostnad på i genomsnitt ca 320 000 euro per företag, av vilket 27 procent utgör arbetskostnader och 73 procent övriga kostnader. De kostnader som är av löpande karaktär uppgår enligt utredningen till i genomsnitt ca 214 000 euro, av vilket 26 procent är arbetskostnader och 74 procent övriga kostnader. Inom livsmedelssektorn uppskattades genomsnittskostnaderna bli lägre än inom tillverkningssektorn. Inom livsmedelssektorn uppskattades engångskostnaderna uppgå till 274 000 euro och de löpande kostnaderna till 148 000 euro. Inom tillverkningssektorn uppskattades engångskostnaderna uppgå till 367 000 euro och de löpande kostnaderna till 279 000 euro. Angivna kostnader bedöms vara en form av maximum. Resultaten av utredningen ansågs inte kunna ge en generell bild av kostnader som uppstår till följd av NIS 2-direktivet, bland annat på grund av det begränsade urvalet av företag. I propositionen anges att kostnadernas storlek i betydande grad påverkas av flera faktorer, bland annat ett företags storlek och företagsstruktur.

För andra sektorer än livsmedelssektorn och tillverkningssektorn går det, enligt den finska propositionen, inte att göra liknande uppskattningar (se RP 57/2024 rd, s. 103). De ekonomiska konsekvenserna av förslagen påverkas bland annat av den allmänna nivån på cybermognad hos sektorerna och aktörerna samt på förmågor som för närvarande varierar såväl mellan olika sektorer som mellan olika aktörer. Det var enligt utredningen inte heller möjligt att säkert bedöma kostnadsnyttan för företagen.

Förutom de kostnader som beror på riskhanteringsskyldigheterna kommer skyldigheten att rapportera betydande incidenter och skyldigheten att anmäla sig till den förteckning över aktörer som tillsynsmyndigheten för, enligt den finska utredningen, att medföra smärre kostnader för aktörerna. Det nämns också att det kan uppstå kostnader för företagen på grund av sådana tillsynsåtgärder som tillsynsmyndigheten riktar mot ett företag.

Det danska lagförslaget väntas få betydande negativa ekonomiska konsekvenser för ca 3 255 företag i Danmark (se Forslag til Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau [NIS 2-loven] s. 42 f.). Baserat på data från en utredning genomförd av det danska Klimat-, energi- och försörjningsministeriet beräknas de administrativa kostnaderna, med stor osäkerhet, uppgå till sammanlagt ca 2,8–3,3 miljarder DKK i engångskostnader och ca 0,7–1,2 miljarder DKK årligen i löpande utgifter. Förslaget beräknas också medföra andra ekonomiska konsekvenser för näringslivet. Det har dock uttalats att de ekonomiska konsekvenserna för enskilda aktörer ska beräknas först efter lagens ikraftträdande.

Konsekvenser för dem som omfattas av den svenska lagen

Den föreslagna regleringen kommer, precis som NIS-lagen, att innehålla bestämmelser som innebär att enskilda aktörer behöver uppfylla vissa krav. Ett antal remissinstanser, bland andra *Svenskt Näringsliv* och *Tech Sverige*, har synpunkter på utredningens beskrivning av vilka konsekvenser som förslagen innebär för enskilda aktörer som omfattas av regelverket. *Regelrådet* bedömer att utredningens konsekvensutredning inte uppfyller kraven i 6 och 7 §§ i den numera upphävda förordningen (2007:1244) om konsekvensutredning vid regelgivning då det inte finns någon information om vilka företag som berörs och hur de påverkas av regleringen. *SJ AB* och *Tågföretagen* bedömer att kraven enligt den nya lagen kommer att medföra betydande merkostnader snarare än besparingar.

Regeringen uppskattar, med stöd av beräkningar som har gjorts inom Regeringskansliet, att drygt 1 500 företag i Sverige med sammanlagt runt 500 000 sysselsatta skulle kunna beröras av den nya lagen och tillhörande föreskrifter. I beräkningen ingår företag som har minst 50 personer anställda. Lagen kommer dock i vissa fall att gälla även för verksamhetsutövare som inte behöver uppfylla ett storlekskrav (se avsnitt 5.3.2).

Vilka företag som träffas av den nya lagen och vilka åtgärder som de ska vidta är i allt väsentligt en följd av direktivets utformning. Det står klart att förslagen kan innebära ökade kostnader och administrativa bördor för de företag som kommer att räknas som enskilda verksamhetsutövare. Detta gäller även med beaktande av den omständigheten att förslagen också, som EU-kommissionen bedömer, kan innebära minskade kostnader för hanteringen av cybersäkerhetsincidenter. Frågan är dock om det går att utveckla vilka ökade kostnader och administrativa bördor som regelverket innebär för enskilda verksamhetsutövare.

När det gäller skyldigheten att göra en anmälan bör det, bland annat med hänvisning till vilken arbetstid som kan komma i fråga för att genomföra denna åtgärd, generellt sett endast bli fråga om mindre kostnader för enskilda verksamhetsutövare. Denna engångskostnad kan till exempel begränsas genom att det införs en möjlighet att göra en anmälan via ett centraliserat system. Det analysarbete som krävs för att bedöma om aktören omfattas av lagen, och om en anmälan därmed ska göras, kommer att underlättas genom stöd och tydlig vägledning från berörda myndigheter.

När det gäller skyldigheten att rapportera betydande incidenter bedömer regeringen att kostnaderna hänförliga till denna skyldighet också bör bli begränsade. Även om incidenter på cybersäkerhetsområdet är vanligt förekommande bör det generellt sett röra sig om ett begränsat antal fall som ett enskilt företag behöver rapportera, särskilt eftersom endast betydande incidenter ska rapporteras. Kostnaderna för rapportering kan också till exempel begränsas genom att det införs en möjlighet att rapportera incidenter via ett centraliserat system. Inte heller fullgörandet av informationsskyldigheten som behandlas i avsnitt 6.6.3 bör innebära någon större kostnad eftersom denna skyldighet enbart gäller vid betydande incidenter och betydande cyberhot. Den bör därför som utgångspunkt inte heller aktualiseras särskilt frekvent.

I fråga om kostnader kopplade till tillsynsåtgärder konstaterar regeringen att möjligheten att vidta sådana åtgärder varierar beroende av om det är fråga om en viktig eller en väsentlig verksamhetsutövare (se avsnitt 5.3.5 och 7.2.4). För sådana som räknas som viktiga verksamhetsutövare får tillsynsåtgärder vidtas endast när en tillsynsmyndighet har anledning att anta att regleringen inte följs. För riktade säkerhetsrevisioner krävs vidare att det föreligger särskilda skäl. Skyldigheten att medverka till tillsynsåtgärder, när sådana väl vidtas, bör inte innebära någon större kostnad för den enskilda verksamhetsutövaren.

Regeringen bedömer att den största kostnaden för enskilda hänför sig till de säkerhetsåtgärder som ska vidtas enligt den nya lagen. Det är tillsynsmyndigheten, eller ytterst en domstol, som avgör vilka åtgärder som en enskild verksamhetsutövare är skyldig att vidta för att uppfylla kraven i den nya lagen och det är inte möjligt att göra några uppskattningar som är relevanta för samtliga verksamhetsutövare. Säkerhetsåtgärderna som ska vidtas ska för varje verksamhetsutövare vara lämpliga och proportionella och säkerställa en nivå på säkerheten som är lämplig i förhållande till risken. De som föreslås räknas som enskilda verksamhetsutövare bedriver verksamhet inom vitt skilda sektorer och deras verksamheter kan se mycket olika ut. Vidare påverkar nivån av cybersäkerhet som verksamhetsutövaren i dagsläget når upp till behovet av ytterligare åtgärder. De kostnader som uppstår för en enskild verksamhetsutövare när den nya lagen träder i kraft påverkas bland annat av om företaget sedan tidigare har hanterat cybersäkerhetsrisker på frivillig grund eller om företaget har varit förpliktat att göra det på grund av sektorsspecifika bestämmelser, till exempel i enlighet med NIS-lagen eller LEK.

Hur pass stora kostnader som uppstår för en enskild verksamhetsutövare med anledning av skyldigheten att bland annat vidta säkerhetsåtgärder påverkas också av verksamhetens art och omfattning samt antalet och kvaliteten på de system som används i verksamheten. Kostnaderna kan bli högre ju större och mer omfattande företagets verksamhet är. För ett mindre företag som använder endast några få system kan kostnaderna på grund av skyldigheterna enligt lagen bli begränsade. Å andra sidan kan även ett mindre företag drabbas av väsentliga kostnader, om dess affärsverksamhet har särdrag som innebär att verksamheten är förenad med särskilda risker. Det kommer att vara svårt att separera kostnaderna som är hänförliga till lagens införande från övriga kostnader med koppling till cybersäkerhet.

Kostnaderna för cybersäkerhet kan inbegripa olika typer av utgifter som utrustning, programvara och datatrafikförbindelser. Andra kostnader som främjar cybersäkerhet kan vara administrativa utgifter, personalutgifter, olika kvalitetsrevisioner och utbildningar. Det kommer till exempel att vara svårt att bedöma vilka kostnader kopplade till systemens fysiska säkerhet som enbart är att hänföra till lagens införande jämfört med vad ett ändamålsenligt verksamhetsskydd rent generellt kräver.

Det är många faktorer som påverkar kostnaderna för exempelvis incidenthantering, som ingår i lagens krav på säkerhetsåtgärder, såsom störningens art och omfattning, dess konsekvenser för kontinuiteten samt hur snabbt verksamhetsutövaren återhämtar sig från incidenten. En betydande incident kan orsaka både direkta utrednings- och reparations-

kostnader och indirekta kostnader på grund av exempelvis avbrott i verksamheten eller ett skadat anseende.

Enligt förslaget som behandlas i avsnitt 6.5 ska ledningen för en verksamhetsutövare genomgå utbildning om säkerhetsåtgärder. Regeringen föreslår att endast ledningen ska genomgå sådan utbildning. Regeringen föreslår, till skillnad från utredningen, inte att även anställda ska erbjudas utbildning. Hur utbildningen ska genomföras och utbildningens närmare innehåll föreslås inte regleras i lag. Regeringen kan dock inte se att kostnaden för denna utbildning skulle innebära någon i sammanhanget större kostnad.

Det går sammanfattningsvis inte att presentera en mer exakt och för samtliga företag relevant uppskattning av kostnaderna kopplade till införandet av den nya lagen, men flera av förslagen bör inte heller innebära några beaktansvärda kostnader. Förslagen kan dock innebära ökade kostnader och kommer att innebära administrativa bördor för enskilda verksamhetsutövare. Det kan konstateras att förslagen i allt väsentligt är nödvändiga för att genomföra NIS 2-direktivet i Sverige. Detta gäller bland annat kraven gällande domännamnsregistreringsuppgifter i avsnitt 10 som *Internetstiftelsen* berör. En utgångspunkt för regeringens bedömning av utredningens förslag som går utöver direktivets krav har varit att det är av vikt att enskilda aktörers kostnader begränsas i den mån det är möjligt. De kostnader och administrativa bördor som förslagen trots detta innebär får anses vara godtagbara givet syftet med regelverket och att regleringen krävs för att genomföra direktivet. *Swedac* bedömer att utredningens förslag gällande tillsynsmyndigheter och föreskriftsrätt kommer att resultera i en komplex struktur både vad gäller tillsynsverksamheten och regelbördan för inblandade aktörer. Denna synpunkt kommer att beaktas inom ramen för arbetet med att ta om hand utredningens förslag till förordning.

Vad avser förslagens inverkan på konkurrensförhållandena kan, precis som *Regelrådet* konstaterar, kostnaderna för att följa regelkrav variera mellan företag. Detta kan i sig påverka konkurrensförhållandena. Regeringen anser att konkurrensförhållandena mellan olika företag också kan påverkas positivt av den ökade harmoniseringen som sker på både nationell nivå och inom EU. Förslagen är i stor utsträckning nödvändiga för att genomföra NIS 2-direktivet i nationell rätt. Högre krav kan förvisso vara resurskrävande och påverka hur mycket resurser en aktör lägger ned på cybersäkerhet jämfört med en konkurrerande verksamhet. Det kan samtidigt stärka en aktörs ställning på marknaden att ha en mer motståndskraftig verksamhet som i mindre utsträckning än andra liknande verksamheter påverkas av incidenter.

Orange Cyberdefense framför att det är viktigt att konkurrensen på marknaden för oberoende säkerhetsgranskningar inte snedvrids. Det föreslås inte regleras i lagen vem som ska genomföra säkerhetsrevisioner. Risken för en omotiverad snedvridning av konkurrensförhållanden får beaktas i framtagandet av föreskrifter på lägre nivå.

Förhållandet till näringsfriheten och den personliga integriteten

Enligt 2 kap. 17 § första stycket regeringsformen får begränsningar i rätten att driva näring införas endast för att skydda angelägna allmänna intressen

och aldrig i syfte att enbart ekonomiskt gynna vissa personer eller företag. Europakonventionen innehåller inget specifikt skydd för näringsfrihet (se prop. 2003/04:65 s. 15). Näringsfriheten är inte absolut utan kan inskränkas för att tillgodose angelägna allmänna intressen.

Frånsett förslaget om förbud att inneha ledningsfunktion, som behandlas i avsnitt 8.6 och som är en direkt följd av NIS 2-direktivets krav, innebär förslagen i denna lagrådsremiss ingen begränsning i rätten att driva näring. Förslaget om förbud att inneha ledningsfunktion syftar, i likhet med övriga förslag, till att åstadkomma en hög nivå av cybersäkerhet i samhället. Skälen för införandet av den nya lagen utvecklas i avsnitt 5.1. Enligt regeringens mening är förslaget både ändamålsenligt och nödvändigt för att möta detta syfte. En ansökan om förbud föreslås endast få göras om ett föreläggande kopplat till en allvarlig överträdelse inte har följts. Ett förbud föreslås dessutom endast kunna träffa en befattningshavare hos en enskild verksamhetsutövare som är väsentlig. En ytterligare förutsättning för en ansökan är därutöver att befattningshavaren uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen. Förslaget syftar inte heller till att gynna vissa personer eller företag. Mot denna bakgrund bedömer regeringen att förslaget är förenligt med näringsfriheten.

I avsnitt 10 lämnas förslag om skyldigheten för vissa verksamhetsutövare att föra ett register i vilket bland annat personuppgifter ska behandlas och göras tillgängliga på visst sätt, dock inte utan samtycke om det handlar om att de ska göras tillgängliga på internet. Att personuppgifter förs in i ett register och görs tillgängliga för andra kan typiskt sett anses inverka på den personliga integriteten. Med hänsyn till personuppgifternas karaktär är det inte fråga om någon stor inverkan. Kravet på register är en följd av genomförandet av NIS 2-direktivet och konsekvenserna för den personliga integriteten är godtagbara givet syftet med regelverket. Frågor om personuppgiftsbehandling behandlas också i avsnitt 12.

Konsekvenserna för företag bör utvärderas

Som följer av resonemanget ovan är det svårt att ge en exakt och för samtliga företag relevant uppskattning av kostnaderna kopplade till införandet av den nya lagen. En utvärdering av konsekvenserna för företagen bör därför ske tre år efter den nya lagens ikraftträdande. I samband med detta bör en översyn av författningarna kopplade till genomförandet av NIS 2-direktivet ske.

14.4 Konsekvenser för den kommunala självstyrelsen

Regeringens bedömning: Förslagen har ingen påverkan på den kommunala självstyrelsen.

Utredningens bedömning överensstämmer inte med regeringens. Utredningen bedömer att förslagen innebär en viss inskränkning men att den, med hänsyn till det stora intresset av att öka cybersäkerheten, är nödvändig.

Remissinstanserna: *Karlstads kommun* menar att kommunerna bör kompenseras för de kostnader som de orsakas till följd av påverkan på den kommunala självstyrelsen. *Totalförsvarets forskningsinstitut (FOI)* gör motsatt bedömning och anser att förslagen tar sikte på ett område som kommunerna inte själva kan besluta om. Övriga remissinstanser yttrar sig inte särskilt över bedömningen.

Skälen för regeringens bedömning: Den kommunala självstyrelsen är grundlagsfäst i Sverige. I 14 kap. 1 § regeringsformen anges att beslutanderätten i kommunerna utövas av valda församlingar. Enligt 2 § sköter kommunerna lokala och regionala angelägenheter av allmänt intresse på den kommunala självstyrelsens grund. Den kommunala självstyrelsen utgör en av grundstenarna för den svenska demokratin (se till exempel prop. 1973:90 s. 188 och bet. 1973:KU26 s. 39).

Principen om den kommunala självstyrelsen framgår av 1 kap. 2 § kommunallagen. Där anges att kommuner och regioner, på demokratins och den kommunala självstyrelsens grund, sköter de angelägenheter som anges i lagen eller i annan författning. Kommuner och regioner får själva ha hand om angelägenheter av allmänt intresse som har anknytning till kommunens eller regionens område eller deras medlemmar och som inte ska tas om hand enbart av staten, en annan kommun, region eller någon annan (2 kap. 1 och 2 §§).

Den kommunala självstyrelsen är inte absolut. Enligt 8 kap. 2 § första stycket 3 regeringsformen beslutar riksdagen genom lag bland annat om kommunernas och regionernas befogenheter och åligganden. Graden av självstyrelse avgörs ytterst av formerna för samverkan mellan staten och den kommunala sektorn (se bland annat prop. 1990/91:117 s. 23 och bet. 2016/17:KU10 s. 86). I 14 kap. 3 § regeringsformen anges att en inskränkning i den kommunala självstyrelsen inte bör gå utöver vad som är nödvändigt med hänsyn till de ändamål som har föranlett den. Vid en sådan proportionalitetsbedömning ska en avvägning göras mellan de kommunala självstyrelseintressena och de nationella intressen som den föreslagna lagstiftningen ska tillgodose.

Ökad säkerhet inom kommuners och regioners nätverks- och informationssystem är en grundläggande förutsättning för att offentlig service ska fungera på ett tillfredsställande sätt. Säkerhetsläget i Sverige och runtom i världen med tilltagande incidenter inom cyberdomänen innebär att hela den offentliga sektorn behöver anpassa sig för att kunna möta de utmaningar som finns med att säkerställa en säker digital offentlig sektor. Sverige och andra medlemsstater har genom NIS 2-direktivet enats på EU-nivå om vad som bör vara grundläggande krav inom cybersäkerhetsarbetet. Förslagen innebär nya skyldigheter för stora delar av samhället och inte endast i förhållande till kommunerna. Regeringen anser, till skillnad från *Karlstads kommun* och *FOI*, att förslagen inte kan sägas innebära särskilda konsekvenser för den kommunala självstyrelsen.

14.5 Övriga konsekvenser

Regeringens bedömning: Förslagen kan få positiv inverkan på det brottsförebyggande arbetet. Förslagen kommer inte att medföra några andra konsekvenser.

Utredningens bedömning överensstämmer i allt väsentligt med regeringens. Utredningen gör ingen bedömning i fråga om inverkan på det brottsförebyggande arbetet.

Remissinstanserna yttrar sig inte särskilt över bedömningen.

Skälen för regeringens bedömning: Krav på säkerhetsåtgärder samt incidentrapportering kan förebygga både avsiktliga angrepp och så kallade handhavandefel. Förslagen bör leda till att brott som riktas mot tjänster inom kritiska sektorer förebyggs, upptäcks, förhindras och beivras. Förslagen bedöms därför få viss betydelse för det brottsförebyggande arbetet. Förslagen bedöms inte ha betydelse för sysselsättning och offentlig service i olika delar av landet. Förslagen bedöms inte heller ha betydelse för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen eller få några andra konsekvenser.

15 Författningskommentar

15.1 Förslaget till cybersäkerhetslag

En ny lag om cybersäkerhet införs, cybersäkerhetslagen. Lagen genomför delvis 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). Cybersäkerhetslagen ersätter lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Allmänna överväganden om behovet av en ny lag finns i avsnitt 5.1. I följande avsnitt kommenteras förslagen till den nya lagen.

1 kap. Inledande bestämmelser

Syftet med lagen och lagens innehåll

1 § Syftet med denna lag är att uppnå en hög nivå av cybersäkerhet i samhället.

Bestämmelserna i lagen genomför delvis 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), i den ursprungliga lydelsen.

I paragrafen anges bland annat lagens syfte. Övervägandena finns i avsnitt 5.1.

Syftet med lagen är att uppnå en hög nivå av cybersäkerhet i samhället. Vad som avses med uttrycket cybersäkerhet framgår av 2 §. I paragrafen anges också att lagen delvis genomför det så kallade NIS 2-direktivet.

Uttryck i lagen

2 § I denna lag betyder

1. *allmänt elektroniskt kommunikationsnät*: detsamma som i 1 kap. 7 § lagen (2022:482) om elektronisk kommunikation,

2. *allmänt tillgänglig elektronisk kommunikationstjänst*: detsamma som i lagen om elektronisk kommunikation,

3. *anknutet företag*: detsamma som i artikel 3 i bilagan till kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag,

4. *betrodd tjänst*: detsamma som i artikel 3.16 i EU:s förordning om elektronisk identifiering,

5. *betydande cyberhot*: ett cyberhot som, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på en verksamhetsutövares nätverks- och informationssystem eller användarna av verksamhetsutövarens tjänster genom att vålla betydande skada,

6. *betydande incident*: en incident som har orsakat eller kan orsaka allvarlig driftstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller en incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande skada,

7. *cyberhot*: en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare av dessa system och andra personer,

8. *cybersäkerhet*: all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot,

9. *datacentraltjänst*: en tjänst som omfattar strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av sådan it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och dataöverföringstjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll,

10. *domännamnssystemtjänst (DNS-tjänst)*: en allmän rekursiv tjänst för att lösa domännamnsfrågor till internetslutanvändare, eller en auktoritativ tjänst för att lösa domännamnsfrågor för användning av tredje part, med undantag för rotnamnsservrar,

11. *enskild verksamhetsutövare*: den som uppfyller kraven i någon av 4–7 §§ och som inte är en offentlig verksamhetsutövare,

12. *EU:s förordning om elektronisk identifiering*: 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,

13. *incident*: en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem,

14. *kvalificerad tillhandahållare av betrodda tjänster*: detsamma som i artikel 3.20 i EU:s förordning om elektronisk identifiering,

15. *marknadsplats online*: en tjänst som använder programvara, inbegripet en webbplats, en del av en webbplats eller en applikation, som administreras av en näringsidkare eller för dennas räkning, som ger konsumenterna möjlighet att ingå distansavtal med andra näringsidkare eller konsumenter,

16. *medelstort företag*: ett företag som, utan beaktande av artikel 3.4, räknas som ett medelstort företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag,

17. *molntjänst*: en digital tjänst som möjliggör administration på begäran och bred fjärråtkomst till en skalbar och elastisk pool av gemensamma dataresurser, inbegripet då sådana resurser är distribuerade på flera platser,

18. *nätverk för leverans av innehåll*: ett nätverk av geografiskt spridda servrar vars syfte är att säkerställa hög tillgänglighet för, tillgång till eller snabb leverans av digitalt innehåll och digitala tjänster till internetanvändare för innehålls- och tjänsteleverantörers räkning,

19. *nätverks- och informationssystem*:

a) ett elektroniskt kommunikationsnät enligt 1 kap. 7 § lagen om elektronisk kommunikation,

b) en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter, eller

c) digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av a och b för att de ska kunna användas, skyddas och underhållas,

20. *offentlig verksamhetsutövare*:

a) en statlig myndighet som omfattas av lagen med stöd av 3 § eller uppfyller kraven i någon av 4–7 §§, eller

b) en region, en kommun eller ett kommunalförbund,

21. *partnerföretag*: detsamma som i artikel 3 i bilagan till kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag,

22. *plattform för sociala nätverkstjänster*: en plattform som gör det möjligt för slutanvändare att interagera, dela och upptäcka innehåll, finna andra användare och kommunicera med andra via flera enheter, särskilt genom chattar, inlägg, videor och rekommendationer,

23. *registreringsenhet för toppdomäner*: en verksamhetsutövare som har delegerats en specifik toppdomän och som ansvarar för administrationen av den, dock inte om toppdomänen används endast för registreringsenhetens eget bruk,

24. *sökmotor*: detsamma som i artikel 2.5 i Europaparlamentets och rådets förordning (EU) 2019/1150 av den 20 juni 2019 om främjande av rättvisa villkor och transparens för företagsanvändare av onlinebaserade förmedlingstjänster,

25. *utlokaliserad driftstjänst*: en tjänst som avser installation, förvaltning, drift eller underhåll av IKT-produkter, IKT-nät, IKT-infrastruktur, IKT-tillämpningar eller andra nätverks- och informationssystem, via bistånd eller aktiv administration antingen i kundernas lokaler eller på distans,

26. *utlokaliserad säkerhetstjänst*: en tjänst som tillhandahålls av en leverantör av utlokaliserade driftstjänster och som innebär hantering av eller utgör stöd för hantering av cybersäkerhetsrisker,

I paragrafen anges vad som avses med vissa uttryck som används i lagen. De flesta punkterna har en definition som är likalydande eller i sak överensstämmande med motsvarande definition i artikel 6 i NIS 2-direktivet. Övervägandena finns i avsnitt 5.1, 5.2, 5.3.1–5.3.5, 6.4, 6.6, 6.7 och 10.

I *punkt 1*, som gäller definitionen av uttrycket allmänt elektroniskt kommunikationsnät, finns en hänvisning till 1 kap. 7 § lagen om elektronisk kommunikation (LEK). Med ett allmänt elektroniskt kommunikationsnät avses således ett elektroniskt kommunikationsnät som helt eller huvudsakligen används för att tillhandahålla allmänt tillgängliga elektro-

niska kommunikationstjänster och som stöder informationsöverföring mellan nätanslutningspunkter. Den närmare innebörden av uttrycket redovisas i författningskommentaren till LEK (se prop. 2021/22:136 s. 400 f.).

Enligt *punkt 2* avses med allmänt tillgänglig elektronisk kommunikationstjänst detsamma som i LEK. Med elektronisk kommunikationstjänst avses enligt 1 kap. 7 § LEK en tjänst som vanligen tillhandahålls mot ersättning via elektroniska kommunikationsnät och som – med undantag för dels tjänster i form av tillhandahållande av innehåll som överförs med hjälp av elektroniska kommunikationsnät och elektroniska kommunikationstjänster, dels tjänster som innebär utövande av redaktionellt ansvar över sådant innehåll – är en viss i den lagen angiven typ av tjänst. Att en elektronisk kommunikationstjänst är allmänt tillgänglig innebär att tjänsten erbjuds till någon annan. Den som själv överför signaler i ett nät för eget bruk tillhandahåller inte allmänt tillgängliga elektroniska kommunikationstjänster (jfr prop. 2021/22:136 s. 406 och prop. 2002/03:110 s. 120).

I *punkt 3* anges vad som avses med anknutet företag genom en hänvisning till artikel 3 i bilagan till kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (härefter bilagan till kommissionens rekommendation). När uttrycket används i lagen har det alltså samma betydelse som i bilagan till kommissionens rekommendation och avser därmed företag som mellan sig upprätthåller vissa i bilagan angivna förbindelser.

I *punkt 4* görs för uttrycket betrodd tjänst en hänvisning till artikel 3.16 i 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 (EU:s förordning om elektronisk identifiering). I förordningen, liksom i lagen, avses med uttrycket betrodd tjänst en elektronisk tjänst som vanligen tillhandahålls mot ersättning och som består av till exempel validering av certifikat för elektroniska underskrifter, skapande av elektroniska underskrifter eller elektroniska stämplar eller tillhandahållande av elektroniska tjänster för rekommenderade leveranser. Hänvisningen till EU-förordningen är dynamisk, det vill säga avser förordningen i den vid varje tidpunkt gällande lydelsen.

Av *punkt 5* framgår definitionen av uttrycket betydande cyberhot. Vad som avses med uttrycket cyberhot framgår av punkt 7. För att räknas som ett betydande cyberhot ska det röra sig om ett cyberhot som, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på sätt som nämns i bestämmelsen. Övervägandena finns i avsnitt 6.6.1.

I *punkt 6* definieras vad som avses med en betydande incident. Vad som avses med incident framgår av punkt 13. I artikel 23.3 i NIS 2-direktivet anges när en incident ska anses vara betydande enligt direktivet och definitionen i lagen motsvarar i allt väsentlig denna bestämmelse. För att det ska röra sig om en betydande incident ska det vara fråga om en incident som allmänt sett kan orsaka allvarlig driftstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren eller som allmänt sett kan påverka andra fysiska eller juridiska personer genom att vålla betydande skada i form av till exempel sakskada eller ren förmögenhetsskada. Därmed omfattas exempelvis en sådan incident som visser-

ligen inte har orsakat någon allvarlig driftsstörning i det enskilda fallet, men som typiskt sett hade gjort det om den inte hade avvärjts.

I 14 § andra stycket 1 anges att regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om vad som utgör en betydande incident. EU-kommissionen har, bland annat i fråga om när en incident ska anses vara betydande, antagit en genomförandeförordning med stöd av artikel 21.5 och 23.11 i NIS 2-direktivet. Det rör sig om 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 driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster (härefter genomförandeförordningen). Genomförandeförordningen är direkt tillämplig, vilket innebär att de verksamhetsutövare som träffas av genomförandeförordningen är skyldiga att följa den. Övervägandena finns i avsnitt 6.6.1.

Av *punkt 7* framgår definitionen av uttrycket cyberhot. Uttrycket definieras på samma sätt som i artikel 2.8 i 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) (härefter EU:s cybersäkerhetsakt). Ett cyberhot kan utnyttja en sårbarhet, till exempel att ett informationssystem är bristfälligt skyddat. Definitionen förutsätter inte att omständighetens, händelsens eller handlingens påverkan realiseras.

I *punkt 8* finns en definition av uttrycket cybersäkerhet, som i sak definieras på samma sätt som i artikel 2.1 i EU:s cybersäkerhetsakt. Uttrycket tar sikte på all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot. Vad som avses med cyberhot och nätverks- och informationssystem framgår av punkt 7 och 19. Förutom användare av systemen inbegriper definitionen även andra berörda personer, till exempel personer som äger information som behandlas i systemen.

I *punkt 9* anges vad som avses med en datacentraltjänst. Interna datacentraler som ägs och drivs av verksamhetsutövaren för egen räkning omfattas inte av uttrycket.

Av *punkt 10* framgår vad som avses med en domännamnssystemtjänst och hur uttrycket förkortas när det används i lagen. Med domännamnssystem, eller DNS, avses ett hierarkiskt distribuerat namnsystem som möjliggör identifieringen av tjänster och resurser på internet, vilket gör det möjligt för slutanvändarenheter att använda internetrouting- och internetuppkopplingstjänster för att nå dessa tjänster och resurser. Utanför definitionen faller den som innehar en auktoritativ namnserver endast för egna domäner.

I *punkt 11* anges vad som avses med uttrycket enskild verksamhetsutövare, som kan avse både en fysisk och juridisk person, när det används i lagen. Av punkt 20 framgår vad som avses med uttrycket offentlig verksamhetsutövare. Kategoriseringen får betydelse för vilka ingripanden som kan komma i fråga med stöd av 4 kap. om verksamhetsutövaren inte uppfyller sina skyldigheter enligt lagen. Enskilda verksamhetsutövare och offentliga verksamhetsutövare benämns som samlingsbegrepp verksamhetsutövare i lagen. En verksamhetsutövare omfattas i sin helhet av lagen oavsett om denne endast bedriver sådan verksamhet som lagen gäller till viss del (jfr dock 11 §).

I *punkt 12* skrivs den fullständiga beteckningen för en EU-förordning ut. Hänvisningen till EU-förordningen är dynamisk.

Av *punkt 13* framgår definitionen av uttrycket incident. Definitionen motsvarar artikel 6.6 i NIS 2-direktivet och har samma innebörd som i direktivet. En incident är varje händelse som äventyrar uppgifternas eller tjänsternas skyddsvärda egenskaper på det sätt som anges i definitionen. Vad som avses med nätverks- och informationssystem framgår av punkt 19. Tjänster som erbjuds genom eller är tillgängliga via ett elektroniskt kommunikationsnät inbegriper såväl grossisttjänster som slutkundstjänster. Övervägandena finns i avsnitt 6.6.1.

Av *punkt 14* följer att en kvalificerad tillhandahållare av betrodda tjänster är en tillhandahållare av betrodda tjänster som tillhandahåller en eller flera kvalificerade betrodda tjänster och som beviljats status som kvalificerad av tillsynsorganet enligt EU:s förordning om elektronisk identifiering. Vad som avses med betrodd tjänst utvecklas i författningskommentaren till punkt 4. Hänvisningen till EU-förordningen är dynamisk.

I *punkt 15* definieras uttrycket marknadsplats online. Definitionen är densamma som i artikel 2 n i Europaparlamentets och rådets direktiv 2005/29/EG av den 11 maj 2005 om otillbörliga affärsmetoder som tillämpas av näringsidkare gentemot konsumenter på den inre marknaden och om ändring av rådets direktiv 84/450/EEG och Europaparlamentets och rådets direktiv 97/7/EG, 98/27/EG och 2002/65/EG samt Europaparlamentets och rådets förordning (EG) nr 2006/2004 (direktiv om otillbörliga affärsmetoder).

Av *punkt 16* framgår definitionen av medelstort företag. Bestämmelsen hänvisar till artikel 2 i bilagan till kommissionens rekommendation. Av den artikeln framgår att ett medelstort företag sysselsätter färre än 250 personer och har en årsomsättning som inte överstiger 50 000 000 euro eller en balansomslutning som inte överstiger 43 000 000 euro per år. Ett medelstort företag ska samtidigt vara större än sådana företag som kategoriseras som små företag. Ett medelstort företag ska därför sysselsätta minst 50 personer eller ha en årsomsättning och balansomslutning som överstiger 10 000 000 euro per år. Artikel 3.4 i bilagan till kommissionens rekommendation ska inte tillämpas vid beräkning av storleken enligt lagen. Enligt artikel 3.4 kan ett företag, utom i de fall som avses i artikel 3.2 andra stycket i samma bilaga, inte anses tillhöra kategorin mikroföretag samt små och medelstora företag, om 25 procent eller mer av dess kapital eller dess röstandel direkt eller indirekt kontrolleras av ett eller flera offentliga organ, individuellt eller gemensamt.

Av *punkt 17* framgår vad som avses med en molntjänst. Uttrycket dataresurser inbegriper bland annat nätverk, servrar eller annan datateknisk infrastruktur, operativsystem, programvara, lagringsutrymme, applikationer och tjänster. Med bred fjärråtkomst avses att dataresurserna tillhandahålls över nätet och nås genom mekanismer som främjar användning av olika klientplattformar, till exempel en mobiltelefon eller en bärbar dator. Skalbarhet tar sikte på att leverantören av molntjänsten kan fördela dataresurserna på ett flexibelt sätt. Uttrycket elastisk pool används för att beskriva att dataresurserna tillhandahålls och utnyttjas beroende på efterfrågan för att tillgängliga resurser snabbt ska kunna utökas och minskas i takt med arbetsbördan.

Punkt 18 och *19* anger hur uttrycken nätverk för leverans av innehåll samt nätverks- och informationssystem definieras. Definitionerna överensstämmer med artikel 6.32 och 6.1 i NIS 2-direktivet. Artikel 6.1 hänvisar till definitionen av elektroniskt kommunikationsnät i artikel 2.1 i Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation, som har genomförts genom 1 kap. 7 § LEK. Där framgår att ett elektroniskt kommunikationsnät avser ett system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt passiva nätdelar och andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier, oberoende av vilken typ av information som överförs. Den närmare innebörden av uttrycket redovisas i författningskommentaren till LEK (se prop. 2021/22:136 s. 407).

I *punkt 20* anges vad som avses med uttrycket offentlig verksamhetsutövare när det används i lagen. Av punkt 11 framgår vad som avses med uttrycket enskild verksamhetsutövare. Kategoriseringen får betydelse för vilka ingripanden som kan komma i fråga med stöd av 4 kap. om verksamhetsutövaren inte uppfyller sina skyldigheter enligt lagen. Vad som avses med uttrycket verksamhetsutövare och vilken del av verksamhetsutövaren som omfattas av lagen utvecklas i författningskommentaren till punkt 11.

Enligt *punkt 21* avses med partnerföretag samma sak som i artikel 3 i bilagan till kommissionens rekommendation. När uttrycket används i lagen har det alltså samma betydelse som i bilagan till kommissionens rekommendation och avser därmed företag som mellan sig upprätthåller vissa i bilagan angivna förbindelser.

I *punkt 22* anges vad som avses med uttrycket plattform för sociala nätverkstjänster.

Av *punkt 23* framgår vad som avses med uttrycket registreringsenhet för toppdomäner. Administration inbegriper registrering av domännamn under toppdomänen och den tekniska driften av toppdomänen. Teknisk drift inbegriper drift av toppdomänens namnservrar, underhåll av toppdomänens databaser och distribution av zonfiler för toppdomänen mellan namnservrar, oberoende av huruvida driften utförs av registreringsenheten själv eller om den har utkontrakterats. Även uttrycket registry för den här typen av aktör.

I *punkt 24* definieras uttrycket sökmotor. Uttrycket betyder, genom hänvisningen till EU-förordningen, en digital tjänst som gör det möjligt för användare att mata in sökfraser för att göra sökningar på i princip alla

webbplatser eller alla webbplatser på ett visst språk på grundval av en fråga om vilket ämne som helst i form av ett nyckelord, en röstbegäran, en fras eller någon annan inmatning och som returnerar resultat i vilket format som helst som innehåller information om det begärda innehållet. Hänvisningen till EU-förordningen är dynamisk.

I *punkt 25* och *26* anges vad som avses med utlokaliserad driftstjänst och utlokaliserad säkerhetstjänst. Uttrycken har sin motsvarighet i definitionerna i artikel 6.39 och 6.40 i den rättade versionen av NIS 2-direktivet. Det följer av definitionerna att en utlokaliserad säkerhetstjänst tillhandahålls av en leverantör av utlokaliserade driftstjänster. Förkortningen IKT står för informations- och kommunikationsteknik.

Lagens tillämpningsområde

3 § Lagen gäller för en verksamhetsutövare som är

1. en statlig myndighet med befogenhet att fatta beslut som påverkar fysiska eller juridiska personers rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital, och
2. en region, en kommun eller ett kommunalförbund.

De övriga statliga myndigheter som regeringen bestämmer ska också omfattas av lagen.

Paragrafen genomför delvis artikel 2.1 samt artiklarna 2.2 f, 2.5 a och 26.1 c i NIS 2-direktivet. Övervägandena finns i avsnitt 5.3.3.

Av *första stycket* framgår att statliga myndigheter som har befogenhet att fatta en viss typ av beslut omfattas av lagen. En myndighet som exempelvis kan fatta beslut om tillhandahållandet av varor på den inre marknaden anses fatta sådana beslut som avses i punkt 1. Statliga myndigheter kan också omfattas av lagen om de uppfyller kraven i någon av 4–7 §§. Vissa statliga myndigheter är undantagna från lagens tillämpningsområde genom 13 §. Regioner, kommuner och kommunalförbund omfattas av lagen enligt punkt 2 men fullmäktige och förbundsdirektion är undantagna enligt 13 §.

Enligt *andra stycket* omfattas också de statliga myndigheter som regeringen bestämmer av lagen.

4 § Lagen gäller också för en verksamhetsutövare som

1. omfattas av bilaga 1 eller 2 till NIS 2-direktivet i den ursprungliga lydelsen, men inte av 5 § 4, 6 § eller 7 § 1–3, eller är en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina,
2. är etablerad i Sverige, och
3. storleksmässigt motsvarar eller är större än ett medelstort företag.

Genom paragrafen genomförs delvis artikel 2.1 och 2.5 b samt artikel 26.1 i NIS 2-direktivet. Övervägandena finns i avsnitt 5.3.2 och 5.3.4.

I *punkt 1* anges det första kriteriet för att en aktör ska omfattas av lagen med stöd av paragrafen. Kriteriet innebär att det till exempel ska röra sig om en aktör som omfattas av bilaga 1 eller 2 till NIS 2-direktivet. Hänvisningen är utformad så att den avser bilagorna till direktivet i deras ursprungliga lydelse, en så kallad statisk hänvisning.

I bilaga 1 till NIS 2-direktivet anges sektorerna energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvårdssektorn, dricksvatten, avloppsvatten, digital infrastruktur, förvaltning av IKT-tjänster mellan företag, offentlig förvaltning och rymden (härefter de högkritiska sektorerna). I bilaga 2 anges sektorerna post- och budtjänster; avfallshantering; tillverkning, produktion och distribution av kemikalier; produktion, bearbetning och distribution av livsmedel; digitala leverantörer; forskning och tillverkning. I den sistnämnda sektorn ingår flera delsektorer, bland annat tillverkning av medicintekniska produkter, elektronikvaror och transportmedel.

Från paragrafens tillämpningsområde undantas vissa aktörer som omfattas av bilaga 1 och 2. För att aktörer som avses i 5 § 4, 6 § eller 7 § 1–3 ska omfattas av lagen gäller särskilda krav som behandlas i författningskommentarerna till dessa paragrafer.

Av punkt 1 följer vidare att en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen om tillstånd att utfärda vissa examina omfattas av lagen om övriga förutsättningar enligt paragrafen är uppfyllda. Av 15 § 1 framgår att regeringen eller den myndighet som regeringen bestämmer i enskilda fall får besluta om undantag från skyldigheterna enligt lagen för sådana enskilda utbildningsanordnare som avses i bestämmelsen, om det finns särskilda skäl.

Enligt *punkt 2* krävs också att aktören är etablerad i Sverige. En aktör anses vara etablerad i Sverige om den bedriver faktisk verksamhet med hjälp av en stabil struktur i landet, oavsett strukturens juridiska form.

Av *punkt 3* framgår storlekskravet som en aktör ska uppfylla för att omfattas av lagen med stöd av paragrafen. Vad som avses med ett medelstort företag framgår av 2 §. Storlekskravet innebär att en verksamhetsutövare som har minst 50 anställda eller en balansomslutning och årsomsättning som överstiger 10 000 000 euro omfattas av lagen.

5 § Lagen gäller också för en verksamhetsutövare som uppfyller kraven i 4 § 1 och 2, om

1. verksamhetsutövaren är den enda leverantören av en tjänst i Sverige som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet,
2. en störning av den tjänst som verksamhetsutövaren tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa eller kan medföra betydande systemrisker,
3. verksamhetsutövaren har särskild betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer som är beroende av verksamhetsutövaren, eller
4. verksamhetsutövaren tillhandahåller betrodda tjänster.

Paragrafen genomför delvis artikel 2.2 a samt artikel 2.2 b-e i NIS 2-direktivet. Övervägandena finns i avsnitt 5.3.2.

Enligt paragrafen omfattas en aktör av lagen om denne uppfyller något av kraven i punkt 1–4 och även kraven i 4 § 1 och 2. Aktören behöver inte uppfylla storlekskravet i 4 § 3 för att omfattas av lagen med stöd av paragrafen. Av 14 § andra stycket 2 framgår att regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om kriterier för när verksamhetsutövare ska omfattas av lagen enligt punkt 1–3. Vad som avses med betrodd tjänst i punkt 4 framgår av 2 §. En sådan aktör som avses i punkt 4 omfattas, under de förutsättningar som i

övrigt anges i paragrafen, av lagen oavsett om denne tillhandahåller en eller flera betrodda tjänster.

6 § Lagen gäller också för en verksamhetsutövare som i Sverige tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster.

Paragrafen genomför delvis artikel 2.2 a samt artikel 26.1 a i NIS 2-direktivet. Övervägandena finns i avsnitt 5.3.2.

Paragrafen innebär att aktörer som i Sverige tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster omfattas av lagen oavsett deras storlek och etablering. Avgörande är att de erbjuder angivna slags nät eller tjänster i Sverige. Vad som avses med allmänt elektroniskt kommunikationsnät och allmänt tillgänglig elektronisk kommunikationstjänst framgår av 2 §. En sådan aktör som avses i paragrafen omfattas av lagen oavsett om denne tillhandahåller ett eller flera sådana nät eller tjänster i Sverige.

7 § Lagen gäller också för en verksamhetsutövare som har huvudsakligt etableringsställe i Sverige eller en företrädare som är etablerad här, om verksamhetsutövaren

1. uppfyller kravet i 4 § 3 eller kraven i någon av 5 § 1–3 och erbjuder molntjänster, datacentraltjänster, nätverk för leverans av innehåll, utlokaliserade driftstjänster, utlokaliserade säkerhetstjänster, marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster,
2. är en registreringsenhet för toppdomäner,
3. erbjuder DNS-tjänster, eller
4. erbjuder domännamnsregistreringstjänster.

Paragrafen genomför delvis artikel 2.1 och 2.2 a samt artiklarna 2.4 och 26.1 b i NIS 2-direktivet. Övervägandena finns i avsnitt 5.3.2.

Av paragrafen följer att särskilda krav på etablering gäller för att en aktör som räknas upp i punkt 1–4 ska omfattas av lagen. Vilka tjänster som avses tydliggörs genom definitionerna i 2 §. Aktören omfattas, under de förutsättningar som anges i paragrafen, av lagen oavsett om denne tillhandahåller en eller flera sådana tjänster.

Enligt *punkt 1* ska en aktör som erbjuder uppräknade slags tjänster, för att omfattas av lagen, ha sitt huvudsakliga etableringsställe i Sverige eller en företrädare som är etablerad i Sverige. Verksamhetsutövaren måste också uppfylla storlekskravet i 4 § 3 eller kraven i någon av 5 § 1–3. Av 14 § första stycket 1 framgår att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vad som utgör huvudsakligt etableringsställe.

I *punkt 2–4* anges att det särskilda kravet på etablering även gäller för en aktör som är en registreringsenhet för toppdomäner eller som erbjuder DNS-tjänster eller domännamnsregistreringstjänster. Sådana aktörer omfattas av lagen oavsett storlek.

Enligt 2 kap. 1 § ska en verksamhetsutövare som erbjuder i paragrafen nämnda tjänster i Sverige, men saknar etablering inom Europeiska ekonomiska samarbetsområdet (EES), utse en företrädare med etablering i Sverige eller i något annat land inom EES där tjänsterna erbjuds.

8 § Som väsentlig verksamhetsutövare räknas

1. en verksamhetsutövare som är en statlig myndighet,
2. en verksamhetsutövare som är större än ett medelstort företag och som

a) är en kommun eller en region,

b) i övrigt omfattas av bilaga 1 till NIS 2-direktivet i den ursprungliga lydelsen men inte av 7 § 2 eller 3, eller

c) är en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina,

3. en verksamhetsutövare som avses i 6 § och som storleksmässigt motsvarar eller är större än ett medelstort företag,
4. en verksamhetsutövare som avses i 7 § 2 eller 3,
5. en verksamhetsutövare som är en kvalificerad tillhandahållare av betrodda tjänster, och
6. en verksamhetsutövare som räknas som väsentlig enligt föreskrifter som har meddelats med stöd av 14 § andra stycket 2.

Verksamhetsutövare som inte är väsentliga är viktiga verksamhetsutövare.

Paragrafen genomför artikel 3.1 och 3.2 i NIS 2-direktivet. Av paragrafen framgår när en verksamhetsutövare kategoriseras som väsentlig respektive viktig. Kategoriseringen är av betydelse för vilka tillsynsåtgärder som kan vidtas med stöd av 3 kap. och vilka ingripanden som kan komma i fråga med stöd av 4 kap. Övervägandena finns i avsnitt 5.3.5.

Av *första stycket 1* följer att en verksamhetsutövare som är en statlig myndighet är väsentlig.

Enligt *punkt 2* kategoriseras en verksamhetsutövare som är en kommun eller en region eller som i övrigt omfattas av delar av bilaga 1 till NIS 2-direktivet som väsentlig om den uppfyller angivet storlekskrav. Hänvisningen till direktivet är statisk. De sektorer som omfattas av bilaga 1 är de högkritiska sektorerna. Även en verksamhetsutövare som är en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen om tillstånd att utfärda vissa examina räknas som väsentlig om den uppfyller storlekskravet. Innebörden av storlekskravet, att verksamheten ska vara större än ett medelstort företag, är att verksamheten ska sysselsätta minst 250 personer eller ha en årsomsättning som överstiger 50 000 000 euro och en balansomslutning som överstiger 43 000 000 euro per år.

I *punkt 3* föreskrivs att en verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster och uppfyller angivet storlekskrav är en väsentlig verksamhetsutövare. Till skillnad från i punkt 2 behöver verksamhetsutövaren inte vara större än ett medelstort företag för att räknas som en väsentlig verksamhetsutövare.

Av *punkt 4* framgår att en verksamhetsutövare som är en registreringsenhet för toppdomäner eller erbjuder DNS-tjänster är en väsentlig verksamhetsutövare. Vad som avses med registreringsenhet för toppdomäner och DNS-tjänst framgår av 2 §.

Enligt *punkt 5* är en kvalificerad tillhandahållare av betrodda tjänster en väsentlig verksamhetsutövare. Vad som avses med kvalificerad tillhandahållare av betrodda tjänster framgår av 2 §.

Av *punkt 6* framgår vad som gäller för att de verksamhetsutövare som avses i 5 § 1–3 ska räknas som väsentliga.

I *andra stycket* anges att de verksamhetsutövare som inte är väsentliga kategoriseras som viktiga verksamhetsutövare.

Undantag från lagens tillämpningsområde

Krav i andra författningar

9 § Om det i lag eller annan författning finns bestämmelser som innehåller krav på säkerhetsåtgärder eller incidentrapportering ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt 2 kap. 3–10 §§, med beaktande av bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna.

Paragrafen utgör ett sådant undantag som medges enligt artikel 4 i NIS 2-direktivet och behandlar undantag från lagens tillämpningsområde. Övervägandena finns i avsnitt 5.4.1.

Med lag eller annan författning avses i paragrafen bland annat EU-förordningar och föreskrifter som har meddelats av en myndighet. Vid jämförelsen av verkan ska hänsyn tas till bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna. Motsvarande bestämmelser om exempelvis säkerhetsåtgärder och incidentrapportering kan finnas till exempel inom sjöfartssektorn, banksektorn och sektorn för finansmarknadsinfrastruktur. De krav på åtgärder kopplat till informationssäkerhet som följer av förordningen (2022:524) om statliga myndigheters beredskap ska inte anses ha motsvarande verkan. Det har inte heller till exempel kraven i 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).

10 § Denna lag gäller inte för verksamhetsutövare som har undantagits enligt artikel 2.4 i 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 (DORA-förordningen).

För en verksamhetsutövare som omfattas av DORA-förordningen gäller inte skyldigheterna enligt 2 kap. 3–10 §§.

Paragrafen utgör ett sådant undantag som medges enligt artikel 2.10 i NIS 2-direktivet och behandlar undantag från lagens tillämpningsområde. Övervägandena finns i avsnitt 5.4.1.

Första stycket innebär att lagen inte ska tillämpas på verksamheter som har undantagits enligt artikel 2.4 i DORA-förordningen. Hänvisningen till förordningen är dynamisk.

Av *andra stycket* framgår att lagens krav på bland annat säkerhetsåtgärder och incidentrapportering inte gäller för verksamhetsutövare som omfattas av DORA-förordningen. Det rör sig om de kreditinstitut som omfattas av sektorn bankverksamhet och de operatörer av handelsplatser och centrala motparter som omfattas av sektorn finansmarknadsinfrastruktur i bilaga 1 till NIS 2-direktivet och som också omfattas av DORA-förordningen. För verksamhetsutövare som omfattas av DORA-förordningen gäller anmälningsskyldigheten enligt 2 kap. 2 § och, i förekommande fall, skyldigheten att utse en företrädare enligt 2 kap. 1 §.

Säkerhetskänslig verksamhet och brottsbekämpande verksamhet

11 § Denna lag gäller inte för en statlig myndighet som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585) eller som till övervägande del bedriver brottsbekämpande verksamhet.

Lagen gäller inte heller för en enskild verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen eller som enbart erbjuder tjänster till sådana statliga myndigheter som avses i första stycket.

För andra verksamhetsutövare som till någon del bedriver sådan verksamhet eller erbjuder sådana tjänster som avses i första eller andra stycket gäller inte skyldigheterna i 2 kap. 3–10 §§ för den delen av verksamheten.

Undantagen i första–tredje styckena gäller inte för en verksamhetsutövare som tillhandahåller betrodda tjänster.

Paragrafen utgör ett sådant undantag som medges enligt artikel 2.6–2.9 i NIS 2-direktivet och behandlar undantag från lagens tillämpningsområde. Övervägandena finns i avsnitt 5.4.2.

Av *första stycket* följer att lagen inte gäller för en statlig myndighet som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen eller som till övervägande del bedriver brottsbekämpande verksamhet. Med brottsbekämpande verksamhet avses sådan verksamhet som en brottsbekämpande myndighet bedriver för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda eller lagföra brott. Med övervägande del avses att myndighetens huvudsakliga verksamhet rör säkerhetskänslig verksamhet eller utgör brottsbekämpning.

I *andra stycket* anges att lagen inte heller gäller för en enskild verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet eller som enbart erbjuder tjänster till en sådan statlig myndighet som avses i första stycket.

Enligt *tredje stycket* gäller kraven i lagen inte fullt ut för verksamhetsutövare som till mindre del än till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet. Kraven gäller inte heller fullt ut för den som till någon mindre del erbjuder tjänster till en sådan statlig myndighet som avses i första stycket. Skyldigheten att bland annat vidta säkerhetsåtgärder och genomföra incidentrapportering gäller inte i förhållande till den säkerhetskänsliga verksamheten, den brottsbekämpande verksamheten eller den del av verksamheten som erbjuder sådana tjänster som anges i bestämmelsen. För den undantagna delen av verksamheten gäller anmälningsskyldigheten enligt 2 kap. 2 § och, i förekommande fall, skyldigheten att utse en företrädare enligt 2 kap. 1 §.

Av *fjärde stycket* följer att en verksamhetsutövare som tillhandahåller betrodda tjänster omfattas av lagen i sin helhet oavsett om den bedriver sådan verksamhet som avses i första–tredje styckena. Vad som avses med betrodd tjänst framgår av 2 §.

12 § Skyldigheterna att lämna uppgifter enligt denna lag gäller inte uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen (2018:585).

Paragrafen utgör ett sådant undantag som medges enligt artikel 2.11 i NIS 2-direktivet. Övervägandena finns i avsnitt 5.4.3.

Paragrafen innebär att en verksamhetsutövare inte är skyldig att till exempel inom ramen för sin rapporteringsskyldighet enligt 2 kap. 5–8 §§

lämna ut säkerhetsskyddsklassificerade uppgifter. Med säkerhetsskyddsklassificerade uppgifter avses detsamma som i 1 kap. 2 § säkerhetsskyddslagen och därmed uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig.

Undantag för viss annan offentlig verksamhet

13 § Denna lag gäller inte för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, myndigheter under riksdagen, domstolar och nämnder som utövar rättskipning.

Lagen gäller inte heller för förbundsfullmäktige eller förbundsdirektion i ett kommunalförbund, kommunfullmäktige och regionfullmäktige.

Paragrafen utgör ett undantag från lagens tillämpningsområde för viss offentlig verksamhet. Övervägandena finns i avsnitt 5.3.3.

Uttrycket utlandsmyndigheter inbegriper ambassader, karriärkonsulat, representationer och delegationer vid internationella organisationer som EU, FN, OECD och Nato. Med domstolar avses samtliga domstolar, inkluderat särskilda domstolar och specialdomstolar. Med nämnder som utövar rättskipning avses nämnder som utför rättskipande uppgifter såsom Rättshjälpsnämnden, Notarienämnden eller Överklagandenämnden för nämndemannauppdrag.

Bemyndigande och beslut om undantag

14 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om

1. vad som utgör huvudsakligt etableringsställe enligt 7 §, och
2. undantag från skyldigheterna enligt denna lag för partnerföretag och anknutna företag som omfattas av lagen med stöd av 4 §.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om

1. vad som utgör en betydande incident enligt 2 § 6, och
2. kriterier för när verksamhetsutövare ska omfattas av lagen enligt 5 § 1–3 och för när sådana verksamhetsutövare ska räknas som väsentliga enligt 8 § första stycket 6.

Paragrafen innehåller bemyndiganden. Övervägandena finns i avsnitt 5.3.2, 5.3.4, 5.3.5 och 6.6.1.

Första stycket innebär att regeringen eller den myndighet som regeringen bestämmer får meddela vissa föreskrifter.

Av *punkt 1* framgår att föreskrifter får meddelas om vad som avses med huvudsakligt etableringsställe i 7 §.

Enligt *punkt 2* får föreskrifter meddelas om undantag för partnerföretag och anknutna företag som omfattas av lagen med stöd av 4 §. Vad som avses med partnerföretag och anknutna företag anges i 2 §. Av 15 § 2 framgår att regeringen eller den myndighet som regeringen bestämmer i enskilda fall får besluta om undantag från skyldigheterna enligt lagen för vissa partnerföretag och anknutna företag, om det finns särskilda skäl.

Andra stycket innebär att regeringen eller den myndighet som regeringen bestämmer får meddela vissa ytterligare föreskrifter, det vill säga föreskrifter som kompletterar lagens bestämmelser.

Enligt *punkt 1* får ytterligare föreskrifter meddelas om vad som utgör en betydande incident enligt lagen. Genomförandeförordningen reglerar när en incident ska anses vara betydande i förhållande till vissa verksamhetsutövare. Sådana verksamhetsutövare som omfattas av genomförandeförordningen är skyldiga att följa förordningen.

Av *punkt 2* framgår att ytterligare föreskrifter får meddelas om när en verksamhetsutövare ska omfattas av lagen enligt 5 § 1–3, dels när en sådan verksamhetsutövare ska räknas som väsentlig.

15 § Regeringen eller den myndighet som regeringen bestämmer får, om det finns särskilda skäl, i enskilda fall besluta om undantag från skyldigheterna enligt denna lag för

1. enskilda utbildningsanordnare som avses i 4 § 1, och
2. partnerföretag och anknutna företag som omfattas av lagen med stöd av 4 §.

Paragrafen innehåller bestämmelser om beslut om undantag. Övervägandena finns i avsnitt 5.3.2 och 5.3.4.

Enligt paragrafen får regeringen eller den myndighet som regeringen bestämmer i enskilda fall, och om det finns särskilda skäl, besluta om undantag från skyldigheterna enligt lagen. För enskilda utbildningsanordnare får bedömningen av om särskilda skäl finns göras utifrån bland annat vilken forskningsverksamhet som bedrivs. Vad som avses med partnerföretag och anknutna företag framgår av 2 §. Särskilda skäl för att undanta partnerföretag eller anknutna företag kan finnas om aktören inte i sig uppfyller storlekskravet i 4 § 3 och därutöver vid en sammantagen bedömning, och med utgångspunkt från lagens syfte, inte behöver omfattas av lagen. Av 14 § första stycket 2 framgår att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om undantag från skyldigheterna enligt lagen för partnerföretag och anknutna företag som omfattas av lagen med stöd av 4 §.

Gemensam kontaktpunkt, enhet för hantering av it-säkerhetsincidenter och cyberkrishanteringsmyndighet

16 § Den myndighet som regeringen bestämmer ska vara gemensam kontaktpunkt, enhet för hantering av it-säkerhetsincidenter och cyberkrishanteringsmyndighet enligt artiklarna 8–10 i NIS 2-direktivet, i den ursprungliga lydelsen.

Paragrafen upplyser om att regeringen har rätt att utse den myndighet som ska inneha angivna slags funktioner enligt NIS 2-direktivet. Övervägandena finns i avsnitt 12.

2 kap. Verksamhetsutövares skyldigheter

Skyldighet att utse företrädare

1 § Sådana verksamhetsutövare som avses i 1 kap. 7 § 1–4 och som erbjuder tjänster i Sverige, men saknar etablering inom Europeiska ekonomiska samarbets-

området (EES), ska utse en företrädare med etablering i Sverige eller i något annat land inom EES där tjänsterna erbjuds.

Paragrafen genomför artikel 26.3 i NIS 2-direktivet. Av paragrafen framgår när en verksamhetsutövare är skyldig att utse en företrädare. En verksamhetsutövare som inte uppfyller sin skyldighet att utse en företrädare kan bli föremål för ingripanden enligt 4 kap. Övervägandena finns i avsnitt 6.1.

Anmälningsskyldighet

2 § Verksamhetsutövare ska så snart det kan ske anmäla sig till den myndighet som regeringen bestämmer.

Verksamhetsutövaren ska anmäla en förändring avseende i anmälan lämnade uppgifter så snart det kan ske, dock senast 14 dagar efter det att förändringen ägde rum.

Paragrafen genomför artiklarna 3.4, 27.2 och 27.3 i NIS 2-direktivet. Den behandlar skyldigheten för alla som omfattas av lagen att göra en anmälan. Övervägandena finns i avsnitt 6.2.

I *första stycket* föreskrivs en skyldighet för verksamhetsutövare att så snart det kan ske göra en anmälan. Anmälan ska göras till den myndighet som regeringen bestämmer. Regeringen, eller den myndighet som regeringen bestämmer, har möjlighet att meddela verkställighetsföreskrifter med stöd av 8 kap. 7 § regeringsformen. Sådana föreskrifter kan bland annat reglera anmälans innehåll.

Tillsynsmyndigheten ska enligt 4 kap. 1 § ingripa om en anmälan inte görs eller om den inte görs i rätt tid. Att en anmälan ska göras så snart det kan ske innebär att en anmälan ska göras i omedelbar anslutning till att lagen träder i kraft om det rör sig om en vid tidpunkten för ikraftträdandet redan etablerad verksamhetsutövare. Om en aktör startar en sådan verksamhet som gör att denne omfattas av lagen, och därmed räknas som verksamhetsutövare, ska en anmälan göras i samband med att verksamheten börjar bedrivas. Detsamma gäller om en verksamhet utvecklas så att aktören till exempel uppfyller kravet på etablering eller storlekskravet i 1 kap. 4 §. Det kommer i det enskilda fallet att vara tillsynsmyndigheten som avgör om en anmälan har gjorts i rätt tid.

Av *andra stycket* framgår att verksamhetsutövaren är skyldig att anmäla en förändring avseende i anmälan lämnade uppgifter så snart det kan ske, dock senast 14 dagar efter det att förändringen ägde rum.

Skyldigheten att göra en anmälan innebär inget krav på att lämna uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen. Detta följer av 1 kap. 12 §.

Säkerhetsåtgärder

3 § Verksamhetsutövare ska vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och systemens fysiska miljö mot incidenter (säkerhetsåtgärder).

Säkerhetsåtgärderna ska utgå från ett allriskperspektiv och säkerställa en nivå på säkerheten i nätverks- och informationssystemen som är lämplig i förhållande till risken. Säkerhetsåtgärderna ska åtminstone avse

1. strategier för riskanalys och för nätverks- och informationssystemens säkerhet,
2. incidenthantering,
3. kontinuitetshantering och krishantering,
4. säkerhet i leveranskedjan,
5. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem,
6. strategier och förfaranden för att bedöma effektiviteten i säkerhetsåtgärderna,
7. grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,
8. strategier och förfaranden för användning av kryptografi samt, vid behov, kryptering,
9. personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning, och
10. vid behov användning av lösningar för autentisering, säkrade kommunikationer och säkrade nödkommunikationssystem.

Paragrafen genomför artikel 21.1–21.3 i NIS 2-direktivet. Paragrafen behandlar de säkerhetsåtgärder som verksamhetsutövare är skyldiga att vidta. Tillsynsmyndigheten ska enligt 4 kap. 1 § ingripa om en verksamhetsutövare åsidosätter denna skyldighet. Övervägandena finns i avsnitt 6.4.

I *första stycket* regleras bland annat syftet med säkerhetsåtgärderna. Verksamhetsutövare ska vidta tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda berörda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. De nätverks- och informationssystem som ska skyddas är de system som verksamhetsutövaren använder för sin verksamhet eller för att tillhandahålla sina tjänster. Det kan till exempel röra sig om åtgärder till skydd mot oönskad förändring av, obehörig insyn i och obehörig åtkomst till sådana system. Det kan vidare röra sig om åtgärder till skydd mot obehöriga personer samt till skydd för lokaler och utrustning av betydelse för säkerheten. Det kan också bland annat handla om att verksamhetsutövaren fördelar ansvar, roller och mandat i organisationen samt utarbetar rutiner och genomför uppföljning och utvärdering. Åtgärderna bör skydda mot, men också minimera konsekvenserna av, incidenter. Vad som avses med en incident framgår av 1 kap. 2 §.

Vid bedömningen av om åtgärderna är proportionella ska hänsyn bland annat tas till verksamhetsutövarens grad av riskexponering och storlek samt till sannolikheten för att incidenter inträffar och incidenternas allvarlighetsgrad, inbegripet deras samhälleliga och ekonomiska konsekvenser. Åtgärderna ska dessutom vara lämpliga. En åtgärd kan exempelvis vara proportionell, men mindre lämplig än någon annan åtgärd i förhållande till en viss risk.

I *andra stycket* anges att säkerhetsåtgärderna ska utgå från ett allriskperspektiv och säkerställa en nivå på säkerheten i nätverks- och informationssystemen som är lämplig i förhållande till risken. Allriskperspektivet innebär att verksamhetsutövare ska sträva efter att bedöma alla risker som finns relaterat till systemen som ska skyddas och att analysera alla möjliga orsaker till att en risk realiseras. Lämplighetsbedömningen enligt bestämmelsen innebär, till skillnad från den som ska göras enligt första stycket och som tar sikte på vilka åtgärder som ska vidtas, att nivån på säkerheten i systemen ska vara anpassad till risken.

I andra stycket finns också en uppräkning av vad säkerhetsåtgärderna ska innefatta som ett minimum. Uppräkningen är inte uttömmande och även andra åtgärder kan krävas för att uppfylla lagens krav. Vilka åtgärder som krävs får avgöras i det enskilda fallet utifrån de omständigheter som anges i paragrafen i övrigt.

Punkt 1 avser skyldigheten att ha strategier för riskanalys samt för säkerheten i nätverks- och informationssystemen. Strategierna kan exempelvis utformas som rutiner. Riskanalysen ska ligga till grund för valet av säkerhetsåtgärder. Verksamhetsutövaren bör bland annat ta hänsyn till att det finns olika modeller för riskanalys och att flera riskanalyser kan vara nödvändiga för att lagens krav ska anses vara uppfyllda.

Punkt 2 avser incidenthantering. Incidenthantering avser alla åtgärder och förfaranden som syftar till att förebygga, upptäcka, analysera, begränsa eller reagera på och återhämta sig från en incident.

Punkt 3, som avser kontinuitetshantering och krishantering, innebär en skyldighet för verksamhetsutövaren att planera för och ha förmåga att upprätthålla sin verksamhet på en tolerabel nivå oavsett vilken störning den utsätts för eller om en kris inträffar. Verksamhetsutövaren bör bland annat överväga vilken säkerhetskopiering som krävs för detta och hur arbetet ska bedrivas för att minska störningen i verksamheten.

I *punkt 4* anges säkerhet i leveranskedjan, vilket bland annat rör förbindelserna mellan verksamhetsutövare och deras direkta leverantörer eller tjänsteleverantörer. Verksamhetsutövaren bör bland annat beakta sårbarheter kopplade till varje direktleverantör och tjänsteleverantör samt kvaliteten på leverantörernas produkter. Verksamhetsutövaren kan även behöva beakta risker som härrör från leverantörer på andra nivåer för att anses uppfylla lagens krav på säkerhetsåtgärder. Resultatet av samordnade säkerhetsriskbedömningar på unionsnivå av kritiska leveranskedjor bör också beaktas. Det får avgöras i varje enskilt fall om en verksamhetsutövare har vidtagit tillräckliga åtgärder i fråga om säkerhet i leveranskedjan, inbegripet åtgärder för att revidera avtal.

Punkt 5 gäller säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem. Verksamhetsutövaren bör bland annat ta hänsyn till vilka risker som ett förvärv av nätverks- eller informationssystem innebär. Bestämmelsen innebär även krav på hantering av sårbarheter och sårbarhetsinformation. Att åtgärderna ska avse säkerhet vid utveckling och underhåll av systemen innebär att verksamhetsutövaren behöver vidta åtgärder för att upprätthålla säkerheten även vid exempelvis utkontraktering och licensiering.

Punkt 6 innebär att verksamhetsutövaren ska ha strategier och förfaranden för att utvärdera sådana säkerhetsåtgärder som har vidtagits. Detta innebär att verksamhetsutövaren ska vidta åtgärder, i form av exempelvis framtagande av interna regler och arbetssätt, för att följa upp att de åtgärder som har vidtagits är lämpliga och tillräckliga. Det bör även vara tydligt vem som ansvarar för att utvärdering sker och på vilket sätt utvärdering ska ske.

Punkt 7 rör grundläggande praxis för cyberhygien och utbildning i cybersäkerhet. Kravet på grundläggande praxis för cyberhygien innebär att verksamhetsutövaren ska ha rutiner för bibehållande av hög säkerhet genom exempelvis programuppdateringar, åtkomsthantering och använ-

darmedvetenhet. Kravet på utbildning i cybersäkerhet innebär inte nödvändigtvis att verksamhetsutövarens personal ska genomgå sådan utbildning, utan att verksamhetsutövaren ska göra en bedömning av vilken utbildning som krävs och vilka i personalen som bör genomgå en sådan. I 4 § finns även ett krav på utbildning som riktar sig till ledningen för en verksamhetsutövare.

Punkt 8 avser strategier och förfaranden för användning av kryptografi samt, vid behov, kryptering. Bestämmelsen innebär bland annat att verksamhetsutövaren ska göra en bedömning av om kryptering krävs för att upprätthålla säkerheten och vid behov ha strategier och förfaranden för användning av sådan.

Punkt 9 gäller personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning. Syftet med personalsäkerhet är att förebygga att personal orsakar incidenter på grund av olämplighet eller okunskap. Kravet på personalsäkerhet kan innebära att verksamhetsutövaren genomför insatser för att höja kompetensen och öka kunskapen hos personalen eller genomför olika typer av kontroller, exempelvis i form av verifiering av kvalifikationer för att motverka mänskliga misstag eller avsiktligt skadliga handlingar. I uttrycket åtkomstkontroll ingår sådana funktioner som syftar till att reglera och kontrollera en användares åtkomst till information och resurser. Det rör sig bland annat om behörighetsstyrning i form av tilldelning, återkallande och hantering av behörigheter samt uppföljning av åtkomst till information och resurser, till exempel genom loggar och andra hjälpmedel.

Punkt 10 innebär bland annat att verksamhetsutövaren ska bedöma om lösningar för autentisering, säkrade kommunikationer och säkrade nödkommunikationssystem krävs och i så fall vilka. Lösningar för autentisering kan bland annat kan ta sikte på att kontrollera en uppgiven identitet vid exempelvis inloggning i ett system. Säkrad kommunikation avser röst-, video- och textkommunikation som bland annat är skyddad mot obehörig avlyssning eller upptagning. Säkrad kommunikation ska, om behovet finns, kunna användas både i den dagliga verksamheten och i nödsituationer.

I 14 § andra stycket anges att regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om säkerhetsåtgärder.

Utbildning

4 § Ledningen för en verksamhetsutövare ska genomgå utbildning om säkerhetsåtgärder.

Paragrafen genomför artikel 20.2 i NIS 2-direktivet och innebär en skyldighet för verksamhetsutövaren att se till att den egna ledningen genomgår utbildning om sådana åtgärder som nämns i 3 §. Tillsynsmyndigheten ska enligt 4 kap. 1 § ingripa om en verksamhetsutövare åsidosätter denna skyldighet. Övervägandena finns i avsnitt 6.5.

Vilka som omfattas av uttrycket ledning beror på verksamhetsutövarens verksamhetsform. I ett aktiebolag avses styrelsen, den verkställande direktören och ersättare för dessa. I ett handelsbolag avses i stället bolagsmännen. För förvaltningsmyndigheter under regeringen utgörs ledningen

av en myndighetschef för enrådighetsmyndigheter, en styrelse för styrelsemyndigheter eller en nämnd för nämndmyndigheter i enlighet med 2 § myndighetsförordningen (2007:515). För regioner och kommuner är det styrelsen som avses i enlighet med 6 kap. 1 § kommunallagen (2017:725).

Utbildningen ska bland annat syfta till att ledningen ska ha tillräcklig kompetens för att kunna identifiera risker och kunna bedöma vilka säkerhetsåtgärder som bör vidtas av verksamhetsutövaren. Vad utbildningen närmare ska omfatta och vilka moment som ska ingå kan variera bland annat utifrån vilken verksamhet som bedrivs. I 14 § första stycket anges att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om utbildningen.

Incidentrapportering och informationsskyldighet

Rapportering av betydande incidenter

5 § Verksamhetsutövare ska upplysa den myndighet som regeringen bestämmer om en betydande incident så snart det kan ske, dock senast 24 timmar efter det att verksamhetsutövaren har fått kännedom om incidenten.

Paragrafen genomför artikel 23.4 a i NIS 2-direktivet och behandlar den första rapporteringsåtgärd som en verksamhetsutövare är skyldig att vidta efter att ha fått kännedom om en betydande incident. Tillsynsmyndigheten ska enligt 4 kap. 1 § ingripa om en verksamhetsutövare åsidosätter skyldigheten. Vad som avses med betydande incident framgår av 1 kap. 2 §. Övervägandena finns i avsnitt 6.6.2.

Verksamhetsutövaren ska lämna upplysningen ske så snart det kan ske, dock senast 24 timmar efter att ha fått kännedom om den betydande incidenten. Detta innebär att upplysningen bör lämnas så snart de första kritiska åtgärderna har vidtagits för att avhjälpa incidenten. Tidsangivelsen om 24 timmar är att betrakta som en bortre tidsgräns. Skyldigheten att rapportera incidenter innebär inget krav på att lämna uppgifter som är säkerhetsskyddsklassificerade. Detta följer av 1 kap. 12 §.

I 14 § första stycket anges att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om incidentrapporteringen.

6 § Verksamhetsutövare ska till samma myndighet som avses i 5 § göra en incidentanmälan om den betydande incidenten så snart det kan ske. Verksamhetsutövare som tillhandahåller betrodda tjänster ska göra anmälan senast 24 timmar efter det att verksamhetsutövaren har fått kännedom om incidenten och övriga verksamhetsutövare senast 72 timmar efter sådan kännedom.

Paragrafen genomför artikel 23.4 b i NIS 2-direktivet och reglerar det andra steget i den rapporteringskedja som verksamhetsutövaren är skyldig att följa vid en betydande incident. Tillsynsmyndigheten ska enligt 4 kap. 1 § ingripa om en verksamhetsutövare åsidosätter skyldigheten. Vad som avses med betydande incident framgår av 1 kap. 2 §. Övervägandena finns i avsnitt 6.6.2.

Incidentanmälan ska göras så snart det kan ske, dock senast 72 timmar efter det att verksamhetsutövaren har fått kännedom om den betydande incidenten. För verksamhetsutövare som tillhandahåller betrodda tjänster gäller i stället en bortre tidsgräns om 24 timmar. Vad som avses med

uttrycket betrodd tjänst framgår av 1 kap. 2 §. Skyldigheten att göra en incidentanmälan innebär inget krav på att lämna uppgifter som är säkerhetsskyddsklassificerade. Detta följer av 1 kap. 12 §.

I 14 § första stycket anges att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om incidentrapporteringen.

7 § På begäran av samma myndighet som avses i 5 § ska verksamhetsutövare lämna en delrapport med relevanta statusuppdateringar för den betydande incidenten.

Paragrafen genomför artikel 23.4 c i NIS 2-direktivet och behandlar skyldigheten för verksamhetsutövare att lämna en delrapport med anledning av en betydande incident. Tillsynsmyndigheten ska enligt 4 kap. 1 § ingripa om en verksamhetsutövare åsidosätter skyldigheten. Vad som avses med betydande incident framgår av 1 kap. 2 §. Övervägandena finns i avsnitt 6.6.2.

Det är upp till myndigheten som avses i 5 § att bedöma om en delrapport behövs och om begäran skulle vara oproportionerligt betungande för verksamhetsutövaren enligt bland annat 5 § tredje stycket förvaltningslagen (2017:900). Skyldigheten att lämna en delrapport innebär inget krav på att lämna uppgifter som är säkerhetsskyddsklassificerade. Detta följer av 1 kap. 12 §.

I 14 § första stycket anges att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om incidentrapporteringen.

8 § Senast en månad efter incidentanmälan enligt 6 § ska verksamhetsutövare lämna en slutrapport till samma myndighet. Om den betydande incidenten fortfarande är pågående ska i stället en lägesrapport lämnas vid denna tidpunkt och därefter en slutrapport inom en månad efter det att incidenten har hanterats.

Paragrafen genomför artikel 23.4 d och e i NIS 2-direktivet och reglerar det sista steget i den rapporteringskedja som verksamhetsutövaren är skyldig att följa vid en betydande incident. Tillsynsmyndigheten ska enligt 4 kap. 1 § ingripa om en verksamhetsutövare åsidosätter skyldigheten. Vad som avses med betydande incident framgår av 1 kap. 2 §. Övervägandena finns i avsnitt 6.6.2.

I paragrafen anges att verksamhetsutövaren senast en månad efter att ha gjort en incidentanmälan ska lämna en slutrapport till den myndighet som avses i 5 §. Om den betydande incidenten fortfarande är pågående en månad efter incidentanmälan, ska i stället en lägesrapport lämnas vid samma tidpunkt. Lägesrapporten ska kompletteras med en slutrapport inom en månad efter det att incidenten har hanterats. En incident ska anses ha hanterats när verksamhetsutövaren inte längre behöver vidta några åtgärder för att förebygga, upptäcka, analysera, begränsa eller reagera på eller återhämta sig från incidenten. Skyldigheten att lämna en slutrapport innebär inget krav på att lämna uppgifter som är säkerhetsskyddsklassificerade. Detta följer av 1 kap. 2 §.

I 14 § första stycket anges att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om incidentrapporteringen.

Information vid betydande incidenter och betydande cyberhot

9 § Om det är lämpligt ska verksamhetsutövare så snart det kan ske informera mottagarna av deras tjänster om en betydande incident som sannolikt inverkar negativt på tillhandahållandet av tjänsterna.

Paragrafen genomför artikel 23.1 i NIS 2-direktivet och reglerar verksamhetsutövares informationsskyldighet vid betydande incidenter. Tillsynsmyndigheten ska enligt 4 kap. 1 § ingripa om en verksamhetsutövare åsidosätter skyldigheten. Vad som avses med betydande incident framgår av 1 kap. 2 §. Övervägandena finns i avsnitt 6.6.3.

Enligt paragrafen ska verksamhetsutövare, om det är lämpligt, informera mottagarna av deras tjänster om betydande incidenter som sannolikt inverkar negativt på tillhandahållandet av tjänsterna. Vem som räknas som mottagare och på vilket sätt informationen ska lämnas får bedömas i det enskilda fallet. Lämplighetsbedömningen kan resultera i slutsatsen att endast vissa mottagare bör informeras. Informationen ska lämnas så snart det kan ske. Verksamhetsutövaren bör göra en bedömning av när informationen kan lämnas utifrån bland annat vilken typ av incident och tjänst det är fråga om. I enlighet med 4 kap. 4 § får dock tillsynsmyndigheten förelägga en verksamhetsutövare att fullgöra informationsskyldigheten. Skyldigheten att lämna uppgifter gäller enligt 1 kap. 12 § inte för uppgifter som är säkerhetsskyddsklassificerade.

I 14 § första stycket anges att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om informationsskyldigheten. I sådana föreskrifter kan det bland annat regleras på vilket sätt informationsskyldigheten ska fullgöras.

10 § Vid ett betydande cyberhot ska verksamhetsutövare så snart det kan ske informera mottagarna av deras tjänster som kan påverkas av hotet om skydds- och motåtgärder som mottagarna kan vidta. Om det är lämpligt ska verksamhetsutövare även informera om själva hotet.

Paragrafen genomför artikel 23.2 i NIS 2-direktivet och reglerar verksamhetsutövares skyldighet att lämna information vid betydande cyberhot. Tillsynsmyndigheten ska enligt 4 kap. 1 § ingripa om en verksamhetsutövare åsidosätter skyldigheten. Vad som avses med betydande cyberhot framgår av 1 kap. 2 §. Övervägandena finns i avsnitt 6.6.3.

Enligt paragrafen ska verksamhetsutövare vid ett betydande cyberhot informera mottagare av deras tjänster, som kan påverkas av hotet, om skydds- och motåtgärder som mottagarna kan vidta. Verksamhetsutövaren ska även informera om själva hotet, om det är lämpligt. Vem som räknas som mottagare får bedömas i det enskilda fallet, men till skillnad från informationsskyldigheten i 9 § är det endast mottagare som kan påverkas av hotet som ska informeras. Informationen ska lämnas så snart det kan ske. Den närmare tidpunkten får avgöras i det enskilda fallet med ledning av bland annat vilken typ av hot det är fråga om och på vilket sätt mottagarna kan påverkas av hotet. I enlighet med 4 kap. 4 § får tillsynsmyndigheten förelägga en verksamhetsutövare att fullgöra informationsskyldigheten. Skyldigheten att lämna information innebär inget krav på att lämna uppgifter som är säkerhetsskyddsklassificerade. Detta följer av 1 kap. 12 §.

I 14 § första stycket anges att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om informationsskyldigheten. I sådana föreskrifter kan bland annat regleras på vilket sätt informationsskyldigheten ska fullgöras.

Skyldighet att föra register över domännamn

11 § En verksamhetsutövare som är en registreringsenhet för toppdomäner eller som erbjuder domännamnsregistreringstjänster ska föra ett register över tilldelade domännamn under toppdomänen och löpande upprätta säkerhetskopior av registeruppgifterna.

Registret ska innehålla

1. domännamnet,
2. namnet på domännamnsinnehavaren och dennes telefonnummer och e-postadress,
3. namnet på den som tekniskt administrerar domännamnet och dennes telefonnummer och e-postadress, och
4. registreringsdatum.

Paragrafen genomför delvis artikel 28 i NIS 2-direktivet och innebär en skyldighet att föra register över tilldelade domännamn under en toppdomän. Paragrafen reglerar också bland annat registrets innehåll. Tillsynsmyndigheten får enligt 4 kap. 5 § ingripa med ett föreläggande om en verksamhetsutövare åsidosätter skyldigheten. Övervägandena finns i avsnitt 10.

Skyldigheten träffar de verksamhetsutövare som är registreringsenheter för toppdomäner eller som erbjuder domännamnsregistreringstjänster. Om en sådan verksamhetsutövare även omfattas av lagen (2006:24) om nationella toppdomäner för Sverige på internet (toppdomänlagen), gäller enligt 13 § i stället skyldigheten att föra register enligt den lagen. Skyldigheten att föra register omfattar även en skyldighet att löpande upprätta säkerhetskopior av registeruppgifterna.

I 14 § första stycket anges att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om registret.

12 § Uppgifterna i registret som avses i 11 § ska kunna hämtas utan avgift via internet. Därutöver ska uppgifter även på begäran lämnas ut skyndsamt och senast 72 timmar från mottagandet av begäran till den som gör en lagligen grundad och motiverad begäran.

Personuppgifter får endast göras tillgängliga på internet om den registrerade har samtyckt till det.

En sådan verksamhetsutövare som avses i 11 § är personuppgiftsansvarig för behandling av personuppgifter i registret.

Paragrafen genomför delvis artikel 28 i NIS 2-direktivet och reglerar bland annat utlämnande av uppgifter ur registret som förs enligt 11 §. Tillsynsmyndigheten får enligt 4 kap. 5 § ingripa med ett föreläggande om en verksamhetsutövare åsidosätter skyldigheten. Övervägandena finns i avsnitt 10.

Uppgifterna i registret ska kunna hämtas utan avgift via internet. Personuppgifter får dock göras tillgängliga på internet endast om den registrerade har samtyckt till det. På begäran ska uppgifterna i registret även lämnas ut skyndsamt till varje fysisk eller juridisk person som gör en

lagligen grundad och motiverad begäran. Att begäran ska vara lagligen grundad innebär att den ska avse ett krav på att få del av uppgifter som framställs med stöd av unionsrätten eller nationell rätt och att den ska vara förenlig med dataskyddslagstiftningen. En begäran kan exempelvis vara grundad på en bestämmelse som ger rätt att få del av uppgifter eller på ett beslut meddelat av domstol, till exempel ett editionsbeslut. Att begäran ska vara motiverad innebär att sökanden måste visa stöd för sin begäran i förhållande till varje specifik domäns registreringsdata. En bedömning av ansökan får göras i det enskilda fallet. Att uppgifterna ska lämnas ut skyndsamt innebär att en begäran om uppgifter ska besvaras utan onödigt dröjsmål. En bortre tidsgräns om 72 timmar gäller.

I 14 § första stycket anges att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om utlämnande av uppgifter ur registret.

13 § De skyldigheter som följer av 11 och 12 §§ gäller inte för den som är domänadministratör enligt lagen (2006:24) om nationella toppdomäner för Sverige på internet. För en sådan domänadministratör gäller skyldighet att föra register enligt 6 § den lagen.

I paragrafen görs ett undantag från skyldigheterna enligt 11 och 12 §§ för en domänadministratör som omfattas av toppdomänlagen. Övervägandena finns i avsnitt 10.

Bemyndigande

14 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om utbildning, incidentrapportering, informationsskyldighet och register enligt 4–12 §§.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om säkerhetsåtgärder enligt 3 §.

Paragrafen innehåller bemyndiganden som ger regeringen eller den myndighet som regeringen bestämmer möjlighet att meddela vissa föreskrifter. Övervägandena finns i avsnitt 6.4, 6.5, 6.6.2, 6.6.3 och 10.

Enligt paragrafen får regeringen eller den myndighet som regeringen bestämmer exempelvis meddela ytterligare föreskrifter om vilka åtgärder som ska vidtas enligt 3 § för att verksamhetsutövaren ska anses uppfylla lagens krav på att vidta säkerhetsåtgärder. Regeringen eller den myndighet som regeringen bestämmer får också bland annat meddela föreskrifter om vilka moment som ska ingå i den utbildning som ledningen ska genomgå enligt 4 §. Enligt paragrafen får föreskrifter också meddelas i fråga om incidentrapporteringen och informationsskyldigheten enligt 5–10 §§. Det kan exempelvis röra sig om föreskrifter som reglerar hur incidentrapporteringen ska genomföras och hur informationsskyldigheten ska fullgöras. Genom paragrafen bemyndigas regeringen eller den myndighet som regeringen bestämmer också att meddela föreskrifter om det register som ska föras enligt 11 § och om de regler som närmare ska gälla för tillhandahållande av uppgifterna i registret enligt 12 §. Föreskrifterna kan exempelvis också gälla förvaring av säkerhetskopior.

Regeringen eller den myndighet som regeringen bestämmer kan också med stöd av 8 kap. 7 § meddela verkställighetsföreskrifter. Sådana kan exempelvis avse vilka uppgifter en anmälan enligt 2 kap. 2 § ska innehålla.

3 kap. Tillsyn

Tillsynsmyndigheten och tillsynsmyndighetens uppdrag

1 § Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet.

Tillsynsmyndigheten ska utöva tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs. Tillsynsmyndigheten ska också utöva tillsyn över att sådana rättsakter följs som har antagits med stöd av artiklarna 21.5 och 23.11 i NIS 2-direktivet, i den ursprungliga lydelsen.

Paragrafen genomför artiklarna 8.1 och 31.1 i NIS 2-direktivet. I paragrafen finns en upplysning om att regeringen bestämmer vilken myndighet som ska vara tillsynsmyndighet och i den regleras också vad som är en tillsynsmyndighets uppgift. Med föreskrifter som har meddelats i anslutning till lagen avses såväl föreskrifter som har meddelats med stöd av lagen som föreskrifter som har meddelats med stöd av 8 kap. 7 § regeringsformen. Tillsynsansvaret omfattar även sådana genomförandeakter som EU-kommissionen antar med stöd av angivna artiklar i NIS 2-direktivet. Övervägandena finns i avsnitt 7.1.

2 § Tillsynsåtgärder enligt 3, 4, 6 och 7 §§ får när det gäller viktiga verksamhetsutövare vidtas endast när tillsynsmyndigheten har anledning att anta att verksamhetsutövarna inte följer

1. denna lag eller föreskrifter som har meddelats i anslutning till lagen, eller
2. sådana rättsakter som har antagits med stöd av artiklarna 21.5 och 23.11 i NIS 2-direktivet, i den ursprungliga lydelsen.

Paragrafen genomför artikel 33.1 i NIS 2-direktivet och reglerar när tillsynsåtgärder får vidtas i förhållande till viktiga verksamhetsutövare. Övervägandena finns i avsnitt 7.2.4.

Vilka verksamhetsutövare som räknas som väsentliga och viktiga framgår av 1 kap. 8 §. För att vidta tillsynsåtgärder mot en viktig verksamhetsutövare krävs, till skillnad mot en väsentlig verksamhetsutövare, att det finns bevis eller indikationer på att verksamhetsutövaren inte uppfyller lagens krav. Om det kan anses finnas anledning i det enskilda fallet får avgöras av tillsynsmyndigheten. Att regelbundna säkerhetsrevisioner enligt 5 § får genomföras endast i förhållande till väsentliga verksamhetsutövare följer redan av den bestämmelsen.

Tillsynsmyndighetens befogenheter

3 § Den som står under tillsyn ska på begäran tillhandahålla tillsynsmyndigheten de uppgifter eller handlingar som behövs för tillsynen.

Paragrafen genomför artiklarna 32.2 e–g och 33.2 d–f i NIS 2-direktivet. Den innebär en skyldighet för verksamhetsutövaren att, på begäran av en tillsynsmyndighet, tillhandahålla tillsynsmyndigheten de uppgifter eller handlingar som myndigheten behöver för att utföra sina uppgifter enligt lagen. Övervägandena finns i avsnitt 7.2.1.

Tillsynsmyndigheten avgör vilka uppgifter eller handlingar som behövs i det enskilda fallet med beaktande av det krav på proportionalitet som följer av bland annat 5 § tredje stycket förvaltningslagen. Om verksamhetsutövaren inte medverkar, kan tillsynsmyndigheten förelägga verksamhetsutövaren enligt 8 § och i sista hand begära handräckning av Kronofogdemyndigheten enligt 9 §.

4 § Tillsynsmyndigheten har i den omfattning det behövs för tillsynen rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamhet som omfattas av tillsyn.

Paragrafen, som genomför artiklarna 32.2 a och 33.2 a i NIS 2-direktivet, reglerar en tillsynsmyndighets rätt att få tillträde till områden, lokaler och andra utrymmen i den utsträckning det behövs för att den ska kunna utöva tillsyn. Rätten omfattar inte bostäder. Övervägandena finns i avsnitt 7.2.1.

Tillträdesrätten motsvaras av en skyldighet för verksamhetsutövaren att ge begärt tillträde. Att det intrång som tillträdet innebär måste stå i proportion till behovet av åtgärden följer bland annat av 5 § tredje stycket förvaltningslagen. Tillträdesrätten ger inte myndigheten rätt att bereda sig tillträde med tvång. Om verksamhetsutövaren inte medverkar, kan tillsynsmyndigheten förelägga verksamhetsutövaren att ge tillträde enligt 8 § och i sista hand begära handräckning av Kronofogdemyndigheten enligt 9 §.

5 § Tillsynsmyndigheten får utföra regelbundna säkerhetsrevisioner eller låta ett oberoende organ utföra sådana säkerhetsrevisioner av väsentliga verksamhetsutövare.

Paragrafen genomför delvis artikel 32.2 b samt artikel 32.2 c i NIS 2-direktivet. Den ger tillsynsmyndigheten möjlighet att besluta om regelbundna säkerhetsrevisioner. Övervägandena finns i avsnitt 7.2.2.

En säkerhetsrevision innebär att det sker en granskning av säkerheten i verksamhetsutövarens nätverks- och informationssystem. En säkerhetsrevision kan omfatta både tekniska och icke-tekniska moment men de granskningsmoment som genomförs ska vara sådana att resultatet av revisionen kan visa på nivån av säkerheten i systemen. Syftet med revisionen är att bedöma om de åtgärder som en verksamhetsutövare har vidtagit för att skydda systemen och säkerställa efterlevnad av lagens krav är ändamålsenliga och effektiva. Regelbundna säkerhetsrevisioner kan endast beslutas i förhållande till väsentliga verksamhetsutövare. Vilka verksamhetsutövare som räknas som väsentliga framgår av 1 kap. 8 §. Det är upp till tillsynsmyndigheten att bestämma med vilken regelbundenhet revisionerna ska ske med beaktande av det krav på proportionalitet som följer av bland annat 5 § tredje stycket förvaltningslagen. Säkerhetsrevisionerna kan utföras av tillsynsmyndigheten eller ett organ som är oberoende i förhållande till tillsynsmyndigheten och verksamhetsutövaren. Organet ska ha den sakkunskap som krävs för säkerhetsrevisionen. Regeringen eller den myndighet som regeringen bestämmer får med stöd av 10 § meddela föreskrifter om säkerhetsrevisioner.

6 § Tillsynsmyndigheten får om det finns särskilda skäl utföra riktade säkerhetsrevisioner eller låta ett oberoende organ utföra sådana säkerhetsrevisioner av den som står under tillsyn.

Paragrafen genomför delvis artikel 32.2 b och artikel 33.2 b i NIS 2-direktivet. Den ger tillsynsmyndigheten möjlighet att besluta om riktade säkerhetsrevisioner. Övervägandena finns i avsnitt 7.2.2.

En riktad säkerhetsrevision innebär att en granskning görs med anledning av någon viss omständighet som är hänförlig till verksamhetsutövaren. En riktad säkerhetsrevision behöver inte avse hela verksamheten utan kan exempelvis avgränsas till vissa delar av en verksamhet som behöver granskas ytterligare. För att en riktad säkerhetsrevision ska få genomföras krävs särskilda skäl. Kravet på särskilda skäl kan till exempel vara uppfyllt om det har framkommit en omständighet vid tillsyn som föranleder bedömningen att ytterligare granskning krävs. Tillsynsmyndigheten avgör om en riktad säkerhetsrevision behövs i det enskilda fallet med beaktande av det krav på proportionalitet som följer av bland annat 5 § tredje stycket förvaltningslagen. Den riktade säkerhetsrevisionen kan utföras av tillsynsmyndigheten eller ett organ som är oberoende i förhållande till tillsynsmyndigheten och verksamhetsutövaren. Organet ska ha den sakkunskap som krävs för säkerhetsrevisionen. Regeringen eller den myndighet som regeringen bestämmer får med stöd av 10 § meddela föreskrifter om säkerhetsrevisioner.

7 § Tillsynsmyndigheten får genomföra säkerhetsskanningar hos den som står under tillsyn.

En säkerhetsskanning ska ske i samarbete med verksamhetsutövaren.

Paragrafen genomför artiklarna 32.2 d och 33.2 c i NIS 2-direktivet och ger tillsynsmyndigheten möjlighet att genomföra säkerhetsskanningar hos den som står under tillsyn. Övervägandena finns i avsnitt 7.2.3.

En säkerhetsskanning görs av nätverks- och informationssystem i syfte att upptäcka sårbarheter eller osäkert konfigurerade delar av systemen. Tillsynsmyndigheten kan både genomföra säkerhetsskanningen på egen hand eller via en extern aktör. Att säkerhetsskanningar ska ske i samarbete med verksamhetsutövaren innebär att tillsynsmyndigheten ska involvera verksamhetsutövaren vid utförandet, men det betyder inte att det måste finnas en samsyn i hur skanningen ska genomföras. Tillsynsmyndigheten avgör om en säkerhetsskanning behövs i det enskilda fallet med beaktande av det krav på proportionalitet som följer av bland annat 5 § tredje stycket förvaltningslagen.

Regeringen eller den myndighet som regeringen bestämmer får med stöd av 10 § meddela föreskrifter om säkerhetsskanningar.

8 § Tillsynsmyndigheten får besluta att förelägga den som står under tillsyn att medverka till tillsynsåtgärder enligt 3–7 §§.

Ett föreläggande får förenas med vite. Ett vitesföreläggande får även riktas mot staten.

Paragrafen reglerar tillsynsmyndighetens möjlighet att fatta beslut om att förelägga den som står under tillsyn att tillhandahålla uppgifter eller handlingar enligt 3 § och ge tillträde enligt 4 §. Paragrafen innebär också

att tillsynsmyndigheten får förelägga den som står under tillsyn att medverka till säkerhetsrevisioner eller säkerhetsskanningar enligt 5–7 §§. Övervägandena finns i avsnitt 7.2.1–7.2.3.

Som utgångspunkt ska tillsynsmyndigheten i första hand försöka förmå verksamhetsutövaren att agera på frivillig väg. Det följer av bland annat 5 § tredje stycket förvaltningslagen att beslut om förelägganden i förhållande till en enskild får fattas endast om det är proportionerligt. Myndigheten ska göra en proportionalitetsbedömning i varje enskilt fall. Ett föreläggande får förenas med vite. Lagen (1985:206) om viten (viteslagen) är då tillämplig.

9 § Tillsynsmyndigheten får begära handräckning av Kronofogdemyndigheten för att genomföra de tillsynsåtgärder som avses i 3 och 4 §§. Vid handräckning gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

Paragrafen reglerar tillsynsmyndighetens möjlighet att begära handräckning av Kronofogdemyndigheten. Övervägandena finns i avsnitt 7.2.1.

Tillsynsmyndigheten får begära handräckning av Kronofogdemyndigheten för att få tillgång till uppgifter eller handlingar enligt 3 § eller för att få tillträde till sådana lokaler och andra utrymmen som anges i 4 §. Vid sådan handräckning gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande. Det innebär att bestämmelserna i 16 kap. 11–12 a §§ utsökningsbalken ska tillämpas, men också fler bestämmelser i samma balk, exempelvis 2 kap. 17 §, där det bland annat anges vilka befogenheter en förrättningsman har.

Bemyndigande

10 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om säkerhetsrevisioner och säkerhetsskanningar enligt 5–7 §§.

Paragrafen innehåller bemyndiganden. Regeringen eller den myndighet som regeringen bestämmer kan, med stöd av paragrafen, bland annat meddela föreskrifter som närmare reglerar när säkerhetsrevisioner och säkerhetsskanningar ska genomföras och vilka moment som ska ingå i dessa. Övervägandena finns i avsnitt 7.2.2 och 7.2.3.

Avgift

11 § Tillsynsmyndigheten får ta ut en handläggningsavgift av en sådan verksamhetsutövare som avses i 1 kap. 6 § och som anmäler verksamhet enligt 2 kap. 2 §. Handläggningsavgiften ska motsvara myndighetens kostnader för handläggningen av ärendet.

Tillsynsmyndigheten ska ta ut en årlig avgift av en sådan verksamhetsutövare som avses i första stycket. De årliga avgifterna ska sammantagna motsvara de kostnader som myndigheten, utöver de kostnader som avses i första stycket, har för sin verksamhet enligt denna lag när det gäller dessa verksamhetsutövare. Avgifterna ska fördelas med skälig andel på var och en av verksamhetsutövarna.

Paragrafen innebär rätt för tillsynsmyndigheten att ta ut en handläggningsavgift och en årlig avgift av vissa verksamhetsutövare. Övervägandena finns i avsnitt 7.3.

Grunden för uttag av avgift är kostnaden för tillsynsmyndighetens verksamhet enligt lagen. Uttag därutöver får inte förekomma. Avgifterna ska fördelas med skälig andel på var och en av verksamhetsutövarna. Avgifternas exakta storlek kan anges i verkställighetsföreskrifter som meddelas med stöd av 8 kap. 7 § regeringsformen.

4 kap. Ingripanden

När och hur tillsynsmyndigheten ska ingripa

1 § Tillsynsmyndigheten ska ingripa om en verksamhetsutövare har åsidosatt sina skyldigheter enligt 2 kap. 1–10 §§ eller enligt föreskrifter som har meddelats i anslutning till de paragraferna eller enligt sådana rättsakter som har antagits med stöd av artiklarna 21.5 och 23.11 i NIS 2-direktivet, i den ursprungliga lydelsen.

Ett ingripande sker genom beslut om föreläggande enligt 4 §, ansökan om förbud att inneha ledningsfunktion enligt 6 §, beslut om sanktionsavgift enligt 10 § eller, om det inte finns skäl att ingripa mot en överträdelse på något annat sätt, genom anmärkning.

Tillsynsmyndigheten får avstå från ett ingripande om någon annan tillsynsmyndighet har vidtagit åtgärder mot verksamhetsutövaren med anledning av överträdelsen och dessa åtgärder bedöms tillräckliga.

Paragrafen genomför delvis artiklarna 32.4 och 33.4 samt artiklarna 21.4, 34.2 i och 36 i NIS 2-direktivet. Den reglerar när och hur tillsynsmyndigheten ska ingripa vid vissa överträdelser. Möjligheten att ingripa mot överträdelser av skyldigheten att föra register och tillhandahålla uppgifter i registret enligt 2 kap. 11 och 12 §§ regleras i 5 §. Övervägandena finns i avsnitt 8.2, 8.3 och 8.8.

Vad de skyldigheter som räknas upp i *första stycket* innebär behandlas i viss mån i författningskommentarerna till angivna paragrafer. Det är obligatoriskt för tillsynsmyndigheten att ingripa om verksamhetsutövaren har åsidosatt någon av skyldigheterna, om det inte finns skäl att avstå från ingripande enligt paragrafens tredje stycke.

I *andra stycket* anges på vilka sätt ingripande kan ske. Om en tillsynsmyndighet inte finner skäl att ingripa på något annat sätt, ska den meddela verksamhetsutövaren en anmärkning. En tillsynsmyndighet kan ingripa på flera sätt mot samma överträdelse. Tillsynsmyndigheten kan exempelvis välja att besluta om sanktionsavgift, även om den dessförinnan har ingripit genom att besluta om ett föreläggande. Detsamma gäller i förhållande till övriga ingripandeformer, förutom anmärkning som endast ska meddelas om ingen annan ingripandeåtgärd vidtas. En sanktionsavgift får dock enligt 12 § inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

Tillsynsmyndigheten får enligt *tredje stycket* avstå från ett ingripande om någon annan tillsynsmyndighet har vidtagit åtgärder mot verksamhetsutövaren med anledning av överträdelsen och tillsynsmyndigheten bedömer att dessa åtgärder är tillräckliga. Tillsynsmyndigheten ska

exempelvis avstå från ett ingripande om ett sådant skulle riskera att bryta mot det så kallade dubbelbestraffningsförbudet.

Omständigheter som ska beaktas vid valet av ingripande

2 § Vid valet av ingripande ska hänsyn tas till hur allvarlig överträdelsen är, hur länge den har pågått och den skada eller risk för skada som uppstått till följd av överträdelsen. Vid bedömningen ska särskilt beaktas

1. om verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse,
2. vad verksamhetsutövaren har gjort för att förhindra eller minska skadan,
3. om överträdelsen har varit uppsåtlig eller berott på oaktsamhet, och
4. den ekonomiska fördel som överträdelsen har inneburit för verksamhetsutövaren.

Paragrafen genomför delvis artiklarna 32.7, 33.5 och 34.3 i NIS 2-direktivet. Paragrafen reglerar vilka omständigheter som ska beaktas vid valet av ingripande, inbegripet utformningen av ingripandet. Det följer av bland annat 5 § tredje stycket förvaltningslagen att tillsynsmyndigheten ska göra en proportionalitetsbedömning i varje enskilt fall, både i valet av ingripande och i utformningen av ingripandet. Övervägandena finns i avsnitt 8.4.1.

Tillsynsmyndigheten ska vid valet av ingripande alltid beakta hur allvarlig överträdelsen är, hur länge den har pågått och den skada eller risk för skada som uppkommit till följd av den. Ju allvarligare en överträdelse bedöms vara, desto mindre blir utrymmet att ingripa genom anmärkning. Dessutom påverkas bedömningen av sanktionsavgiftens storlek, om ett beslut om sanktionsavgift fattas enligt 10 §.

I bedömningen av överträdelsens allvar ingår att bedöma betydelsen av de bestämmelser som har överträtts och överträdelsens omfattning. Skyldigheten att vidta säkerhetsåtgärder enligt 2 kap. 3 § samt att genomföra incidentrapportering och lämna information enligt 2 kap. 5–10 §§ är de mest centrala skyldigheterna som följer av lagen. Överträdelser av dessa bestämmelser bör ses som försvårande vid den bedömning som ska göras enligt paragrafen. Vad gäller överträdelsens omfattning så kan de olika skyldigheterna fullgöras i större eller mindre mån, vilket ska avspeglas i valet av ingripande. Exempelvis ska en överträdelse av bestämmelserna som gäller skyldigheten att rapportera incidenter anses vara mer omfattande om det inte har skett någon rapportering alls jämfört med om endast en delrapport enligt 2 kap. 7 § har uteblivit. Även de omständigheter som ska beaktas enligt 3 § ska vägas in i bedömningen av överträdelsens allvar.

I bedömningen av skada eller risk för skada som har uppstått till följd av överträdelsen bör tillsynsmyndigheten bland annat beakta ekonomiska förluster för andra än verksamhetsutövaren, effekter på andra tjänster och antal användare som berörs.

Av paragrafen framgår att vissa omständigheter ska beaktas särskilt vid bedömningen av vilket ingripande som bör ske. Vid bedömningen enligt *punkt 1*, av om verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse, bör tiden mellan den tidigare och den aktuella överträdelsen vägas in. Det bör även bland annat beaktas om överträdelserna är likartade.

Enligt *punkt 2* ska särskilt beaktas vad verksamhetsutövaren har gjort för att förhindra eller minska en skada. Det bör beaktas vilka verksamma

åtgärder verksamhetsutövaren har vidtagit. Den omständigheten att en verksamhetsutövare har efterlevt godkända uppförandekoder eller certifieringsmekanismer och att en överträdelse har skett trots en lojal tillämpning av dessa kan till exempel beaktas i förmildrande riktning. Att verksamhetsutövaren tidigt har vidtagit rättelse eller åtgärder för att begränsa en skada kan också tala för en lindrigare typ av ingripande eller en lägre sanktionsavgift om ett beslut om sanktionsavgift fattas. Detsamma gäller om verksamhetsutövaren aktivt har samarbetat med tillsynsmyndigheten. I motsatt riktning talar exempelvis att verksamhetsutövaren har vidtagit åtgärder först efter påtryckningar från tillsynsmyndigheten eller att verksamhetsutövaren har vägrat att samarbeta med myndigheten.

Enligt *punkt 3* ska det beaktas om överträdelsen har varit uppsåtlig eller berott på oaktsamhet. Om verksamhetsutövaren har överträtt reglerna fullt medveten om överträdelsen bör det i princip vara uteslutet att meddela en anmärkning enligt 1 § eller bestämma en sanktionsavgift till ett lågt belopp om ett beslut om sanktionsavgift fattas. Om en överträdelse har skett med uppsåt eller av oaktsamhet är det graden av uppsåt eller oaktsamhet som påverkar vilket utrymme som finns för att besluta om en lindrigare form av ingripande. Ju ringare oaktsamheten är, desto starkare skäl kan det finnas att välja en mindre ingripande åtgärd. Om den som har överträtt reglerna har gjort rimliga ansträngningar för att agera korrekt men felbedömt rättsläget är utrymmet också större att välja en mindre ingripande åtgärd. Det kan dock inte uteslutas att tillsynsmyndigheten bedömer att en anmärkning inte är ett alternativ eller att en sanktionsavgift bör tas ut till ett högre belopp även om omständigheterna är förmildrande. Så kan vara fallet om överträdelsen har fått eller riskerat att få allvarliga konsekvenser.

Enligt *punkt 4* ska den ekonomiska fördel som överträdelsen har inneburit för verksamhetsutövaren beaktas. Ekonomisk fördel inbegriper både fastställbara vinster och sådana kostnader som har undvikits till följd av överträdelsen.

3 § En överträdelse ska betraktas som allvarlig om verksamhetsutövaren

1. har begått upprepade överträdelser,
2. inte har fullgjort sin skyldighet att rapportera eller informera enligt 2 kap. 5–9 §§,
3. inte har avhjälpt en betydande incident,
4. inte har följt ett föreläggande enligt 4 § första stycket,
5. har hindrat en tillsynsåtgärd enligt 3 kap. 3–7 §§, eller
6. har lämnat falska eller andra grovt oriktiga uppgifter i fråga om säkerhetsåtgärder enligt 2 kap. 3 § eller i samband med incidentrapportering eller fullgörande av informationsskyldighet enligt 2 kap. 5–10 §§.

Paragrafen genomför delvis artiklarna 32.7, 33.5 och 34.3 i NIS 2-direktivet och reglerar i vilka fall en överträdelse alltid är att betrakta som allvarlig. Att en överträdelse bedöms vara allvarlig är en av förutsättningarna för att tillsynsmyndigheten ska kunna ansöka om förbud att inneha ledningsfunktion enligt 6 § och en av omständigheterna som ska beaktas vid valet av ingripande enligt 2 §. Övervägandena finns i avsnitt 8.4.2.

En överträdelse ska betraktas som allvarlig om verksamhetsutövaren enligt *punkt 1* har begått upprepade överträdelser. Att det ska röra sig om

upprepade överträdelser innebär att det ska röra sig om fler än två tidigare överträdelser. Tiden mellan de tidigare överträdelserna och den aktuella överträdelsen bör vägas in. Det bör även beaktas om överträdelserna är likartade.

Enligt *punkt 2* ska en överträdelse betraktas som allvarlig om verksamhetsutövaren inte har fullgjort skyldigheten att rapportera eller informera om betydande incidenter. Bestämmelsen avser inte skyldigheten att informera mottagare av tjänster vid betydande cyberhot enligt 2 kap. 10 §.

I *punkt 3* anges att en överträdelse ska betraktas som allvarlig om verksamhetsutövaren inte har avhjälpt en betydande incident. Med att avhjälpa en incident avses att så långt som möjligt åtgärda brister eller lindra effekterna av incidenten.

Av *punkt 4* framgår att en överträdelse ska anses vara allvarlig om en verksamhetsutövare inte har följt ett föreläggande från en tillsynsmyndighet om att fullgöra vissa skyldigheter enligt lagen. Bedömningen bör nyanseras om verksamhetsutövaren uppenbart har försökt följa föreläggandet, men inte lyckats fullt ut.

Enligt *punkt 5* ska ageranden som innebär att verksamhetsutövaren har hindrat tillsynsåtgärder, till exempel en säkerhetsrevision, innebära att en överträdelse är att betrakta som allvarlig. Det bör krävas någon form av passiv eller aktiv obstruktion av åtgärden, till exempel i form av att vägra tillsynsmyndigheten tillträde till verksamhetsutövarens lokaler. Att en verksamhetsutövare har hindrat tillsynsåtgärder omfattar även att verksamhetsutövaren har försvårat eller utan giltigt skäl försenat sådana åtgärder.

I *punkt 6* anges att en överträdelse ska betraktas som allvarlig om verksamhetsutövaren har lämnat falska eller andra grovt oriktiga uppgifter i fråga om säkerhetsåtgärder eller i samband med incidentrapportering eller information till mottagare av tjänster. Med oriktiga uppgifter avses felaktiga och missvisande uppgifter, men även utelämnade uppgifter som borde ha lämnats. Det kan exempelvis röra sig om en grovt oriktig uppgift om en uppgift av central betydelse har utelämnats och avsaknaden av den har lett till att tillsynsmyndigheten har underlåtit att vidta en viss tillsynsåtgärd i förhållande till verksamhetsutövaren. Om verksamhetsutövaren har lämnat en missvisande uppgift av mindre betydelse bör uppgiften inte anses vara grovt oriktig.

Förelägganden

4 § Tillsynsmyndigheten får besluta de förelägganden som behövs för att verksamhetsutövare ska fullgöra skyldigheterna som avses i 1 §.

Tillsynsmyndigheten får också förelägga verksamhetsutövare att offentliggöra information om överträdelser av sådana skyldigheter som avses i första stycket.

Ett föreläggande får förenas med vite. Ett vitesföreläggande får även riktas mot staten.

Paragrafen genomför delvis artiklarna 32.4 b–f och h, 33.4 b–g och 34.6 i NIS 2-direktivet. Övervägandena finns i avsnitt 8.5.

Första stycket fastställer tillsynsmyndighetens rätt att besluta de förelägganden som behövs för att få en verksamhetsutövare att fullgöra vissa skyldigheter enligt lagen. Den lämplighetsbedömning som ska ske

enligt 2 kap. 9 och 10 §§ hindrar inte att tillsynsmyndigheten förelägger en verksamhetsutövare att fullgöra sin informationsskyldighet enligt nämnda paragrafer.

Andra stycket ger tillsynsmyndigheten möjlighet att förelägga en verksamhetsutövare att offentliggöra information om en överträdelse. Tillsynsmyndigheten får, med beaktande av proportionalitetsprincipen i bland annat 5 § tredje stycket förvaltningslagen, besluta hur och var ett sådant offentliggörande ska ske samt vad offentliggörandet ska innehålla för uppgifter.

Tredje stycket innebär att förelägganden får förenas med vite. Viteslagen är då tillämplig.

5 § Tillsynsmyndigheten får besluta de förelägganden som behövs för att verksamhetsutövare ska fullgöra skyldigheterna enligt 2 kap. 11 och 12 §§ eller enligt föreskrifter som har meddelats i anslutning till de paragraferna.

Ett föreläggande får förenas med vite. Ett vitesföreläggande får även riktas mot staten.

Paragrafen genomför delvis artiklarna 32.4 b–f och h, 33.4 b–g och 34.6 i NIS 2-direktivet. Övervägandena finns i avsnitt 10.

Första stycket fastställer tillsynsmyndighetens rätt att besluta de förelägganden som behövs för att få verksamhetsutövare som är registreringsenheter för toppdomäner eller som erbjuder domännamnsregistreringstjänster att bland annat föra register över tilldelade domännamn under toppdomänen och att lämna ut uppgifter ur registret. Det är inte möjligt att vidta åtgärder enligt 1 § vid åsidosättande av skyldigheterna enligt 2 kap. 11 och 12 §§.

Andra stycket innebär att förelägganden får förenas med vite. Viteslagen är då tillämplig.

Förbud att inneha ledningsfunktion

6 § Om ett föreläggande enligt 4 § första stycket inte följs får tillsynsmyndigheten ansöka om förbud att inneha ledningsfunktion för den som är befattningshavare enligt 3 § andra stycket lagen (2014:836) om näringsförbud hos en enskild verksamhetsutövare som är väsentlig.

En ansökan enligt första stycket får göras endast om överträdelsen som ligger till grund för föreläggandet är allvarlig och befattningshavaren uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen.

Paragrafen genomför delvis artikel 32.5 b i NIS 2-direktivet. Övervägandena finns i avsnitt 8.6.1.

En ansökan får, om de omständigheter som anges i paragrafen i övrigt föreligger, riktas mot befattningshavare enligt 3 § andra stycket lagen om näringsförbud. Det ska därmed röra sig om till exempel en styrelseledamot eller verkställande direktör samt ersättare för dessa i aktiebolag. Ingripande genom förbud får endast ske i förhållande till en befattningshavare hos en enskild verksamhetsutövare som är väsentlig. Vad som avses med uttrycket enskild verksamhetsutövare framgår av 1 kap. 2 §. En ansökan om förbud kan inte avse en person i ledningsställning hos en offentlig verksamhetsutövare. Vilka enskilda verksamhetsutövare som räknas som väsentliga följer av 1 kap. 8 §.

7 § En ansökan enligt 6 § ska göras till allmän förvaltningsdomstol.

Ansökan ska innehålla uppgifter om den person, befattning och verksamhetsutövare som ansökan avser. Den ska också innehålla uppgift om överträdelsen och de omständigheter som behövs för att kännetecknа den samt de bestämmelser som är tillämpliga på överträdelsen.

Ansökan ska lämnas in till den förvaltningsrätt inom vars domkrets tillsynsmyndigheten är belägen och målet ska prövas skyndsamt av domstolen.

Paragrafen genomför delvis artikel 32.5 b i NIS 2-direktivet. Övervägandena finns i avsnitt 8.6.2.

I paragrafen anges att ansökan om förbud ska göras till allmän förvaltningsdomstol och vilka uppgifter ansökan ska innehålla. Bestämmelserna kompletterar de allmänna krav på en ansökans innehåll som följer av 3 och 4 §§ förvaltningsprocesslagen (1971:291). Ansökan ska lämnas in till den domstol inom vars domkrets tillsynsmyndigheten är belägen, det vill säga där myndighetens huvudkontor är beläget, och ska prövas skyndsamt av domstolen. Skyndsamhetskravet gäller både vid förvaltningsrättens prövning av ansökan och vid en överinstans hantering av ett överklagande.

8 § Ett förbud att inneha ledningsfunktion ska gälla lägst ett år och högst tre år.

Tillsynsmyndigheten ska omedelbart begära att förbudet ska upphävas om den bedömer att det inte längre finns förutsättningar för ett förbud enligt 6 §. Den enskilde ska vid ett beslut om förbud upplysas om sin rätt att begära att förbudet ska upphävas enligt 9 §.

Paragrafen genomför delvis artikel 32.5 b i NIS 2-direktivet. Övervägandena finns i avsnitt 8.6.2.

Om domstolen beslutar om förbud i enlighet med paragrafen, ska ett förbud vara tidsbegränsat. Förbudet innebär i praktiken att befattningshavaren blir omedelbart obehörig att inneha ledningsfunktioner hos verksamhetsutövaren under viss tid. Med att inneha ledningsfunktion avses att inneha någon av de befattningar som framgår av 3 § lagen om näringsförbud. En person som har varit verkställande direktör hos en verksamhetsutövare kan därmed inte heller vara till exempel styrelseledamot hos verksamhetsutövaren efter ett förbud. Däremot innebär förbudet inte att personen är förhindrad att utföra andra arbetsuppgifter hos verksamhetsutövaren.

Tillsynsmyndigheten ska omedelbart begära att förbudet ska upphävas om den bedömer att det inte längre finns förutsättningar för ett sådant. Den enskilde ska upplysas om sin rätt att begära att ett förbud ska upphävas enligt 9 § i samband med att förbudet beslutas.

9 § Om tillsynsmyndigheten eller den enskilde begär det ska den domstol som avses i 7 § pröva om förbudet ska upphävas. Ett förbud ska upphävas omedelbart om det inte längre finns förutsättningar för det enligt 6 §.

Paragrafen genomför delvis artikel 32.5 b i NIS 2-direktivet. Övervägandena finns i avsnitt 8.6.2.

Domstolen ska pröva om ett förbud enligt 8 § ska upphävas om tillsynsmyndigheten eller den enskilde begär det. Den enskilde ska enligt 8 §

upplysas om sin rätt att begära att ett förbud ska upphävas i samband med att förbudet beslutas.

Ett förbud ska upphävas omedelbart om det inte längre finns förutsättningar för ett sådant enligt 6 §. Det kan exempelvis röra sig om att verksamhetsutövaren har följt det föreläggande som ligger till grund för förbudet eller att en annan bedömning görs i ett senare skede i uppsåts- eller oaktsamhetsfrågan eller i fråga om överträdelsens allvar.

Sanktionsavgift

10 § Tillsynsmyndigheten får besluta att ta ut en sanktionsavgift av en verksamhetsutövare till följd av en överträdelse av de skyldigheter som avses i 1 §.

Paragrafen genomför delvis artikel 34.3 samt artiklarna 32.4 i, 33.4 h och 34.1 i NIS 2-direktivet. Paragrafen reglerar uttömmande när en sanktionsavgift får tas ut. Övervägandena finns i avsnitt 8.7.1.

Det är inte obligatoriskt att ta ut en sanktionsavgift när en överträdelse har konstaterats, utan tillsynsmyndigheten avgör om en avgift ska tas ut i det enskilda fallet. En avgift kan tas ut även om överträdelsen varken har varit uppsåtlig eller berott på oaktsamhet. Att överträdelsen har varit uppsåtlig eller berott på oaktsamhet är en omständighet som särskilt ska beaktas vid bedömningen enligt 2 § och omständigheten kan därmed påverka både om en avgift ska tas ut och sanktionsavgiftens storlek. Innan myndigheten tar ut en sanktionsavgift ska den avgiftsskyldige ges tillfälle att yttra sig. Detta följer av 13 §.

11 § Sanktionsavgiften ska bestämmas till lägst 5 000 kronor och högst till

1. det högsta av 2 procent av den totala globala årsomsättningen närmast föregående räkenskapsår eller ett belopp i kronor motsvarande 10 000 000 euro för en enskild verksamhetsutövare som är väsentlig,
2. det högsta av 1,4 procent av den totala globala årsomsättningen närmast föregående räkenskapsår eller ett belopp i kronor motsvarande 7 000 000 euro för en enskild verksamhetsutövare som är viktig, eller
3. 10 000 000 kronor för en offentlig verksamhetsutövare.

Paragrafen genomför artikel 34.4, 34.5 och 34.7 i NIS 2-direktivet. Paragrafen fastställer minimi- och maximibelopp för sanktionsavgifter. Övervägandena finns i avsnitt 8.7.2.

Av paragrafen framgår att det lägsta belopp som en sanktionsavgift kan bestämmas till är 5 000 kronor. Maximinivån beror på vilken typ av verksamhetsutövare det är fråga om. Vad som avses med uttrycken enskild verksamhetsutövare och offentlig verksamhetsutövare framgår av 1 kap. 2 §. Vilka enskilda verksamhetsutövare som räknas som väsentliga följer av 1 kap. 8 §. Hur avgiftens storlek närmare ska bestämmas regleras genom 2 och 3 §§. Belopp i den övre delen av beloppsintervallen bör komma i fråga endast för mycket allvarliga överträdelser.

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

Paragrafen syftar till att förhindra att en överträdelse blir föremål för både sanktionsavgift och utdömande av vite enligt ett tidigare föreläggande. Övervägandena finns i avsnitt 8.7.3.

Bestämmelsen innebär att tillsynsmyndigheten är förhindrad att besluta om en sanktionsavgift, om överträdelsen omfattas av ett vitesföreläggande för samma överträdelse och en domstolsprocess har inletts om utdömande av vitet. En sanktionsavgift får inte heller tas ut av verksamhetsutövaren om en sådan avgift har tagits ut enligt ett annat regelverk för samma överträdelse. Detta följer inte av paragrafen utan av det så kallade dubbelbestraffningsförbudet.

13 § En sanktionsavgift får beslutas endast om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

Paragrafen reglerar bland annat den bortre tidsgränsen för när en sanktionsavgift får beslutas. Övervägandena finns i avsnitt 8.7.3.

Sanktionsavgift får inte tas ut om kommunikation enligt förvaltningslagen med den som avgiften ska tas ut av inte har skett inom två år från överträdelsen. Det är tillsynsmyndighetens ansvar att kontrollera att kommunikation har skett. Av paragrafen följer vidare att ett beslut om sanktionsavgift ska delges den avgiftsskyldige, vilket innebär att tillsynsmyndigheten ska använda sig av de metoder för delgivning som regleras i delgivningslagen (2010:1932) för att säkerställa att den som beslutet gäller får del av underrättelsen.

14 § En sanktionsavgift ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas i rätt tid, ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

Sanktionsavgiften tillfaller staten.

Paragrafen innehåller bestämmelser om betalning och indrivning av sanktionsavgifter. Övervägandena finns i avsnitt 8.7.3.

15 § En sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Paragrafen innebär att skyldigheten att betala en sanktionsavgift kan falla bort. Övervägandena finns i avsnitt 8.7.3.

5 kap. Överklagande

1 § Tillsynsmyndighetens beslut enligt denna lag får överklagas till allmän förvaltningsdomstol. När ett sådant beslut överklagas är tillsynsmyndigheten motpart i domstolen. Övriga beslut får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen reglerar överklagande av tillsynsmyndighetens beslut enligt lagen. Övervägandena finns i avsnitt 9.

Tillsynsmyndighetens beslut som överklagas ska prövas av den förvaltningsrätt inom vars domkrets ärendet först prövats i enlighet med 14 § andra stycket lagen (1971:289) om allmänna förvaltningsdomstolar. Förvaltningsrättens avgörande kan överklagas till behörig kammarrätt. Prövningstillstånd krävs vid överklagande till kammarrätten. Att förvaltningsrättens beslut om förbud att inneha ledningsfunktion enligt 4 kap. 8 § kan överklagas framgår av 33 § förvaltningsprocesslagen.

Paragrafen reglerar endast förutsättningarna att överklaga tillsynsmyndighetens beslut enligt lagen. Vid handräckning gäller, som framgår av 3 kap. 9 §, bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande. Utsökningsbalkens bestämmelser om överklagande gäller därmed också i det sammanhanget.

Regeringen får enligt 1 kap. 15 §, om det finns särskilda skäl, fatta beslut om undantag i enskilda fall från skyldigheterna enligt lagen för enskilda utbildningsanordnare med visst tillstånd att utfärda examina och partnerföretag och anknutna företag. Regeringens beslut kan bli föremål för rättsprövning enligt lagen (2006:304) om rättsprövning av vissa regeringsbeslut, om beslutet innefattar en prövning av enskildas civila rättigheter och skyldigheter enligt artikel 6 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

Kravet på prövningstillstånd i paragrafen gäller endast för de mål som har inletts genom ett överklagande och inte förvaltningsrättens beslut om förbud att inneha ledningsfunktion.

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 15 januari 2026.
2. Genom lagen upphävs lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.
3. Den upphävda lagen gäller dock fortfarande för överträdelser som har skett före ikraftträdandet.

Övervägandena finns i avsnitt 13.

Enligt *punkt 1* träder lagen i kraft den 15 januari 2026. Bestämmelsen hindrar inte att en verksamhetsutövare före dess vidtar åtgärder som kan behövas för att lagen ska kunna tillämpas i sin helhet i verksamheten från och med ikraftträdandet.

Av *punkt 2* följer att den så kallade NIS-lagen upphävs genom lagen.

Enligt *punkt 3* gäller NIS-lagen för överträdelser som har skett före ikraftträdandet.

15.2 Förslaget till lag om ändring i lagen (2006:24) om nationella toppdomäner för Sverige på internet

Lagförslaget är en följd av genomförandet av artikel 28 i NIS 2-direktivet. I det följande kommenteras endast de ändringar i lagen som innebär en ändring i sak. Övriga ändringar är av språklig och redaktionell karaktär.

6 § En domänadministratör *ska* föra ett register över tilldelade domännamn under toppdomänen och löpande upprätta säkerhetskopior av registeruppgifterna.

Registret *ska* innehålla

1. domännamnet,
2. namnet på domännamnsinnehavaren och dennes telefonnummer och *e-postadress*,
3. namnet på den som tekniskt administrerar domännamnet och dennes telefonnummer och *e-postadress*,
4. uppgifter om de namnservrar som är knutna till domännamnet,
5. övrig teknisk information som behövs för att administrera domännamnet*, och*
6. *registreringsdatum.*

Uppgifterna i registret *ska* kunna hämtas utan avgift via *internet*. *Därutöver ska uppgifter även på begäran lämnas ut skyndsamt och senast 72 timmar efter mottagandet av begäran till den som gör en lagligen grundad och motiverad begäran.*

Personuppgifter får dock göras tillgängliga på *internet* endast om den registrerade har samtyckt till det.

Domänadministratören är personuppgiftsansvarig för behandling av personuppgifter i registret.

Ändringen av *andra stycket* innebär att även registreringsdatum ska ingå i registret men inte postadress. I stycket görs också redaktionella ändringar.

Ändringarna i *tredje stycket* innebär att uppgifter, förutom att kunna hämtas utan avgift via internet, på begäran även ska lämnas ut skyndsamt och senast 72 timmar efter mottagandet av begäran till varje fysisk eller juridisk person som gör en lagligen grundad och motiverad begäran. Att begäran ska vara lagligen grundad innebär att den ska avse ett krav på att få del av uppgifter som framställs med stöd av unionsrätten eller nationell rätt och att den ska vara förenlig med dataskyddslagstiftningen. En begäran kan exempelvis vara grundad på en bestämmelse som ger rätt att få del av uppgifter eller på ett beslut meddelat av domstol, till exempel ett editionsbeslut. Att begäran ska vara motiverad innebär att sökanden måste visa stöd för sin begäran i förhållande till varje specifik domäns registreringsdata. En bedömning av ansökan får göras i det enskilda fallet. Att uppgifterna ska lämnas ut skyndsamt innebär att en begäran om uppgifter ska besvaras utan onödigt dröjsmål. En bortre tidsgräns om 72 timmar gäller enligt paragrafen. Tillsynsmyndigheten får med stöd av 9 § meddela föreskrifter om registret.

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

15 kap.

3 c § *Sekretessen enligt 1 a § hindrar inte att Myndigheten för samhällsskydd och beredskap i egenskap av en sådan gemensam kontaktpunkt, enhet för hantering av it-säkerhetsincidenter eller cyberkrishanteringsmyndighet som avses i 1 kap. 16 § cybersäkerhetslagen (2025:000) lämnar en uppgift till en tillsynsmyndighet enligt samma lag, om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag.*

Sekretessen hindrar inte heller att en sådan tillsynsmyndighet som avses i första stycket lämnar en uppgift till Myndigheten för samhällsskydd och beredskap, om uppgiften behövs för att Myndigheten för samhällsskydd och beredskap ska kunna

fullgöra sitt uppdrag som sådan gemensam kontaktpunkt, enhet för hantering av it-säkerhetsincidenter eller cyberkrishanteringsmyndighet som avses i första stycket.

En uppgift enligt första eller andra stycket får lämnas endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

Paragrafen, som är ny, innehåller sekretessbrytande bestämmelser för dels Myndigheten för samhällsskydd och beredskap (MSB), dels tillsynsmyndigheterna enligt cybersäkerhetslagen när det gäller sekretess i det internationella samarbetet. Övervägandena finns i avsnitt 12.

Första stycket gör det möjligt för MSB att lämna vidare en uppgift som omfattas av sekretess i det internationella samarbetet och som myndigheten har fått del av i egenskap av i paragrafen angivna funktioner, om uppgiften behövs för att den mottagande tillsynsmyndigheten ska kunna fullgöra sitt uppdrag enligt cybersäkerhetslagen.

Enligt *andra stycket* är det även möjligt för en tillsynsmyndighet att vidarebefordra en uppgift som omfattas av sekretess i det internationella samarbetet till MSB, om uppgiften behövs för att MSB ska kunna fullgöra sina uppgifter i egenskap av angivna funktioner.

Enligt *tredje stycket* bryts sekretessen endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda. Det ska alltså göras en intresseavvägning.

18 kap.

8 b § *Sekretess gäller för uppgift i en incidentrapport enligt cybersäkerhetslagen (2025:000) och för uppgift om vilka åtgärder som en verksamhetsutövare har vidtagit till följd av incidenten, om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens framtida verksamhet skadas eller syftet med vidtagen åtgärd motverkas.*

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

Paragrafen, som är ny, innehåller bestämmelser om sekretess för uppgifter i incidentrapporter enligt cybersäkerhetslagen och uppgifter om vilka åtgärder som en verksamhetsutövare har vidtagit med anledning av sådana incidenter som har rapporterats. Övervägandena finns i avsnitt 12.

Enligt *första stycket* skyddas uppgifter i incidentrapporterna och uppgifter om vilka åtgärder som har vidtagits till följd av 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 den rapporterande verksamhetsutövarens framtida verksamhet skadas eller syftet med den vidtagna åtgärden motverkas.

Enligt *andra stycket* gäller sekretessen i högst fyrtio år.

19 § Den tystnadsplikt som följer av 5–7, 8, *8 b*, 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 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.

I paragrafen regleras rätten att meddela och offentliggöra uppgifter. Paragrafen ändras så att den nya 8 b § omfattas av den uppräkning av paragrafer som görs i första stycket. Rätten att meddela och offentliggöra uppgifter får därmed inte företräde framför den tystnadsplikt som följer av 8 b §. Övervägandena finns i avsnitt 12.

15.4 Förslaget till lag om ändring i lagen (2022:482) om elektronisk kommunikation

Lagförslaget är en följd av att artiklarna 40 och 41 i Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation har upphävts och ersatts av bestämmelser i NIS 2-direktivet. Bestämmelserna i 8 kap. 1–4 §§, som genomför artiklarna, upphävs. Nuvarande 8 kap. 5–9 §§ ändrar som en följd av detta beteckning till 8 kap. 1–5 §§. Följdändringar görs också i 1 kap. 7 § och 12 kap. 1 §. I nya 1 kap. 4 a § förs det in en upplysningsbestämmelse. I det följande kommenteras endast den senare ändringen.

1 kap.

4 a § *I cybersäkerhetslagen (2025:000) finns det bestämmelser om säkerhetsåtgärder, säkerhetsrevision, incidentrapportering och informationsskyldighet.*

Paragrafen, som är ny, upplyser om att det i cybersäkerhetslagen finns krav som anknyter till lagen. Övervägandena finns i avsnitt 11.

Bestämmelserna i cybersäkerhetslagen gäller bland annat för verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster i Sverige (se 1 kap. 6 § den lagen). Kravet på att vidta säkerhetsåtgärder gäller i den utsträckning som det följer av 2 kap. 3 § cybersäkerhetslagen. Förutsättningarna för en säkerhetsrevision regleras i 3 kap. 5 och 6 §§ samma lag. Skyldigheten för en verksamhetsutövare att genomföra incidentrapportering och fullgöra viss informationsskyldighet regleras genom 2 kap. 5–10 §§ samma lag.

L 333/80 SV Europeiska unionens officiella tidning 27.12.2022

DIREKTIV

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)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

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 centralbankens yttrande ([1]),

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([2]),

efter att ha hört Regionkommittén,

i enlighet med det ordinarie lagstiftningsförfarandet ([3]), och

av följande skäl:

(1) Syftet med Europaparlamentets och rådets direktiv (EU) 2016/1148 ([4]) var att bygga upp cybersäkerhetskapaciteten i hela unionen, begränsa hoten mot nätverks- och informationssystem som används för att tillhandahålla samhällsviktiga tjänster i centrala sektorer och säkerställa kontinuiteten i sådana tjänster när de utsätts för incidenter, och därigenom bidra till unionens säkerhet och till att dess ekonomi och samhälle kan fungera effektivt.

(2) Sedan direktiv (EU) 2016/1148 trädde i kraft har betydande framsteg gjorts med att öka unionens nivå av cyberresiliens. Översynen av det direktivet har visat att det har fungerat som katalysator för den institutionella och lagstiftningsmässiga strategin för cybersäkerhet i unionen och har banat väg för en betydande attitydförändring. Direktivet har säkerställt fullbordandet av nationella ramar för säkerhet i nätverks- och informationssystem genom att fastställa nationella strategier för säkerhet i nätverks- och informationssystem och inrätta nationell kapacitet och genom att genomföra lagstiftningsåtgärder som omfattar väsentliga infrastrukturer och entiteter som identifierats av varje medlemsstat. Direktiv (EU) 2016/1148 har också bidragit till samarbete på unionsnivå genom inrättandet av samarbetsgruppen samt nätverket av nationella it-incidentcentrum. Trots dessa framsteg har översynen av direktiv (EU) 2016/1148 avslöjat inneboende brister som hindrar det från att effektivt hantera befintliga och framväxande utmaningar på cybersäkerhetsområdet.

(3) Nätverks- och informationssystem har utvecklats till ett centralt inslag i vardagslivet i och med den snabba digitala omställningen och sammankopplingen av samhället, vilket även gäller vid gränsöverskridande utbyten. Denna utveckling har lett till en utvidgad cyberhotbild, som medfört nya utmaningar som kräver anpassade, samordnade och innovativa svarsåtgärder i alla medlemsstater. Incidenter, som blir allt fler och mer omfattande, sofistikerade och vanliga och får allt större inverkan, utgör ett allvarligt hot mot nätverks- och informationssystemens funktion. Därför kan sådana incidenter hindra utövandet av ekonomisk verksamhet på den inre marknaden, generera

([1]) EUT C 233, 16.6.2022, s. 22.
([2]) EUT C 286, 16.7.2021, s. 170.
([3]) Europaparlamentets ståndpunkt av den 10 november 2022 (ännu inte offentliggjord i EUT) och rådets beslut av den 28 november 2022.
([4]) 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 (EUT L 194, 19.7.2016, s. 1).

ekonomisk förlust, undergräva användarnas förtroende och orsaka allvarlig skada för unionens ekonomi och samhälle. Beredskap och ändamålsenlighet på cybersäkerhetsområdet är därför nu viktigare än någonsin för att den inre marknaden ska fungera väl. Cybersäkerhet är dessutom en viktig förutsättning för att många kritiska sektorer ska kunna tillgodogöra sig den digitala omställningen och fullt ut utnyttja digitaliseringens ekonomiska, sociala och hållbarhetsmässiga fördelar.

(4) Den rättsliga grunden för direktiv (EU) 2016/1148 var artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), vars mål är att upprätta den inre marknaden och säkerställa dess funktion genom att förbättra åtgärderna för tillnärmning av nationella regler. De cybersäkerhetskrav som åläggs entiteter som tillhandahåller tjänster eller utför verksamhet som är ekonomiskt betydelsefull varierar avsevärt mellan medlemsstaterna vad gäller typen av krav, kravens utförlighet och tillsynsmetoden. Dessa skillnader medför extra kostnader och gör det svårt för entiteterna att erbjuda varor och tjänster över gränserna. Krav som ställs av en medlemsstat och som skiljer sig från, eller till och med står i strid med, krav som ställs av en annan medlemsstat kan väsentligt påverka sådan gränsöverskridande verksamhet. Det är dessutom sannolikt att otillräckligt utformade eller genomförda cybersäkerhetskrav i en medlemsstat kommer att få återverkningar för cybersäkerhetsnivån i andra medlemsstater, särskilt med tanke på det intensiva utbytet över gränserna. Översynen av direktiv (EU) 2016/1148 har visat på stora skillnader i medlemsstaternas genomförande, även vad gäller dess tillämpningsområde, då avgränsningen av detta i stor utsträckning har överlåtits på medlemsstaterna. Direktiv (EU) 2016/1148 gav också medlemsstaterna mycket stort utrymme för skönsmässig bedömning vad gäller genomförandet av de säkerhets- och incidentrapporteringsskyldigheter som fastställs i det. Dessa skyldigheter genomfördes därför på väsentligt skilda sätt på nationell nivå. Det finns liknande skillnader i genomförandet av bestämmelserna om tillsyn och efterlevnadskontroll i direktiv (EU) 2016/1148.

(5) Alla dessa skillnader medför en fragmentering av den inre marknaden och kan ha en skadlig inverkan på dess funktion, vilket påverkar i synnerhet tillhandahållandet av tjänster över gränserna och nivån av cyberresiliens till följd av tillämpningen av ett spektrum av åtgärder. Dessa skillnader kan till sist leda till att vissa medlemsstater har större sårbarhet för cyberhot, med potentiella spridningseffekter i hela unionen. Direktivets mål är att undanröja dessa stora skillnader mellan medlemsstaterna, särskilt genom att föreskriva minimiregler för ett fungerande samordnat regelverk genom att fastställa mekanismer för effektivt samarbete mellan de ansvariga myndigheterna i varje medlemsstat, genom att uppdatera förteckningen över sektorer och verksamheter som omfattas av skyldigheter vad gäller cybersäkerhet och genom att föreskriva effektiva rättsmedel och efterlevnadskontrollåtgärder, vilket är centralt för att upprätthålla en effektiv kontroll av att dessa skyldigheter efterlevs. Därför bör direktiv (EU) 2016/1148 upphävas och ersättas av det här direktivet.

(6) I och med upphävandet av direktiv (EU) 2016/1148 bör tillämpningsområdet med avseende på olika sektorer utvidgas till en större del av ekonomin så att den ger en omfattande täckning av sektorer och tjänster som är av avgörande betydelse för viktiga samhälleliga och ekonomiska verksamheter på den inre marknaden. I synnerhet syftar det här direktivet till att åtgärda bristerna i fråga om differentieringen mellan leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, vilken har visat sig vara inaktuell eftersom den inte speglar den betydelse som dessa sektorer och tjänster har för samhälleliga och ekonomiska verksamheter på den inre marknaden.

(7) Enligt direktiv (EU) 2016/1148 hade medlemsstaterna ansvaret för att identifiera de entiteter som uppfyllde kriterierna för att klassificeras som leverantörer av samhällsviktiga tjänster. För att undanröja de stora skillnaderna mellan medlemsstaterna i detta avseende och säkerställa rättslig säkerhet vad gäller riskhanteringsåtgärderna för cybersäkerhet och rapporteringsskyldigheterna för alla relevanta entiteter, bör det fastställas ett enhetligt kriterium för vilka entiteter som ska omfattas av tillämpningsområdet för detta direktiv. Kriteriet bör bestå i tillämpningen av en storleksbaserad regel som innebär att alla entiteter som betraktas som medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG ([3]), eller överstiger de trösklar för medelstora företag som fastställs i punkt 1 i den artikeln, och som är verksamma i de sektorer och tillhandahåller de typer av tjänster eller

([3]) 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).

bedriver de verksamheter som omfattas av det här direktivet också omfattas av tillämpningsområdet för det här direktivet. Medlemsstaterna bör även föreskriva att vissa små företag och mikroföretag, enligt definitionen i artikel 2.2 och 2.3 i den bilagan, som uppfyller specifika kriterier som visar deras nyckelroll för samhället, ekonomin eller för särskilda sektorer eller typer av tjänster ska omfattas av tillämpningsområdet för det här direktivet.

(8) Undantaget för offentliga förvaltningsentiteter från detta direktivs tillämpningsområde bör omfatta entiteter vars verksamhet till övervägande del bedrivs på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet verksamhet som rör utredning, förebyggande, upptäckt och lagföring av brott. Offentliga förvaltningsentiteter vars verksamhet endast marginellt hänför sig till dessa områden bör dock inte vara undantagna från direktivets tillämpningsområde. Vid tillämpningen av detta direktiv anses entiteter med tillsynsbefogenheter inte bedriva verksamhet på brottsbekämpningsområdet, och de är därför inte undantagna från tillämpningsområdet för detta direktiv. Offentliga förvaltningsentiteter som inrättats gemensamt med ett tredjeland i enlighet med ett internationellt avtal är undantagna från detta direktivs tillämpningsområde. Detta direktiv är inte tillämpligt på medlemsstaters diplomatiska och konsulära beskickningar i tredjeländer eller på deras nätverks- och informationssystem, såvida dessa system är belägna inom beskickningen eller drivs för användare i ett tredjeland.

(9) Medlemsstaterna bör kunna vidta de åtgärder som är nödvändiga för att skydda väsentliga nationella säkerhetsintressen, upprätthålla allmän ordning och säkerhet och möjliggöra förebyggande, utredning, upptäckt och lagföring av brott. I detta syfte bör medlemsstaterna kunna undanta särskilda entiteter som bedriver verksamhet på områdena, nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott, från vissa skyldigheter i detta direktiv med avseende på sådan verksamhet. Om en entitet tillhandahåller tjänster uteslutande för en offentlig förvaltningsentitet som är undantagen från detta direktivs tillämpningsområde bör medlemsstaterna kunna undanta den entiteten från vissa skyldigheter enligt detta direktiv med avseende på dessa tjänster. Vidare bör ingen medlemsstat vara skyldig att lämna information vars avslöjande skulle strida mot dess väsentliga intressen i fråga om nationell säkerhet, allmän säkerhet eller försvar. Unionsregler eller nationella regler till skydd för säkerhetsskyddsklassificerade uppgifter, sekretessavtal samt informella sekretessavtal såsom Traffic Light Protocol bör beaktas i detta sammanhang. Traffic Light Protocol bör ses som ett medel för att informera om eventuella begränsningar i vidarespridningen av information. Det används inom nästan alla enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter) och av vissa informations- och analyscentraler.

(10) Även om detta direktiv tillämpas på entiteter som bedriver verksamhet inom produktion av el från kärnkraftverk kan viss verksamhet vara kopplad till den nationella säkerheten. När så är fallet bör en medlemsstat kunna utöva sitt ansvar för att skydda den nationella säkerheten i samband med sådan verksamhet, inklusive verksamhet inom kärnenergins värdekedja, i enlighet med fördragen.

(11) Vissa entiteter bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott, samtidigt som de även tillhandahåller betrodda tjänster. Tillhandahållare av betrodda tjänster som omfattas av Europaparlamentets och rådets förordning (EU) nr 910/2014 ([6]) bör omfattas av detta direktiv för att säkerställa samma nivå på säkerhetskraven och tillsynen som den som tidigare fastställdes i den förordningen vad gäller tillhandahållare av betrodda tjänster. I överensstämmelse med undantaget för vissa specifika tjänster från förordning (EU) nr 910/2014 bör detta direktiv inte vara tillämpligt på tillhandahållande av betrodda tjänster som på grund av nationell rätt eller avtal mellan en avgränsad grupp deltagare endast används inom slutna system.

([6]) 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).

(12) Tillhandahållare av posttjänster enligt definitionen i Europaparlamentets och rådets direktiv 97/67/EG ([7]), inklusive tillhandahållare av budtjänster, bör omfattas av detta direktiv om de tillhandahåller minst ett led i postleveranskedjan, särskilt insamling, sortering, transport eller distribution av postförsändelser, inklusive upphämtning, samtidig som hänsyn tas till den grad i vilken de är beroende av nätverks- och informationssystem. Transporttjänster som inte utförs i samband med något av dessa led bör vara undantagna från tillämpningsområdet för posttjänster.

(13) Med tanke på att cyberhoten intensifieras och blir alltmer sofistikerade bör medlemsstaterna sträva efter att säkerställa att entiteter som är undantagna från detta direktivs tillämpningsområde uppnår en hög cybersäkerhetsnivå och stödja tillämpningen av likvärdiga riskhanteringsåtgärder för cybersäkerhet som speglar dessa entiteters känsliga natur.

(14) Unionens dataskyddslagstiftning och integritetslagstiftning är tillämplig på all behandling av personuppgifter inom ramen för detta direktiv. I synnerhet påverkar detta direktiv inte tillämpningen av Europaparlamentets och rådets förordning (EU) 2016/679 ([8]) och Europaparlamentets och rådets direktiv 2002/58/EG ([9]). Därför bör detta direktiv inte påverka exempelvis uppgifterna och befogenheterna för de myndigheter som är behöriga att övervaka efterlevnaden av unionens tillämpliga dataskyddslagstiftning och integritetslagstiftning.

(15) De entiteter som omfattas av tillämpningsområdet för detta direktiv med avseende på efterlevnad av riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter bör indelas i två kategorier, väsentliga entiteter och viktiga entiteter, vilket speglar i vilken mån de är av kritisk betydelse med avseende på sektor eller de typer av tjänster de tillhandahåller samt deras storlek. I detta avseende bör vederbörlig hänsyn i förekommande fall tas till eventuella relevanta sektorsspecifika riskbedömningar eller vägledning från de behöriga myndigheterna. Tillsyns- och efterlevnadskontrollsystemen för dessa båda kategorier av entiteter bör differentieras för att säkerställa en rättvis balans mellan riskbaserade krav och skyldigheter å ena sidan och den administrativa börda som följer av tillsynen av efterlevnaden å den andra.

(16) För att undvika att entiteter som har partnerföretag eller som är anknutna företag betraktas som väsentliga eller viktiga entiteter när detta vore oproportionellt kan medlemsstaterna ta hänsyn till vilken grad av oberoende som entiteten åtnjuter i förhållande till sin partner eller de anknutna företagen vid tillämpningen av artikel 6.2 i bilagan till rekommendation 2003/361/EG. I synnerhet kan medlemsstaterna ta hänsyn till att en entitet är oberoende av sin partner eller de anknutna företagen med avseende på de nätverks- och informationssystem som entiteten använder vid tillhandahållandet av sina tjänster och med avseende på de tjänster som entiteten tillhandahåller. På grundval av detta kan medlemsstaterna när det är lämpligt anse att en sådan entitet inte betraktas som ett medelstort företag enligt artikel 2 i bilagan till rekommendation 2003/361/EG, eller inte överstiger de trösklar för ett medelstort företag som fastställs i punkt 1 i den artikeln, om entiteten, med hänsyn tagen till dess grad av oberoende, inte skulle ha ansetts betraktas som ett medelstort företag eller överstiga dessa trösklar om bara dess egna data hade tagits i beaktande. Detta påverkar inte skyldigheterna enligt detta direktiv för partnerföretag och anknutna företag som omfattas av direktivets tillämpningsområde.

(17) Medlemsstaterna bör kunna besluta att entiteter som före detta direktivs ikraftträdande har identifierats som leverantörer av samhällsviktiga tjänster i enlighet med direktiv (EU) 2016/1148 ska betraktas som väsentliga entiteter.

([7]) Europaparlamentets och rådets direktiv 97/67/EG av den 15 december 1997 om gemensamma regler för utvecklingen av gemenskapens inre marknad för posttjänster och för förbättring av kvaliteten på tjänsterna (EGT L 15, 21.1.1998, s. 14).

([8]) 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).

([9]) 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) (EGT L 201, 31.7.2002, s. 37).

(18) För att skapa en tydlig överblick över entiteter som omfattas av detta direktivs tillämpningsområde bör medlemsstaterna upprätta en förteckning över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster. I detta syfte bör medlemsstaterna ålägga entiteter att till de behöriga myndigheterna lämna åtminstone följande information: namn, adress och aktuella kontaktuppgifter, inklusive entitetens e-postadresser, IP-adressintervall och telefonnummer, och i tillämpliga fall den relevanta sektor och delsektor som avses i de bilagorna samt i tillämpliga fall en förteckning över de medlemsstater där de tillhandahåller tjänster som omfattas av detta direktivs tillämpningsområde. I detta syfte bör kommissionen, med bistånd från Europeiska unionens cybersäkerhetsbyrå (Enisa), utan onödigt dröjsmål tillhandahålla riktlinjer och mallar avseende skyldigheten att lämna information. I syfte att underlätta upprättandet och uppdateringen av förteckningen över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster bör medlemsstaterna kunna fastställa nationella mekanismer för att entiteter ska kunna registrera sig själva. Om det finns register på nationell nivå kan medlemsstaterna besluta om lämpliga mekanismer som gör det möjligt att identifiera entiteter som omfattas av detta direktiv.

(19) Medlemsstaterna bör ansvara för att förse kommissionen åtminstone med uppgifter om antalet väsentliga och viktiga entiteter för varje sektor och delsektor enligt bilagorna samt relevant information om antalet identifierade entiteter och den bestämmelse i detta direktiv på vars grundval dessa identifierats, och den typ av tjänster de tillhandahåller. Medlemsstaterna uppmuntras att utbyta information med kommissionen om väsentliga och viktiga entiteter och, i händelse av en storskalig cybersäkerhetsincident, relevant information såsom den berörda entitetens namn.

(20) Kommissionen bör, i samarbete med samarbetsgruppen och efter samråd med relevanta intressenter, tillhandahålla riktlinjer om genomförandet av de kriterier som ska tillämpas på mikroföretag och små företag för att bedöma om de omfattas av detta direktiv. Kommissionen bör även säkerställa att mikroföretag och små företag som omfattas av detta direktiv får lämplig vägledning. Kommissionen bör, med bistånd från medlemsstaterna, göra information tillgänglig för mikroföretag och små företag i detta avseende.

(21) Kommissionen kan tillhandahålla vägledning för att bistå medlemsstaterna med att genomföra bestämmelserna i detta direktiv om tillämpningsområde och med att utvärdera proportionaliteten i de åtgärder som ska vidtas i enlighet med direktivet, särskilt vad gäller entiteter med komplexa affärsmodeller eller driftsmiljöer, varvid en entitet samtidigt kan uppfylla kriterierna för både väsentliga och viktiga entiteter eller samtidigt kan bedriva viss verksamhet som omfattas av, och viss verksamhet som är undantagen från, detta direktiv.

(22) I detta direktiv fastställs referensscenariot för riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter i alla sektorer som omfattas av dess tillämpningsområde. För att undvika fragmentering av cybersäkerhetsbestämmelserna i unionsrättsakter bör kommissionen, när ytterligare sektorsspecifika unionsrättsakter om riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter anses nödvändiga för att säkerställa en hög cybersäkerhetsnivå i hela unionen, bedöma om sådana ytterligare bestämmelser kan fastställas i en genomförandeakt inom ramen för detta direktiv. Om en sådan genomförandeakt inte är lämplig för detta ändamål skulle sektorsspecifika unionsrättsakter kunna bidra till att säkerställa en hög cybersäkerhetsnivå i hela unionen, samtidigt som de berörda sektorernas särdrag och komplexitet beaktas fullt ut. Därför hindrar detta direktiv inte antagandet av ytterligare sektorsspecifika unionsrättsakter innehållande riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter som tar vederbörlig hänsyn till behovet av en övergripande och konsekvent cybersäkerhetsram. Detta direktiv påverkar inte de befintliga genomförandebefogenheter som har tilldelats kommissionen med avseende på ett antal sektorer, däribland transport och energi.

(23) Om en sektorsspecifik unionsrättsakt innehåller bestämmelser som föreskriver att väsentliga eller viktiga entiteter ska anta riskhanteringsåtgärder för cybersäkerhet eller anmäla betydande incidenter, och om dessa krav har minst samma verkan som de skyldigheter som fastställs i detta direktiv, bör de bestämmelserna, inbegripet om tillsyn och

efterlevnadskontroll, tillämpas på sådana entiteter. Om en sektorsspecifik unionsrättsakt inte omfattar alla entiteter inom en viss sektor som omfattas av detta direktivs tillämpningsområde bör de relevanta bestämmelserna i detta direktiv fortsätta att tillämpas på de entiteter som inte omfattas av den rättsakten.

(24) Om bestämmelserna i en sektorsspecifik unionsrättsakt föreskriver att väsentliga eller viktiga entiteter ska uppfylla rapporteringskrav som har minst samma verkan som rapporteringsskyldigheterna enligt detta direktiv bör samstämdhet och ändamålsenlighet säkerställas vid hanteringen av incidentanmälningar. I detta syfte bör den sektorsspecifika unionsrättsaktens bestämmelser om incidentanmälan föreskriva att CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna för cybersäkerhet (de gemensamma kontaktpunkterna) enligt detta direktiv ska ha omedelbar tillgång till de incidentanmälningar som lämnats in i enlighet med den sektorsspecifika unionsrättsakten. I synnerhet kan sådan omedelbar tillgång säkerställas om incidentanmälningar vidarebefordras utan onödigt dröjsmål till CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten enligt detta direktiv. När det är lämpligt bör medlemsstaterna införa en automatisk och direkt rapporteringsmekanism som säkerställer systematisk och omedelbar informationsdelning med CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna angående hanteringen av sådana incidentanmälningar. I syfte att förenkla rapporteringen och genomföra den automatiska och direkta rapporteringsmekanismen kan medlemsstaterna, i enlighet med den sektorsspecifika unionsrättsakten, använda en gemensam kontaktpunkt.

(25) Sektorsspecifika unionsrättsakter som föreskriver riskhanteringsåtgärder för cybersäkerhet eller rapporteringsskyldigheter som minst har samma verkan som de som fastställs i detta direktiv kan föreskriva att behöriga myndigheter inom ramen för de rättsakterna utövar sina tillsyns- och efterlevnadskontrollbefogenheter avseende sådana åtgärder eller skyldigheter med bistånd av de behöriga myndigheterna enligt detta direktiv. De berörda behöriga myndigheterna kan upprätta samarbetsarrangemang för detta ändamål. Sådana samarbetsarrangemang kan bland annat specificera förfarandena för samordning av tillsynsverksamheten, inbegripet förfarandena för utredningar och för inspektioner på plats i enlighet med nationell rätt och en mekanism för utbyte av relevant information om tillsyn och efterlevnadskontroll mellan de behöriga myndigheterna, inklusive tillgång till cyberrelaterad information som begärts av de behöriga myndigheterna enligt detta direktiv.

(26) Om sektorsspecifika unionsrättsakter innehåller skyldigheter eller incitament för entiteter att anmäla betydande cyberhot bör medlemsstaterna även uppmuntra till informationsdelning om betydande cyberhot med CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna enligt detta direktiv för att öka dessa organs medvetenhet om cyberhotbilden och göra det möjligt för dem att reagera ändamålsenligt och i lämplig tid om de betydande cyberhoten skulle bli verklighet.

(27) Framtida sektorsspecifika unionsrättsakter bör ta vederbörlig hänsyn till de definitioner och den ram för tillsyn och efterlevnadskontroll som fastställs i detta direktiv.

(28) Europaparlamentets och rådets förordning (EU) 2022/2554 ([10]) bör betraktas som en sektorsspecifik unionsrättsakt vid tillämpning av detta direktiv med avseende på finansiella entiteter. Bestämmelserna i förordning (EU) 2022/2554 avseende riskhanteringsåtgärder för informations- och kommunikationsteknik (IKT), hantering av IKT-relaterade incidenter, särskilt rapportering om större IKT-relaterade incidenter, samt avseende testning av digital operativ motståndskraft, arrangemang för informationsutbyte och IKT-tredjepartsrisk bör tillämpas i stället för dem som fastställs i detta direktiv. Medlemsstaterna bör därför inte tillämpa detta direktivs bestämmelser om riskhanterings- och rapporteringsskyldigheter beträffande cybersäkerhet och om tillsyn och efterlevnadskontroll på finansiella entiteter som omfattas av förordning (EU) 2022/2554. Det är samtidigt viktigt att upprätthålla starka förbindelser och informationsutbyte med finanssektorn inom ramen för detta direktiv. Därför gör förordning (EU) 2022/2554 det möjligt för de europeiska tillsynsmyndigheterna och de behöriga myndigheterna enligt den förordningen att delta i samarbetsgruppens verksamhet och att utbyta information och samarbeta med de gemensamma kontaktpunkterna och med CSIRT-enheterna och de behöriga myndigheterna enligt detta direktiv. De behöriga myndigheterna enligt förordning (EU) 2022/2554[++] bör även översända uppgifter om större IKT-relaterade incidenter och, i förekommande fall, betydande cyberhot till CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna enligt detta direktiv. Detta kan ske genom att ge omedelbar tillgång till incidentan-

([10]) 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 (se sidan 1 i detta nummer av EUT).

mälningar, och antingen vidarebefordra dem direkt eller genom en gemensam kontaktpunkt. Vidare bör medlemsstaterna fortsätta att inkludera finanssektorn i sina strategier för cybersäkerhet, och CSIRT-enheterna kan inbegripa finanssektorn i sin verksamhet.

(29) För att undvika luckor eller överlappning mellan de cybersäkerhetsskyldigheter som åläggs entiteter inom luftfartssektorn bör de nationella myndigheterna enligt Europaparlamentets och rådets förordningar (EG) nr 300/2008 ([11]) och (EU) 2018/1139 ([12]) och de behöriga myndigheterna enligt detta direktiv samarbeta när det gäller genomförandet av riskhanteringsåtgärder för cybersäkerhet och tillsynen av efterlevnaden av de åtgärderna på nationell nivå. En entitets efterlevnad av de säkerhetskrav som fastställs i förordningarna (EG) nr 300/2008 och (EU) 2018/1139 och i relevanta delegerade akter och genomförandeakter som antagits i enlighet med de förordningarna kan av de behöriga myndigheterna enligt detta direktiv anses utgöra efterlevnad av motsvarande krav som fastställs i detta direktiv.

(30) Med tanke på kopplingarna mellan cybersäkerhet och entiteters fysiska säkerhet bör man säkerställa samstämmighet mellan Europaparlamentets och rådets direktiv (EU) 2022/2557 ([13]) och det här direktivet. För att uppnå detta bör entiteter som identifieras som kritiska entiteter enligt direktiv (EU) 2022/2557 anses vara väsentliga entiteter enligt det här direktivet. Vidare bör varje medlemsstat säkerställa att dess nationella strategi för cybersäkerhet tillhandahåller en politisk ram för ökad samordning inom den medlemsstaten mellan dess behöriga myndigheter enligt detta direktiv och de behöriga myndigheterna enligt direktiv (EU) 2022/2557 när det gäller informationsutbyte om risker, cyberhot och incidenter, liksom om icke-cyberrelaterade risker, hot och incidenter, samt utövande av tillsynsuppgifter. De behöriga myndigheterna enligt det här direktivet och direktiv (EU) 2022/2557 bör samarbeta och utbyta information utan onödigt dröjsmål, särskilt när det gäller identifiering av kritiska entiteter, risker, cyberhot och incidenter samt när det gäller icke-cyberrelaterade risker, hot och incidenter som påverkar kritiska entiteter, inbegripet cybersäkerhetsåtgärder och fysiska åtgärder som vidtas av kritiska entiteter samt resultaten av den tillsynsverksamhet som bedrivs med avseende på sådana entiteter.

För att effektivisera tillsynsverksamheten mellan de behöriga myndigheterna enligt det här direktivet och direktiv (EU) 2022/2557 och för att minimera den administrativa bördan för de berörda entiteterna bör de behöriga myndigheterna dessutom sträva efter att harmonisera mallarna för incidentanmälningar och tillsynsförfaranden. När så är lämpligt bör behöriga myndigheter enligt direktiv (EU) 2022/2557 kunna begära att behöriga myndigheter enligt det här direktivet utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll gentemot en entitet som identifieras som en kritisk entitet enligt direktiv (EU) 2022/2557. Det här direktivet och direktiv (EU) 2022/2557 bör, om möjligt i realtid, samarbeta och utbyta information i detta syfte.

(31) Entiteter som tillhör sektorn för digital infrastruktur är i huvudsak baserade på nätverks- och informationssystem, och därför bör de skyldigheter som åläggs dessa entiteter genom det här direktivet på ett övergripande sätt omfatta den fysiska säkerheten i sådana system som en del av deras riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter. Eftersom dessa frågor omfattas av det här direktivet är de skyldigheter som fastställs i kapitlen III, IV och VI i direktiv (EU) 2022/2557 inte tillämpliga på sådana entiteter.

([11]) Europaparlamentets och rådets förordning (EG) nr 300/2008 av den 11 mars 2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002 (EUT L 97, 9.4.2008, s. 72).

([12]) 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).

([13]) 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 (se sidan 164 i detta nummer av EUT).

(32) Att upprätthålla och bevara ett tillförlitligt, resilient och säkert domännamnssystem (DNS) är viktiga faktorer för att upprätthålla internets integritet och är avgörande för en kontinuerlig och stabil drift, vilket den digitala ekonomin och samhället är beroende av. Därför bör detta direktiv vara tillämpligt på registreringsenheter för toppdomäner och leverantörer av DNS-tjänster, som bör förstås som entiteter som tillhandahåller allmänt tillgängliga rekursiva tjänster för att lösa domännamnsfrågor för internetslutanvändare eller auktoritativa tjänster för att lösa domännamnsfrågor för tredjepartsanvändning. Detta direktiv bör inte vara tillämpligt på rotnamnsservrar.

(33) Molntjänster bör omfatta digitala tjänster som möjliggör administration av beställtjänster och bred fjärråtkomst till en skalbar och elastisk pool av delbara och distribuerade dataresurser, även när sådana resurser är distribuerade på flera platser. Beräkningsresurser omfattar resurser såsom nätverk, servrar eller annan infrastruktur, operativsystem, programvara, lagring, applikationer och tjänster. Tjänstemodellerna för molntjänster omfattar bland annat infrastruktur som en tjänst, plattform som en tjänst, program som en tjänst och nätverk som en tjänst. Distribueringsmodellerna för molntjänster bör omfatta privat moln, gemensamt moln, offentligt moln och hybridmoln. Molntjänste- och distribueringsmodellerna har samma innebörd som termerna tjänste- och distribueringsmodeller som definieras i standarden ISO/IEC 17788:2014. Molnanvändarens kapacitet att ensidigt, självständigt tillhandahålla datorkapacitet, såsom servertid eller nätlagring, utan någon mänsklig medverkan från leverantören av molntjänster, kan beskrivas som beställtjänster.

Termen *bred fjärråtkomst* används för att beskriva att molnkapaciteten tillhandahålls över nätet och nås genom mekanismer som främjar användning av heterogena tunna eller tjocka klientplattformar, däribland mobiltelefoner, surfplattor, bärbara datorer och arbetsstationer. Termen *skalbar* avser beräkningsresurser som leverantören av molntjänster fördelar på ett flexibelt sätt, oberoende av resursernas geografiska läge, för att hantera fluktuationer i efterfrågan. Termen *elastisk pool* används för att beskriva beräkningsresurser som tillhandahålls och utnyttjas beroende på efterfrågan för att tillgängliga resurser snabbt ska kunna utökas och minskas i takt med arbetsbördan. Termen *delbar* används för att beskriva beräkningsresurser som tillhandahålls flera användare som delar en gemensam åtkomst till tjänsten där behandlingen genomförs separat för varje användare, även om tjänsten tillhandahålls från samma elektroniska utrustning. Termen *distribuerad* används för att beskriva beräkningsresurser som finns på olika nätverksanslutna datorer eller enheter och som kommunicerar och samordnar sig sinsemellan genom meddelandepassning.

(34) Med tanke på framväxten av innovativ teknik och nya affärsmodeller förväntas nya molntjänste- och distribueringsmodeller uppstå på den inre marknaden som svar på kundernas föränderliga behov. I detta sammanhang kan molntjänster levereras i en mycket distribuerad form, ännu närmare den plats där data genereras eller samlas in, och därmed övergå från den traditionella modellen till en mycket distribuerad modell (*edge computing*).

(35) Tjänster som erbjuds av leverantörer av datacentraltjänster tillhandahålls inte alltid i form av molntjänster. Därför ingår inte datacentraler alltid i en molninfrastruktur. För att hantera alla risker för säkerheten i nätverks- och informationssystem bör detta direktiv därför omfatta leverantörer av datacentraltjänster som inte är molntjänster. Vid tillämpningen av detta direktiv bör termen *datacentraltjänst* omfatta strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och datatransporttjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll. Termen *datacentraltjänst* bör inte vara tillämplig på interna datacentraler som ägs och drivs av den berörda entiteten för egen räkning.

(36) Forskningsverksamhet spelar en nyckelroll i utvecklingen av nya produkter och processer. Mycket av den verksamheten genomförs av entiteter som delar, sprider eller utnyttjar resultaten av sin forskning i kommersiella syften. Dessa entiteter kan därför vara viktiga aktörer i värdekedjor, vilket gör säkerheten i deras nätverks- och informationssystem till en integrerad del av den övergripande cybersäkerheten på den inre marknaden. Forskningsorganisationer bör anses inbegripa entiteter som riktar in större delen av sin verksamhet på tillämpad forskning eller experimentell utveckling i den mening som avses i "Frascatimanualen 2015: Riktlinjer för insamling och

rapportering av uppgifter om forskning och experimentell utveckling" från Organisationen för ekonomiskt samarbete och utveckling, i syfte att utnyttja sina resultat i kommersiella syften, såsom tillverkning eller utveckling av en produkt eller process, tillhandahållande av en tjänst, eller marknadsföring därav.

(37) De växande ömsesidiga beroendeförhållandena är resultatet av ett allt mer gränsöverskridande nätverk av tillhandahållande av tjänster, med ett inbördes beroende, som använder central infrastruktur över hela unionen inom sektorer såsom energi, transport, digital infrastruktur, dricks- och avloppsvatten, hälso- och sjukvård, vissa aspekter av offentlig förvaltning, samt rymden i den mån tillhandahållandet av vissa tjänster som är beroende av markbaserad infrastruktur som ägs, förvaltas och drivs av medlemsstater eller privata parter berörs; därför omfattas inte infrastruktur som ägs, förvaltas eller drivs av unionen eller på unionens vägnar som en del av dess rymdprogram. Dessa beroendeförhållanden innebär att alla störningar, även sådana som inledningsvis är begränsade till en entitet eller sektor, kan få dominoeffekter i vidare bemärkelse, vilket kan leda till långtgående och långvariga effekter på tillhandahållandet av tjänster på hela den inre marknaden. De intensifierade cyberattackerna under covid-19-pandemin har visat sårbarheten hos alltmer av varandra beroende samhällena är för risker med låg sannolikhet.

(38) Mot bakgrund av skillnaderna i nationella förvaltningsstrukturer, och för att skydda befintliga sektorsspecifika arrangemang eller unionens tillsyns- och regleringsorgan, bör medlemsstaterna kunna utse eller inrätta en eller flera behöriga myndigheter med ansvar för cybersäkerhet och för tillsynsuppgifterna enligt detta direktiv.

(39) För att underlätta gränsöverskridande samarbete och kommunikation mellan myndigheter och för att göra det möjligt att genomföra detta direktiv på ett effektivt sätt måste varje medlemsstat utse en gemensam kontaktpunkt med ansvar för samordningen av frågor angående säkerhet i nätverks- och informationssystem och gränsöverskridande samarbete på unionsnivå.

(40) De gemensamma kontaktpunkterna bör säkerställa effektivt gränsöverskridande samarbete med relevanta myndigheter i en annan medlemsstat och, när det är lämpligt, med kommissionen och Enisa. De gemensamma kontaktpunkterna bör därför ges i uppgift att vidarebefordra underrättelser om betydande incidenter med gränsöverskridande verkningar till de gemensamma kontaktpunkterna i andra berörda medlemsstater på begäran av CSIRT-enheten eller den behöriga myndigheten. På nationell nivå bör de gemensamma kontaktpunkterna möjliggöra smidigt sektorsövergripande samarbete med andra behöriga myndigheter. De gemensamma kontaktpunkterna kan också vara mottagare av relevant information om incidenter rörande finansiella entiteter från de behöriga myndigheterna enligt förordning (EU) 2022/2554, som de bör kunna vidarebefordra till CSIRT-enheterna eller de behöriga myndigheterna enligt detta direktiv, beroende på vad som är lämpligt.

(41) Medlemsstaterna bör ha både den tekniska och organisatoriska kapacitet som krävs för att förebygga, upptäcka, vidta åtgärder mot och begränsa incidenter och risker. Medlemsstaterna bör därför inrätta eller utse en eller flera CSIRT-enheter enligt detta direktiv och säkerställa att de har tillräckligt med resurser och teknisk kapacitet. CSIRT-enheterna bör uppfylla kraven enligt detta direktiv i syfte att garantera effektiv och kompatibel kapacitet att hantera incidenter och risker och säkerställa ett effektivt samarbete på unionsnivå. Medlemsstaterna bör kunna utse befintliga incidenthanteringsorganisationer (Cert) till CSIRT-enheter. För att stärka förtroendeförhållandet mellan entiteterna och CSIRT-enheterna bör medlemsstaterna, när en CSIRT-enhet är en del av de behörig myndighet, kunna överväga funktionell åtskillnad mellan de operativa uppgifter som utförs av CSIRT-enheterna, särskilt när det gäller informationsutbyte och bistånd till entiteterna, och de behöriga myndigheternas tillsynsverksamhet.

(42) CSIRT-enheterna ansvarar för incidenthantering. Detta omfattar behandling av stora mängder ibland känsliga uppgifter. Medlemsstaterna bör säkerställa att CSIRT-enheterna har en infrastruktur för utbyte och behandling av information, samt väl rustad personal, som säkerställer verksamhetens konfidentialitet och trovärdighet. CSIRT-enheterna kan även anta uppförandekoder i detta avseende.

(43) Vad gäller personuppgifter bör CSIRT-enheterna, i enlighet med förordning (EU) 2016/679, på begäran av en väsentlig eller viktig entitet tillhandahålla en proaktiv skanning av de nätverks- och informationssystem som används för att tillhandahålla entitetens tjänster. När det är tillämpligt bör medlemsstaterna sträva efter att säkerställa en lika hög nivå av teknisk kapacitet hos alla sektorsspecifika CSIRT-enheter. Medlemsstaterna bör kunna begära Enisas bistånd vid inrättandet av sina CSIRT-enheter.

(44) CSIRT-enheter bör ha förmåga att, på en väsentlig eller viktig entitets begäran, övervaka entitetens internettillvända tillgångar, både inom och utanför lokalerna, för att identifiera, förstå och hantera entitetens övergripande organisatoriska risker med avseende på nyligen identifierade kompromisser i leveranskedjan eller kritiska sårbarheter. Entiteten bör uppmuntras att meddela CSIRT-enheten om den har ett privilegierat hanteringsgränssnitt, då detta kan påverka hur snabbt begränsningsåtgärder kan vidtas.

(45) Med tanke på vikten av internationellt samarbete på området cybersäkerhet bör CSIRT-enheterna kunna delta i internationella samarbetsnätverk utöver det CSIRT-nätverk som inrättas genom detta direktiv. För att utföra sina uppgifter bör CSIRT-enheterna och de behöriga myndigheterna därför kunna utbyta information, inklusive personuppgifter, med de nationella enheterna för hantering av it-säkerhetsincidenter eller behöriga myndigheter i tredjeländer, förutsatt att villkoren i unionens dataskyddslagstiftning för överföring av personuppgifter till tredjeländer är uppfyllda, bland annat villkoren i artikel 49 i förordning (EU) 2016/679.

(46) Det är angeläget att säkerställa tillräckliga resurser för att uppnå målen för detta direktiv och göra det möjligt för de behöriga myndigheterna och CSIRT-enheterna att utföra de uppgifter som fastställs i detta direktiv. Medlemsstaterna kan på nationell nivå införa en finansieringsmekanism för att täcka de nödvändiga utgifterna i samband med att offentliga entiteter med ansvar för cybersäkerheten i medlemsstaterna utför sina uppgifter i enlighet med detta direktiv. En sådan mekanism bör vara förenlig med unionsrätten samt proportionell och icke-diskriminerande och bör beakta olika tillvägagångssätt för att tillhandahålla säkra tjänster.

(47) CSIRT-nätverket bör fortsätta att bidra till att stärka förtroendet och tilliten och främja snabbt och effektivt operativt samarbete mellan medlemsstaterna. För att stärka det operativa samarbetet på unionsnivå bör CSIRT-nätverket överväga att bjuda in unionsorgan och -byråer som arbetar med frågor som rör cybersäkerhetspolitiken, såsom Europol, att delta i dess arbete.

(48) För att uppnå och behålla en hög cybersäkerhetsnivå bör de nationella strategier för cybersäkerhet som krävs enligt detta direktiv bestå av enhetliga ramar med strategiska mål och prioriteringar på cybersäkerhetsområdet samt en styrningsram för att uppnå dem. Dessa strategier kan bestå av ett eller flera instrument av lagstiftningskaraktär eller annan karaktär.

(49) Riktlinjer för cyberhygien utgör grunden för att skydda nätverks- och informationssystemens infrastruktur, maskinvara, programvara och säkerhet för onlinetillämpningar samt affärs- eller slutanvändardata som entiteter förlitar sig på. Riktlinjer för cyberhygien som omfattar en gemensam grundläggande uppsättning rutiner, bland annat uppdateringar av programvara och maskinvara, byte av lösenord, hantering av nya installationer, begränsning av användarkonton på administratörsnivå och säkerhetskopiering av data, möjliggör en proaktiv ram för beredskap samt övergripande säkerhet och trygghet i händelse av incidenter eller cyberhot. Enisa bör övervaka och analysera medlemsstaternas riktlinjer för cyberhygien.

(50) Medvetenhet om cybersäkerhet och cyberhygien är av väsentlig betydelse för att stärka cybersäkerheten inom unionen, särskilt mot bakgrund av det ökande antalet uppkopplade enheter som i tilltagande grad används vid cyberattacker. Ansträngningar bör göras för att öka den allmänna medvetenheten om risker kopplade till sådana enheter, samtidigt som bedömningar på unionsnivå kan bidra till att säkerställa samsyn i fråga om sådana risker på den inre marknaden.

(51) Medlemsstaterna bör uppmuntra användningen av all innovativ teknik, däribland artificiell intelligens, som kan förbättra upptäckten och förebyggandet av cyberattacker och göra det möjligt att styra över resurser till cyberattacker på ett effektivare sätt. Medlemsstaterna bör därför i sin nationella strategi för cybersäkerhet uppmuntra forsknings- och utvecklingsverksamhet för att underlätta användningen av sådan teknik, särskilt sådan som avser automatiserade eller halvautomatiserade cybersäkerhetsverktyg, och i förekommande fall utbyte av data som behövs för att utbilda användarna av sådan teknik och förbättra den. Användningen av innovativ teknik, däribland artificiell intelligens, bör vara förenlig med unionens dataskyddslagstiftning, däribland dataskyddsprinciperna om uppgifternas korrekthet, uppgiftsminimering, rättvisa och transparens samt datasäkerhet, såsom avancerad krypteringsteknik. Kraven på inbyggt dataskydd och dataskydd som standard enligt förordning (EU) 2016/679 bör utnyttjas till fullo.

(52) Cybersäkerhetsverktyg och applikationer med öppen källkod kan bidra till en högre grad av öppenhet och inverka positivt på effektiviteten i industriell innovation. Öppna standarder främjar interoperabilitet mellan säkerhetsverktyg, vilket gynnar säkerheten för berörda parter inom industrin. Cybersäkerhetsverktyg och applikationer med öppen källkod kan dra nytta av utvecklargemenskapen i stort och möjliggöra diversifiering av leverantörer. Öppen källkod kan leda till en mer transparent verifieringsprocess för cybersäkerhetsrelaterade verktyg och till en gemenskapsdriven process för att upptäcka sårbarheter. Medlemsstaterna bör därför kunna främja användningen av programvara med öppen källkod och öppna standarder genom att tillämpa riktlinjer för användning av öppna data och öppen källkod som ett led i säkerhet genom transparens. Riktlinjer som främjar införande och hållbar användning av cybersäkerhetsverktyg med öppen källkod är särskilt viktig för små och medelstora företag som har stora genomförandekostnader som kan minimeras om behovet av specifika applikationer eller verktyg minskades.

(53) Allmännyttiga tjänster är alltmer uppkopplade mot digitala nätverk i städer i syfte att förbättra städernas transportnät, uppgradera anläggningar för vattenförsörjning och avfallshantering och effektivisera belysning och uppvärmning i byggnader. Dessa digitaliserade allmännyttiga tjänster är sårbara för cyberattacker och riskerar i händelse av en lyckad cyberattack att vålla medborgarna omfattande skada på grund av att de är sammankopplade. Medlemsstaterna bör, som ett led i sin nationella strategi för cybersäkerhet, ta fram riktlinjer som hanterar utvecklingen av sådana sammankopplade eller smarta städer, och deras potentiella inverkan på samhället.

(54) På senare år har unionen upplevt en exponentiell ökning av attacker genom utpressningsprogram där sabotageprogram krypterar data och system och kräver en lösensumma för att låsa upp dem. Att attacker genom utpressningsprogram blir vanligare och allvarligare kan bero på flera faktorer, såsom olika attackmönster, kriminella affärsmodeller som kretsar kring ”utpressningsprogram som service” och kryptovalutor, krav på lösensumma och ökat antal attacker i leveranskedjan. Medlemsstaterna bör ta fram riktlinjer för att hantera det ökande antalet utpressningsattacker som ett led i sin nationella strategi för cybersäkerhet.

(55) Offentlig-privata partnerskap inom cybersäkerhet kan utgöra en lämplig ram för kunskapsutbyte, utbyte av bästa praxis och utveckling av samsyn bland berörda parter. Medlemsstaterna bör främja riktlinjer som stöder inrättande av cybersäkerhetsspecifika offentlig-privata partnerskap. Sådana riktlinjer bör bland annat klargöra tillämpningsområdet och de berörda aktörerna, styrningsmodellen, de tillgängliga finansieringsalternativen och samspelet mellan deltagande aktörer i samband med offentlig-privata partnerskap. Offentlig-privata partnerskap kan dra nytta av expertisen hos privata entiteter för att bistå behöriga myndigheter vid utvecklingen av avancerade tjänster och processer med informationsutbyte, tidiga varningar, cyberhots- och incidentövningar, krishantering och resiliensplanering.

(56) Medlemsstaterna bör i sina nationella strategier för cybersäkerhet ta itu med små och medelstora företags särskilda cybersäkerhetsbehov. Små och medelstora företag står, i hela unionen, för en stor andel av industri- och affärsmarknaden och har ofta svårt att anpassa sig till nya affärsmetoder i en mer uppkopplad värld, och till den digitala miljön, med anställda som arbetar hemifrån och en verksamhet som i allt högre grad bedrivs online. Vissa små och medelstora företag upplever särskilda cybersäkerhetsutmaningar, såsom låg cybermedvetenhet, bristande it-säkerhet på distans, höga kostnader för cybersäkerhetslösningar och en förhöjd hotnivå, t.ex. genom utpressningsprogram, och bör för detta få vägledning och bistånd. Små och medelstora företag blir i allt högre grad måltavlor för attacker i leveranskedjan på grund av att de har mindre strikta åtgärder för hantering av cybersäkerhetsrisker och attacker och på grund av det faktum att de har begränsade säkerhetsresurser. Sådana attacker i leveranskedjan påverkar inte bara små och medelstora företag och deras verksamhet isolerat utan kan också få en dominoeffekt i fråga om större attacker mot entiteter som de levererat till. Medlemsstaterna bör genom sina nationella strategier för cybersäkerhet hjälpa små och medelstora företag att ta itu med utmaningarna i sina

leveranskedjor. Medlemsstaterna bör ha en kontaktpunkt för små och medelstora företag på nationell eller regional nivå som antingen ger vägledning och bistånd till små och medelstora företag eller hänvisar dem till lämpliga organ för vägledning och bistånd i cybersäkerhetsrelaterade frågor. Medlemsstaterna uppmanas även att erbjuda tjänster såsom konfiguration av webbplatser och möjliggörande av loggning för mikroföretag och små företag som saknar sådan kapacitet.

(57) Inom ramen för sina nationella strategier för cybersäkerhet bör medlemsstaterna anta riktlinjer för främjande av ett aktivt cyberskydd som ett led i en vidare försvarsstrategi. I stället för reaktiva insatser innebär ett aktivt cyberskydd förebyggande, upptäckt, övervakning, analys och begränsning av överträdelser av nätverkssäkerheten, i kombination med användning av kapacitet som satts in inom och utanför det angripna nätverket. Detta kan bland annat innebära att medlemsstaterna erbjuder vissa entiteter kostnadsfria tjänster eller verktyg, t.ex. självbetjäningskontroller, upptäcktsverktyg och borttagningstjänster. Förmågan att snabbt och automatiskt utbyta och förstå information om och analyser av hot, varningar om cyberverksamhet samt motåtgärder är avgörande för att med förenade ansträngningar lyckas förebygga, upptäcka, hantera och blockera attacker mot nätverks- och informationssystem. Ett aktivt cyberskydd bygger på en defensiv strategi som utesluter offensiva åtgärder.

(58) Eftersom utnyttjandet av sårbarheter i nätverks- och informationssystem kan orsaka betydande störningar och skada, är snabb identifiering och snabbt åtgärdande av sådana sårbarheter en viktig faktor för att minska risken. Entiteter som utvecklar eller administrerar nätverks- och informationssystem bör därför inrätta lämpliga förfaranden för att hantera sårbarheter när de upptäcks. Eftersom sårbarheter ofta upptäcks och meddelas av tredjeparter, bör tillverkaren eller leverantören av IKT-produkter eller IKT-tjänster även införa nödvändiga förfaranden för att motta sårbarhetsinformation från tredjeparter. I detta avseende ger de internationella standarderna ISO/IEC 30111 och ISO/IEC 29147 vägledning om sårbarhetshantering och om delgivning av information om sårbarheter. En stärkt samordning mellan rapporterande fysiska och juridiska personer och tillverkare eller leverantörer av IKT-produkter eller IKT-tjänster är särskilt viktig för att underlätta den frivilliga ramen för delgivning av information om sårbarheter. Samordnad delgivning av information om sårbarheter specificerar en strukturerad process genom vilken sårbarheter rapporteras till tillverkaren eller leverantören av de potentiellt sårbara IKT-produkterna eller IKT-tjänsterna på ett sätt som gör det möjligt för denne att diagnostisera och åtgärda sårbarheten innan detaljerad information om sårbarheten meddelas tredjeparter eller allmänheten. Samordnad delgivning av information om sårbarheter bör även inbegripa samordning mellan den rapporterande fysiska eller juridiska personen och tillverkaren eller leverantören av de potentiellt sårbara IKT-produkterna eller IKT-tjänsterna vad gäller tidpunkten för åtgärdandet och offentliggörandet av sårbarheter.

(59) Kommissionen, Enisa och medlemsstaterna bör fortsätta att främja anpassningar till internationella standarder och befintlig bästa branschpraxis inom hantering av cybersäkerhetrisker, exempelvis inom säkerhetsbedömningar i leveranskedjan, informationsutbyte och delgivning av information om sårbarheter.

(60) Medlemsstaterna bör, i samarbete med Enisa, vidta åtgärder för att underlätta samordnad delgivning av information om sårbarheter genom att fastställa en relevant nationell policy. Som ett led i den nationella policyn bör medlemsstaterna 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 kan riskera straff- och civilrättsligt ansvar i vissa medlemsstater uppmuntras medlemsstaterna att anta riktlinjer för icke-lagföring av forskare i informationssäkerhet och befrielse från civilrättsligt ansvar för deras verksamhet.

(61) Medlemsstaterna bör utse en av sina CSIRT-enheter till samordnare, som bör fungera som betrodd mellanhand mellan rapporterande fysiska eller juridiska personer och tillverkare eller leverantörer av IKT-produkter eller IKT-tjänster som sannolikt kommer att påverkas av sårbarheten, när detta är nödvändigt. Den CSIRT-enhet som utsetts till samordnare bör bland annat ha i uppgift att identifiera och kontakta de berörda entiteterna, bistå de fysiska eller juridiska personer som rapporterar en sårbarhet, förhandla om tidsfrister för delgivning av information och hantera

sårbarheter som påverkar flera entiteter (samordnad delgivning av information om sårbarheter omfattande flera parter). Om den rapporterade sårbarheten kan ha en betydande påverkan på entiteter i fler än en medlemsstat bör de CSIRT-enheter som utsetts till samordnare samarbeta inom CSIRT-nätverket när så är lämpligt.

(62) Tillträde till korrekt information i lämplig tid om sårbarheter som påverkar IKT-produkter och IKT-tjänster bidrar till en förbättrad riskhantering på cybersäkerhetsområdet. Källor till offentligt tillgänglig information om sårbarheter är ett viktigt verktyg för entiteterna och användarna av deras tjänster, men även för behöriga myndigheter och CSIRT-enheter. Av denna anledning bör Enisa upprätta en europeisk sårbarhetsdatabas där entiteter, oberoende av om de omfattas av tillämpningsområdet för detta direktiv, och deras leverantörer av nätverks- och informationssystem, samt de behöriga myndigheterna och CSIRT-enheterna på frivillig basis kan meddela information om och registrera allmänt kända sårbarheter för att möjliggöra för användarna att vidta lämpliga riskreducerande åtgärder. Syftet med databasen är att hantera de unika utmaningar som risker innebär för entiteter i unionen. Vidare bör Enisa inrätta ett lämpligt förfarande för offentliggörandet för att ge entiteterna tid att vidta riskreducerande åtgärder när det gäller deras sårbarheter och använda avancerade riskhanteringsåtgärder på cybersäkerhetsområdet samt maskinläsbara dataset och motsvarande gränssnitt. För att uppmuntra en kultur där information lämnas om sårbarheter bör informationslämnande inte få negativa effekter för den rapporterande fysiska eller juridiska personen.

(63) Även om liknande sårbarhetsregister eller -databaser finns, förvaltas och underhålls de av entiteter som inte är etablerade i unionen. En europeisk sårbarhetsdatabas som underhålls av Enisa skulle ge förbättrad insyn i processen för offentliggörande innan sårbarheten meddelas offentligt samt motståndskraft i händelse av en störning eller ett avbrott i tillhandahållandet av liknande tjänster. För att i möjligaste mån undvika dubbelarbete och eftersträva komplementaritet bör Enisa undersöka möjligheten att ingå avtal om strukturerat samarbete med liknande register eller databaser som omfattas av ett tredjelands jurisdiktion. Enisa bör särskilt undersöka möjligheten till ett nära samarbete med operatörerna av systemet för gemensamma sårbarheter och exponeringar (*Common Vulnerabilities and Exposures* – CVE).

(64) Samarbetsgruppen bör stödja och underlätta strategiskt samarbete och informationsutbyte samt stärka förtroendet och tilliten mellan medlemsstaterna. Samarbetsgruppen bör upprätta ett arbetsprogram vartannat år. Arbetsprogrammet bör omfatta de åtgärder som samarbetsgruppen ska vidta för att genomföra sina mål och uppgifter. Tidsramen för att inrätta det första arbetsprogrammet enligt detta direktiv bör anpassas till tidsramen för det senaste arbetsprogram som inrättats enligt direktiv (EU) 2016/1148 i syfte att undvika potentiella avbrott i samarbetsgruppens arbete.

(65) Vid utarbetandet av vägledningsdokument bör samarbetsgruppen konsekvent kartlägga nationella lösningar och erfarenheter, bedöma hur samarbetsgruppens resultat påverkar nationella strategier, diskutera utmaningar i samband med genomförandet och formulera särskilda rekommendationer, särskilt om hur ett samordnat införlivande av direktivet kan underlättas bland medlemsstaterna, som bör beaktas genom ett bättre genomförande av befintliga bestämmelser. Samarbetsgruppen skulle även kunna kartlägga de nationella lösningarna för att främja kompatibiliteten mellan de cybersäkerhetslösningar som tillämpas inom varje specifik sektor i unionen. Detta är särskilt relevant för sektorer av internationell eller gränsöverskridande karaktär.

(66) Samarbetsgruppen bör förbli ett flexibelt forum och kunna reagera på föränderliga och nya politiska prioriteringar och utmaningar samtidigt som tillgången till resurser beaktas. Den kan anordna regelbundna gemensamma möten med relevanta privata intressenter från hela unionen för att diskutera samarbetsgruppens verksamhet och inhämta uppgifter och synpunkter avseende framväxande politiska frågor. Dessutom bör samarbetsgruppen göra en regelbunden bedömning av läget när det gäller cyberhot eller incidenter, såsom utpressningsprogram. För att stärka

samarbetet på unionsnivå bör samarbetsgruppen överväga att bjuda in relevanta unionsinstitutioner, -organ, -kontor och -byråer som arbetar med frågor som rör cybersäkerhetspolitiken, såsom Europaparlamentet, Europol, Europeiska dataskyddsstyrelsen, Europeiska unionens byrå för luftfartssäkerhet, som inrättats genom förordning (EU) 2018/1139, och Europeiska unionens rymdprogrambyrå, som inrättats genom Europaparlamentets och rådets förordning (EU) 2021/696 ([14]), att delta i dess arbete.

(67) De behöriga myndigheterna och CSIRT-enheterna bör kunna delta i utbytesprogram för tjänstemän från andra medlemsstater inom en särskild ram och, i tillämpliga fall, efter det erforderliga säkerhetsgodkännandet för tjänstemän som deltar i sådana utbytesprogram, i syfte att förbättra samarbetet och stärka tilliten mellan medlemsstaterna. De behöriga myndigheterna bör vidta nödvändiga åtgärder för att tjänstemän från andra medlemsstater ska kunna spela en faktisk roll i verksamheten inom den behöriga värdmyndigheten eller CSIRT-värdenheten.

(68) Medlemsstaterna bör bidra till inrättandet av en EU-ram för hantering av cyberkriser enligt kommissionens rekommendation (EU) 2017/1584 ([15]) genom de befintliga samarbetsnätverken, särskilt Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), CSIRT-nätverket och samarbetsgruppen. EU- CyCLONe och CSIRT-nätverket bör samarbeta på grundval av förfaranden som specificerar detaljerna för detta samarbete och undvika dubbelarbete. Arbetsordningen för EU-CyCLONe bör ytterligare specificera de arrangemang enligt vilka det nätverket ska fungera, däribland nätverkets roller, samarbetsformer, samverkan med andra relevanta aktörer och mallar för informationsutbyte, samt kommunikationsmedel. För krishantering på unionsnivå bör berörda parter stödja sig på EU-arrangemangen för integrerad politisk krishantering enligt rådets genomförandebeslut (EU) 2018/1993 ([16]) (IPCR-arrangemang). Kommissionen bör använda Argus-förfarandet för gränsöverskridande krissamordning på hög nivå för detta ändamål. Om krisen har en yttre dimension eller en dimension som rör den gemensamma säkerhets- och försvarspolitiken (GSFP) och denna dimension är betydande, bör Europeiska utrikestjänstens krishanteringsmekanism aktiveras.

(69) I enlighet med bilagan till rekommendation (EU) 2017/1584 bör en storskalig incident anses vara en cybersäkerhetsincident som orsakar störningar som är så omfattande att en medlemsstat inte kan hantera dem eller som har en betydande påverkan på minst två medlemsstater. Beroende på orsak och verkan kan storskaliga cybersäkerhetsincidenter eskalera och förvandlas till fullt utvecklade kriser som hindrar den inre marknaden från att fungera korrekt eller som allvarligt hotar den allmänna tryggheten och säkerheten för entiteter eller medborgare i flera medlemsstater eller i unionen som helhet. Med beaktande av sådana incidenters stora omfattning och, i de flesta fall, gränsöverskridande karaktär, bör medlemsstater och relevanta unionsinstitutioner, -organ, -kontor och -byråer samarbeta på teknisk, operativ och politisk nivå i syfte att på lämpligt sätt samordna insatserna i hela unionen.

(70) Storskaliga cybersäkerhetsincidenter och kriser på unionsnivå kräver samordnade åtgärder för att säkerställa snabba och effektiva insatser på grund av den höga graden av ömsesidigt beroende mellan sektorer och medlemsstater. Tillgången till cyberresilienta nätverks- och informationssystem och uppgifternas tillgänglighet, konfidentialitet och riktighet är av vital betydelse för unionens säkerhet och skyddet av dess medborgare, företag och institutioner mot incidenter och cyberhot och för att stärka människors och organisationers tilltro till unionens förmåga att främja och skydda en global, öppen, fri, stabil och säker cyberrymd som bygger på mänskliga rättigheter, grundläggande friheter, demokrati och rättsstatliga principer.

([14]) Europaparlamentets och rådets förordning (EU) 2021/696 av den 28 april 2021 om inrättande av unionens rymdprogram och Europeiska unionens rymdprogrambyrå och om upphävande av förordningarna (EU) nr 912/2010, (EU) nr 1285/2013 och (EU) nr 377/2014 och beslut nr 541/2014/EU (EUT L 170, 12.5.2021, s. 69).

([15]) Kommissionens rekommendation (EU) 2017/1584 av den 13 september 2017 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser (EUT L 239, 19.9.2017, s. 36).

([16]) Rådets genomförandebeslut (EU) 2018/1993 av den 11 december 2018 om EU-arrangemangen för integrerad politisk krishantering (EUT L 320, 17.12.2018, s. 28).

(71) EU-CyCLONe bör fungera som mellanhand mellan den tekniska och politiska nivån under storskaliga cybersäkerhetsincidenter och kriser och bör stärka samarbetet på operativ nivå och stödja beslutsfattandet på politisk nivå. I samarbete med kommissionen, och med beaktande av kommissionens behörighet inom krishantering, bör EU-CyCLONe ta fasta på CSIRT-nätverkets slutsatser och använda sin egen kapacitet för att göra en konsekvensanalys av storskaliga cybersäkerhetsincidenter och kriser.

(72) Cyberattacker är av en gränsöverskridande natur, och en betydande incident kan störa och skada kritisk informationsinfrastruktur som en välfungerande inre marknad är beroende av. Rekommendation (EU) 2017/1584 tar upp alla relevanta aktörers roller. Vidare är kommissionen inom ramen för unionens civilskyddsmekanism, som inrättats genom Europaparlamentets och rådets beslut nr 1313/2013/EU ([17]), ansvarig för allmänna beredskapsåtgärder, bland annat för att förvalta centrumet för samordning av katastrofberedskap och det gemensamma kommunikations- och informationssystemet för olyckor, upprätthålla och vidareutveckla situationsmedvetenhet och analyskapacitet samt upprätta och förvalta kapacitet att mobilisera och sända ut expertgrupper vid förfrågan om bistånd från en medlemsstat eller ett tredjeland. Kommissionen är även ansvarig för tillhandahållande av analytiska rapporter inför IPCR-arrangemang enligt genomförandebeslut (EU) 2018/1993, bland annat med avseende på situationsmedvetenhet och beredskap på cybersäkerhetsområdet, samt för situationsmedvetenhet och krishantering på områdena jordbruk, ogynnsamma väderförhållanden, kartläggning av och prognoser för konflikter, system för tidig varning vid naturkatastrofer, hälsokriser, övervakning av infektionssjukdomar, växtskydd, kemiska incidenter, livsmedels- och fodersäkerhet, djurhälsa, migration, tull, nukleära och radiologiska nödsituationer och energi.

(73) Unionen kan när det är lämpligt ingå internationella avtal, i enlighet med artikel 218 i EUF-fördraget, med tredjeländer eller internationella organisationer och därvid tillåta och organisera deras deltagande i särskild verksamhet inom samarbetsgruppen, CSIRT-nätverket och EU-CyCLONe. Sådana avtal bör säkerställa unionens intressen och ändamålsenligt skydd av uppgifter. Detta bör inte utesluta medlemsstaternas rätt att samarbeta med tredjeländer om hantering av sårbarheter och riskhantering på cybersäkerhetsområdet och därvid underlätta rapportering och allmänt informationsutbyte i enlighet med unionsrätten.

(74) För att underlätta ett effektivt genomförande av detta direktiv i fråga om bland annat hantering av sårbarheter, riskhanteringsåtgärder för cybersäkerhet, rapporteringsskyldigheter och arrangemang för informationsutbyte om cybersäkerhet kan medlemsstaterna samarbeta med tredjeländer och bedriva verksamhet som anses lämplig för detta ändamål, bland annat informationsutbyte om cyberhot, incidenter, sårbarheter, verktyg, metoder, taktik, tekniker och förfaranden, beredskap och övningar för cybersäkerhetskrishantering, utbildning, förtroendeskapande åtgärder och arrangemang för ett strukturerat informationsutbyte.

(75) Sakkunnigbedömningar bör införas i syfte att dra lärdom av delade erfarenheter, stärka det ömsesidiga förtroendet och uppnå en hög gemensam cybersäkerhetsnivå. Sakkunnigbedömningarna kan leda till värdefulla insikter och rekommendationer som kan stärka den övergripande cybersäkerhetskapaciteten, skapa ytterligare en funktionell väg för utbyte av bästa praxis mellan medlemsstater och bidra till att förbättra medlemsstaternas mognadsnivå inom cybersäkerhet. Vidare bör sakkunnigbedömningarna beakta resultaten av liknande mekanismer, såsom systemet för sakkunnigbedömning inom ramen för CSIRT-nätverket, samt tillföra mervärde och undvika dubbelarbete. Genomförandet av sakkunnigbedömningarna bör inte påverka tillämpningen av unionsrätt eller nationell rätt om skydd av konfidentiella eller säkerhetsskyddsklassificerade uppgifter.

(76) Samarbetsgruppen bör fastställa en självbedömningsmetod för medlemsstaterna för att täcka in faktorer såsom genomförandenivån för riskhanteringsåtgärderna för cybersäkerhet och rapporteringsskyldigheterna, kapacitetsnivån och effektiviteten i utförandet av de behöriga myndigheternas uppgifter, CSIRT-enheternas operativa kapacitet, genomförandenivån för det ömsesidiga biståndet, genomförandenivån för arrangemangen för informationsutbyte om cybersäkerhet eller särskilda frågor av gränsöverskridande eller sektorsövergripande karaktär. Medlemsstaterna bör uppmuntras att regelbundet genomföra självbedömningar och att presentera och diskutera resultaten av sina självbedömningar i samarbetsgruppen.

([17]) Europaparlamentets och rådets beslut nr 1313/2013/EU av den 17 december 2013 om en civilskyddsmekanism för unionen (EUT L 347, 20.12.2013, s. 924).

(77) Ansvaret för att säkerställa säkerheten i nätverks- och informationssystemen vilar i hög grad på väsentliga och viktiga entiteter. En riskhanteringskultur som inbegriper riskbedömningar och genomförande av riskhanteringsåtgärder för cybersäkerhet som är anpassade till riskerna bör främjas och utvecklas.

(78) Riskhanteringsåtgärder för cybersäkerhet bör ta hänsyn till i vilken grad den väsentliga eller viktiga entiteten är beroende av nätverks- och informationssystem och omfatta åtgärder för att identifiera eventuella incidentrisker, för att förebygga, upptäcka, hantera och återhämta sig från incidenter och för att begränsa deras inverkan. Säkerheten i nätverks- och informationssystem bör omfatta lagrade, överförda och behandlade uppgifters säkerhet. Riskhanteringsåtgärder för cybersäkerhet bör föreskriva systemanalys, med beaktande av den mänskliga faktorn, för att få en fullständig bild av nätverks- och informationssystemets säkerhet.

(79) Eftersom hot mot säkerheten i nätverks- och informationssystem kan ha olika ursprung bör riskhanteringsåtgärder för cybersäkerhet bygga på en allriskansats som syftar till att skydda nätverks- och informationssystem och dessa systems fysiska miljö mot händelser såsom stöld, brand, översvämning, telekommunikations- eller elavbrott eller obehörig fysisk åtkomst till och skada eller störning på en väsentlig eller viktig entitets information och informationsbehandlingsresurser, som kan undergräva tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem. Riskhanteringsåtgärderna för cybersäkerhet bör därför också omfatta den fysiska säkerheten och miljösäkerheten i nätverks- och informationssystem genom att inbegripa åtgärder för att skydda sådana system mot systemfel, mänskliga misstag, avsiktligt skadliga handlingar eller naturfenomen i överensstämmelse med europeiska och internationella standarder, såsom de som ingår i ISO/IEC 27000-serien. I detta avseende bör väsentliga och viktiga entiteter som ett led i sina riskhanteringsåtgärder för cybersäkerhet också ägna sig åt personalsäkerhet och inrätta lämpliga strategier för åtkomstkontroll. Dessa åtgärder bör vara förenliga med direktiv (EU) 2022/2557.

(80) För att påvisa efterlevnaden av riskhanteringsåtgärder för cybersäkerhet, och i frånvaro av lämpliga europeiska ordningar för cybersäkerhetscertifiering som antagits i enlighet med Europaparlamentets och rådets förordning (EU) 2019/881 ([18]), bör medlemsstaterna efter samråd med samarbetsgruppen och den europeiska gruppen för cybersäkerhetscertifiering främja användningen av relevanta europeiska och internationella standarder bland väsentliga och viktiga entiteter, eller så får de ålägga entiteter att använda certifierade IKT-produkter, IKT-tjänster och IKT-processer.

(81) För att undvika oproportionella finansiella och administrativa bördor för väsentliga och viktiga entiteter bör riskhanteringsåtgärderna för cybersäkerhet stå i proportion till riskerna för det berörda nätverks- och informationssystemet, med beaktande av teknikens ståndpunkt i fråga om sådana åtgärder, och i förekommande fall relevanta europeiska och internationella standarder, samt kostnaden för deras genomförande.

(82) Riskhanteringsåtgärder för cybersäkerhet bör stå i proportion till den väsentliga eller viktiga entitetens grad av exponering för risker och samhälleliga och ekonomiska konsekvenser som en incident skulle få. Vid fastställandet av riskhanteringsåtgärder för cybersäkerhet som är anpassade till väsentliga och viktiga entiteter bör vederbörlig hänsyn tas till väsentliga och viktiga entiteters olika riskexponering, t.ex. hur kritisk entiteten är, vilka risker, inklusive samhällsrisker, som den är exponerad för, hur stor entiteten är, hur sannolikt det är med incidenter och hur allvarliga de är, inklusive deras samhälleliga och ekonomiska konsekvenser.

([18]) 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).

(83) Väsentliga och viktiga entiteter bör säkerställa säkerheten i de nätverks- och informationssystem som de använder i sin verksamhet. Det rör sig framför allt om privata nätverks- och informationssystem som antingen förvaltas av de väsentliga och viktiga entiteternas interna it-personal eller vilkas säkerhet har lagts ut på entreprenad. De riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter som fastställs i detta direktiv bör tillämpas på de relevanta väsentliga och viktiga entiteterna oavsett om dessa entiteter underhåller sina nätverks- och informationssystem internt eller lägger ut underhållet på entreprenad.

(84) Med beaktande av deras gränsöverskridande karaktär bör leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster, leverantörer av marknadsplatser online, sökmotorer och plattformar för sociala nätverkstjänster samt tillhandahållare av betrodda tjänster omfattas av en hög nivå av harmonisering på unionsnivå. Genomförandet av riskhanteringsåtgärder för cybersäkerhet vad gäller dessa entiteter bör därför underlättas genom en genomförandeakt.

(85) Det är särskilt viktigt att hantera risker som härrör från en entitets leveranskedja och dess förhållande till sina leverantörer, såsom leverantörer av datalagrings- och databehandlingstjänster eller leverantörer av hanterade säkerhetstjänster och programredigerare, med tanke på förekomsten av incidenter där entiteter har varit föremål för cyberattacker och där inkräktare med avsikt att vålla skada har kunnat äventyra säkerheten i en entitets nätverks- och informationssystem genom att utnyttja sårbarheter som påverkar tredje parts produkter och tjänster. Väsentliga och viktiga entiteter bör därför bedöma och beakta den övergripande kvaliteten och resiliensen hos produkter och tjänster och de riskhanteringsåtgärder för cybersäkerhet som är inbyggda i dem samt cybersäkerhetspraxis hos sina leverantörer och tjänsteleverantörer, inbegripet deras förfaranden för säker utveckling. Väsentliga och viktiga entiteter bör framför allt uppmuntras att införliva riskhanteringsåtgärder för cybersäkerhet i avtal med sina direkta leverantörer och tjänsteleverantörer. Dessa entiteter kan beakta risker som härrör från leverantörer och tjänsteleverantörer på andra nivåer.

(86) Bland tjänsteleverantörerna har leverantörer av hanterade 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 hanterade säkerhetstjänster har dock också själva varit mål för cyberattacker, och eftersom de är nära integrerade i entiteternas verksamhet utgör de en särskild risk. Väsentliga och viktiga entiteter bör därför visa större noggrannhet vid valet av en leverantör av hanterade säkerhetstjänster.

(87) De behöriga myndigheterna kan också inom ramen för sina tillsynsuppgifter dra nytta av cybersäkerhetstjänster såsom säkerhetsrevisioner, penetrationstester eller incidenthantering.

(88) Väsentliga och viktiga entiteter bör också hantera risker som härrör från deras samverkan och förbindelser med andra intressenter inom ett vidare ekosystem, bland annat med avseende på att motverka industrispionage och skydda företagshemligheter. I synnerhet bör dessa entiteter vidta lämpliga åtgärder för att säkerställa att deras samarbete med akademiska institutioner och forskningsinstitut sker i linje med deras cybersäkerhetstrategier och följer god praxis när det gäller säker tillgång till och spridning av information i allmänhet och skydd av immateriella rättigheter i synnerhet. Likaså bör de väsentliga och viktiga entiteterna, med tanke på hur viktiga och värdefulla data är för deras verksamhet, vidta alla lämpliga riskhanteringsåtgärder för cybersäkerhet när de förlitar sig på dataomvandlings- och dataanalystjänster från tredje parter.

(89) Väsentliga och viktiga entiteter bör anta ett brett spektrum av grundläggande cyberhygienrutiner, såsom nollförtroende-principer, programuppdateringar, enhetskonfiguration, nätverkssegmentering, identitets- och åtkomsthantering eller användarmedvetenhet, anordna utbildning för sin personal och öka medvetenheten om cyberhot, nätfiske eller sociala manipuleringstekniker. Vidare bör dessa entiteter utvärdera sin egen cybersäkerhetskapacitet och när det är lämpligt fortsätta att integrera teknik för ökad cybersäkerhet, såsom artificiell intelligens eller maskininlärningssystem, för att förbättra sin kapacitet och säkerheten i nätverks- och informationssystemen.

(90) För att ytterligare hantera centrala risker i leveranskedjan och bistå väsentliga och viktiga entiteter som är verksamma i sektorer som omfattas av detta direktiv att på lämpligt sätt hantera risker i leveranskedjan och leverantörsrelaterade risker bör samarbetsgruppen, i samarbete med kommissionen och Enisa, och när så är lämpligt efter samråd med relevanta intressenter, även från industrin, utföra samordnade säkerhetsriskbedömningar av kritiska leveranskedjor, vilket redan gjorts för 5G-nät efter kommissionens rekommendation (EU) 2019/534 ([19]), i syfte att per sektor identifiera kritiska IKT-tjänster, IKT-system eller IKT-produkter, relevanta hot och sårbarheter. Sådana samordnade säkerhetsriskbedömningar bör fastställa åtgärder, riskreduceringsplaner och bästa praxis för att motverka kritiska beroenden, potentiella felkritiska systemdelar, hot, sårbarheter och andra risker kopplade till leveranskedjan och bör undersöka olika sätt att ytterligare uppmuntra en bredare användning av dessa från väsentliga och viktiga entiteters sida. Potentiella icke-tekniska riskfaktorer, såsom otillbörlig påverkan från ett tredjeland på leverantörer och tjänsteleverantörer, särskilt i samband med alternativa styrningsmodeller, inbegriper dolda sårbarheter eller bakdörrar och potentiella systemiska leveransstörningar, särskilt i samband med teknikinlåsning eller leverantörsberoende.

(91) De samordnade säkerhetsriskbedömningarna av kritiska leveranskedjor bör, mot bakgrund av den berörda sektorns särdrag, ta hänsyn till både tekniska och när så är lämpligt icke-tekniska faktorer, inbegripet de som anges i rekommendation (EU) 2019/534, i EU:s samordnade riskbedömning av cybersäkerheten för 5G-nät och i EU:s verktygslåda för 5G-cybersäkerhet som samarbetsgruppen enats om. För att identifiera de leveranskedjor som bör bli föremål för en samordnad säkerhetsriskbedömning bör följande kriterier beaktas: i) i vilken utsträckning väsentliga och viktiga entiteter använder och förlitar sig på specifika kritiska IKT-tjänster, IKT-system eller IKT-produkter, ii) specifika kritiska IKT-tjänsters, IKT-systems eller IKT-produkters relevans för att utföra kritiska eller känsliga funktioner, inbegripet behandling av personuppgifter, iii) tillgången till alternativa IKT-tjänster, IKT-system eller IKT-produkter, iv) motståndskraften i hela leveranskedjan för IKT-tjänster, IKT-system eller IKT-produkter under deras livscykel mot störningar, och v) för framväxande IKT-tjänster, IKT-system eller IKT-produkter, deras potentiella framtida betydelse för entiteternas verksamhet. Vidare bör särskild tonvikt läggas vid IKT-tjänster, IKT-system eller IKT-produkter som omfattas av särskilda krav som härrör från tredjeländer.

(92) För att rationalisera de skyldigheter som åläggs tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster, och tillhandahållare av betrodda tjänster, med anknytning till säkerheten i deras nätverks- och informationssystem, samt för att göra det möjligt för dessa entiteter och de behöriga myndigheterna enligt Europaparlamentets och rådets direktiv (EU) 2018/1972 ([20]) respektive förordning (EU) nr 910/2014 att dra nytta av den rättsliga ram som inrättas genom detta direktiv, inbegripet utnämning av en CSIRT-enhet med ansvar för risk- och incidenthantering och deltagande av berörda behöriga myndigheter i samarbetsgruppens och CSIRT-nätverkets verksamhet, bör dessa entiteter omfattas av tillämpningsområdet för detta direktiv. De motsvarande bestämmelser som anges i förordning (EU) nr 910/2014 och i direktiv (EU) 2018/1972och som gäller införande av säkerhets- och anmälningskrav för dessa typer av entiteter bör därför utgå. De regler om rapporteringsskyldigheter som fastställs i det här direktivet bör inte påverka tillämpningen av förordning (EU) 2016/679 och direktiv 2002/58/EG.

(93) De cybersäkerhetsskyldigheter som fastställs i detta direktiv bör anses komplettera de krav som åläggs tillhandahållare av betrodda tjänster enligt förordning (EU) nr 910/2014. Tillhandahållare av betrodda tjänster bör vara skyldiga att vidta alla lämpliga och proportionella åtgärder för att hantera riskerna för sina tjänster, även med avseende på kunder och tredje parter som förlitar sig på dessa tjänster, och att rapportera incidenter enligt detta direktiv. Sådana cybersäkerhets- och rapporteringsskyldigheter bör även avse det fysiska skyddet av de tjänster som tillhandahålls. De krav för kvalificerade tillhandahållare av betrodda tjänster som fastställs i artikel 24 i förordning (EU) nr 910/2014 bör fortsätta att vara tillämpliga.

([19]) Kommissionens rekommendation (EU) 2019/534 av den 26 mars 2019 om it-säkerhet i 5G-nät (EUT L 88, 29.3.2019, s. 42).

([20]) Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (EUT L 321, 17.12.2018, s. 36).

(94) Medlemsstaterna kan utse tillsynsorganen enligt förordning (EU) nr 910/2014 till behöriga myndigheter för betrodda tjänster för att säkerställa att nuvarande praxis upprätthålls och för att ta fasta på den kunskap och erfarenhet som förvärvats genom tillämpningen av den förordningen. I detta fall bör de behöriga myndigheterna enligt detta direktiv samarbeta nära och i lämplig tid med dessa tillsynsorgan genom att utbyta relevant information i syfte att säkerställa att tillsynen är effektiv och att tillhandahållare av betrodda tjänster uppfyller kraven i detta direktiv och i förordning (EU) nr 910/2014. I förekommande fall bör CSIRT-enheten eller den behöriga myndigheten enligt detta direktiv omedelbart informera tillsynsorganet enligt förordning (EU) nr 910/2014 om eventuella betydande cyberhot eller incidenter som anmälts och som påverkar betrodda tjänster samt ifall en tillhandahållare av betrodda tjänster bryter mot detta direktiv. Medlemsstaterna kan för rapporteringsändamål i förekommande fall använda den gemensamma kontaktpunkt som inrättats för att uppnå en gemensam och automatisk rapportering av incidenter till både tillsynsorganet enligt förordning (EU) nr 910/2014 och CSIRT-enheten eller den behöriga myndigheten enligt detta direktiv.

(95) När så är lämpligt och för att undvika onödiga störningar bör befintliga nationella riktlinjer som antagits för att införliva bestämmelserna om säkerhetsåtgärder i artiklarna 40 och 41 i direktiv (EU) 2018/1972 beaktas vid införlivandet av det här direktivet för att ta fasta på den kunskap och kompetens som redan förvärvats inom ramen för direktiv (EU) 2018/1972 avseende säkerhetsåtgärder och incidentunderrättelser. Enisa kan också ta fram vägledning om säkerhetskrav och rapporteringsskyldigheter för tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster för att underlätta harmonisering och övergång och minimera störningar. Medlemsstaterna kan utse de nationella regleringsmyndigheterna till behöriga myndigheter för elektronisk kommunikation enligt direktiv (EU) 2018/1972 för att säkerställa att nuvarande praxis upprätthålls och för att ta fasta på den kunskap och erfarenhet som förvärvats som en följd av genomförandet av det direktivet.

(96) Mot bakgrund av den ökande betydelsen av nummeroberoende interpersonella kommunikationstjänster enligt definitionen i direktiv (EU) 2018/1972 är det nödvändigt att säkerställa att sådana tjänster också omfattas av lämpliga säkerhetskrav med tanke på deras särskilda karaktär och ekonomiska betydelse. I takt med att attackytan fortsätter att växa blir nummeroberoende interpersonella kommunikationstjänster, såsom meddelandetjänster, utbredda attackvektorer. Inkräktare med uppsåt att vålla skada använder plattformar för att kommunicera och locka offer att öppna komprometterade webbsidor, vilket ökar sannolikheten för incidenter som involverar utnyttjande av personuppgifter och i förlängningen säkerhet i nätverks- och informationssystemen. Tillhandahållare av nummeroberoende interpersonella kommunikationstjänster bör säkerställa en säkerhetsnivå i nätverks- och informationssystemen som är lämplig i förhållande till de föreliggande riskerna. Eftersom tillhandahållare av nummeroberoende interpersonella kommunikationstjänster i allmänhet inte utövar faktisk kontroll över överföringen av signaler via nät kan graden av risk för sådana tjänster i vissa avseenden anses lägre än för traditionella elektroniska kommunikationstjänster. Detsamma gäller för interpersonella kommunikationstjänster enligt definitionen i direktiv (EU) 2018/1972 som använder nummer och som inte utövar faktisk kontroll över signalöverföringen.

(97) Den inre marknaden är mer beroende av ett fungerande internet än någonsin. Tjänster från nästan alla väsentliga och viktiga entiteter är beroende av tjänster som tillhandahålls via internet. För att säkerställa ett smidigt tillhandahållande av tjänster som levereras av väsentliga och viktiga entiteter är det viktigt att alla tillhandahållare av allmänna elektroniska kommunikationsnät har infört lämpliga riskhanteringsåtgärder för cybersäkerhet och rapporterar betydande incidenter i samband med dessa. Medlemsstaterna bör säkerställa att säkerheten i de allmänna elektroniska kommunikationsnäten upprätthålls och att deras vitala säkerhetsintressen skyddas mot sabotage och spionage. Eftersom internationell konnektivitet förstärker och påskyndar en konkurrenskraftig digitalisering av unionen och dess ekonomi bör incidenter som påverkar undervattenskablar rapporteras till CSIRT-enheten eller i förekommande fall den behöriga myndigheten. Den nationella strategin för cybersäkerhet bör när så är relevant beakta cybersäkerheten för undervattenskablar och inbegripa kartläggning av potentiella cybersäkerhetsrisker och riskreduceringsåtgärder för att säkerställa högsta skyddsnivå för dem.

(98) För att trygga säkerheten för allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster bör användningen av krypteringsteknik främjas, särskilt totalsträckskryptering samt datacentrerade säkerhetskoncept, såsom kartografi, segmentering, taggning, åtkomstpolicy och åtkomsthantering samt automatiserade beslut om åtkomst. Vid behov bör användningen av kryptering, särskilt totalsträckskryptering, vara obligatorisk för tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster i enlighet med principerna om automatisk och inbyggd säkerhet och automatiskt och inbyggt integritetsskydd vid tillämpningen av detta direktiv. Användningen av totalsträckskryptering bör förenas med medlemsstaternas befogenheter att säkerställa skyddet av sina väsentliga säkerhetsintressen och sin allmänna säkerhet och att möjliggöra förebyggande, utredning, upptäckt och lagföring av brott i enlighet med unionsrätten. Detta bör dock inte försvaga totalsträckskrypteringen, som är en kritisk teknik för ett effektivt dataskydd, integritet och kommunikationssäkerhet.

(99) I syfte att trygga säkerheten för, och förebygga missbruk och manipulering av, allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster bör användningen av säkra dirigeringsstandarder främjas för att säkerställa dirigeringsfunktionernas integritet och robusthet längs hela ekosystemet av internetåtkomstleverantörer.

(100) I syfte att skydda internets funktion och integritet och främja domännamnssystemets säkerhet och resiliens bör relevanta intressenter, däribland privata unionsentiteter, tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster, särskilt internetåtkomstleverantörer, och leverantörer av sökmotorer uppmuntras att anta en strategi för diversifiering av DNS-uppslagning. Vidare bör medlemsstaterna uppmuntra utvecklingen och användningen av en allmän och säker europeisk DNS-resolvertjänst.

(101) I detta direktiv fastställs en flerstegsstrategi för rapportering av betydande incidenter för att hitta rätt balans mellan, å ena sidan, snabb rapportering som bidrar till att begränsa den potentiella spridningen av betydande incidenter och gör det möjligt för väsentliga och viktiga entiteter att söka bistånd och, å andra sidan, ingående rapportering som drar värdefulla lärdomar av enskilda incidenter och med tiden förbättrar cyberresiliensen hos enskilda entiteter och hela sektorer. I detta avseende bör detta direktiv omfatta rapportering av incidenter som, baserat på en första bedömning som utförts av den berörda entiteten, kan orsaka allvarliga störningar i tjänsterna eller ekonomiska förluster för den berörda entiteten eller påverka andra fysiska eller juridiska personer genom att orsaka betydande materiell eller immateriell skada. En sådan inledande bedömning bör bland annat ta hänsyn till de drabbade nätverks- och informationssystemen, särskilt deras betydelse för tillhandahållandet av entitetens tjänster, allvaret i och de tekniska egenskaperna hos cyberhotet och eventuella underliggande sårbarheter som utnyttjas, samt entitetens erfarenhet av liknande incidenter. Indikatorer såsom i vilken utsträckning tjänstens funktion påverkas, hur länge incidenten pågår eller hur många tjänstemottagare som drabbas kan spela en viktig roll när man fastställer om tjänstens driftsstörning är allvarlig.

(102) Om väsentliga eller viktiga entiteter får kännedom om en betydande incident bör de vara skyldiga att lämna in en tidig varning utan onödigt dröjsmål och under alla omständigheter inom 24 timmar. Denna tidiga varning bör åtföljas av en incidentanmälan. De berörda entiteterna bör lämna in en incidentanmälan utan onödigt dröjsmål och under alla omständigheter inom 72 timmar efter att ha fått kännedom om den betydande incidenten, särskilt i syfte att uppdatera den information som lämnats via den tidiga varningen och göra en inledande bedömning av den betydande incidenten, inbegripet dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer. En slutrapport bör lämnas in senast en månad efter incidentunderrättelsen. Den tidiga varningen bör endast innehålla den information som är nödvändig för att göra CSIRT-enheten, eller i förekommande fall den behöriga myndigheten, medveten om den betydande incidenten och ge den berörda entiteten möjlighet att vid behov söka bistånd. Den tidiga varningen bör i tillämpliga fall ange om den betydande incidenten misstänks vara orsakad av olagliga eller avsiktligt skadliga handlingar och om det är troligt att den kommer att få gränsöverskridande verkningar. Medlemsstaterna bör säkerställa att skyldigheten att lämna in den tidiga varningen, eller den efterföljande incidentunderrättelsen, inte avleder den underrättande entitetens resurser från verksamheter i samband med incidenthantering som bör prioriteras, i syfte att förhindra att skyldigheterna att rapportera incidenter antingen avleder resurser från hantering av betydande incidenter eller på annat sätt undergräver entitetens ansträngningar i

detta avseende. I händelse av en pågående incident vid den tidpunkt då slutrapporten lämnas in bör medlemsstaterna säkerställa att berörda entiteter tillhandahåller en lägesrapport vid den tidpunkten och en slutrapport inom en månad efter det att de hanterat den betydande incidenten.

(103) I tillämpliga fall bör väsentliga och viktiga entiteter utan dröjsmål underrätta sina tjänstemottagare om eventuella åtgärder eller avhjälpande arrangemang som dessa kan genomföra för att begränsa de risker som följer av ett betydande cyberhot. När så är lämpligt, och i synnerhet om det är sannolikt att det betydande cyberhotet kommer att förverkligas, bör dessa entiteter även informera sina tjänstemottagare om själva hotet. Kravet på att informera dessa mottagare om betydande cyberhot bör uppfyllas efter bästa förmåga men bör inte befria entiteter från skyldigheten att på egen bekostnad vidta lämpliga och omedelbara åtgärder för att förebygga eller avhjälpa sådana hot och återställa tjänstens normala säkerhetsnivå. Sådan information om betydande cyberhot bör tillhandahållas tjänstemottagarna kostnadsfritt och vara formulerad på ett lättbegripligt sätt.

(104) Tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster bör tillämpa inbyggd säkerhet och säkerhet som standard och informera sina tjänstemottagare om betydande cyberhot och om åtgärder dessa kan vidta för att skydda säkerheten för sina enheter och sin kommunikation, t.ex. genom att använda särskilda typer av programvara eller krypteringsteknik.

(105) En proaktiv strategi mot cyberhot är en viktig del av riskhanteringsåtgärderna för cybersäkerhet som bör göra det möjligt för de behöriga myndigheterna att effektivt förhindra att cyberhot blir incidenter som kan vålla betydande materiell eller immateriell skada. Det är därför av avgörande vikt att cyberhot anmäls. I detta syfte uppmuntras entiteter att rapportera cyberhot på frivillig basis.

(106) För att förenkla rapporteringen av information som krävs enligt detta direktiv och för att minska den administrativa bördan för entiteter bör medlemsstaterna tillhandahålla tekniska hjälpmedel såsom en gemensam kontaktpunkt, automatiserade system, onlineformulär, användarvänliga gränssnitt, mallar och särskilda plattformar för entiteter, oberoende av om de omfattas av tillämpningsområdet för detta direktiv, som de kan använda för att lämna in den relevanta information som ska rapporteras. Unionsfinansiering till stöd för genomförandet av detta direktiv, särskilt inom programmet för ett digitalt Europa, som inrättats genom Europaparlamentets och rådets förordning (EU) 2021/694 ([21]), kan inkludera stöd till gemensamma kontaktpunkter. Vidare befinner sig entiteter ofta i en situation där en viss incident på grund av sina särdrag måste rapporteras till flera olika myndigheter till följd av underrättelseskyldigheter enligt olika rättsliga instrument. Sådana fall skapar ytterligare administrativa bördor och kan också leda till osäkerhet om format och förfaranden för sådana underrättelser. Om en gemensam kontaktpunkt inrättas, uppmuntras medlemsstaterna även att använda denna gemensamma kontaktpunkt för underrättelser om säkerhetsincidenter enligt annan unionsrätt, såsom förordning (EU) 2016/679 och direktiv 2002/58/EG. Användningen av en sådan gemensam kontaktpunkt 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 den oberoende ställningen för de myndigheter som avses i dessa. Enisa bör i samarbete med samarbetsgruppen utarbeta gemensamma mallar för underrättelser med hjälp av riktlinjer för att förenkla och rationalisera den information som ska rapporteras enligt unionsrätten och minska den administrativa bördan för de underrättande entiteterna.

(107) Om en incident misstänks ha samband med allvarlig brottslig verksamhet enligt unionsrätt eller nationell rätt, bör medlemsstaterna uppmuntra väsentliga och viktiga entiteter att, på grundval av tillämpliga straffrättsliga bestämmelser i enlighet med unionsrätten, rapportera incidenter som misstänks vara av allvarlig brottslig art till de relevanta rättsvårdande myndigheterna. Där så är lämpligt, och utan att det påverkar de bestämmelser om skydd av personuppgifter som gäller för Europol, är det önskvärt att samordning mellan behöriga myndigheter och rättsvårdande myndigheter i olika medlemsstater underlättas av Europeiska it-brottcentrumet (EC3) och Enisa.

([21]) Europaparlamentets och rådets förordning (EU) 2021/694 av den 29 april 2021 om inrättande av programmet för ett digitalt Europa och om upphävande av beslut (EU) 2015/2240 (EUT L 166, 11.5.2021, s. 1).

(108) Säkerheten för personuppgifter undergrävs ofta till följd av incidenter. I detta sammanhang bör de behöriga myndigheterna samarbeta och utbyta information om alla relevanta frågor med de myndigheter som avses i förordning (EU) 2016/679 och direktiv 2002/58/EG.

(109) Att upprätthålla korrekta och fullständiga databaser med registreringsuppgifter för domännamn (WHOIS-data) och ge laglig åtkomst till sådana uppgifter är avgörande för att säkerställa domännamnssystemets säkerhet, stabilitet och resiliens, vilket i sin tur bidrar till en hög gemensam nivå av cybersäkerhet i hela unionen. För detta specifika ändamål bör registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster vara skyldiga att behandla vissa uppgifter som är nödvändiga för detta. Sådan behandling bör vara en rättslig förpliktelse i den mening som avses i artikel 6.1 c i förordning (EU) 2016/679. Denna förpliktelse bör inte påverka möjligheten att samla in registreringsuppgifter för domännamn för andra ändamål, exempelvis på grundval av avtal eller rättsliga skyldigheter som fastställs i annan unionsrätt eller nationell rätt. Denna förpliktelse syftar till att erhålla en fullständig och korrekt uppsättning registreringsuppgifter och bör inte resultera i att samma uppgifter samlas in flera gånger. Registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör samarbeta med varandra för att undvika dubbelarbete.

(110) Tillgänglighet avseende, och åtkomst i lämplig tid till, domännamnsregistreringsuppgifter för legitima åtkomstsökande är avgörande för att förebygga och bekämpa missbruk av domännamnssystem och för att förebygga, upptäcka och reagera på incidenter. Legitima åtkomstsökande bör tolkas som varje fysisk eller juridisk person som gör en begäran i enlighet med unionsrätten eller nationell rätt. Det kan inbegripa myndigheter som är behöriga enligt detta direktiv och sådana som enligt unionsrätten eller nationell rätt är behöriga i fråga om förebyggande, utredning, upptäckt eller lagföring av brott, samt Cert eller CSIRT-enheter. Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör vara skyldiga att möjliggöra för legitima åtkomstsökande att få laglig åtkomst till specifika domännamnsregistreringsuppgifter som är nödvändiga för åtkomstbegärans syfte, i enlighet med unionsrätten och nationell rätt. Begäran från legitima åtkomstsökande bör åtföljas av en motivering som gör det möjligt att bedöma nödvändigheten av att få åtkomst till uppgifterna.

(111) För att säkerställa tillgången till korrekta och fullständiga registreringsuppgifter för domännamn bör registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster samla in registreringsuppgifter för domännamn och garantera deras integritet och tillgänglighet. I synnerhet bör registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster fastställa policyer och förfaranden för insamling och lagring av korrekta och fullständiga registreringsuppgifter för domännamn samt för att förhindra och korrigera felaktiga registreringsuppgifter i enlighet med unionens dataskyddslagstiftning. Dessa policyer och förfaranden bör så långt det är möjligt beakta de standarder som utvecklats av flerpartsförvaltningsstrukturerna på internationell nivå. Registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör anta och genomföra proportionella förfaranden för att verifiera registreringsuppgifterna för domännamn. Dessa förfaranden bör spegla bästa branschpraxis och, så långt det är möjligt, de framsteg som gjorts inom elektronisk identifiering. Exempel på verifieringsförfaranden kan vara förhandskontroller som görs i samband med registreringen och efterhandskontroller som görs efter registreringen. Registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör, i synnerhet, verifiera minst ett av registrantens kontaktsätt.

(112) Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör vara skyldiga att offentliggöra domännamnsregistreringsuppgifter som inte omfattas av unionens dataskyddslagstiftning, till exempel uppgifter som rör juridiska personer, i överensstämmelse med ingressen till förordning (EU) 2016/679. När det gäller juridiska personer bör registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster offentliggöra åtminstone registrantens namn och telefonnummer. E-postadressen bör också offentliggöras förutsatt att den inte innehåller några personuppgifter, såsom när det gäller e-postalias eller funktionsbrevlådor. Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör också möjliggöra för legitima åtkomstsökande att få laglig åtkomst till specifika domännamnsregistreringsuppgifter som rör fysiska personer, i enlighet med unionens dataskyddslagstiftning. Medlemsstaterna bör ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att utan onödigt dröjsmål besvara ansökningar om utlämnande av registreringsuppgifter för domännamn från legitima åtkomstsökande. Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör fastställa policyer och förfaranden för offentliggörande och utlämnande av registreringsuppgifter, inbegripet servicenivåavtal för att hantera ansökningar om åtkomst från legitima åtkomstsökande. Dessa policyer och förfaranden bör så långt det är möjligt beakta eventuell vägledning

och de standarder som utvecklats av flerpartsförvaltningsstrukturerna på internationell nivå. Åtkomstförfarandet kan också omfatta användning av ett gränssnitt, en portal eller annat tekniskt verktyg som ett effektivt system för att begära och få tillgång till registreringsuppgifter. I syfte att främja harmoniserad praxis på hela den inre marknaden kan kommissionen, utan att det påverkar Europeiska dataskyddsstyrelsens befogenheter, tillhandahålla riktlinjer för sådana förfaranden, som i möjligaste mån beaktar de standarder som utvecklats av flerpartsförvaltningsstrukturerna på internationell nivå. Medlemsstaterna bör säkerställa att alla typer av åtkomst till registreringsuppgifter för domännamn, både personuppgifter och icke-personuppgifter, är kostnadsfria.

(113) Entiteter som omfattas av detta direktivs tillämpningsområde bör anses omfattas av jurisdiktionen i den medlemsstat där de är etablerade. Tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster bör dock anses omfattas av jurisdiktionen i den medlemsstat där de tillhandahåller sina tjänster. Leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer och plattformar för sociala nätverkstjänster bör anses omfattas av jurisdiktionen i den medlemsstat där de har sitt huvudsakliga etableringsställe i unionen. Offentliga förvaltningsentiteter bör anses omfattas av jurisdiktionen i den medlemsstat som inrättat dem. Om entiteten tillhandahåller tjänster eller är etablerad i mer än en medlemsstat bör den omfattas av dessa medlemsstaters separata och parallella jurisdiktioner samtidigt. De behöriga myndigheterna i dessa medlemsstater bör samarbeta, ge varandra ömsesidigt bistånd och när det är lämpligt genomföra gemensamma tillsynsåtgärder. När medlemsstater utövar jurisdiktion bör de inte påföra efterlevnadskontrollåtgärder eller sanktioner mer än en gång för samma beteende, i överensstämmelse med principen *ne bis in idem*.

(114) För att ta hänsyn till den gränsöverskridande karaktären hos de tjänster och den verksamhet som utförs av leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer och plattformar för sociala nätverkstjänster bör endast en medlemsstat ha jurisdiktion över dessa entiteter. Jurisdiktion bör tilldelas den medlemsstat där den berörda entiteten har sitt huvudsakliga etableringsställe i unionen. Kriteriet för etableringsställe i detta direktiv förutsätter att verksamhet faktiskt bedrivs genom en stabil struktur. Den rättsliga formen för en sådan struktur, oavsett om det är en filial eller ett dotterföretag med status som juridisk person, bör inte vara den avgörande faktorn i detta avseende. Huruvida kriteriet är uppfyllt bör inte vara beroende av om nätverks- och informationssystemen är fysiskt belägna på en viss plats. Förekomsten och användningen av sådana system utgör inte i sig en sådan huvudsaklig etablering och är därför inte avgörande kriterier för att fastställa det huvudsakliga etableringsstället. Det huvudsakliga etableringsstället bör anses ligga i den medlemsstat där besluten om åtgärder för att hantera cybersäkerhetsrisker i huvudsak fattas i unionen. Detta motsvarar vanligtvis platsen för entiteternas huvudkontor i unionen. Om en sådan medlemsstat inte kan fastställas eller om sådana beslut inte fattas i unionen bör det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där cybersäkerhetsoperationer utförs. Om en sådan medlemsstat inte kan fastställas bör det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där entiteten har etableringsstället med flest anställda i unionen. Om tjänsterna utförs av en koncern bör det kontrollerande företagets huvudsakliga etableringsställe betraktas som koncernens huvudsakliga etableringsställe.

(115) När en allmänt tillgänglig rekursiv DNS-tjänst tillhandahålls av en tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster endast som en del av internetanslutningstjänsten, bör entiteten anses omfattas av jurisdiktionen i alla de medlemsstater där dess tjänster tillhandahålls.

(116) Om en leverantör av DNS-tjänster, en registreringsenhet för toppdomäner, en entitet som tillhandahåller domännamnsregistreringstjänster, en leverantör av molntjänster, en leverantör av datacentraltjänster, en leverantör av nätverk för leverans av innehåll, driftsentreprenad, en leverantör av hanterade säkerhetstjänster eller en leverantör av en marknadsplats online, en sökmotor eller en plattform för sociala nätverkstjänster, vilken inte är etablerad i unionen, erbjuder tjänster inom unionen bör den utse en företrädare i unionen. I syfte att fastställa om en sådan entitet erbjuder tjänster inom unionen bör det kontrolleras om entiteten planerar att erbjuda tjänster till personer i en eller flera medlemsstater. Enbart den omständigheten att en entitets eller en mellanhands webbplats eller en e-postadress eller andra kontaktuppgifter är tillgängliga i unionen, eller att ett språk används som allmänt används i det tredjeland där entiteten är etablerad, bör inte betraktas som tillräcklig för att fastställa en sådan avsikt. Emellertid kan faktorer som att det används ett visst språk eller en viss valuta som allmänt används i en eller flera medlemsstater med möjligheten att beställa tjänster på det språket, eller att kunder eller användare i unionen omnämns, göra det uppenbart att entiteten planerar att erbjuda tjänster inom unionen. Företrädaren bör agera på entitetens vägnar, och det bör vara möjligt för de behöriga myndigheterna eller CSIRT-enheterna att vända sig till företrädaren. Företrädaren bör utses uttryckligen genom en skriftlig fullmakt från entiteten att agera på dess vägnar med avseende på dess skyldigheter enligt detta direktiv, inklusive incidentrapportering.

(117) För att säkerställa en tydlig överblick över leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer och plattformar för sociala nätverkstjänster, vilka tillhandahåller tjänster i unionen som omfattas av detta direktivs tillämpningsområde, bör Enisa skapa och upprätthålla ett register över sådana entiteter på grundval av information från medlemsstaterna, i förekommande fall via nationella mekanismer som inrättats för entiteter att registrera sig. De gemensamma kontaktpunkterna bör till Enisa vidarebefordra informationen och eventuella ändringar av densamma. För att säkerställa att den information som ska ingå i registret är korrekt och fullständig kan medlemsstaterna till Enisa lämna in den information som finns tillgänglig i nationella register om dessa entiteter. Enisa och medlemsstaterna bör vidta åtgärder för att underlätta kompatibilitet mellan sådana register, samtidigt som skydd av konfidentiell eller säkerhetsskyddsklassificerade uppgifter säkerställs. Enisa bör införa lämplig klassificering av information och förvaltningsprotokoll för att säkerställa den utlämnade informationens säkerhet och konfidentialitet och begränsa åtkomsten till samt lagringen och överföringen av sådan information till de avsedda användarna.

(118) Om uppgifter som är säkerhetsskyddsklassificerade enligt unionsrätt eller nationell rätt utbyts, rapporteras eller på annat sätt delas enligt detta direktiv, bör motsvarande regler för hantering av säkerhetsskyddsklassificerade uppgifter tillämpas. Vidare bör Enisa ha infrastruktur, förfaranden och regler för att hantera känsliga och säkerhetsskyddsklassificerade uppgifter i enlighet med tillämpliga säkerhetsregler för skydd av säkerhetsskyddsklassificerade EU-uppgifter.

(119) I och med att cyberhoten blir mer komplexa och sofistikerade är god upptäckt av sådana hot och förebyggande åtgärder mot dem i stor utsträckning beroende av ett regelbundet utbyte av underrättelser om hot och sårbarhet mellan entiteter. Informationsutbyte bidrar till ökad medvetenhet om cyberhot, vilket i sin tur ökar entiteternas förmåga att förhindra att hot blir till incidenter och gör det möjligt för entiteterna att bättre begränsa effekterna av incidenter och återhämta sig mer effektivt. I avsaknad av vägledning på unionsnivå verkar olika faktorer ha hindrat sådant utbyte av underrättelser, särskilt osäkerheten om förenligheten med konkurrens- och ansvarsreglerna.

(120) Entiteter bör uppmuntras och bistås av medlemsstaterna för att kollektivt utnyttja sina individuella kunskaper och praktiska erfarenheter på strategisk, taktisk och operativ nivå i syfte att förbättra sin förmåga att på lämpligt sätt förebygga, upptäcka, reagera på eller återhämta sig från incidenter eller begränsa deras verkningar. Det är därför nödvändigt att på unionsnivå möjliggöra framväxten av arrangemang för frivilligt informationsutbyte om cybersäkerhet. I detta syfte bör medlemsstaterna aktivt bistå och uppmuntra entiteter, såsom de som erbjuder cybersäkerhetstjänster och forskning, samt relevanta entiteter som inte omfattas av detta direktiv, att delta i sådana arrangemang för informationsutbyte om cybersäkerhet. Dessa arrangemang bör fastställas i enlighet med unionens konkurrensregler och unionens dataskyddslagstiftning.

(121) Behandling av personuppgifter i den utsträckning som är nödvändig och proportionell för att säkerställa säkerhet i nätverks- och informationssystem genom väsentliga och viktiga entiteter kan anses vara laglig på grund av att sådan behandling är förenlig med en rättslig förpliktelse som åvilar den personuppgiftsansvarige i enlighet med kraven i artikel 6.1 c och artikel 6.3 i förordning (EU) 2016/679. Behandling av personuppgifter kan även vara nödvändig på grund av berättigade intressen hos väsentliga och viktiga entiteter, samt tillhandahållare av säkerhetsteknik och säkerhetstjänster som agerar på dessa entiteters vägnar, i enlighet med artikel 6.1 f i förordning (EU) 2016/679, bland annat när sådan behandling är nödvändig för arrangemang för informationsutbyte om cybersäkerhet eller frivillig underrättelse om relevant information i enlighet med detta direktiv. Åtgärder som rör förebyggande, upptäckt, identifiering, begränsning, analys och hantering av incidenter, åtgärder för att öka medvetenheten om specifika cyberhot, informationsutbyte i samband med avhjälpande av sårbarheter och samordnat meddelande av sårbarhetsinformation, frivilligt informationsutbyte om sådana incidenter samt cyberhot och sårbarheter, angreppsindikatorer, taktik, tekniker och förfaranden, cybersäkerhetsvarningar och konfigurationsverktyg kan kräva behandling av vissa kategorier av personuppgifter, såsom ip-adresser, webbadresser (URL), domännamn, e-postadresser och tidsstämplar, när dessa avslöjar personuppgifter. Personuppgiftsbehandling av behöriga myndigheter, gemensamma kontaktpunkter och CSIRT-enheter kan utgöra en rättslig förpliktelse eller anses vara nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den ansvariges myndighetsutövning i enlighet med artikel 6.1 c eller e och artikel 6.3 i förordning (EU) 2016/679 eller på grund av ett berättigat intresse hos de väsentliga och viktiga entiteterna enligt vad som avses i artikel 6.1 f i den förordningen. Vidare kan nationell rätt innehålla bestämmelser som tillåter att behöriga myndigheter, gemensamma kontaktpunkter och CSIRT-enheter, i den utsträckning som är nödvändig och proportionell för att säkerställa säkerhet i nätverks- och informationssystem hos väsentliga och viktiga entiteter, behandlar särskilda kategorier av personuppgifter i enlighet med artikel 9 i förordning (EU) 2016/679, särskilt genom att föreskriva lämpliga och särskilda åtgärder för att skydda fysiska personers grundläggande rättigheter och intressen, däribland tekniska begränsningar för vidareutnyttjande av sådana uppgifter samt användning av moderna säkerhetsåtgärder och integritetsbevarande åtgärder, såsom pseudonymisering, eller kryptering där anonymisering avsevärt kan påverka det eftersträvade ändamålet.

(122) För att stärka de tillsynsbefogenheter och tillsynsåtgärder som bidrar till att säkerställa ett effektivt fullgörande av skyldigheter bör detta direktiv innehålla en minimiförteckning över tillsynsåtgärder och tillsynsmedel genom vilka behöriga myndigheter kan utöva tillsyn över väsentliga och viktiga entiteter. Dessutom bör detta direktiv fastställa en differentiering av tillsynssystemet mellan väsentliga och viktiga entiteter i syfte att säkerställa en rättvis balans vad gäller skyldigheterna för dessa entiteter och de behöriga myndigheterna. Väsentliga entiteter bör därför omfattas av ett heltäckande tillsynssystem med förhandstillsyn och efterhandstillsyn, medan viktiga entiteter bör omfattas av enklare tillsyn, endast i efterhand. Viktiga entiteter bör därför inte vara skyldiga att systematiskt dokumentera efterlevnad av riskhanteringsåtgärderna för cybersäkerhet, medan de behöriga myndigheterna bör tillämpa en reaktiv efterhandstillsyn och därmed inte ha någon allmän skyldighet att utöva tillsyn över dessa entiteter. Efterhandstillsynen av viktiga entiteter kan utlösas av bevis, indikationer eller uppgifter som har kommit till de behöriga myndigheternas kännedom och som enligt dessa myndigheter tyder på potentiella överträdelser av detta direktiv. Sådana bevis, indikationer eller uppgifter kan exempelvis vara av den typ som de behöriga myndigheterna mottar från andra myndigheter, entiteter, medborgare, medier eller andra källor eller offentligt tillgänglig information eller härröra från annan verksamhet som de behöriga myndigheterna bedriver i samband med fullgörandet av sina uppgifter.

(123) Behöriga myndigheters utförande av tillsynsuppgifter bör inte i onödan hämma den berörda entitetens affärsverksamhet. När behöriga myndigheter utför sina tillsynsuppgifter avseende väsentliga entiteter, bland annat genom inspektioner på plats och distansbaserad tillsyn, utredning av överträdelser av detta direktiv, säkerhetsrevisioner eller säkerhetsskanningar, bör de minimera konsekvenserna för den berörda entitetens affärsverksamhet.

(124) Vid genomförandet av förhandstillsyn bör de behöriga myndigheterna kunna besluta att prioritera användningen av de tillsynsåtgärder och tillsynsmedel som står till deras förfogande på ett proportionellt sätt. Detta innebär att de behöriga myndigheterna kan besluta om en sådan prioritering på grundval av tillsynsmetoder som bör bygga på en riskbaserad ansats. Mer specifikt kan sådana metoder omfatta kriterier eller riktmärken för klassificering av väsentliga entiteter i riskkategorier och motsvarande tillsynsåtgärder och tillsynsmedel som rekommenderas per riskkategori, såsom användning av frekvens för eller typ av inspektion på plats, riktade säkerhetsrevisioner eller säkerhetsskanningar, vilken typ av information som ska begäras och detaljnivån på denna information. Sådana

tillsynsmetoder skulle även kunna åtföljas av arbetsprogram och utvärderas och ses över regelbundet, inklusive med avseende på aspekter som resursfördelning och resursbehov. När det gäller offentliga förvaltningsentiteter bör tillsynsbefogenheterna utövas i överensstämmelse med nationella lagstiftningsmässiga och institutionella ramar.

(125) De behöriga myndigheterna bör säkerställa att deras tillsynsuppgifter med avseende på väsentliga och viktiga entiteter utförs av utbildad personal, som bör ha de nödvändiga färdigheterna för att utföra dessa uppgifter, särskilt i fråga om att genomföra inspektioner på plats och distansbaserad tillsyn, bland annat identifiering av svagheter i databaser, maskinvara, brandväggar, kryptering och nätverk. Inspektionerna och tillsynen bör utföras på ett objektivt sätt.

(126) I vederbörligen motiverade fall bör den behöriga myndigheten, när den fått kännedom om ett betydande cyberhot eller en överhängande risk, kunna fatta omedelbara beslut om efterlevnadskontroll i syfte att förhindra eller reagera på en incident.

(127) För att efterlevnadskontrollen ska bli effektiv bör det fastställas en minimiförteckning över efterlevnadskontrollbefogenheter som kan utövas för brott mot de riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter som föreskrivs i detta direktiv, med en tydlig och konsekvent ram för sådan efterlevnadskontroll i hela unionen. Vederbörlig hänsyn bör tas till arten, allvarlighetsgraden och varaktigheten av överträdelsen av detta direktiv, de materiella eller immateriella skador som orsakats, om överträdelsen var avsiktlig eller berodde på försumlighet, åtgärder som vidtagits för att förhindra eller begränsa de materiella eller immateriella skadorna, graden av ansvar eller relevanta tidigare överträdelser, graden av samarbete med den behöriga myndigheten och andra försvårande eller förmildrande omständigheter. Efterlevnadskontrollåtgärderna, inklusive administrativa sanktionsavgifter, bör vara proportionella och påförandet av dem bör omfattas av lämpliga rättssäkerhetsgarantier i enlighet med de allmänna principerna i unionsrätten och Europeiska unionens stadga om de grundläggande rättigheterna (*stadgan*), inbegripet rätten till ett effektivt rättsmedel och till en opartisk domstol, oskuldspresumtion och rätten till försvar.

(128) Detta direktiv ålägger inte medlemsstaterna att föreskriva att fysiska personer med ansvar för att säkerställa att en entitet efterlever direktivet ska omfattas av straffrättsligt eller civilrättsligt ansvar för skada som åsamkats tredjeparter till följd av en överträdelse av direktivet.

(129) För att säkerställa en effektiv efterlevnadskontroll av de skyldigheter som fastställs i detta direktiv bör varje behörig myndighet ha befogenhet att påföra eller begära påförande av administrativa sanktionsavgifter.

(130) Om en administrativ sanktionsavgift påförs en väsentlig eller viktig entitet som är ett företag, bör ett företag i detta sammanhang anses vara ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget. Om en administrativ sanktionsavgift 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. Medlemsstaterna bör fastställa om och i vilken utsträckning myndigheter ska omfattas av administrativa sanktionsavgifter. Föreläggande av en administrativ sanktionsavgift påverkar inte de behöriga myndigheternas tillämpning av andra befogenheter eller andra sanktioner som fastställs i de nationella bestämmelser som införlivar detta direktiv.

(131) Medlemsstaterna bör kunna fastställa bestämmelser om straffrättsliga påföljder för överträdelser av de nationella bestämmelser som införlivar detta direktiv. Påförandet av straffrättsliga påföljder för överträdelser av sådana nationella bestämmelser och relaterade administrativa sanktioner bör dock inte medföra ett åsidosättande av principen *ne bis in idem* enligt Europeiska unionens domstols tolkning.

(132) När detta direktiv inte harmoniserar administrativa sanktioner eller när så är nödvändigt i andra fall, till exempel i händelse av en allvarlig överträdelse av detta direktiv, bör medlemsstaterna genomföra ett system med effektiva, proportionella och avskräckande sanktioner. Dessa påföljders art, och frågan om de är straffrättsliga eller administrativa, bör fastställas i nationell rätt.

(133) För att de sanktioner som är tillämpliga på överträdelser av efterlevnadskontrollåtgärder detta direktiv ska bli mer effektiva och avskräckande bör de behöriga myndigheterna ges befogenhet att tillfälligt upphäva eller begära tillfälligt upphävande av en certifiering eller auktorisation för en del av eller alla relevanta tjänster som tillhandahålls av en väsentlig entitet samt begära införande av ett tillfälligt förbud för en fysisk person som har ledningsansvar på nivån för verkställande direktör eller juridiskt ombud att utöva ledande funktioner. Med tanke på deras stränghet och påverkan på entiteternas verksamheter och i sista hand på användarna bör sådana tillfälliga upphävanden eller förbud endast tillämpas proportionellt mot överträdelsens allvarlighetsgrad och med beaktande av omständigheterna i varje enskilt fall, inbegripet om överträdelsen var avsiktlig eller berodde på försumlighet, samt åtgärder som vidtagits för att förhindra eller begränsa de materiella eller immateriella skadorna. Sådana tillfälliga upphävanden eller förbud bör endast tillämpas som sista utväg, dvs. först efter det att de andra relevanta åtgärder för efterlevnadskontroll som fastställs i detta direktiv har uttömts, och endast fram till dess att den berörda entiteten vidtar nödvändiga åtgärder för att avhjälpa de brister eller uppfylla de krav från den behöriga myndigheten för vilka de tillfälliga upphävandena eller förbuden tillämpades. Införandet av sådana tillfälliga upphävanden eller förbud bör omfattas av lämpliga rättssäkerhetsgarantier i enlighet med de allmänna principerna i unionsrätten och stadgan, inbegripet rätten till ett effektivt rättsmedel och till en opartisk domstol, oskuldspresumtion och rätten till försvar.

(134) För att säkerställa att entiteter fullgör sina skyldigheter enligt detta direktiv bör medlemsstaterna samarbeta med och bistå varandra med avseende på tillsyns- och efterlevnadskontrollåtgärder, särskilt om en entitet tillhandahåller tjänster i mer än en medlemsstat eller om dess nätverks- och informationssystem är belägna i en annan medlemsstat än den där den tillhandahåller tjänster. När den tillfrågade behöriga myndigheten tillhandahåller bistånd bör den vidta åtgärder för tillsyns- och efterlevnadskontrollåtgärder i enlighet med nationell rätt. För att säkerställa ett välfungerande ömsesidigt bistånd enligt detta direktiv bör de behöriga myndigheterna använda samarbetsgruppen som ett forum där de kan diskutera fall och enskilda biståndsansökningar.

(135) För att säkerställa effektiv tillsyn och efterlevnadskontroll, framför allt i en situation med en gränsöverskridande dimension, bör de medlemsstater som har mottagit en begäran om ömsesidigt bistånd, inom ramen för begäran, vidta lämpliga tillsyns- och efterlevnadskontrollåtgärder med avseende på den entitet som är föremålet för den begäran och som tillhandahåller tjänster eller som har ett nätverks- och informationssystem inom den medlemsstatens territorium.

(136) Detta direktiv bör fastställa regler för samarbete mellan de behöriga myndigheterna och tillsynsmyndigheterna enligt förordning (EU) 2016/679 för att hantera överträdelser av detta direktiv som rör personuppgifter.

(137) Detta direktiv bör syfta till att säkerställa en hög ansvarsnivå för riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter för väsentliga och viktiga entiteter. Därför bör ledningsorganen för väsentliga och viktiga entiteter godkänna riskåtgärderna för cybersäkerhet och övervaka deras genomförande.

(138) För att säkerställa en hög gemensam cybersäkerhetsnivå i unionen på grundval av detta direktiv bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på att komplettera detta direktiv genom att ange vilka kategorier av väsentliga och viktiga 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. 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 ([22]). 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.

([22]) EUT L 123, 12.5.2016, s. 1.

(139) För att säkerställa enhetliga villkor för genomförandet av detta direktiv bör kommissionen tilldelas genomförandebefogenheter för att fastställa de förfaranden som krävs för samarbetsgruppens verksamhet och de tekniska och metodologiska kraven samt sektorskraven avseende riskhanteringsåtgärder för cybersäkerhet, samt ytterligare precisera typen av information samt formatet och förfarandet för underrättelser om incidenter, cyberhot och tillbud och för kommunikation om betydande cyberhot, samt i vilka fall en incident ska betraktas som betydande. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([23]).

(140) Detta direktiv bör med jämna mellanrum ses över av kommissionen i samråd med berörda parter, främst i syfte att avgöra huruvida det är lämpligt att föreslå ändringar med hänsyn till samhällsutvecklingen, den politiska utvecklingen, den tekniska utvecklingen eller ändrade marknadsvillkor. Som en del av de översynerna bör kommissionen bedöma vilken relevans de berörda entiteternas storlek och de sektorer, delsektorer och typer av entiteter som avses i bilagorna till detta direktiv har för ekonomins och samhällets funktion när det gäller cybersäkerhet. Kommissionen bör bland annat bedöma huruvida leverantörer som omfattas av tillämpningsområdet för detta direktiv vilka klassificeras som mycket stora onlineplattformar i den mening som avses i artikel 33 i Europaparlamentets och rådets förordning (EU) 2022/2065 ([24]) kan identifieras som väsentliga entiteter enligt detta direktiv.

(141) Detta direktiv skapar nya uppgifter för Enisa och stärker därigenom dess roll, och kan också leda till att Enisa tvingas utföra sina befintliga uppgifter enligt förordning (EU) 2019/881 på en högre nivå än tidigare. För att säkerställa att Enisa har de ekonomiska resurser och den personal som krävs för att utföra befintliga och nya uppgifter och uppnå en eventuellt högre nivå på genomförandet av dessa uppgifter till följd av dess utökade roll, bör dess budget ökas i motsvarande grad. För att säkerställa en effektiv resursanvändning bör Enisa dessutom ges större flexibilitet när det gäller möjligheten att fördela resurser internt, i syfte att kunna utföra sina uppgifter och infria förväntningarna på ett ändamålsenligt sätt.

(142) Eftersom målet för detta direktiv, nämligen att uppnå en hög gemensam cybersäkerhetsnivå i unionen, 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 detta direktiv inte utöver vad som är nödvändigt för att uppnå detta mål.

(143) Detta direktiv respekterar de grundläggande rättigheterna och iakttar de principer som erkänns i stadgan, i synnerhet rätten till respekt för privatliv och kommunikationer, skydd av personuppgifter, näringsfriheten, rätten till egendom, rätten till ett effektivt rättsmedel och till en opartisk domstol, oskuldspresumtion och rätten till försvar. Rätten till ett effektivt rättsmedel inbegriper mottagarna av tjänster som tillhandahålls av väsentliga och viktiga entiteter. Detta direktiv bör genomföras i enlighet med dessa rättigheter och principer.

(144) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([25]) och avgav ett yttrande den 11 mars 2021 ([26]).

([23]) 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).

([24]) 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 (rättsakten om digitala tjänster) (EUT L 277, 27.10.2022, s. 1).

([25]) 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).

([26]) EUT C 183, 11.5.2021, s. 3.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Innehåll

1. I detta direktiv fastställs åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen, i syfte att förbättra den inre marknadens funktion.

2. Direktivet fastställer i detta syfte följande:

a) Skyldigheter som ålägger medlemsstaterna att anta nationella strategier för cybersäkerhet och att utse eller inrätta behöriga myndigheter, myndigheter för hantering av cyberkriser, gemensamma kontaktpunkter för cybersäkerhet (gemensamma kontaktpunkter) och enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter).

b) Riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter för entiteter av den typ som avses i bilaga I eller II samt för entiteter som identifieras som kritiska entiteter enligt direktiv (EU) 2022/2557.

c) Regler och skyldigheter när det gäller informationsutbyte om cybersäkerhet.

d) Skyldigheter för medlemsstaterna när det gäller tillsyn och efterlevnadskontroll.

Artikel 2

Tillämpningsområde

1. Detta direktiv är tillämpligt på offentliga eller privata entiteter av den typ som avses i bilaga I eller II som betecknas som medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG eller överstiger de trösklar för medelstora företag som avses i punkt 1 i den artikeln och som tillhandahåller sina tjänster eller bedriver sin verksamhet i unionen.

Artikel 3.4 i bilagan till den rekommendationen är inte tillämplig med avseende på detta direktiv.

2. Oavsett entiteternas storlek är detta direktiv också tillämpligt på entiteter av en typ som avses i bilaga I eller II, i följande fall:

a) Om tjänster tillhandahålls av

   i) tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster,

   ii) tillhandahållare av betrodda tjänster,

   iii) registreringsenheter för toppdomäner och leverantörer av domännamnssystemtjänster.

b) Om entiteten är den enda leverantören i en medlemsstat av en tjänst som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet.

c) Om en störning av den tjänst som entiteten tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa.

d) Om en störning av den tjänst som entiteten tillhandahåller kan medföra betydande systemrisker, särskilt för de sektorer där sådana störningar kan få gränsöverskridande konsekvenser.

e) Entiteten är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer i medlemsstaten som är beroende av denna entitet.

f) Om entiteten är en offentlig förvaltningsentitet

i) på statlig nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt, eller

ii) på regional nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt, som enligt en riskbaserad bedömning tillhandahåller tjänster vars störning kan ha en betydande effekt på kritisk samhällelig eller ekonomisk verksamhet.

3. Oavsett entiteternas storlek är detta direktiv tillämpligt på entiteter som identifieras som kritiska entiteter enligt direktiv (EU) 2022/2557.

4. Oavsett entiteternas storlek är detta direktiv tillämpligt på entiteter som tillhandahåller domännamnsregistreringstjänster.

5. Medlemsstaterna får föreskriva att detta direktiv ska tillämpas på

a) offentliga förvaltningsentiteter på lokal nivå,

b) utbildningsinstitut, särskilt om de utför kritisk forskningsverksamhet.

6. Detta direktiv påverkar inte medlemsstaternas ansvar för att skydda nationell säkerhet och deras befogenhet att skydda andra väsentliga statliga funktioner, inbegripet att säkerställa statens territoriella integritet och upprätthålla lag och ordning.

7. Detta direktiv är inte tillämpligt på offentliga förvaltningsentiteter som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott.

8. Medlemsstaterna får undanta särskilda entiteter som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott, eller som tillhandahåller tjänster uteslutande till en offentlig förvaltningsentitet som avses i punkt 7 i den här artikeln, från skyldigheterna i artikel 21 eller 23 med avseende på sådan verksamhet eller sådana tjänster. I sådana fall ska de tillsyns- och efterlevnadskontrollåtgärder som avses i kapitel VII inte tillämpas på denna specifika verksamhet eller dessa specifika tjänster. Om entiteterna bedriver verksamhet eller tillhandahåller tjänster uteslutande av den typ som avses i den här punkten, får medlemsstaterna besluta att befria dessa entiteter också från skyldigheterna i artiklarna 3 och 27.

9. Punkterna 7 och 8 är inte tillämpliga om en entitet agerar som tillhandahållare av betrodda tjänster.

10. Detta direktiv är inte tillämpligt på entiteter som medlemsstaterna har undantagit från tillämpningsområdet för förordning (EU) 2022/2554 i enlighet med artikel 2.4 i den förordningen.

11. De skyldigheter som fastställs i detta direktiv ska inte medföra tillhandahållande av information vars utlämnande strider mot väsentliga intressen i fråga om medlemsstaternas nationella säkerhet, allmänna säkerhet eller försvar.

12. Detta direktiv påverkar inte tillämpningen av förordning (EU) 2016/679, direktiv 2002/58/EG, Europaparlamentets och rådets direktiv 2011/93/EU ([27]) och 2013/40/EU ([28]) och direktiv (EU) 2022/2557.

13. Utan att det påverkar tillämpningen av artikel 346 i EUF-fördraget ska information som är konfidentiell enligt unionsbestämmelser eller nationella bestämmelser, såsom bestämmelser om affärshemligheter, utbytas med kommissionen och andra berörda myndigheter i enlighet med detta direktiv endast när ett sådant utbyte är nödvändigt för att tillämpa detta direktiv. Den information som utbyts ska begränsas till vad som är relevant och proportionellt för ändamålet med utbytet. Vid utbytet ska informationens konfidentialitet bevaras och berörda entiteters säkerhets- och affärsintressen skyddas.

([27]) Europaparlamentets och rådets direktiv 2011/93/EU av den 13 december 2011 om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi samt om ersättande av rådets rambeslut 2004/68/RIF (EUT L 335, 17.12.2011, s. 1).

([28]) Europaparlamentets och rådets direktiv 2013/40/EU av den 12 augusti 2013 om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF (EUT L 218, 14.8.2013, s. 8).

14. Entiteter, behöriga myndigheter, gemensamma kontaktpunkter och CSIRT-enheter ska behandla personuppgifter i den utsträckning som krävs för tillämpningen av detta direktiv och i enlighet med förordning (EU) 2016/679, i synnerhet ska sådan behandling baseras på artikel 6 i denna.

Behandlingen av personuppgifter enligt detta direktiv av tillhandahållare av allmänna elektroniska kommunikationsnät eller tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster ska utföras i enlighet med unionens dataskydds- och integritetslagstiftning, särskilt direktiv 2002/58/EG.

Artikel 3

Väsentliga och viktiga entiteter

1. Med avseende på tillämpningen av detta direktiv ska följande entiteter anses vara väsentliga entiteter:

a) Entiteter av en typ som avses i bilaga I som överstiger trösklarna för medelstora företag som fastställs i artikel 2.1 i bilagan till rekommendation 2003/361/EG.

b) Kvalificerade tillhandahållare av betrodda tjänster och registreringsenheter för toppdomäner samt leverantörer av DNS-tjänster, oavsett storlek.

c) Tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster som betraktas som medelstora företag enligt artikel 2 i bilagan till rekommendation 2003/361/EG.

d) Offentliga förvaltningsentiteter som avses i artikel 2.2 f i.

e) Alla andra entiteter av en typ som avses i bilaga I eller II som av en medlemsstat identifierats som väsentliga entiteter i enlighet med artikel 2.2 b–e.

f) Entiteter som identifierats som kritiska entiteter enligt direktiv (EU) 2022/2557, som avses i artikel 2.3 i det här direktivet.

g) Entiteter som medlemsstaterna före den 16 januari 2023 har identifierat som leverantörer av samhällsviktiga tjänster i enlighet med direktiv (EU) 2016/1148 eller nationell rätt, om så föreskrivs av medlemsstaten.

2. Vid tillämpningen av detta direktiv ska alla entiteter av en typ som avses i bilaga I eller II och som inte betraktas som väsentliga entiteter enligt punkt 1 i denna artikel betraktas som viktiga entiteter. Detta inkluderar entiteter som av en medlemsstat identifierats som viktiga entiteter i enlighet med artikel 2.2 b–e.

3. Senast den 17 april 2025 ska medlemsstaterna upprätta en förteckning över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster. Medlemsstaterna ska regelbundet och minst vartannat år därefter se över förteckningen och när det är lämpligt uppdatera den.

4. Vid upprättandet av den förteckning som avses i punkt 3 ska medlemsstaterna ålägga de entiteter som avses i den punkten att lämna minst följande information till de behöriga myndigheterna:

a) Entitetens namn.

b) Adress och aktuella kontaktuppgifter, inklusive e-postadresser, IP-adresser och telefonnummer.

c) I tillämpliga fall, den eller de relevanta sektorer och delsektorer som avses i bilaga I eller II.

d) I tillämpliga fall, en förteckning över de medlemsstater där de tillhandahåller tjänster som omfattas av detta direktiv.

De entiteter som avses i punkt 3 ska meddela alla ändringar av de uppgifter som de lämnat in enligt första stycket i denna punkt utan dröjsmål och under alla omständigheter inom två veckor från datumet för ändringen.

Kommissionen ska, med bistånd från Europeiska unionens cybersäkerhetsbyrå (Enisa), utan onödigt dröjsmål tillhandahålla riktlinjer och mallar för de skyldigheter som fastställs i denna punkt.

Medlemsstaterna får inrätta nationella mekanismer som gör det möjligt för entiteterna att registrera sig själva.

5. Senast den 17 april 2025 och därefter vartannat år ska de behöriga myndigheterna

a) underrätta kommissionen och samarbetsgruppen om antalet väsentliga och viktiga entiteter som förtecknats enligt punkt 3 för varje sektor och delsektor som avses i bilaga I eller II, och

b) lämna relevant information till kommissionen om antalet väsentliga och viktiga entiteter som identifierats i enlighet med artikel 2.2 b–e, den sektor och delsektor som avses i bilaga I eller II som de tillhör, den typ av tjänst som de tillhandahåller och de bestämmelser i artikel 2.2 b–e i enlighet med vilka de identifierades.

6. Fram till den 17 april 2025 och på begäran av kommissionen får medlemsstaterna meddela kommissionen namnen på de väsentliga och viktiga entiteter som avses i punkt 5 b.

Artikel 4

Sektorsspecifika unionsrättsakter

1. Om det i sektorsspecifika unionsrättsakter föreskrivs att väsentliga eller viktiga entiteter ska anta riskhanteringsåtgärder för cybersäkerhet eller underrätta om betydande incidenter, och om dessa krav har minst samma verkan som de skyldigheter som fastställs i detta direktiv, ska de relevanta bestämmelserna i detta direktiv, inbegripet bestämmelserna om tillsyn och efterlevnadskontroll i kapitel VII, inte tillämpas på sådana entiteter. Om de sektorsspecifika unionsrättsakterna inte omfattar alla entiteter inom en viss sektor som omfattas av detta direktivs tillämpningsområde, ska de relevanta bestämmelserna i detta direktiv fortsätta att tillämpas på de entiteter som inte omfattas av dessa sektorsspecifika unionsrättsakter.

2. De krav som avses i punkt 1 i denna artikel ska anses ha samma verkan som de skyldigheter som fastställs i detta direktiv om

a) riskhanteringsåtgärderna för cybersäkerhet minst är likvärdiga som de åtgärder som föreskrivs i artikel 21.1 och 21.2, eller

b) respektive sektorsspecifik unionsrättsakt föreskriver omedelbar, och när det är lämpligt automatisk och direkt, tillgång till incidentunderrättelser från CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna enligt detta direktiv och om kraven på underrättelse av betydande incidenter har minst samma verkan som de krav som fastställs i artikel 23.1–23.6 i detta direktiv.

3. Kommissionen ska senast den 17 juli 2023 tillhandahålla riktlinjer som klargör tillämpningen av punkterna 1 och 2. Kommissionen ska regelbundet se över dessa riktlinjer. Vid utarbetandet av dessa riktlinjer ska kommissionen ta hänsyn till eventuella synpunkter från samarbetsgruppen och Enisa.

Artikel 5

Minimiharmonisering

Detta direktiv hindrar inte medlemsstaterna från att anta eller behålla bestämmelser som säkerställer en högre cybersäkerhetsnivå, förutsatt att sådana bestämmelser står i överensstämmelse med medlemsstaternas förpliktelser enligt unionsrätten.

Artikel 6

Definitioner

I detta direktiv gäller följande definitioner:

1. nätverks- och informationssystem:

   a) Ett elektroniskt kommunikationsnät enligt definitionen i artikel 2.1 i direktiv (EU) 2018/1972.

b) En enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter.

c) Digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av leden a och b för att de ska kunna drivas, användas, skyddas och underhållas.

2. *säkerhet i nätverks- och informationssystem*: nätverks- och informationssystems förmåga att med en viss tillförlitlighetsnivå motstå händelser som kan undergräva tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via dessa nätverks- och informationssystem.

3. *cybersäkerhet*: cybersäkerhet enligt definitionen i artikel 2.1 i förordning (EU) 2019/881.

4. *nationell strategi för cybersäkerhet*: en enhetlig ram i en medlemsstat med strategiska mål och prioriteringar på cybersäkerhetsområdet och en styrningsram för att uppnå dem i den medlemsstaten.

5. *tillbud*: en händelse som kunde ha undergrävt tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem, men som framgångsrikt hindrades från att utvecklas eller som inte uppstod.

6. *incident*: en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem.

7. *storskalig cybersäkerhetsincident*: en incident som orsakar störningar som är så omfattande att den berörda medlemsstaten inte kan hantera dem eller som har en betydande påverkan på minst två medlemsstater.

8. *incidenthantering*: alla åtgärder och förfaranden som syftar till att förebygga, upptäcka, analysera, begränsa eller reagera på och återhämta sig från en incident.

9. *risk*: 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 en sådan incident inträffar.

10. *cyberhot*: ett cyberhot enligt definitionen i artikel 2.8 i förordning (EU) 2019/881.

11. *betydande cyberhot*: ett cyberhot som, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på en entitets nätverks- och informationssystem eller användarna av entitetens tjänster genom att vålla betydande materiell eller immateriell skada.

12. *IKT-produkt*: en IKT-produkt enligt definitionen i artikel 2.12 i förordning (EU) 2019/881.

13. *IKT-tjänst*: en IKT-tjänst enligt definitionen i artikel 2.13 i förordning (EU) 2019/881.

14. *IKT-process*: en IKT-process enligt definitionen i artikel 2.14 i förordning (EU) 2019/881.

15. *sårbarhet*: en svaghet, känslighet eller brist hos IKT-produkter eller IKT-tjänster som kan utnyttjas genom ett cyberhot.

16. *standard*: en standard enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 1025/2012 ([29]).

17. *teknisk specifikation*: en teknisk specifikation enligt definitionen i artikel 2.4 i förordning (EU) nr 1025/2012.

([29]) 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 (EUT L 316, 14.11.2012, s. 12).

18. *internetknutpunkt*: en nätfacilitet som möjliggör sammankoppling av mer än två oberoende nät (autonoma system), främst i syfte att underlätta utbytet av internettrafik, som tillhandahåller sammankoppling enbart för autonoma system och som varken kräver att den internettrafik som passerar mellan två deltagande autonoma system ska passera genom ett tredje autonomt system eller ändrar trafiken eller påverkar den på något annat sätt.

19. *domännamnssystem* eller *DNS*: ett hierarkiskt distribuerat namnsystem som möjliggör identifieringen av tjänster och resurser på internet, vilket gör det möjligt för slutanvändarenheter att använda internetrouting- och internetuppkopplingstjänster för att nå dessa tjänster och resurser.

20. *leverantör av DNS-tjänster*: en entitet som tillhandahåller

    a) allmänna rekursiva tjänster för att lösa domännamnsfrågor till internetslutanvändare, eller

    b) auktoritativa tjänster för att lösa domännamnsfrågor för användning av tredje part, med undantag för rotnamnsservrar.

21. *registreringsenhet för toppdomäner* eller *TLD-registreringsenhet*: en enhet som har delegerats en specifik toppdomän och som ansvarar för administrationen av toppdomänen, inbegripet registreringen av domännamn under toppdomänen och den tekniska driften av toppdomänen, inbegripet drift av dess namnservrar, underhåll av dess databaser och distribution av zonfiler för toppdomänen mellan namnservrar, oberoende av huruvida någon aspekt av denna drift utförs av enheten själv eller har utkontrakterats, dock inte situationer där toppdomäner används av en registreringsenhet endast för dess eget bruk.

22. *entitet som erbjuder domännamnsregistreringstjänster*: en registrar som verkar på uppdrag av en regeringsenhet eller ett ombud för en registreringsenhet, såsom återförsäljare och leverantörer av integritetsregistreringstjänster och proxyregistreringstjänster.

23. *digital tjänst*: en tjänst enligt definitionen i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 ([30]).

24. *betrodd tjänst*: en betrodd tjänst enligt definitionen i artikel 3.16 i förordning (EU) nr 910/2014.

25. *tillhandahållare av betrodda tjänster*: en tillhandahållare av betrodda tjänster enligt definitionen i artikel 3.19 i förordning (EU) nr 910/2014.

26. *kvalificerad betrodd tjänst*: en kvalificerad betrodd tjänst enligt definitionen i artikel 3.17 i förordning (EU) nr 910/2014.

27. *kvalificerad tillhandahållare av betrodda tjänster*: en kvalificerad tillhandahållare av betrodda tjänster enligt definitionen i artikel 3.20 i förordning (EU) nr 910/2014.

28. *marknadsplats online*: en marknadsplats online enligt definitionen i artikel 2 n i Europaparlamentets och rådets direktiv 2005/29/EG ([31]).

29. *sökmotor*: en sökmotor enligt definitionen i artikel 2.5 i Europaparlamentets och rådets förordning (EU) 2019/1150 ([32]).

30. *molntjänst*: en digital tjänst som möjliggör administration på begäran och bred fjärråtkomst till en skalbar och elastisk pool av gemensamma beräkningstjänster, inbegripet när sådana resurser är distribuerade på flera platser.

([30]) Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (EUT L 241, 17.9.2015, s. 1).

([31]) Europaparlamentets och rådets direktiv 2005/29/EG av den 11 maj 2005 om otillbörliga affärsmetoder som tillämpas av näringsidkare gentemot konsumenter på den inre marknaden och om ändring av rådets direktiv 84/450/EEG och Europaparlamentets och rådets direktiv 97/7/EG, 98/27/EG och 2002/65/EG samt Europaparlamentets och rådets förordning (EG) nr 2006/2004 (direktiv om otillbörliga affärsmetoder) (EUT L 149, 11.6.2005, s. 22).

([32]) Europaparlamentets och rådets förordning (EU) 2019/1150 av den 20 juni 2019 om främjande av rättvisa villkor och transparens för företagsanvändare av onlinebaserade förmedlingstjänster (EUT L 186, 11.7.2019, s. 57).

31. *datacentraltjänst*: en tjänst som omfattar strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och dataöverföringstjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll.

32. *nätverk för leverans av innehåll*: ett nätverk av geografiskt spridda servrar vars syfte är att säkerställa hög tillgänglighet för, tillgång till eller snabb leverans av digitalt innehåll och digitala tjänster till internetanvändare för innehålls- och tjänsteleverantörers räkning.

33. *plattform för sociala nätverkstjänster*: en plattform som gör det möjligt för slutanvändare att interagera, dela och upptäcka innehåll, finna andra användare och kommunicera med andra via flera enheter, särskilt genom chattar, inlägg, videor och rekommendationer.

34. *företrädare*: en i unionen etablerad fysisk eller juridisk person som uttryckligen har utsetts att agera för en leverantör av DNS-tjänster, en registreringsenhet för toppdomäner, en entitet som tillhandahåller domännamnsregistreringstjänster, en leverantör av molntjänster, en leverantör av datacentraltjänster, en leverantör av nätverk för leverans av innehåll, driftsentreprenad, en leverantör av hanterade säkerhetstjänster, en leverantör av marknadsplatser online, av sökmotorer eller av en plattform för sociala nätverkstjänster som inte är etablerad i unionen, till vilka en behörig myndighet eller en CSIRT-enhet kan vända sig i stället för entiteten, i frågor som gäller de skyldigheter som den entiteten har enligt detta direktiv.

35. *offentlig förvaltningsentitet*: en entitet som erkänts som sådan i en medlemsstat i enlighet med nationell rätt, med undantag för rättsväsendet, parlament och centralbanker, som uppfyller följande kriterier:

    a) Den har inrättats för att tillgodose behov i det allmännas intresse och har inte industriell eller kommersiell karaktär.

    b) Den har ställning som juridisk person eller har lagstadgad rätt att agera för en annan entitet som har ställning som juridisk person.

    c) Den finansieras till största delen av staten, regionala myndigheter eller andra offentligrättsliga organ, står under administrativ tillsyn av dessa myndigheter eller organ, eller har ett förvaltnings-, lednings- eller kontrollorgan där mer än hälften av ledamöterna utses av staten, regionala myndigheter eller andra offentligrättsliga organ.

    d) Den har befogenhet att rikta administrativa eller reglerande beslut till fysiska eller juridiska personer som påverkar deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital.

36. *allmänt elektroniskt kommunikationsnät*: ett allmänt elektroniskt kommunikationsnät enligt definitionen i artikel 2.8 i direktiv (EU) 2018/1972.

37. *elektronisk kommunikationstjänst*: en elektronisk kommunikationstjänst enligt definitionen i artikel 2.4 i direktiv (EU) 2018/1972.

38. *entitet*: en fysisk eller juridisk person som bildats och erkänts som sådan enligt nationell rätt där den etablerats och som i eget namn får utöva rättigheter och ha skyldigheter.

39. *driftsentreprenad*: en entitet som tillhandahåller tjänster som rör installation, förvaltning, drift eller underhåll av IKT-produkter, IKT-nät, IKT-infrastruktur, IKT-tillämpningar eller andra nätverks- och informationssystem, via bistånd eller aktiv administration antingen i kundernas lokaler eller på distans.

40. *leverantör av hanterade säkerhetstjänster*: en leverantör av hanterade säkerhetstjänster som utför eller tillhandahåller stöd för verksamhet som rör hantering av cybersäkerhetsrisker.

41. *forskningsorganisation*: en entitet vars främsta mål är att bedriva tillämpad forskning eller experimentell utveckling i syfte att utnyttja resultaten av denna forskning i kommersiellt syfte, men som inte inbegriper utbildningsinstitutioner.

KAPITEL II

SAMORDNADE RAMVERK FÖR CYBERSÄKERHET

Artikel 7

Nationell strategi för cybersäkerhet

1. Varje medlemsstat ska anta en nationell strategi för cybersäkerhet som tillhandahåller strategiska mål, de resurser som krävs för att uppnå dessa mål och relevanta politiska och reglerande åtgärder, i syfte att uppnå och upprätthålla en hög cybersäkerhetsnivå. Den nationella strategin för cybersäkerhet ska inbegripa

a) mål och prioriteringar för medlemsstatens strategi för cybersäkerhet som särskilt omfattar de sektorer som avses i bilagorna I och II,

b) en styrningsram för att uppnå de mål och prioriteringar som avses i led a i denna punkt, inbegripet de politiska åtgärder som avses i punkt 2,

c) en styrningsram som klargör roller och ansvarsområden för relevanta intressenter på nationell nivå och som stöder samarbetet och samordningen på nationell nivå mellan de gemensamma myndigheterna, de gemensamma kontaktpunkterna och CSIRT-enheterna enligt detta direktiv, samt samordningen och samarbetet mellan dessa organ och behöriga myndigheter enligt sektorsspecifika unionsrättsakter,

d) en mekanism för att identifiera relevanta tillgångar och en bedömning av riskerna i den medlemsstaten,

e) en identifiering av åtgärder som säkerställer beredskap inför, svar på och återställande efter incidenter, inklusive samarbete mellan offentlig och privat sektor,

f) en förteckning över de olika myndigheter och intressenter som är involverade i genomförandet av den nationella strategin för cybersäkerhet,

g) en politisk ram för förbättrad samordning mellan de behöriga myndigheterna enligt detta direktiv och de behöriga myndigheterna enligt direktiv (EU) 2022/2557, i syfte att utbyta information om risker, cyberhot och incidenter och icke-cyberrelaterade risker, hot och incidenter och utföra tillsynsuppgifter, beroende på vad som är lämpligt,

h) en plan, med nödvändiga åtgärder, för att höja medborgarnas allmänna medvetenhet om cybersäkerhetshot.

2. Som en del av den nationella strategin för cybersäkerhet ska medlemsstaterna särskilt anta följande:

a) Riktlinjer för cybersäkerhet i leveranskedjan för IKT-produkter och IKT-tjänster som används av entiteter när de tillhandahåller sina tjänster.

b) Riktlinjer för att inkludera och specificera cybersäkerhetsrelaterade krav för IKT-produkter och IKT-tjänster vid offentlig upphandling, inbegripet vad gäller cybersäkerhetscertifiering, kryptering och användning av cybersäkerhetsprodukter med öppen källkod.

c) Riktlinjer för hantering av sårbarheter, inbegripet främjande och underlättande av samordnad delgivning av information om sårbarheter enligt artikel 12.1.

d) Riktlinjer för att upprätthålla den allmänna tillgängligheten, integriteten och konfidentialiteten hos den offentliga kärnan i det öppna internet, inbegripet, i tillämpliga fall, cybersäkerheten hos undervattenskablar.

e) Riktlinjer för att främja utveckling och integrering av relevant avancerad teknik som syftar till att genomföra moderna riskhanteringsåtgärder för cybersäkerhet.

f) Riktlinjer för att främja och utveckla cybersäkerhetsutbildning, cybersäkerhetskompetens, medvetandehöjande åtgärder och forsknings- och utvecklingsinitiativ, samt vägledning om god praxis och kontroll för cyberhygien som riktar sig till medborgare, intressenter och entiteter.

g) Riktlinjer för stöd till akademiska institutioner och forskningsinstitut för att utveckla, förbättra och främja användningen av cybersäkerhetsverktyg och säker nätinfrastruktur.

h) Riktlinjer, inbegripet relevanta förfaranden och lämpliga verktyg för informationsutbyte för att stödja ett frivilligt informationsutbyte om cybersäkerhet mellan entiteter i enlighet med unionsrätten.

i) Riktlinjer som stärker cyberresiliensen och cyberhygienen hos små och medelstora företag, särskilt de som inte omfattas av detta direktiv, genom att tillhandahålla lättillgänglig vägledning och stöd för deras specifika behov.

j) Riktlinjer för att främja ett aktivt cyberskydd.

3. Medlemsstaterna ska meddela sina nationella strategier för cybersäkerhet till kommissionen inom tre månader från det att de antagits. Härvid får medlemsstaterna undanta information som rör den nationella säkerheten.

4. Medlemsstaterna ska regelbundet och minst vart femte år bedöma sina nationella strategier för cybersäkerhet på grundval av centrala resultatindikatorer och vid behov uppdatera dem. Enisa ska på medlemsstaternas begäran bistå medlemsstaterna vid utarbetandet eller uppdateringen av en nationell strategi för cybersäkerhet och centrala resultatindikatorer för bedömningen av strategin, i syfte att anpassa den till de krav och skyldigheter som fastställs i detta direktiv.

Artikel 8

Behöriga myndigheter och gemensamma kontaktpunkter

1. Varje medlemsstat ska utse eller inrätta en eller flera behöriga myndigheter med ansvar för cybersäkerhet och för de tillsynsuppgifter som avses i kapitel VII (behöriga myndigheter).

2. De behöriga myndigheter som avses i punkt 1 ska övervaka genomförandet av detta direktiv på nationell nivå.

3. Varje medlemsstat ska utse eller inrätta en gemensam kontaktpunkt. Om en medlemsstat bara utser eller inrättar en behörig myndighet i enlighet med punkt 1, ska denna behöriga myndighet också vara den gemensamma kontaktpunkten i den medlemsstaten.

4. Varje gemensam kontaktpunkt ska utöva en sambandsfunktion som säkerställer ett gränsöverskridande samarbete mellan medlemsstatens myndigheter och relevanta myndigheter i andra medlemsstater och, när det är lämpligt, kommissionen och Enisa samt ett sektorsövergripande samarbete med andra behöriga myndigheter i medlemsstaten.

5. Medlemsstaterna ska säkerställa att deras behöriga myndigheter och gemensamma kontaktpunkter har tillräckliga resurser för att på ett ändamålsenligt och effektivt sätt utföra de uppgifter de tilldelas och därigenom uppnå målen med detta direktiv.

6. Varje medlemsstat ska utan onödigt dröjsmål meddela kommissionen identiteten för den behöriga myndighet som avses i punkt 1 och den gemensamma kontaktpunkt som avses i punkt 3, dessa myndigheters uppgifter samt eventuella senare ändringar. Varje medlemsstat ska offentliggöra sin behöriga myndighets identitet. Kommissionen ska upprätta en förteckning över offentligt tillgängliga gemensamma kontaktpunkter.

Artikel 9

Nationella ramar för hantering av cybersäkerhetskriser

1. Varje medlemsstat ska utse eller inrätta en eller flera behöriga myndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser (cyberkrishanteringsmyndigheter). Medlemsstaterna ska säkerställa att dessa myndigheter har tillräckliga resurser för att kunna utföra sina uppgifter på ett ändamålsenligt och effektivt sätt. Medlemsstaterna ska säkerställa samstämmighet med befintliga ramar för allmän nationell krishantering.

2. Om en medlemsstat utser eller inrättar mer än en cyberkrishanteringsmyndighet enligt punkt 1 ska den tydligt ange vilken av dessa myndigheter som ska samordna hanteringen av storskaliga cybersäkerhetsincidenter och kriser.

3. För tillämpning av detta direktiv ska varje medlemsstat identifiera vilka kapaciteter, tillgångar och förfaranden som kan användas i händelse av en kris.

4. Varje medlemsstat ska anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser där mål och villkor för hanteringen av storskaliga cybersäkerhetsincidenter och kriser fastställs. Planen ska särskilt innehålla följande:

a) Målen för nationella beredskapsåtgärder och beredskapsverksamheter.

b) Cyberkrishanteringsmyndigheternas uppgifter och ansvarsområden.

c) Cyberkrishanteringsförfaranden, inbegripet deras integrering i den allmänna nationella ramen för krishantering och kanaler för informationsutbyte.

d) Nationella beredskapsåtgärder, inbegripet övningar och utbildningsverksamhet.

e) Berörda offentliga och privata intressenter och berörd infrastruktur.

f) Nationella förfaranden och arrangemang mellan relevanta nationella myndigheter och organ för att säkerställa att medlemsstaten på ett ändamålsenligt sätt kan delta i och stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och kriser på unionsnivå.

5. Inom tre månader från det att den cyberkrishanteringsmyndighet som avses i punkt 1 har utsetts eller inrättats ska varje medlemsstat meddela kommissionen sin myndighets identitet samt alla senare ändringar. Medlemsstaterna ska till kommissionen och Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) lämna relevant information avseende kraven i punkt 4 om sina nationella planer för hanteringen av storskaliga cybersäkerhetsincidenter och kriser inom tre månader från det att dessa planer antagits. Medlemsstaterna får undanta information om och i den utsträckning det är nödvändigt för den nationella säkerheten.

Artikel 10

Enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter)

1. Varje medlemsstat ska utse eller inrätta en eller flera CSIRT-enheter. CSIRT-enheterna får utses eller inrättas inom en behörig myndighet. CSIRT-enheterna ska uppfylla kraven i artikel 11.1, ska omfatta minst de sektorer, delsektorer och typer av entiteter som avses i bilagorna I och II och ska ansvara för incidenthantering i enlighet med ett tydligt fastställt förfarande.

2. Medlemsstaterna ska säkerställa att varje CSIRT-enhet har tillräckliga resurser för att på ett ändamålsenligt sätt kunna utföra sina uppgifter enligt artikel 11.3.

3. Medlemsstaterna ska säkerställa att varje CSIRT-enhet har tillgång till en lämplig, säker och motståndskraftig kommunikations- och informationsinfrastruktur för utbyte av information med väsentliga och viktiga entiteter och andra relevanta intressenter. För detta ändamål ska medlemsstaterna säkerställa att varje CSIRT-enhet bidrar till införandet av säkra verktyg för informationsutbyte.

4. CSIRT-enheterna ska samarbeta och, när det är lämpligt, utbyta relevant information i enlighet med artikel 29 med sektoriella eller sektorsövergripande grupper av väsentliga och viktiga entiteter.

5. CSIRT-enheterna ska delta i sakkunnigbedömningar som organiseras i enlighet med artikel 19.

6. Medlemsstaterna ska säkerställa ett ändamålsenligt, effektivt och säkert samarbete mellan sina CSIRT-enheter i CSIRT-nätverket.

7. CSIRT-enheter får upprätta samarbetsförbindelser med tredjeländers nationella enheter för hantering av it-säkerhetsincidenter. Som en del av sådana samarbetsförbindelser ska medlemsstaterna underlätta ett ändamålsenligt, effektivt och säkert informationsutbyte med dessa nationella enheter för hantering av it-säkerhetsincidenter i tredjeländer, med hjälp av relevanta protokoll för informationsutbyte, inbegripet Traffic Light Protocol. CSIRT-enheter får utbyta relevant information med tredjeländers nationella enheter för hantering av it-säkerhetsincidenter, inbegripet personuppgifter i enlighet med unionens dataskyddslagstiftning.

8. CSIRT-enheter får samarbeta med tredjeländers nationella enheter för hantering av it-säkerhetsincidenter eller motsvarande organ i tredjeländer, särskilt i syfte att ge dem cybersäkerhetsstöd.

9. Varje medlemsstat ska utan onödigt dröjsmål meddela kommissionen identiteten för den CSIRT-enhet som avses i punkt 1 i denna artikel och för den CSIRT-enhet som utsetts till samordnare i enlighet med artikel 12.1, deras respektive uppgifter i förhållande till de väsentliga och viktiga entiteterna samt alla senare ändringar.

10. Medlemsstaterna får begära Enisas bistånd vid inrättandet av sina CSIRT-enheter.

Artikel 11

Krav på CSIRT-enheter och deras tekniska kapacitet och uppgifter

1. CSIRT-enheter ska uppfylla följande krav:

a) CSIRT-enheterna ska säkerställa en hög nivå av tillgänglighet för sina kommunikationskanaler genom att undvika felkritiska systemdelar och ska kunna kontaktas och kontakta andra när som helst och på flera olika sätt. De ska tydligt ange kommunikationskanalerna och underrätta användargrupper och samarbetspartner om dessa.

b) CSIRT-enheternas lokaler och de informationssystem som de använder sig av ska vara belägna på säkra platser.

c) CSIRT-enheterna ska ha ett ändamålsenligt system för handläggning och dirigering av förfrågningar, särskilt för att underlätta ändamålsenliga och effektiva överlämnanden.

d) CSIRT-enheterna ska säkerställa verksamhetens konfidentialitet och trovärdighet.

e) CSIRT-enheterna ska ha tillräckligt med personal för att säkerställa att deras tjänster är ständigt tillgängliga och de ska säkerställa att personalen har fått lämplig utbildning.

f) CSIRT-enheterna ska utrustas med redundanta system och reservlokaler för att säkerställa kontinuiteten i deras tjänster.

De ska kunna delta i internationella samarbetsnätverk.

2. Medlemsstaterna ska säkerställa att deras CSIRT-enheter tillsammans har nödvändig teknisk kapacitet för att utföra de uppgifter som avses i punkt 3. Medlemsstaterna ska säkerställa att tillräckliga resurser anslås till deras CSIRT-enheter för att säkerställa en tillräcklig personalstyrka för att göra det möjligt för CSIRT-enheterna att utveckla sin tekniska kapacitet.

3. CSIRT-enheterna ska ha följande uppgifter:

a) Övervakning och analys av cyberhot, sårbarheter och incidenter på nationell nivå och, på begäran, tillhandahållande av stöd till berörda väsentliga och viktiga entiteter avseende realtidsövervakning eller nära realtidsövervakning av deras nätverks- och informationssystem.

b) Tillhandahållande av tidiga varningar, larm, meddelanden och spridning av information till väsentliga och viktiga entiteter samt till behöriga myndigheter och andra relevanta intressenter om cyberhot, sårbarheter och incidenter, om möjligt i nära realtid.

c) Vidtagande av åtgärder till följd av incidenter och, i tillämpliga fall, tillhandahållande av stöd till de berörda väsentliga och viktiga entiteterna.

d) Insamling och analys av forensiska uppgifter och tillhandahållande av dynamisk risk- och incidentanalys och situationsmedvetenhet när det gäller cybersäkerhet.

e) Tillhandahållande, på begäran av den väsentliga eller viktiga entiteten, av en proaktiv skanning av den berörda entitetens nätverks- och informationssystem i syfte att upptäcka sårbarheter med en potentiellt betydande påverkan.

f) Deltagande i CSIRT-nätverket och ömsesidigt bistånd i enlighet med deras kapacitet och befogenheter till andra medlemmar i CSIRT-nätverket på deras begäran.

g) I tillämpliga fall, fungera som processamordnare för den samordnade delgivningen av information om sårbarheter enligt artikel 12.1.

h) Bidrag till införandet av säkra verktyg för informationsutbyte enligt artikel 10.3.

CSIRT-enheterna får utföra en proaktiv, icke-inkräktande skanning av väsentliga och viktiga entiteters allmänt tillgängliga nätverks- och informationssystem. Sådan skanning ska utföras för att upptäcka sårbara eller osäkert konfigurerade nätverks- och informationssystem och informera de berörda enheterna. Sådan skanning får inte ha någon negativ inverkan på hur entiteternas tjänster fungerar.

När CSIRT-enheterna utför de uppgifter som avses i första stycket får de prioritera särskilda uppgifter på grundval av en riskbaserad metod.

4. CSIRT-enheterna ska upprätta samarbetsförbindelser med relevanta intressenter inom den privata sektorn i syfte att uppnå målen för detta direktiv.

5. För att underlätta det samarbete som avses i punkt 4 ska CSIRT-enheterna främja antagande och användning av gemensamma eller standardiserade metoder, klassificeringssystem och taxonomier när det gäller

a) förfaranden för incidenthantering,

b) krishantering, och

c) samordnad delgivning av information om sårbarheter enligt artikel 12.1.

Artikel 12

Samordnad delgivning av information om sårbarheter och en europeisk sårbarhetsdatabas

1. Varje medlemsstat ska utse en av sina CSIRT-enheter till samordnare för den samordnade delgivningen av informationen om sårbarheter. Den CSIRT-enhet som utsetts till samordnare ska fungera som betrodd mellanhand och vid behov underlätta interaktionen mellan en fysisk eller juridisk person som rapporterar en sårbarhet och tillverkaren eller leverantören av de potentiellt sårbara IKT-produkterna eller IKT-tjänsterna, på begäran av endera parten. Den CSIRT-enhet som utsetts till samordnare ska bland annat

a) identifiera och kontakta de berörda entiteterna,

b) stödja de fysiska eller juridiska personer som rapporterar en sårbarhet, och

c) förhandla om tidsramar för delgivning av information och hantera sårbarheter som påverkar flera entiteter.

Medlemsstaterna ska säkerställa att fysiska eller juridiska personer kan, anonymt om de så begär, rapportera en sårbarhet till den CSIRT-enhet som utsetts till samordnare. Den CSIRT-enhet som utsetts till samordnare ska säkerställa att skyndsamma uppföljningsåtgärder vidtas med avseende på den rapporterade sårbarheten och ska säkerställa anonymiteten för den fysiska eller juridiska person som rapporterar sårbarheten. Om en rapporterad sårbarhet kan ha en betydande påverkan på entiteter i fler än en medlemsstat, ska den CSIRT-enhet som utsetts till samordnare i varje berörd medlemsstat, när det är lämpligt, samarbeta med andra CSIRT-enheter som utsetts till samordnare inom CSIRT-nätverket.

2. Enisa ska, efter samråd med samarbetsgruppen, utveckla och underhålla en europeisk sårbarhetsdatabas. I detta syfte ska Enisa inrätta och underhålla lämpliga informationssystem, riktlinjer och förfaranden och anta nödvändiga tekniska och organisatoriska åtgärder för att säkerställa den europeiska sårbarhetsdatabasens säkerhet och integritet, särskilt för att göra det möjligt för entiteter, oberoende om de omfattas av tillämpningsområdet för detta direktiv, och deras leverantörer av nätverks- och informationssystem, att på frivillig basis lämna information om och registrera allmänt kända sårbarheter hos IKT-produkter eller IKT-tjänster. Alla intressenter ska få tillgång till informationen om de sårbarheter som finns i den europeiska sårbarhetsdatabasen. Databasen ska innehålla

a) information som beskriver sårbarheten,

b) den berörda IKT-produkten eller IKT-tjänsten och hur allvarlig sårbarheten är med tanke på de omständigheter under vilka den kan utnyttjas,

c) tillgången till relaterade programfixar och, i avsaknad av tillgängliga programfixar, vägledning som tillhandahållits av behöriga myndigheter eller CSIRT-enheter riktad till användare av sårbara IKT-produkter och IKT-tjänster om hur riskerna med meddelade sårbarheter kan begränsas.

Artikel 13

Samarbete på nationell nivå

1. Om de är separata ska de behöriga myndigheterna, den gemensamma kontaktpunkten och CSIRT-enheterna i en och samma medlemsstat samarbeta sinsemellan när det gäller fullgörandet av skyldigheter enligt detta direktiv.

2. Medlemsstaterna ska säkerställa att deras CSIRT-enheter eller, i tillämpliga fall, deras behöriga myndigheter, mottar underrättelser om betydande incidenter enligt artikel 23, och incidenter, cyberhot och tillbud enligt artikel 30.

3. Medlemsstaterna ska säkerställa att deras CSIRT-enheter eller, i tillämpliga fall, deras behöriga myndigheter informerar sina gemensamma kontaktpunkter om de underrättelser om incidenter, cyberhot och tillbud som lämnas in i enlighet med detta direktiv.

4. För att säkerställa att de behöriga myndigheternas, de gemensamma kontaktpunkternas och CSIRT-enheternas uppgifter och skyldigheter utförs på ett effektivt sätt, ska medlemsstaterna, i den utsträckning det är möjligt, säkerställa ett lämpligt samarbete mellan dessa organ och brottsbekämpande myndigheter, dataskyddsmyndigheter, nationella myndigheter enligt förordningarna (EG) nr 300/2008 och (EU) 2018/1139, tillsynsorganen enligt förordning (EU) nr 910/2014, behöriga myndigheter enligt förordning (EU) 2022/2554, nationella regleringsmyndigheter enligt direktiv (EU) 2018/1972, behöriga myndigheter enligt direktiv (EU) 2022/2557 samt behöriga myndigheter enligt andra sektorsspecifika unionsrättsakter, i den medlemsstaten.

5. Medlemsstaterna ska säkerställa att deras behöriga myndigheter enligt detta direktiv och deras behöriga myndigheter enligt direktiv (EU) 2022/2557 regelbundet samarbetar och utbyter information avseende identifieringen av kritiska entiteter, om risker, cyberhot och incidenter samt icke-cyberrelaterade risker, hot och incidenter som berör väsentliga entiteter som identifierats som kritiska i enlighet med direktiv (EU) 2022/2557, samt om de åtgärder som vidtagits till följd av sådana risker, hot och incidenter. Medlemsstaterna ska också säkerställa att deras behöriga myndigheter enligt detta direktiv och deras behöriga myndigheter enligt förordning (EU) nr 910/2014, förordning (EU) 2022/2554 och direktiv (EU) 2018/1972 regelbundet utbyter relevant information, även när det gäller relevanta incidenter och cyberhot.

6. Medlemsstaterna ska förenkla rapporteringen med tekniska medel för de underrättelser som avses i artiklarna 23 och 30.

KAPITEL III

SAMARBETE PÅ UNIONSNIVÅ OCH PÅ INTERNATIONELL NIVÅ

Artikel 14

Samarbetsgrupp

1. För att stödja och underlätta strategiskt samarbete och informationsutbyte mellan medlemsstaterna samt stärka förtroende och tillit inrättas härmed en samarbetsgrupp.

2. Samarbetsgruppen ska utföra sina uppgifter på grundval av de tvååriga arbetsprogram som avses i punkt 7.

3. Samarbetsgruppen ska bestå av företrädare för medlemsstater, kommissionen och Enisa. Europeiska utrikestjänsten ska delta som observatör i samarbetsgruppens verksamhet. De europeiska tillsynsmyndigheterna och de behöriga myndigheterna i enlighet med förordning (EU) 2022/2554 får delta i samarbetsgruppens verksamhet i enlighet med artikel 47.1 i den förordningen.

När så är lämpligt får samarbetsgruppen bjuda in Europaparlamentet och företrädare för relevanta intressenter att delta i arbetet.

Kommissionen ska tillhandahålla sekretariatet.

4. Samarbetsgruppen ska ha följande uppgifter:

a) Tillhandahålla vägledning till behöriga myndigheter angående införlivande och genomförande av detta direktiv.

b) Tillhandahålla vägledning till behöriga myndigheter angående utarbetande och genomförande av strategier för den samordnade delgivningen av information om sårbarheter som avses i artikel 7.2 c.

c) Utbyte av bästa praxis och information i fråga om genomförandet av detta direktiv, bland annat när det gäller cyberhot, incidenter, sårbarheter, tillbud, initiativ för att öka medvetenheten, utbildning, övningar och kompetens, kapacitetsuppbyggnad, standarder och tekniska specifikationer, samt identifiering av väsentliga och viktiga entiteter i enlighet med artikel 2.2 b–e.

d) Utbyta råd och samarbeta med kommissionen om framväxande politiska initiativ för cybersäkerhet samt om den övergripande förenligheten mellan sektorsspecifika cybersäkerhetskrav.

e) Utbyta råd och samarbeta med kommissionen om utkast till delegerade akter eller genomförandeakter som antas i enlighet med detta direktiv.

f) Utbyta bästa praxis och information med relevanta institutioner, organ och byråer på unionsnivå.

g) Diskutera genomförandet av sektorsspecifika unionsrättsakter som innehåller bestämmelser om cybersäkerhet.

h) När så är lämpligt, diskutera de rapporter från sakkunnigbedömningar som avses i artikel 19.9 samt utarbeta slutsatser och rekommendationer.

i) Genomföra samordnade säkerhetsriskbedömningar av kritiska leveranskedjor i enlighet med artikel 22.1.

j) Diskutera fall av ömsesidigt bistånd, inbegripet erfarenheter och resultat av sådan gränsöverskridande gemensam tillsynsverksamhet som avses i artikel 37.

k) På begäran av en eller flera berörda medlemsstater, diskutera särskilda begäranden om ömsesidigt bistånd som avses i artikel 37.

l) Tillhandahålla strategisk vägledning till CSIRT-nätverket och EU-CyCLONe om specifika framväxande frågor.

m) Utbyta åsikter om politiken för uppföljningsåtgärder efter storskaliga cybersäkerhetsincidenter och kriser på grundval av lärdomarna från CSIRT-nätverket och EU-CyCLONe.

n) Bidra till cybersäkerhetskapaciteten i hela unionen genom att underlätta utbytet av nationella tjänstemän i form av ett kapacitetsuppbyggnadsprogram som inbegriper personal från behöriga myndigheter eller CSIRT-enheter.

o) Anordna regelbundna gemensamma möten med relevanta privata intressenter från hela unionen för att diskutera samarbetsgruppens verksamhet och inhämta synpunkter på framväxande politiska frågor.

p) Diskutera det arbete som utförts i samband med cybersäkerhetsövningar, inbegripet det arbete som utförs av Enisa.

q) Fastställa metoder och organisatoriska aspekter för de sakkunnigbedömningar som avses i artikel 19.1 samt fastställa en självbedömningsmetod för medlemsstaterna i enlighet med artikel 19.5, med bistånd av kommissionen och Enisa, och, i samarbete med kommissionen och Enisa, utarbeta uppförandekoder som ligger till grund för de utsedda cyberssäkerhetsexperternas arbetsmetoder i enlighet med artikel 19.6.

r) Utarbeta rapporter för den översyn som avses i artikel 40 om de erfarenheter som förvärvats på strategisk nivå och från sakkunnigbedömningar.

s) Regelbundet diskutera och genomföra en bedömning av läget när det gäller cyberhot eller cyberincidenter, såsom utpressningsprogram.

Samarbetsgruppen ska överlämna de rapporter som avses i första stycket led r till kommissionen, Europaparlamentet och rådet.

5. Medlemsstaterna ska säkerställa att deras företrädare i samarbetsgruppen samarbetar på ett ändamålsenligt, effektivt och säkert sätt.

6. Samarbetsgruppen får begära en teknisk rapport från CSIRT-nätverket om utvalda frågor.

7. Samarbetsgruppen ska senast den 1 februari 2024 och därefter vartannat år utarbeta ett arbetsprogram för de åtgärder som ska vidtas för att genomföra dess mål och uppgifter.

8. Kommissionen får anta genomförandeakter i vilka de förfaranden som krävs för samarbetsgruppens verksamhet fastställs.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Kommissionen ska utbyta råd och samarbeta med samarbetsgruppen om de utkast till genomförandeakter som avses i första stycket i denna punkt i enlighet med punkt 4 e.

9. Samarbetsgruppen ska regelbundet och under alla omständigheter minst en gång om året sammanträda med den grupp för kritiska entiteters motståndskraft som inrättats enligt direktiv (EU) 2022/2557, för att främja och underlätta strategiskt samarbete och informationsutbyte.

Artikel 15

CSIRT-nätverk

1. För att bidra till utvecklingen av förtroende och tillit och för att främja ett snabbt och ändamålsenligt operativt samarbete mellan medlemsstaterna inrättas härmed ett nätverk för nationella CSIRT-enheter.

2. CSIRT-nätverket ska bestå av företrädare för de CSIRT-enheter som utsetts eller inrättats i enlighet med artikel 10 och incidenthanteringsorganisationen för unionens institutioner, organ och byråer (Cert-EU). Kommissionen ska som observatör delta i CSIRT-nätverket. Enisa ska tillhandahålla sekretariatet och aktivt bidra med stöd till samarbetet mellan CSIRT-enheterna.

3. CSIRT-nätverket ska ha följande uppgifter:

a) Utbyta information om CSIRT-enheternas kapacitet.

b) Underlätta delning, överföring och utbyte av teknik och relevanta åtgärder, strategier, verktyg, processer, bästa praxis och ramar mellan CSIRT-enheterna.

c) Utbyta relevant information om incidenter, tillbud, cyberhot, risker och sårbarheter.

d) Utbyta information med avseende på publikationer och rekommendationer om cybersäkerhet.

e) Säkerställa interoperabilitet när det gäller specifikationer och protokoll för informationsutbyte.

f) På begäran av en medlem av CSIRT-nätverket som potentiellt berörs av en incident, utbyta och diskutera information om den incidenten och relaterade cyberhot, risker och sårbarheter.

g) På begäran av en medlem av CSIRT-nätverket, diskutera och om möjligt genomföra en samordnad åtgärd till följd av en incident som har identifierats inom den medlemsstatens jurisdiktion.

h) Ge medlemsstaterna stöd när det gäller att hantera gränsöverskridande incidenter i enlighet med detta direktiv.

i) Samarbeta och utbyta bästa praxis med och ge stöd till CSIRT-enheter som utsetts till samordnare i enlighet med artikel 12.1 när det gäller hanteringen av samordnad information om sårbarheter som kan ha en betydande påverkan på entiteter i mer än en medlemsstat.

j) Diskutera och identifiera ytterligare former av operativt samarbete, inbegripet när det gäller

   i) kategorier av cyberhot och incidenter,

   ii) tidiga varningar,

   iii) ömsesidigt bistånd,

   iv) principer och metoder för samordning i samband med åtgärder mot gränsöverskridande risker och incidenter,

   v) bidrag till den nationella plan för hantering av storskaliga cybersäkerhetsincidenter och kriser som avses i artikel 9.4 på begäran av en medlemsstat.

k) Informera samarbetsgruppen om sin verksamhet och om ytterligare former av operativt samarbete som diskuteras enligt led j och vid behov begära vägledning i detta avseende.

l) Utvärdera cybersäkerhetsövningar, bland annat sådana som anordnas av Enisa.

m) På begäran av en enskild CSIRT-enhet diskutera den enhetens kapacitet och beredskap.

n) Samarbeta och utbyta information med säkerhetscentrum (SOC) på regional nivå och unionsnivå, för att förbättra den gemensamma situationsmedvetenheten om incidenter och cyberhot i hela unionen.

o) När så är lämpligt, diskutera de rapporter från sakkunnigbedömningar som avses i artikel 19.9.

p) Tillhandahålla riktlinjer för att underlätta en mer enhetlig operativ praxis när det gäller tillämpningen av bestämmelserna i denna artikel om operativt samarbete.

4. CSIRT-nätverket ska senast den 17 januari 2025 och därefter vartannat år, i samband med den översyn som avses i artikel 40, bedöma de framsteg som gjorts när det gäller det operativa samarbetet och anta en rapport. Rapporten ska särskilt innehålla slutsatser och rekommendationer om resultaten av de sakkunnigbedömningar som avses i artikel 19, som utförs med avseende på de nationella CSIRT-enheterna. Rapporten ska lämnas till samarbetsgruppen.

5. CSIRT-nätverket ska anta sin arbetsordning.

6. CSIRT-nätverket och EU-CyCLONe ska komma överens om förfaranden och samarbeta på grundval av dessa.

Artikel 16

Det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe)

1. EU-CyCLONe inrättas för att stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och kriser på operativ nivå och säkerställa ett regelbundet utbyte av relevant information mellan medlemsstaterna och unionens institutioner, organ och byråer.

2. EU-CyCLONe ska bestå av företrädare för medlemsstaternas myndigheter för hantering av cyberkriser samt, i fall där en potentiell eller pågående storskalig cybersäkerhetsincident har eller sannolikt kommer att ha en betydande påverkan på tjänster och verksamhet som omfattas av detta direktiv, kommissionen. I andra fall ska kommissionen delta som observatör i arbetet inom EU-CyCLONe.

Enisa ska tillhandahålla EU-CyCLONes sekretariat och stödja ett säkert informationsutbyte samt tillhandahålla nödvändiga verktyg för att stödja samarbete mellan medlemsstaterna så att ett säkert informationsutbyte säkerställs.

När så är lämpligt får EU-CyCLONe bjuda in företrädare för relevanta intressenter att delta i arbetet som observatörer.

3. EU-CyCLONe ska ha följande uppgifter:

a) Öka beredskapen för hantering av storskaliga cybersäkerhetsincidenter och kriser.

b) Utveckla en gemensam situationsmedvetenhet om storskaliga cybersäkerhetsincidenter och kriser.

c) Bedöma konsekvenserna och effekterna av relevanta storskaliga cybersäkerhetsincidenter och kriser och föreslå möjliga begränsningsåtgärder.

d) Samordna hanteringen av storskaliga cybersäkerhetsincidenter och kriser och ge stöd till beslutsfattande på politisk nivå i samband med sådana incidenter och kriser.

e) På begäran av en berörd medlemsstat, diskutera de nationella planer för hantering av storskaliga nationella cybersäkerhetsincidenter och kriser som avses i artikel 9.4.

4. EU-CyCLONe ska anta sin arbetsordning.

5. EU-CyCLONe ska regelbundet rapportera till samarbetsgruppen om hanteringen av storskaliga cybersäkerhetsincidenter och kriser, samt om trender, med särskild inriktning på deras inverkan på väsentliga och viktiga entiteter.

6. EU-CyCLONe ska samarbeta med CSIRT-nätverket på grundval av överenskomna förfaranden i enlighet med artikel 15.6.

7. Senast den 17 juli 2024 och därefter var 18:e månad ska EU-CyCLONe lägga fram en rapport för Europaparlamentet och rådet med en bedömning av sitt arbete.

Artikel 17

Internationellt samarbete

Unionen får, när det är lämpligt, ingå internationella avtal, i enlighet med artikel 218 i EUF-fördraget, med tredjeländer eller internationella organisationer, och därvid tillåta och organisera deras deltagande i vissa av samarbetsgruppens, CSIRT-nätverkets och EU-CyCLONes verksamheter. Sådana avtal ska vara förenliga med unionens dataskyddslagstiftning.

Artikel 18

Rapport om cybersäkerhetssituationen i unionen

1. Enisa ska, i samarbete med kommissionen och samarbetsgruppen, vartannat år anta en rapport om cybersäkerhetssituationen i unionen samt lämna in den till och lägga fram den för Europaparlamentet. Rapporten ska, bland annat, göras tillgänglig i maskinläsbart format och innehålla följande:

a) En riskbedömning av cybersäkerheten på unionsnivå, med beaktande av cyberhotbilden.

b) En bedömning av utvecklingen av cybersäkerhetskapaciteten i den offentliga och privata sektorn i hela unionen.

c) En bedömning av den allmänna nivån av cybersäkerhetsmedvetenhet och cyberhygien bland medborgare och entiteter, inbegripet små och medelstora företag.

d) En aggregerad bedömning av resultaten av de sakkunnigbedömningar som avses i artikel 19.

e) En aggregerad bedömning av nivån på cybersäkerhetskapaciteten och cybersäkerhetsresurserna i hela unionen, inbegripet på sektorsnivå, samt av i vilken utsträckning medlemsstaternas nationella cybersäkerhetsstrategier är anpassade till varandra.

2. Rapporten ska innehålla särskilda politiska rekommendationer, i syfte att åtgärda brister och höja cybersäkerhetsnivån i hela unionen, och en sammanfattning av resultaten för den aktuella perioden från de tekniska lägesrapporter om cybersäkerheten i EU som Enisa utarbetat i enlighet med artikel 7.6 i förordning (EU) 2019/881.

3. Enisa ska, i samarbete med kommissionen, samarbetsgruppen och CSIRT-nätverket, utarbeta metoderna, bland annat de relevanta variablerna, såsom kvalitativa och kvantitativa indikatorer, för den aggregerade bedömning som avses i punkt 1 e.

Artikel 19

Sakkunnigbedömningar

1. Samarbetsgruppen ska med bistånd av kommissionen och Enisa och, i relevanta fall, av CSIRT-nätverket, och senast den 17 januari 2025, fastställa metoden för och de organisatoriska aspekterna av sakkunnigbedömningar i syfte att dra lärdom av delade erfarenheter, stärka det ömsesidiga förtroendet, uppnå en hög gemensam cybersäkerhetsnivå samt stärka medlemsstaternas nödvändiga cybersäkerhetskapacitet och cybersäkerhetsriktlinjer för att genomföra detta direktiv. Deltagandet i sakkunnigbedömningar är frivilligt. Sakkunnigbedömningarna ska utföras av cybersäkerhetsexperter. Experterna för cybersäkerhet ska utses av minst två medlemsstater, andra än den medlemsstat som granskas.

Sakkunnigbedömningarna ska omfatta åtminstone ett av följande:

a) Genomförandenivån för de riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter som fastställs i artiklarna 21 och 23.

b) Kapacitetsnivån, inbegripet tillgängliga ekonomiska, tekniska och mänskliga resurser, och effektiviteten i de behöriga myndigheternas arbete.

c) CSIRT-enheternas operativa kapacitet.

d) Genomförandenivån för det ömsesidiga bistånd som avses i artikel 37.

e) Genomförandenivån för de arrangemang för informationsutbyte om cybersäkerhet som avses i artikel 29.

f) Särskilda frågor av gränsöverskridande eller sektorsövergripande karaktär.

2. Den metod som avses i punkt 1 ska innefatta objektiva, icke-diskriminerande, rättvisa och transparenta kriterier på grundval av vilka medlemsstaterna utser de cybersäkerhetsexperter som ska få utföra sakkunnigbedömningarna. Kommissionen och Enisa ska delta som observatörer i sakkunnigbedömningarna.

3. Medlemsstaterna får identifiera sådana särskilda frågor som avses i punkt 1 f, med avseende på en sakkunnigbedömning.

4. Innan en sakkunnigbedömning som avses i punkt 1 inleds ska medlemsstaterna meddela de deltagande medlemsstaterna omfattningen av sakkunnigbedömningen, inbegripet de särskilda frågor som identifierats i enlighet med punkt 3.

5. Innan sakkunnigbedömningen inleds får medlemsstaterna genomföra en självbedömning av de granskade aspekterna och tillhandahålla denna självbedömning till de utsedda experterna för cybersäkerhet. Samarbetsgruppen ska, med bistånd av kommissionen och Enisa, fastställa metoden för medlemsstaternas självbedömning.

6. Sakkunnigbedömningar ska inbegripa fysiska eller virtuella besök på plats och distansbaserade informationsutbyten. Med hänsyn till principen om gott samarbete ska den medlemsstat som är föremål för sakkunnigbedömningen förse de utsedda cybersäkerhetsexperterna med den information som krävs för bedömningen, utan att det påverkar unionsrätten eller nationell rätt om skydd av konfidentiella eller säkerhetsskyddsklassificerade uppgifter samt skyddet av väsentliga statliga funktioner, såsom nationell säkerhet. Samarbetsgruppen ska, i samarbete med kommissionen och Enisa, utarbeta lämpliga uppförandekoder till stöd för de utsedda cybersäkerhetsexperternas arbetsmetoder. All information som erhålls genom sakkunnigbedömningen får endast användas för dess ändamål. De cybersäkerhetsexperter som deltar i sakkunnigbedömningen får inte lämna ut känslig eller konfidentiell information som erhållits under sakkunnigbedömningen till någon tredje part.

7. När aspekter har varit föremål för en sakkunnigbedömning i en medlemsstat ska de inte bli föremål för ytterligare sakkunnigbedömning i den medlemsstaten under de två år som följer på slutförandet av sakkunnigbedömningen, om inte annat begärs av medlemsstaten eller beslutas efter ett förslag från samarbetsgruppen.

8. Medlemsstaterna ska säkerställa att de andra medlemsstaterna, samarbetsgruppen, kommissionen och Enisa får information om alla risker för intressekonflikter som rör utsedda cybersäkerhetsexperter innan sakkunnigbedömningen inleds. Den medlemsstat som är föremål för sakkunnigbedömningen får invända mot utnämningen av särskilda cybersäkerhetsexperter av vederbörligen motiverade skäl som meddelas den medlemsstat som utser dessa.

9. Cybersäkerhetsexperter som deltar i sakkunnigbedömningar ska utarbeta rapporter om resultat och slutsatser av dessa. De medlemsstater som är föremål för en sakkunnigbedömning får lämna synpunkter på de utkast till rapporter som berör dem och sådana synpunkter ska bifogas rapporterna. Rapporterna ska innefatta rekommendationer som möjliggör förbättringar när det gäller de aspekter som ingår i sakkunnigbedömningen. Rapporterna ska i relevanta fall överlämnas till samarbetsgruppen och CSIRT-nätverket. En medlemsstat som är föremål för sakkunnigbedömningen får besluta att offentliggöra sin rapport eller en redigerad version av den.

KAPITEL IV

ÅTGÄRDER FÖR RISKHANTERING OCH RAPPORTERINGSKRAV FÖR CYBERSÄKERHET

Artikel 20

Styrning

1. Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteters ledningsorgan godkänner de riskhanteringsåtgärder för cybersäkerhet som dessa entiteter vidtar för att följa artikel 21, övervakar genomförandet av dem och kan ställas till svars för entiteternas överträdelser av den artikeln.

Tillämpningen av denna punkt påverkar inte nationell rätt när det gäller de ansvarsregler som är tillämpliga på offentliga institutioner, samt ansvaret för statligt anställda och valda eller utnämnda tjänstepersoner.

2. Medlemsstaterna ska säkerställa att medlemmarna i väsentliga och viktiga entiteters ledningsorgan är skyldiga att genomgå utbildning, och ska uppmuntra väsentliga och viktiga entiteter att regelbundet erbjuda liknande utbildning till sina anställda för att de ska få tillräckligt med kunskap och kompetens för att kunna identifiera risker och bedöma riskhanteringspraxis för cybersäkerhet och deras inverkan på de tjänster som tillhandahålls av entiteten.

Artikel 21

Riskhanteringsåtgärder för cybersäkerhet

1. Medlemsstaterna ska säkerställa att väsentliga och viktiga 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 och för att förhindra eller minimera incidenters påverkan på mottagarna av deras tjänster och på andra tjänster.

Med beaktande av de senaste, och i tillämpliga fall, relevanta europeiska och internationella standarder samt genomförandekostnaderna, ska de åtgärder som avses i första stycket säkerställa en nivå på säkerheten i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken. Vid bedömningen av dessa åtgärders proportionalitet ska vederbörlig hänsyn tas till entitetens grad av riskexponering, entitetens storlek samt sannolikheten för att incidenter inträffar och deras allvarlighetsgrad, inbegripet deras samhälleliga och ekonomiska konsekvenser.

2. De åtgärder som avses i punkt 1 ska baseras på en allriskansats som syftar till att skydda nätverks- och informationssystem och dessa systems fysiska miljö från incidenter, och ska minst inbegripa

a) strategier för riskanalys och informationssystemens säkerhet,

b) incidenthantering,

c) driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering, och krishantering,

d) säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje entitet och dess direkta leverantörer eller tjänsteleverantörer,

e) säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av sårbarheter och sårbarhetsinformation,

f) strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet,

g) grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,

h) strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering,

i) personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning,

j) användning inom entiteten, när så är lämpligt, av lösningar för multifaktorautentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem.

3. Medlemsstaterna ska säkerställa att entiteter, när de överväger lämpliga åtgärder enligt punkt 2 d i denna artikel, beaktar de sårbarheter som är specifika för varje direktleverantör och tjänsteleverantör och den övergripande kvaliteten på deras leverantörers och tjänsteleverantörers produkter och cybersäkerhetspraxis, inbegripet deras förfaranden för säker utveckling. Medlemsstaterna ska också säkerställa att entiteter, när de överväger lämpliga åtgärder enligt den punkten är skyldiga att beakta resultatet av de samordnade säkerhetsriskbedömningar av kritiska leveranskedjor som utförs i enlighet med artikel 22.1.

4. Medlemsstaterna ska säkerställa att en entitet som finner att den inte följer de åtgärder som föreskrivs i punkt 2 utan onödigt dröjsmål vidtar alla nödvändiga, lämpliga och proportionella korrigerande åtgärder.

5. Senast den 17 oktober 2024 ska kommissionen anta genomförandeakter för att fastställa de tekniska och metodologiska specifikationerna för de åtgärder som avses i punkt 2 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 hanterade tjänster, leverantörer av hanterade säkerhetstjänster, leverantörer av marknadsplatser online, sökmotorer och för plattformar för sociala nätverkstjänster samt kvalificerade tillhandahållare av betrodda tjänster.

Kommissionen får anta genomförandeakter för att fastställa tekniska och metodologiska krav samt, vid behov, sektorskrav för de åtgärder som avses i punkt 2 med avseende på andra väsentliga och viktiga entiteter än de som avses i första stycket i denna punkt.

När kommissionen utarbetar de genomförandeakter som avses i första och andra stycket i denna punkt ska den i största möjliga utsträckning följa europeiska och internationella standarder samt relevanta tekniska specifikationer. Kommissionen ska utbyta råd och samarbeta med samarbetsgruppen och Enisa om de utkast till genomförandeakter som avses i artikel 14.4 e.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Artikel 22

Samordnade säkerhetsriskbedömningar på unionsnivå av kritiska leveranskedjor

1. Samarbetsgruppen får, i samarbete med kommissionen och Enisa, utföra samordnade säkerhetsriskbedömningar av specifika kritiska leveranskedjor för IKT-tjänster, IKT-system eller IKT-produkter, med beaktande av tekniska och, i relevanta fall, icke-tekniska riskfaktorer.

2. Kommissionen ska, efter samråd med samarbetsgruppen och Enisa och, vid behov, relevanta intressenter, identifiera de specifika kritiska IKT-tjänster, IKT-system eller IKT-produkter som kan bli föremål för den samordnade säkerhetsrisk-bedömning som avses i punkt 1.

Artikel 23

Rapporteringsskyldigheter

1. Varje medlemsstat ska säkerställa att väsentliga och viktiga entiteter utan onödigt dröjsmål underrättar sin CSIRT-enhet eller, i tillämpliga fall, sin behöriga myndighet i enlighet med punkt 4 om alla incidenter som har en betydande inverkan på tillhandahållandet av deras tjänster enligt punkt 3 (betydande incident). När så är lämpligt ska berörda entiteter utan onödigt dröjsmål underrätta mottagarna av deras tjänster om betydande incidenter som sannolikt inverkar negativt på tillhandahållandet av de tjänsterna. Varje medlemsstat ska säkerställa att dessa entiteter bland annat rapporterar information som gör det möjligt för CSIRT-enheten eller, i tillämpliga fall, den behöriga myndigheten att fastställa incidentens eventuella gränsöverskridande verkningar. Själva underrättelsen ska inte medföra ökat ansvar för den underrättande entiteten.

Om de berörda entiteterna underrättar den behöriga myndigheten om en betydande incident enligt första stycket ska medlemsstaten säkerställa att den behöriga myndigheten vidarebefordrar underrättelsen till CSIRT-enheten vid mottagandet.

Vid en gränsöverskridande eller sektorsövergripande betydande incident ska medlemsstaterna säkerställa att deras gemensamma kontaktpunkter i god tid förses med relevant information som meddelats i enlighet med punkt 4.

2. I tillämpliga fall ska medlemsstaterna säkerställa att väsentliga och viktiga entiteter utan onödigt dröjsmål underrättar de mottagare av deras tjänster som kan påverkas av ett betydande cyberhot om eventuella åtgärder eller avhjälpande arrangemang som dessa mottagare kan vidta som svar på hotet. När så är lämpligt ska entiteterna också informera dessa mottagare om själva det betydande cyberhotet.

3. En incident ska anses vara betydande om

a) den har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för den berörda entiteten,

b) den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

4. När det gäller det underrättelseförfarande som avses i punkt 1 ska medlemsstaterna säkerställa att de berörda entiteterna lämnar följande till CSIRT-enheten eller, i tillämpliga fall, den behöriga myndigheten:

a) Utan onödigt dröjsmål och under alla omständigheter inom 24 timmar efter att ha fått kännedom om den betydande incidenten, en tidig varning som i tillämpliga fall ska ange om den betydande incidenten misstänks ha orsakats av olagliga eller avsiktligt skadliga handlingar eller kan ha gränsöverskridande verkningar.

b) Utan onödigt dröjsmål och under alla omständigheter inom 72 timmar efter att ha fått kännedom om den betydande incidenten, en incidentanmälan som, i tillämpliga fall, ska uppdatera den information som avses i led a och ange en inledande bedömning av den betydande incidenten, dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer.

c) På begäran av en CSIRT-enhet eller, i tillämpliga fall, den behöriga myndigheten, en delrapport om relevanta statusuppdateringar.

d) Senast en månad efter inlämningen av den incidentanmälan som avses i led b, en slutrapport som ska innehålla 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 begränsande åtgärder.

   iv) I tillämpliga fall, incidentens gränsöverskridande verkningar.

e) I händelse av en pågående incident vid tidpunkten för inlämnandet av den slutrapport som avses i led d ska medlemsstaterna säkerställa att de berörda entiteterna tillhandahåller en lägesrapport vid den tidpunkten och en slutrapport inom en månad efter det att de hanterat incidenten.

Genom undantag från första stycket b ska en tillhandahållare av betrodda tjänster, när det gäller betydande incidenter som påverkar tillhandahållandet av de betrodda tjänsterna, utan onödigt dröjsmål och under alla omständigheter inom 24 timmar efter att ha fått kännedom om den betydande incidenten, underrätta CSIRT-enheten eller, i tillämpliga fall, den behöriga myndigheten.

5. CSIRT-enheten eller den behöriga myndigheten ska utan onödigt dröjsmål och om möjligt inom 24 timmar från mottagandet av den tidiga varning som avses i punkt 4 a lämna ett svar till den underrättande entiteten, inbegripet initial återkoppling om den betydande incidenten och, på entitetens begäran, vägledning eller operativa råd om genomförandet av möjliga begränsande åtgärder. Om CSIRT-enheten inte är den ursprungliga mottagaren av den underrättelse som avses i punkt 1 ska vägledningen tillhandahållas av den behöriga myndigheten i samarbete med CSIRT-enheten. CSIRT-enheten ska tillhandahålla ytterligare tekniskt stöd om den berörda entiteten begär det. Om den betydande incidenten misstänks vara av brottslig art ska CSIRT-enheten eller den behöriga myndigheten också tillhandahålla vägledning om rapporteringen av den betydande incidenten till de brottsbekämpande myndigheterna.

6. När så är lämpligt, och särskilt om den betydande incidenten berör två eller flera medlemsstater, ska CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten utan onödigt dröjsmål informera andra berörda medlemsstater och Enisa om den betydande incidenten. Sådan information ska åtminstone inbegripa den typ av information som mottagits i enlighet med punkt 4. Därvid ska CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten, i enlighet med unionsrätten eller nationell rätt, bevara entitetens säkerhets- och affärsintressen samt den tillhandahållna informationens konfidentialitet.

7. Om allmänhetens medvetenhet är nödvändig för att förhindra en betydande incident eller för att hantera en pågående betydande incident, eller om information om den betydande incidenten på annat sätt ligger i allmänhetens intresse, får en medlemsstats CSIRT-enhet eller, i tillämpliga fall, dess behöriga myndighet och, om det är lämpligt, CSIRT-enheterna eller de behöriga myndigheterna i andra berörda medlemsstater, efter samråd med den berörda entiteten, informera allmänheten om den betydande incidenten eller ålägga entiteten att göra detta.

8. På begäran av CSIRT-enheten eller den behöriga myndigheten ska den gemensamma kontaktpunkten vidarebefordra underrättelser som mottagits i enlighet med punkt 1 till de gemensamma kontaktpunkterna i andra berörda medlemsstater.

9. Den gemensamma kontaktpunkten ska var tredje månad lämna in en sammanfattande rapport till Enisa med anonymiserade och aggregerade uppgifter om betydande incidenter, incidenter, cyberhot och tillbud om vilket underrättats i enlighet med punkt 1 i denna artikel och med artikel 30. För att bidra till att jämförbar information lämnas får Enisa anta teknisk vägledning om parametrarna för den information som ska tas med i den sammanfattande rapporten. Enisa ska var sjätte månad informera samarbetsgruppen och CSIRT-nätverket om sina slutsatser om de mottagna anmälningarna.

10. CSIRT-enheterna eller, i tillämpliga fall, de behöriga myndigheterna ska förse de behöriga myndigheterna enligt direktiv (EU) 2022/2557 med information om betydande incidenter, incidenter, cyberhot och tillbud om vilket underrättats i enlighet med punkt 1 i denna artikel och med artikel 30 av entiteter som identifierats som kritiska i enlighet med direktiv (EU) 2022/2557.

11. Kommissionen får anta genomförandeakter som närmare anger typen av information i och formatet och förfarandet för underrättelser som lämnas i enlighet med punkt 1 i denna artikel och med artikel 30 samt för underrättelser som lämnas i enlighet med punkt 2 i den här artikeln.

Senast den 17 oktober 2024 ska kommissionen, 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 hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer eller av plattformar för sociala nätverkstjänster, anta genomförandeakter som närmare anger i vilka fall en incident ska anses vara betydande enligt punkt 3. Kommissionen får anta sådana genomförandeakter med avseende på andra väsentliga och viktiga entiteter.

Kommissionen ska utbyta råd och samarbeta med samarbetsgruppen om de utkast till genomförandeakter som avses i första och andra stycket i denna punkt i enlighet med artikel 14.4 e.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Artikel 24

Användning av europeiska ordningar för cybersäkerhetscertifiering

1. För att visa att vissa krav enligt artikel 21 är uppfyllda får medlemsstaterna ålägga väsentliga och viktiga entiteter att använda särskilda IKT-produkter, IKT-tjänster och IKT-processer, som har utvecklats av den väsentliga eller viktiga entiteten eller upphandlats från tredje parter, som är certifierade enligt europeiska ordningar för cybersäkerhetscertifiering som antagits i enlighet med artikel 49 i förordning (EU) 2019/881. Medlemsstaterna ska dessutom uppmuntra väsentliga och viktiga entiteter att använda kvalificerade betrodda tjänster.

2. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 38 för att komplettera detta direktiv genom att ange vilka kategorier av väsentliga eller viktiga 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 förordning (EU) 2019/881. Dessa delegerade akter ska antas om det har fastställts att cybersäkerhetsnivån är otillräcklig och ska omfatta en genomförandeperiod.

Innan kommissionen antar sådana delegerade akter ska den göra en konsekvensbedömning och genomföra samråd i enlighet med artikel 56 i förordning (EU) 2019/881.

3. I fall där det inte finns en lämplig europeisk ordning för cybersäkerhetscertifiering med avseende på tillämpningen av punkt 2 i denna artikel kan kommissionen, efter samråd med samarbetsgruppen och europeiska gruppen för cybersäkerhetscertifiering, begära att Enisa utarbetar ett förslag till certifieringsordning enligt artikel 48.2 i förordning (EU) 2019/881.

Artikel 25

Standardisering

1. För att främja en enhetlig tillämpning av artikel 21.1 och 21.2 ska medlemsstaterna, utan att föreskriva eller gynna användning av en viss typ av teknik, uppmuntra användningen av europeiska och internationella standarder och tekniska specifikationer av relevans för säkerheten i nätverks- och informationssystem.

2. Enisa ska i samarbete med medlemsstaterna och, när så är lämpligt, efter samråd med relevanta intressenter, utarbeta råd och riktlinjer för de tekniska områden som ska beaktas när det gäller punkt 1 samt för redan befintliga standarder, inklusive nationella standarder, som skulle göra det möjligt att täcka dessa områden.

KAPITEL V

JURISDIKTION OCH REGISTRERING

Artikel 26

Jurisdiktion och territorialitet

1. Entiteter som omfattas av detta direktivs tillämpningsområde ska anses omfattas av jurisdiktionen i den medlemsstat där de är etablerade, utom när det gäller följande:

a) Tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster, som ska anses omfattas av jurisdiktionen i den medlemsstat där de tillhandahåller sina tjänster.

b) Leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster och leverantörer av hanterade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster, vilka ska anses omfattas av jurisdiktionen i den medlemsstat där de har sitt huvudsakliga etableringsställe i unionen i enlighet med punkt 2.

c) Offentliga förvaltningsentiteter, som ska anses omfattas av jurisdiktionen i den medlemsstat som inrättade dem.

2. Vid tillämpning av detta direktiv ska en entitet som avses i punkt 1 b anses ha sitt huvudsakliga etableringsställe i unionen i den medlemsstat där besluten om riskhanteringsåtgärder för cybersäkerhet i huvudsak fattas. Om en sådan medlemsstat inte kan fastställas eller om sådana beslut inte fattas i unionen ska det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där cybersäkerhetsoperationer utförs. Om en sådan medlemsstat inte kan fastställas ska det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där den berörda entiteten har det etableringsställe som har flest anställda i unionen.

3. Om en entitet som avses i punkt 1 b inte är etablerad i unionen, men erbjuder tjänster inom unionen, ska den utse en företrädare i unionen. Företrädaren ska vara etablerad i en av de medlemsstater där tjänsterna erbjuds. Entiteten ska anses omfattas av jurisdiktionen i den medlemsstat där företrädaren är etablerad. Om det inte finns en utsedd företrädare i unionen enligt denna punkt får varje medlemsstat där entiteten tillhandahåller tjänster vidta rättsliga åtgärder mot entiteten för överträdelsen av detta direktiv.

4. Det faktum att en entitet som avses i punkt 1 b utsett en företrädare ska inte påverka eventuella rättsliga åtgärder mot entiteten i sig.

5. De medlemsstater som har mottagit en begäran om ömsesidigt bistånd med avseende på en entitet som avses i punkt 1 b får, inom ramen för den begäran, vidta lämpliga tillsyns- och efterlevnadskontrollåtgärder med avseende på den berörda entitet som tillhandahåller tjänster eller som har ett nätverks- och informationssystem inom deras territorium.

Artikel 27

Register över entiteter

1. Enisa ska skapa och upprätthålla ett register över leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leveransleverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt leverantörer av internetbaserade marknadsplatser online, internetbaserade sökmotorer och plattformar för sociala nätverkstjänster, på grundval av den information som mottagits från de gemensamma kontaktpunkterna i enlighet med punkt 4. Enisa ska på begäran ge de behöriga myndigheterna tillgång till detta register, samtidigt som skydd av informationens konfidentialitet säkerställs i tillämpliga fall.

2. Medlemsstaterna ska ålägga de entiteter som avses i punkt 1 att lämna följande uppgifter till de behöriga myndigheterna senast den 17 januari 2025:

a) Entitetens namn.

b) Den relevanta sektorn och delsektorn samt typen av entitet enligt bilaga I eller II i tillämpliga fall.

c) Adressen till entitetens huvudsakliga etableringsställe och andra rättsligt giltiga etableringsställen i unionen eller, om entiteten inte är etablerad i unionen, till dess företrädare som utsetts i enlighet med artikel 26.3.

d) Aktuella kontaktuppgifter, inklusive e-postadresser och telefonnummer till entiteten och, i tillämpliga fall, till dess företrädare som utsetts i enlighet med artikel 26.3.

e) De medlemsstater där entiteten tillhandahåller tjänster.

f) Entitetens IP-adressintervall.

3. Medlemsstaterna ska säkerställa att de entiteter som avses i punkt 1 underrättar den behöriga myndigheten om alla ändringar av de uppgifter som de lämnat enligt punkt 2 utan dröjsmål och under alla omständigheter inom tre månader från dagen för ändringen.

4. När den gemensamma kontaktpunkten i den berörda medlemsstaten mottagit den information som avses i punkterna 2 och 3, med undantag för den information som avses i punkt 2 f, ska den utan dröjsmål vidarebefordra den informationen till Enisa.

5. Den information som avses i punkterna 2 och 3 i denna artikel ska, i tillämpliga fall, lämnas genom den nationella mekanism som avses i artikel 3.4 fjärde stycket.

Artikel 28

Databas över domännamnsregistreringsuppgifter

1. För att bidra till domännamnssystemets säkerhet, stabilitet och motståndskraft ska medlemsstaterna ålägga registreringsenheter för toppdomäner och de enheter som tillhandahåller domännamnsregistreringstjänster att samla in och upprätthålla korrekta och fullständiga registreringsuppgifter för domännamn i en särskild databas med tillbörlig aktsamhet i enlighet med unionens dataskyddslagstiftning när det gäller personuppgifter.

2. För tillämpningen av punkt 1 ska medlemsstaterna föreskriva att databasen med registreringsuppgifter för domännamn innehåller nödvändig information för att identifiera och kontakta innehavarna av domännamnen och de kontaktpunkter som administrerar domännamnen under toppdomänerna. Denna information ska omfatta följande:

a) Domännamn.

b) Registreringsdatum.

c) Registrantens namn, e-postadress och telefonnummer.

d) E-postadress och telefonnummer till den kontaktpunkt som administrerar domännamnet om dessa inte är desamma som för registranten.

3. Medlemsstaterna ska ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att ha strategier och förfaranden, inbegripet kontrollförfaranden, för att säkerställa att de databaser som avses i punkt 1 innehåller korrekt och fullständig information. Medlemsstaterna ska föreskriva att sådana strategier och förfaranden offentliggörs.

4. Medlemsstaterna ska ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att utan onödigt dröjsmål efter registreringen av ett domännamn offentliggöra registreringsuppgifter för domännamn som inte är personuppgifter.

5. Medlemsstaterna ska ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att ge åtkomst till specifika registreringsuppgifter för domännamn på lagliga och vederbörligen motiverade begäranden från legitima åtkomstsökande, i enlighet med unionens dataskyddslagstiftning. Medlemsstaterna ska ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att utan onödigt dröjsmål och under alla omständigheter inom 72 timmar från mottagandet besvarar en begäran om åtkomst. Medlemsstaterna ska föreskriva att strategier och förfaranden för utlämning av sådana uppgifter offentliggörs.

6. Fullgörandet av de skyldigheter som fastställs i punkterna 1–5 får inte leda till dubblerad insamling av registreringsuppgifter för domännamn. I detta syfte ska medlemsstaterna ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att samarbeta med varandra.

KAPITEL VI

INFORMATIONSUTBYTE

Artikel 29

Arrangemang för informationsutbyte om cybersäkerhet

1. Medlemsstaterna ska säkerställa att entiteter som omfattas av tillämpningsområdet för detta direktiv och, i relevanta fall, andra relevanta entiteter som inte omfattas av detta direktivs tillämpningsområde på frivillig basis har möjlighet att utbyta relevant information om cybersäkerhet sinsemellan, inbegripet information om cyberhot, tillbud, sårbarheter, tekniker och förfaranden, angreppsindikatorer, fientlig taktik, specifik information om fientliga aktörer, cybersäkerhetsvarningar och rekommendationer avseende konfigurationsverktyg för cybersäkerhet för att upptäcka cyberattacker, om sådant informationsutbyte

a) syftar till att förebygga, upptäcka, reagera på eller återhämta sig från incidenter eller begränsa deras inverkan,

b) höjer cybersäkerhetsnivån, särskilt genom att öka medvetenheten om cyberhot, begränsa eller hindra sådana hots förmåga att sprida sig, stödja en rad defensiva förmågor, avhjälpande av sårbarheter och delgivning av information om sårbarheter, metoder för att upptäcka och förebygga hot, strategier för begränsning av hot eller reaktions- och återhämtningsfaser, eller genom att främja forskningssamverkan om cyberhot bland offentliga och privata entiteter.

2. Medlemsstaterna ska säkerställa att informationsutbytet sker inom grupper av väsentliga och viktiga entiteter, och i relevanta fall, deras leverantörer eller tjänsteleverantörer. Sådant utbyte ska genomföras med hjälp av arrangemang för informationsutbyte om cybersäkerhet med hänsyn till den potentiellt känsliga karaktären hos den information som utbyts.

3. Medlemsstaterna ska underlätta inrättandet av de arrangemang för informationsutbyte om cybersäkerhet som avses i punkt 2 i denna artikel. Sådana arrangemang får ange operativa aspekter, inbegripet användning av särskilda IKT-plattformar och automatiseringsverktyg, innehållet i och villkoren för de arrangemangen för informationsutbyte. Medlemsstaterna får, i samband med fastställandet av närmare bestämmelser om offentliga myndigheters deltagande i sådana arrangemang, införa villkor för den information som tillgängliggörs av behöriga myndigheter eller CSIRT-enheter. Medlemsstaterna ska erbjuda stöd för tillämpningen av sådana arrangemang i enlighet med de riktlinjer som avses i artikel 7.2 h.

4. Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter underrättar de behöriga myndigheterna om sitt deltagande i de arrangemang för informationsutbyte om cybersäkerhet som avses i punkt 2, när de ingår sådana arrangemang eller, om de utträder ur sådana arrangemang, när utträdet får verkan.

5. Enisa ska tillhandahålla stöd för inrättandet av de arrangemang för informationsutbyte om cybersäkerhet som avses i punkt 2 genom att utbyta bästa praxis och erbjuda vägledning.

Artikel 30

Frivillig underrättelse om relevant information

1. Medlemsstaterna ska säkerställa att underrättelser, utöver den underrättelseskyldighet som föreskrivs i artikel 23, kan lämnas in till CSIRT-enheterna eller, i tillämpliga fall, de behöriga myndigheterna, på frivillig basis av

a) väsentliga och viktiga entiteter med avseende på incidenter, cyberhot och tillbud,

b) andra entiteter än de som avses i led a, oberoende av om de omfattas av detta direktiv, vad gäller om betydande incidenter, cyberhot och tillbud.

2. Medlemsstaterna ska behandla de underrättelser som avses i punkt 1 i denna artikel i enlighet med det förfarande som anges i artikel 23. Medlemsstaterna får ge behandling av obligatoriska underrättelser företräde framför behandling av frivilliga underrättelser.

CSIRT-enheterna, och i tillämpliga fall, de behöriga myndigheterna ska vid behov informera de gemensamma kontaktpunkterna om underrättelser som mottagits i enlighet med denna artikel, och samtidigt säkerställa att informationen från den underrättande entiteten förblir konfidentiell och skyddas på lämpligt sätt. Utan att det påverkar förebyggande, utredning, avslöjande och lagföring av brott får frivillig rapportering inte leda till att den underrättande entiteten åläggs ytterligare skyldigheter som den inte skulle ha blivit föremål för om den inte hade lämnat in underrättelsen.

KAPITEL VII

TILLSYN OCH EFTERLEVNADSKONTROLL

Artikel 31

Allmänna aspekter på tillsyn och efterlevnadskontroll

1. Medlemsstaterna ska säkerställa att deras behöriga myndigheter på ett ändamålsenligt sätt övervakar och vidtar de åtgärder som krävs för att säkerställa att detta direktiv efterlevs.

2. Medlemsstaterna får tillåta sina behöriga myndigheter att prioritera tillsyn. Denna prioritering ska baseras på en riskbaserad metod. När de behöriga myndigheterna utövar sina tillsynsuppgifter enligt artiklarna 32 och 33 får de i detta syfte fastställa tillsynsmetoder som gör det möjligt att prioritera sådana uppgifter enligt en riskbaserad metod.

3. De behöriga myndigheterna ska ha ett nära samarbete med tillsynsmyndigheterna enligt förordning (EU) 2016/679 när de behandlar incidenter som medför personuppgiftsincidenter, utan att det påverkar tillsynsmyndigheternas befogenheter och uppgifter enligt den förordningen.

4. Utan att det påverkar de nationella rättsliga och institutionella ramarna ska medlemsstaterna säkerställa att de behöriga myndigheterna, vid tillsynen av de offentliga förvaltningsentiteternas efterlevnad av detta direktiv och införandet av efterlevnadskontrollåtgärder vid överträdelser av detta direktiv, har lämpliga befogenheter att utföra dessa uppgifter och är operativt oberoende i förhållande till de offentliga förvaltningsentiteter som övervakas. Medlemsstaterna får besluta att införa lämpliga, proportionella och effektiva tillsyns- och efterlevnadskontrollåtgärder med avseende på dessa entiteter i enlighet med de nationella rättsliga och institutionella ramarna.

Artikel 32

Tillsyns- och efterlevnadskontrollåtgärder i fråga om väsentliga entiteter

1. Medlemsstaterna ska säkerställa att de tillsyns- eller efterlevnadskontrollåtgärder som åläggs väsentliga entiteter angående de skyldigheter som anges i detta direktiv är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall.

2. Medlemsstaterna ska säkerställa att behöriga myndigheter, när de utövar sina tillsynsuppgifter avseende väsentliga entiteter, har befogenhet att åtminstone underställa dessa entiteter

a) inspektioner på plats och distansbaserad tillsyn, inklusive slumpvisa kontroller som utförs av utbildad personal,

b) regelbundna och riktade säkerhetsrevisioner som utförs av ett oberoende organ eller en behörig myndighet,

c) ad hoc-revisioner, inbegripet när detta är motiverat på grund av en betydande incident eller av en väsentlig entitets överträdelse av detta direktiv,

d) säkerhetsskanningar på grundval av objektiva, icke-diskriminerande, rättvisa och transparenta riskbedömningskriterier, vid behov i samarbete med den berörda entiteten,

e) begäranden om sådan information som behövs för att bedöma de riskhanteringsåtgärder för cybersäkerhet som antagits av den berörda entiteten, inbegripet dokumenterade cybersäkerhetsstrategier, samt fullgörandet av skyldigheten att lämna information till de behöriga myndigheterna i enlighet med artikel 27,

f) begäranden om tillgång till uppgifter, handlingar och information som behövs för att de ska kunna utföra sina tillsynsuppgifter,

g) begäranden om bevis på genomförandet av cybersäkerhetsstrategier, t.ex. resultaten av säkerhetsrevisioner som utförts av en kvalificerad revisor och respektive underliggande bevis.

De riktade säkerhetsrevisioner som avses i första stycket led b ska baseras på riskbedömningar som utförs av den behöriga myndigheten eller den granskade entiteten, eller på annan tillgänglig riskrelaterad information.

Resultaten av alla riktade säkerhetsrevisioner ska göras tillgängliga för den behöriga myndigheten. Kostnaderna för sådana riktade säkerhetsrevisioner som utförs av ett oberoende organ ska betalas av den granskade entiteten, utom i vederbörligen motiverade fall när den behöriga myndigheten beslutar något annat.

3. När de behöriga myndigheterna utövar sina befogenheter enligt punkt 2 e, f eller g ska de ange syftet med en begäran och specificera den begärda informationen.

4. Medlemsstaterna ska säkerställa att deras behöriga myndigheter, när de utövar sina befogenheter med avseende på efterlevnadskontroll gentemot väsentliga entiteter, åtminstone har befogenhet att

a) utfärda varningar om berörda entiteters överträdelser av detta direktiv,

b) anta bindande instruktioner, också om vilka åtgärder som krävs för att förebygga eller avhjälpa en incident, samt tidsgränser för genomförandet av sådana åtgärder och för rapporteringen om deras genomförande, eller ett föreläggande om att de berörda entiteterna ska avhjälpa konstaterade brister eller överträdelser av detta direktiv,

c) ålägga de berörda entiteterna att upphöra med beteenden som utgör en överträdelse av detta direktiv och att avstå från att upprepa sådana beteenden,

d) ålägga de berörda entiteterna att säkerställa att deras riskhanteringsåtgärder för cybersäkerhet överensstämmer med artikel 21 eller att fullgöra de rapporteringsskyldigheter som fastställs i artikel 23, på ett specificerat sätt och inom en angiven tidsperiod,

e) ålägga de berörda entiteterna att informera de fysiska eller juridiska personer till vilka de tillhandahåller tjänster eller utför verksamheter som potentiellt kan beröras av ett betydande cyberhot om hotets karaktär och om eventuella skyddsåtgärder eller avhjälpande åtgärder som dessa fysiska eller juridiska personer kan vidta som svar på hotet,

f) ålägga de berörda entiteterna att inom en rimlig tidsfrist genomföra de rekommendationer som lämnats till följd av en säkerhetsrevision,

g) utse en övervakningsansvarig med väldefinierade uppgifter för en fastställd tidsperiod för att övervaka att de berörda entiteterna efterlever artiklarna 21 och 23,

h) ålägga de berörda entiteterna att offentliggöra aspekter av överträdelser av detta direktiv på ett specificerat sätt,

i) påföra eller begära att relevanta organ eller domstolar i enlighet med nationell rätt påför administrativa sanktionsavgifter enligt artikel 34 utöver någon av de åtgärder som avses i leden a–h i denna punkt.

5. Om efterlevnadskontrollåtgärder som antas enligt punkt 4 a–d och f är ineffektiva ska medlemsstaterna säkerställa att deras behöriga myndigheter har befogenhet att fastställa en tidsfrist inom vilken en väsentlig entitet ska vidta nödvändiga åtgärder för att avhjälpa bristerna eller uppfylla dessa myndigheters krav. Om de begärda åtgärderna inte vidtas inom den fastställda tidsfristen ska medlemsstaterna säkerställa att de behöriga myndigheterna har befogenhet att

a) tillfälligt upphäva eller begära att ett certifierings- eller auktorisationsorgan, eller en domstol, i enlighet med nationell rätt, tillfälligt upphäver en certifiering eller auktorisation för en del av eller alla relevanta tjänster som tillhandahålls eller verksamheter som utövas av den väsentliga entiteten,

b) begära att relevanta organ eller domstolar, i enlighet med nationell rätt, inför ett tillfälligt förbud för varje fysisk person som på nivån för verkställande direktör eller juridiskt ombud har ledningsansvar i den väsentliga entiteten att utöva ledningsfunktioner i den entiteten.

Tillfälliga upphävanden eller förbud i enlighet med denna punkt ska tillämpas endast till dess att den berörda entiteten vidtar nödvändiga åtgärder för att avhjälpa bristerna eller uppfylla de krav från den behöriga myndigheten som gav upphov till sådana efterlevnadskontrollåtgärder. Sådana tillfälliga upphävanden eller förbud får komma i fråga endast om lämpliga rättssäkerhetsgarantier i enlighet med de allmänna principerna i unionsrätten och stadgan iakttas, inbegripet rätten till ett effektivt rättsmedel och en rättvis rättegång, oskuldspresumtion och rätten till försvar.

De efterlevnadskontrollåtgärder som föreskrivs i denna punkt är inte tillämpliga på sådana offentliga förvaltningsentiteter som omfattas av detta direktiv.

6. Medlemsstaterna ska säkerställa att varje fysisk person som ansvarar för eller agerar som juridiskt ombud för en väsentlig entitet har befogenhet att säkerställa att entiteten efterlever detta direktiv, på grundval av en befogenhet att företräda entiteten, att fatta beslut på dess vägnar eller att utöva kontroll över entiteten. Medlemsstaterna ska säkerställa att dessa fysiska personer kan hållas ansvariga för överträdelser av sitt uppdrag att säkerställa att detta direktiv efterlevs.

När det gäller offentliga förvaltningsentiteter påverkar inte denna punkt nationell rätt avseende det ansvar som åligger statligt anställda och valda eller utnämnda tjänstepersoner.

7. När de behöriga myndigheterna tillämpar efterlevnadskontrollåtgärder som avses i punkt 4 eller 5 ska de iaktta rätten till försvar och ta hänsyn till omständigheterna i varje enskilt fall och som ett minimum ta vederbörlig hänsyn till följande:

a) Överträdelsens allvar och betydelsen av de bestämmelser som har överträtts, med beaktande av att bland annat följande alltid ska anses vara en allvarlig överträdelse:

   i) Upprepade överträdelser.

   ii) Underlåtenhet att underrätta om eller avhjälpa betydande incidenter.

   iii) Underlåtenhet att avhjälpa brister enligt bindande instruktioner från behöriga myndigheter.

   iv) Hindrande av revisioner eller övervakningsverksamhet som den behöriga myndigheten beordrat efter det att en överträdelse konstaterats.

   v) Tillhandahållande av falsk eller grovt felaktig information i fråga om riskhanteringsåtgärder för cybersäkerhet eller rapporteringsskyldigheter enligt artiklarna 21 och 23.

b) Överträdelsens varaktighet.

c) Eventuella tidigare relevanta överträdelser från den berörda entitetens sida.

d) Den materiella eller immateriella skada som uppstått, inbegripet finansiella eller ekonomiska förluster, effekter på andra tjänster och det antal användare som berörs.

e) Uppsåt eller oaktsamhet från den som har gjort sig skyldig till överträdelsen.

f) De åtgärder som entiteten har vidtagit för att förhindra eller begränsa den materiella eller immateriella skadan.

g) Efterlevnad av godkända uppförandekoder eller godkända certifieringsmekanismer.

h) I vilken utsträckning de fysiska eller juridiska personer som hålls ansvariga samarbetar med de behöriga myndigheterna.

8. De behöriga myndigheterna ska utförligt motivera sina efterlevnadskontrollåtgärder. Innan sådana åtgärder antas ska de behöriga myndigheterna underrätta de berörda entiteterna om sina preliminära slutsatser. De ska också ge dessa entiteter en rimlig tidsfrist för att lämna synpunkter, utom i vederbörligen motiverade fall där omedelbara åtgärder för att förhindra eller reagera på incidenter annars skulle hindras.

9. Medlemsstaterna ska säkerställa att deras behöriga myndigheter enligt detta direktiv informerar de relevanta behöriga myndigheterna inom samma medlemsstat i enlighet med direktiv (EU) 2022/2557 när de utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll för att säkerställa att en entitet som identifierats som en kritisk entitet i enlighet med direktiv (EU) 2022/2557 efterlever detta direktiv. När så är lämpligt får behöriga myndigheter enligt direktiv (EU) 2022/2557 begära att behöriga myndigheter enligt detta direktiv utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll gentemot en entitet som identifieras som en kritisk entitet i enlighet med direktiv (EU) 2022/2557.

10. Medlemsstaterna ska säkerställa att deras behöriga myndigheter enligt detta direktiv samarbetar med de relevanta behöriga myndigheterna i den berörda medlemsstaten enligt förordning (EU) 2022/2554. Medlemsstaterna ska särskilt säkerställa att deras behöriga myndigheter enligt detta direktiv informerar det tillsynsforum som inrättats enligt artikel 32.1 i förordning (EU) 2022/2554 när de utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll för att säkerställa att en väsentlig entitet som har identifierats som en kritisk tredjepartsleverantör av IKT-tjänster enligt artikel 31 i förordning (EU) 2022/2554 efterlever detta direktiv.

Artikel 33

Tillsyns- och efterlevnadskontrollåtgärder i fråga om viktiga entiteter

1. När medlemsstaterna får bevis, indikationer på eller information om att en viktig entitet påstås underlåta att fullgöra detta direktiv, särskilt artiklarna 21 och 23, ska de säkerställa att de behöriga myndigheterna vid behov vidtar åtgärder i form av tillsynsåtgärder i efterhand. Medlemsstaterna ska säkerställa att dessa åtgärder är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall.

2. Medlemsstaterna ska säkerställa att de behöriga myndigheterna, när de utövar sina tillsynsuppgifter avseende viktiga entiteter, har befogenhet att åtminstone underställa dessa entiteter

a) inspektioner på plats och distansbaserad tillsyn i efterhand, som utförs av utbildad personal,

b) riktade säkerhetsrevisioner utförda av ett oberoende organ eller en behörig myndighet,

c) säkerhetsskanningar på grundval av objektiva, icke-diskriminerande, rättvisa och transparenta riskbedömningskriterier, vid behov i samarbete med den berörda entiteten,

d) begäranden om information som behövs för att i efterhand bedöma de riskhanteringsåtgärder för cybersäkerhet som antagits av den berörda entiteten, inbegripet dokumenterade cybersäkerhetsstrategier, samt fullgörandet av skyldigheten att lämna information till de behöriga myndigheterna i enlighet med artikel 27,

e) begäranden om tillgång till uppgifter, handlingar och information som behövs för att utföra sina tillsynsuppgifter,

f) begäranden om bevis på genomförandet av cybersäkerhetsstrategier, t.ex. resultaten av säkerhetsrevisioner som utförts av en kvalificerad revisor och respektive underliggande bevis.

De riktade säkerhetsrevisioner som avses i första stycket led b ska baseras på riskbedömningar som utförs av den behöriga myndigheten eller den granskade entiteten, eller på annan tillgänglig riskrelaterad information.

Resultaten av alla riktade säkerhetsrevisioner ska göras tillgängliga för den behöriga myndigheten. Kostnaderna för sådana riktade säkerhetsrevisioner som utförs av ett oberoende organ ska betalas av den granskade entiteten, utom i vederbörligen motiverade fall när den behöriga myndigheten beslutar något annat.

3. När de behöriga myndigheterna utövar sina befogenheter enligt punkt 2 d, e eller f ska de ange syftet med en begäran och specificera den begärda informationen.

4. Medlemsstaterna ska säkerställa att de behöriga myndigheterna, när de utövar sina befogenheter med avseende på efterlevnadskontroll gentemot viktiga entiteter åtminstone har befogenhet att

a) utfärda varningar om de berörda entiteternas överträdelser av detta direktiv,

b) anta bindande instruktioner eller ett föreläggande om att de berörda entiteterna ska avhjälpa konstaterade brister eller överträdelser av detta direktiv,

c) ålägga de berörda entiteterna att upphöra med beteenden som utgör en överträdelse av detta direktiv och att avstå från att upprepa sådana beteenden,

d) ålägga de berörda entiteterna att säkerställa att deras riskhanteringsåtgärder för cybersäkerhet överensstämmer med artikel 21 eller att fullgöra de rapporteringsskyldigheter som fastställs i artikel 23, på ett specificerat sätt och inom en angiven tidsperiod,

e) ålägga de berörda entiteterna att informera de fysiska eller juridiska personer till vilka de tillhandahåller tjänster eller utför verksamheter som potentiellt kan beröras av ett betydande cyberhot om hotets karaktär och om eventuella skyddsåtgärder eller avhjälpande åtgärder som dessa fysiska eller juridiska personer kan vidta som svar på hotet,

f) ålägga de berörda entiteterna att inom en rimlig tidsfrist genomföra de rekommendationer som lämnats till följd av en säkerhetsrevision,

g) ålägga de berörda entiteterna att offentliggöra aspekter av överträdelser av detta direktiv på ett specificerat sätt,

h) påföra eller begära att relevanta organ eller domstolar i enlighet med nationell rätt påför administrativa sanktionsavgifter enligt artikel 34 utöver någon av de åtgärder som avses i leden a–g i denna punkt.

5. Artikel 32.6, 32.7 och 32.8 ska i tillämpliga delar tillämpas på de tillsyns- och efterlevnadskontrollåtgärder som föreskrivs i denna artikel för viktiga entiteter.

6. Medlemsstaterna ska säkerställa att deras behöriga myndigheter enligt detta direktiv samarbetar med de relevanta behöriga myndigheterna i den berörda medlemsstaten i enlighet med förordning (EU) 2022/2554. Medlemsstaterna ska särskilt säkerställa att deras behöriga myndigheter enligt detta direktiv informerar det tillsynsforum som inrättats enligt artikel 32.1 i förordning (EU) 2022/2554 när de utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll för att säkerställa att en viktig entitet som har identifierats som en kritisk tredjepartsleverantör av IKT-tjänster i enlighet med artikel 31 i förordning (EU) 2022/2554 efterlever detta direktiv.

Artikel 34

Allmänna villkor för påförande av administrativa sanktionsavgifter för väsentliga och viktiga entiteter

1. Medlemsstaterna ska säkerställa att de administrativa sanktionsavgifter som påförs väsentliga och viktiga entiteter enligt denna artikel för överträdelser av detta direktiv är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall.

2. Administrativa sanktionsavgifter ska påföras utöver någon av de åtgärder som avses i artikel 32.4 a–h, artikel 32.5 och artikel 33.4 a–g.

3. När beslut fattas om huruvida administrativa sanktionsavgifter ska påföras och om avgiftsbeloppet i varje enskilt fall, ska vederbörlig hänsyn tas till åtminstone de faktorer som anges i artikel 32.7.

4. Medlemsstaterna ska säkerställa att väsentliga entiteter som överträder artikel 21 eller 23, i enlighet med punkterna 2 och 3 i den här artikeln påförs administrativa sanktionsavgifter på högst 10 000 000 EUR eller högst 2 % av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den väsentliga entiteten tillhör, beroende på vilken siffra som är högst.

5. Medlemsstaterna ska säkerställa att viktiga entiteter som överträder artikel 21 eller 23, i enlighet med punkterna 2 och 3 i den här artikeln påförs administrativa sanktionsavgifter på högst 7 000 000 EUR eller högst 1,4 % av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den viktiga entiteten tillhör, beroende på vilken siffra som är högst.

6. Medlemsstaterna får föreskriva befogenhet att förelägga viten för att tvinga en väsentlig eller viktig entitet att upphöra med en överträdelse av detta direktiv i enlighet med ett föregående beslut av den behöriga myndigheten.

7. Utan att det påverkar behöriga myndigheters befogenheter enligt artiklarna 32 och 33 får varje medlemsstat fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga förvaltningsentiteter som omfattas av de skyldigheter som fastställs i detta direktiv.

8. Om administrativa sanktionsavgifter inte föreskrivs i en medlemsstats rättssystem ska den medlemsstaten säkerställa att denna artikel tillämpas på ett sådant sätt att förfarandet inleds av den behöriga myndigheten och sanktionsavgifterna sedan påförs av behöriga nationella domstolar, varvid det säkerställs att dessa rättsmedel är effektiva och har samma verkan som de administrativa sanktionsavgifter som påförs av de behöriga myndigheterna. De påförda sanktionsavgifterna ska i alla händelser vara effektiva, proportionella och avskräckande. Medlemsstaten ska underrätta kommissionen om bestämmelserna i de lagar som den antar i enlighet med denna punkt senast den 17 oktober 2024 och, utan dröjsmål, om eventuella senare ändringslagstiftning eller ändringar som berör dem.

Artikel 35

Överträdelser som innebär personuppgiftsincidenter

1. Om de behöriga myndigheterna under tillsyn eller efterlevnadskontroll får kännedom om att en väsentlig eller viktig entitets överträdelse av de skyldigheter som fastställs i artiklarna 21 och 23 i detta direktiv kan innebära en personuppgiftsincident, enligt definitionen i artikel 4.12 i förordning (EU) 2016/679, som ska anmälas i enlighet med artikel 33 i den förordningen, ska de utan onödigt dröjsmål informera de tillsynsmyndigheter som avses i artikel 55 eller 56 i den förordningen.

2. Om de tillsynsmyndigheter som avses i artikel 55 eller 56 i förordning (EU) 2016/679 påför administrativa sanktionsavgifter enligt artikel 58.2 i) i den förordningen ska de behöriga myndigheterna inte påföra administrativa sanktionsavgifter enligt artikel 34 i detta direktiv för en överträdelse som avses i punkt 1 i den här artikeln som följer av samma beteende som det som den administrativa sanktionsavgiften avsåg enligt artikel 58.2 i) i förordning (EU) 2016/679. De behöriga myndigheterna får emellertid tillämpa de efterlevnadskontrollåtgärder som föreskrivs i artikel 32.4 a–h, artikel 32.5 och artikel 33.4 a–g i detta direktiv.

3. Om den tillsynsmyndighet som är behörig enligt förordning (EU) 2016/679 är etablerad i en annan medlemsstat än den behöriga myndigheten, ska den behöriga myndigheten informera den tillsynsmyndighet som är etablerad i dess egen medlemsstat om det potentiella dataintrång som avses i punkt 1.

Artikel 36

Sanktioner

Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av nationella åtgärder som antagits enligt detta direktiv 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 senast den 17 januari 2025 samt utan dröjsmål eventuella ändringar som berör dem.

Artikel 37

Ömsesidigt bistånd

1. Om en entitet tillhandahåller tjänster i mer än en medlemsstat eller tillhandahåller tjänster i en eller flera medlemsstater och dess nätverks- och informationssystem är belägna i en eller flera andra medlemsstater ska de behöriga myndigheterna i de berörda medlemsstaterna vid behov samarbeta med och bistå varandra. Detta samarbete ska åtminstone omfatta följande:

a) Att de behöriga myndigheter som tillämpar tillsyns- eller efterlevnadskontrollåtgärder i en medlemsstat via den gemensamma kontaktpunkten informerar och samråder med de behöriga myndigheterna i övriga berörda medlemsstater om de tillsyns- och efterlevnadskontrollåtgärder som vidtagits.

b) Att en behörig myndighet får begära att en annan behörig myndighet vidtar tillsyns- eller efterlevnadskontrollåtgärder.

c) Att en behörig myndighet, efter att ha mottagit en motiverad begäran från en annan behörig myndighet, ska tillhandahålla ömsesidigt bistånd till den andra behöriga myndigheten i proportion till sina egna resurser så att tillsyns- eller efterlevnadskontrollåtgärderna kan genomföras på ett ändamålsenligt, effektivt och konsekvent sätt.

Det ömsesidiga bistånd som avses i första stycket led c får omfatta begäranden om information och tillsynsåtgärder, inbegripet begäranden om att utföra inspektioner på plats, distansbaserad tillsyn eller riktade säkerhetsrevisioner. En behörig myndighet till vilken en begäran om bistånd riktas får inte avslå begäran om det inte fastställs att myndigheten antingen inte är behörig att tillhandahålla det begärda biståndet, att det begärda biståndet inte står i proportion till den behöriga myndighetens tillsynsuppgifter eller att begäran avser information eller omfattar verksamhet som, om den lämnas ut eller utförs, skulle strida mot den medlemsstatens väsentliga nationella säkerhetsintressen, allmänna säkerhet eller försvar. Innan den behöriga myndigheten avslår en sådan begäran ska den samråda med övriga berörda behöriga myndigheter samt, på begäran av en av de berörda medlemsstaterna, med kommissionen och Enisa.

2. När så är lämpligt får behöriga myndigheter från olika medlemsstater i samförstånd genomföra de gemensamma tillsynsåtgärderna.

KAPITEL VIII

DELEGERADE AKTER OCH GENOMFÖRANDEAKTER

Artikel 38

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 artikel 24.2 ska ges till kommissionen för en period på fem år från och med den 16 januari 2023 .

3. Den delegering av befogenhet som avses i artikel 24.2 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 artikel 24.2 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 39

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 IX

SLUTBESTÄMMELSER

Artikel 40

Översyn

Senast den 17 oktober 2027 och därefter var 36:e månad ska kommissionen se över hur detta direktiv fungerar och rapportera resultatet till Europaparlamentet och rådet. Rapporten ska särskilt bedöma relevansen av de berörda enheternas storlek och sektorer, delsektorer och typer när det gäller den entitet som avses i bilagorna I och II för ekonomins och samhällets funktion när det gäller cybersäkerhet. För detta ändamål och för att ytterligare främja det strategiska och operativa samarbetet ska kommissionen beakta rapporterna från samarbetsgruppen och CSIRT-nätverket om de erfarenheter som förvärvats på strategisk och operativ nivå. Rapporten ska vid behov åtföljas av ett lagstiftningsförslag.

Artikel 41

Införlivande

1. Medlemsstaterna ska senast den 17 oktober 2024 anta och offentliggöra de bestämmelser som är nödvändiga för att följa detta direktiv. De ska genast underrätta kommissionen om detta.

De ska tillämpa dessa bestämmelser från och med den 18 oktober 2024.

2. När en medlemsstat antar de bestämmelser som avses i punkt 1 ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

Artikel 42

Ändring av förordning (EU) nr 910/2014

I förordning (EU) nr 910/2014 ska artikel 19 utgå med verkan från och med den 18 oktober 2024.

Artikel 43

Ändring av direktiv (EU) 2018/1972

I direktiv (EU) 2018/1972 ska artiklarna 40 och 41 utgå med verkan från och med den 18 oktober 2024.

Artikel 44

Upphävande

Direktiv (EU) 2016/1148 ska upphöra att gälla med verkan från och med den 18 oktober 2024.

Hänvisningar till det upphävda direktivet ska anses som hänvisningar till det här direktivet och ska läsas i enlighet med jämförelsetabellen i bilaga III.

Artikel 45

Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 46

Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Strasbourg den 14 december 2022.

På Europaparlamentets vägnar	*På rådets vägnar*
R. METSOLA	M. BEK
Ordförande	*Ordförande*

BILAGA I

HÖGKRITISKA SEKTORER

Sektor	Delsektor	Typ av entitet
1. Energi	a) Elektricitet	— Elföretag enligt definitionen i artikel 2.57 i Europaparlamentets och rådets direktiv (EU) 2019/944 ([1])som bedriver *leverans* enligt definitionen i artikel 2.12 i det direktivet
		— Systemansvariga för distributionssystem enligt definitionen i artikel 2.29 i direktiv (EU) 2019/944
		— Systemansvariga för överföringssystem enligt definitionen i artikel 2.35 i direktiv (EU) 2019/944
		— Producenter enligt definitionen i artikel 2.38 i direktiv (EU) 2019/944
		— Nominerade elmarknadsoperatörer enligt definitionen i artikel 2.8 i Europaparlamentets och rådets förordning (EU) 2019/943 ([2]) — Marknadsaktörer enligt definitionen i artikel 2.25 i förordning (EU) 2019/943 och som tillhandahåller aggregering, efterfrågeflexibilitet eller energilagringstjänster enligt definitionen i artikel 2.18, 2.20 och 2.59 i direktiv (EU) 2019/944 — Laddningsoperatörer som har ansvar för förvaltning och drift av en laddningspunkt och som tillhandahåller en laddningstjänst till slutanvändare, även när detta utförs på uppdrag av en leverantör av mobilitetstjänster och i dess namn
	b) Fjärrvärme eller fjärrkyla	— Operatörer av fjärrvärme eller fjärrkyla enligt definitionen i artikel 2.19 i Europaparlamentets och rådets direktiv (EU) 2018/2001 ([3])
	c) Olja	— Operatörer av oljeledningar
		— Operatörer av anläggningar för oljeproduktion, raffinaderier, bearbetningsanläggningar och anläggningar för lagring och överföring av olja
		— Centrala lagringsenheter enligt definitionen i artikel 2 f i rådets direktiv 2009/119/EG ([4])
	d) Gas	— Gashandelsföretag eller gashandlare enligt definitionen i artikel 2.8 i Europaparlamentets och rådets direktiv 2009/73/EG ([5])
		— Systemansvariga för distributionssystemet enligt definitionen i artikel 2.6 i direktiv 2009/73/EG
		— Systemansvariga för överföringssystemet enligt definitionen i artikel 2.4 i direktiv 2009/73/EG
		— Systemansvariga för lagringssystemet enligt definitionen i artikel 2.10 i direktiv 2009/73/EG
		— Systemansvariga för en LNG-anläggning enligt definitionen i artikel 2.12 i direktiv 2009/73/EG
		— Naturgasföretag enligt definitionen i artikel 2.1 i direktiv 2009/73/EG
		— Operatörer av raffinaderier och bearbetningsanläggningar för naturgas
	e) Vätgas	— Operatörer av anläggningar för produktion, lagring och överföring av vätgas

Sektor	Delsektor	Typ av entitet
2. Transporter	a) Lufttransport	— Lufttrafikföretag enligt definitionen i artikel 3.4 i förordning (EG) nr 300/2008 och som används för kommersiella syften
		— Flygplatsens ledningsenheter enligt definitionen i artikel 2.2 i Europaparlamentets och rådets direktiv 2009/12/EG ([6]), flygplatser enligt definitionen i artikel 2.1 i det direktivet, inbegripet de huvudflygplatser som förtecknas i avsnitt 2 i bilaga II till Europaparlamentets och rådets förordning (EU) nr 1315/2013 ([7]), och enheter som driver närliggande anläggningar inom flygplatser
		— Operatörer inom trafikstyrning och trafikledning som tillhandahåller flygkontrolltjänst enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EG) nr 549/2004 ([8])
	b) Järnvägstransport	— Infrastrukturförvaltare enligt definitionen i artikel 3.2 i Europaparlamentets och rådets direktiv 2012/34/EU ([9])
		— Järnvägsföretag enligt definitionen i artikel 3.1 i direktiv 2012/34/EU, inbegripet tjänsteleverantörer enligt definitionen i artikel 3.12 i det direktivet
	c) Sjöfart	— Transportföretag som bedriver persontrafik och godstrafik på inre vattenvägar, till havs och längs kuster, enligt definitionerna för sjötransport i bilaga I till Europaparlamentets och rådets förordning (EG) nr 725/2004 ([10]), exklusive de enskilda fartyg som drivs av dessa företag
		— Ledningsenheter för hamnar enligt definitionen i artikel 3.1 i Europaparlamentets och rådets direktiv 2005/65/EG ([11]), inbegripet deras hamnanläggningar enligt definitionen i artikel 2.11 i förordning (EG) nr 725/2004, och enheter som sköter anläggningar och utrustning i hamnar
		— Operatörer av sjötrafikinformationstjänst (VTS) enligt definitionen i artikel 3 o i Europaparlamentets och rådets direktiv 2002/59/EG ([12])
	d) Vägtransport	— Vägmyndigheter enligt definitionen i artikel 2.12 i kommissionens delegerade förordning (EU) 2015/962 ([13]) med ansvar för trafikstyrning, med undantag för offentliga entiteter för vilka trafikstyrning eller driften av intelligenta transportsystem är en icke väsentlig del av deras allmänna verksamhet
		— Operatörer av intelligenta transportsystem enligt definitionen i artikel 4.1 i Europaparlamentets och rådets direktiv 2010/40/EU ([14])
3. Bankverksamhet		Kreditinstitut enligt definitionen i artikel 4.1 i Europaparlamentets och rådets förordning (EU) nr 575/2013 ([15])
4. Finansmarknads-infrastruktur		— Operatörer av handelsplatser enligt definitionen i artikel 4.24 i Europaparlamentets och rådets direktiv 2014/65/EU ([16])
		— Centrala motparter enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 648/2012 ([17])

Sektor	Delsektor	Typ av entitet
5. Hälso- och sjukvårdssektorn		— Vårdgivare enligt definitionen i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU ([18])
		— EU-referenslaboratorier som avses i artikel 15 i Europaparlamentets och rådets förordning (EU) 20222/2371 ([19])
		— Entiteter som bedriver forskning och utveckling avseende läkemedel enligt definitionen i artikel 1.2 i Europaparlamentets och rådets direktiv 2001/83/EG ([20]) — Entiteter som tillverkar farmaceutiska basprodukter och läkemedel som avses i avsnitt C huvudgrupp 21 i Nace Rev. 2 — Entiteter som tillverkar medicintekniska produkter som anses vara kritiska vid ett hot mot folkhälsan (förteckning över kritiska medicintekniska produkter vid ett hot mot folkhälsan) i den mening som avses i artikel 22 i Europaparlamentets och rådets förordning (EU) 2022/123 ([21])
6. Dricksvatten		Leverantörer och distributörer av dricksvatten enligt definitionen i artikel 2.1 a i Europaparlamentets och rådets direktiv (EU) 2020/2184 ([22]) undantaget distributörer för vilka distribution av dricksvatten utgör en icke väsentlig del av deras allmänna verksamhet, som består i distribution av andra förnödenheter och varor
7. Avloppsvatten		Företag som samlar ihop, släpper ut och renar avloppsvatten från tätbebyggelse, hushållsspillvatten eller industrispillvatten enligt definitionen i artikel 2.1–2.3 i rådets direktiv 91/271/EEG ([23]), undantaget företag som samlar ihop, släpper ut eller renar avloppsvatten från tätbebyggelse, hushållsspillvatten eller industrispillvatten som en icke väsentlig del av sin allmänna verksamhet
8. Digital infrastruktur		— Leverantörer av internetknutpunkter
		— Leverantörer av DNS-tjänster, med undantag för operatörer av rotnamnsservrar
		— Registreringsenheter för toppdomäner
		— Leverantörer av molntjänster
		— Leverantörer av datacentraltjänster
		— Leverantörer av nätverk för leverans av innehåll
		— Tillhandahållare av betrodda tjänster
		— Tillhandahållare av allmänna elektroniska kommunikationsnät
		— Tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster
9. Förvaltning av IKT-tjänster (mellan företag)		— Leverantörer av hanterade tjänster — Leverantörer av hanterade säkerhetstjänster

Sektor	Delsektor	Typ av entitet
10. Offentlig förvaltning		— Offentliga förvaltningsentiteter hos nationella regeringar såsom de definieras av en medlemsstat i enlighet med nationell rätt
		— Offentliga förvaltningsentiteter på regional nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt
11. Rymden		Operatörer av markbaserad infrastruktur som ägs, förvaltas och drivs av medlemsstater eller privata parter och som stöder tillhandahållandet av rymdbaserade tjänster, undantaget tillhandahållare av allmänna elektroniska kommunikationsnät

(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).
(2) Europaparlamentets och rådets förordning (EU) 2019/943 av den 5 juni 2019 om den inre marknaden för el (EUT L 158, 14.6.2019, s. 54).
(3) Europaparlamentets och rådets direktiv (EU) 2018/2001 av den 11 december 2018 om främjande av användningen av energi från förnybara energikällor (EUT L 328, 21.12.2018, s. 82).
(4) Rådets direktiv 2009/119/EG av den 14 september 2009 om skyldighet för medlemsstaterna att inneha minimilager av råolja och/eller petroleumprodukter (EUT L 265, 9.10.2009, s. 9).
(5) Europaparlamentets och rådets direktiv 2009/73/EG av den 13 juli 2009 om gemensamma regler för den inre marknaden för naturgas och om upphävande av direktiv 2003/55/EG (EUT L 211, 14.8.2009, s. 94).
(6) Europaparlamentets och rådets direktiv 2009/12/EG av den 11 mars 2009 om flygplatsavgifter (EUT L 70, 14.3.2009, s. 11).
(7) Europaparlamentets och rådets förordning (EU) nr 1315/2013 av den 11 december 2013 om unionens riktlinjer för utbyggnad av det transeuropeiska transportnätet och om upphävande av beslut nr 661/2010/EU (EUT L 348, 20.12.2013, s. 1).
(8) Europaparlamentets och rådets förordning (EG) nr 549/2004 av den 10 mars 2004 om ramen för inrättande av det gemensamma europeiska luftrummet ("ramförordning") (EUT L 96, 31.3.2004, s. 1).
(9) Europaparlamentets och rådets direktiv 2012/34/EU av den 21 november 2012 om inrättande av ett gemensamt europeiskt järnvägsområde (EUT L 343, 14.12.2012, s. 32).
(10) Europaparlamentets och rådets förordning (EG) nr 725/2004 av den 31 mars 2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar (EUT L 129, 29.4.2004, s. 6).
(11) Europaparlamentets och rådets direktiv 2005/65/EG av den 26 oktober 2005 om ökat hamnskydd (EUT L 310, 25.11.2005, s. 28).
(12) Europaparlamentets och rådets direktiv 2002/59/EG av den 27 juni 2002 om inrättande av ett övervaknings- och informationssystem för sjötrafik i gemenskapen och om upphävande av rådets direktiv 93/75/EEG (EUT L 208, 5.8.2002, s. 10).
(13) Kommissionens delegerade förordning (EU) 2015/962 av den 18 december 2014 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller tillhandahållande av EU-omfattande realtidstrafikinformationstjänster (EUT L 157, 23.6.2015, s. 21).
(14) Europaparlamentets och rådets direktiv 2010/40/EU av den 7 juli 2010 om ett ramverk för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportslag (EUT L 207, 6.8.2010, s. 1).
(15) Europaparlamentets och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och om ändring av förordning (EU) nr 648/2012 (EUT L 176, 27.6.2013, s. 1).
(16) Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU (EUT L 173, 12.6.2014, s. 349).
(17) Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister (EUT L 201, 27.7.2012, s. 1).
(18) Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).

(19) Europaparlamentets och rådets förordning (EU) 2022/2371 av den 23 november 2022 om allvarliga gränsöverskridande hot mot människors hälsa och om upphävande av beslut nr 1082/2013/EU (EUT L 314, 6.12.2022, s. 26).
(20) Europaparlamentets och rådets direktiv 2001/83/EG av den 6 november 2001 om upprättande av gemenskapsregler för humanläkemedel (EGT L 311, 28.11.2001, s. 67).
(21) Europaparlamentets och rådets förordning (EU) 2022/123 av den 25 januari 2022 om en förstärkt roll för Europeiska läkemedelsmyndigheten vid krisberedskap och krishantering avseende läkemedel och medicintekniska produkter (EUT L 20, 31.1.2022, s. 1).
(22) Europaparlamentets och rådets direktiv (EU) 2020/2184 av den 16 december 2020 om kvaliteten på dricksvatten (EUT L 435, 23.12.2020, s. 1).
(23) Rådets direktiv 91/271/EEG av den 21 maj 1991 om rening av avloppsvatten från tätbebyggelse (EGT L 135, 30.5.1991, s. 40).

BILAGA II

ANDRA KRITISKA SEKTORER

Sektor	Delsektor	Typ av entitet
1. Post- och budtjänster		Tillhandahållare av posttjänster enligt definitionen i artikel 2.1a i direktiv 97/67/EG, inbegripet tillhandahållare av budtjänster
2. Avfallshantering		Verksamhetsutövare som bedriver avfallshantering enligt definitionen i artikel 3.9 i Europaparlamentets och rådets direktiv 2008/98/EG ([1]), dock undantaget verksamhetsutövare vars huvudsakliga näringsverksamhet inte är av avfallshantering
3. Tillverkning, produktion och distribution av kemikalier		Företag som tillverkar ämnen och distribuerar ämnen eller blandningar som avses i artikel 3.9 och 3.14 i Europaparlamentets och rådets förordning (EG) nr 1907/2006 ([2]) samt företag som producerar varor enligt definitionen i artikel 3.3 i den förordningen genom att använda ämnen och blandningar
4. Produktion, bearbetning och distribution av livsmedel		Livsmedelsföretag enligt definitionen i artikel 3.2 i Europaparlamentets och rådets förordning (EG) nr 178/2002 ([3]) som bedriver grossisthandel och industriell produktion och bearbetning
5. Tillverkning	a) Tillverkning av medicintekniska produkter och medicintekniska produkter för *in vitro*-diagnostik	Entiteter som tillverkar medicintekniska produkter enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) 2017/745 ([4])nligt definitionen i artikel 2.2 i Europaparlamentets och rådets förordning (EU) 2017/746 ([5]), med undantag av entiteter som tillverkar sådana medicintekniska produkter som avses i punkt 5 femte strecksatsen i bilaga I i detta direktiv
	b) Tillverkning av datorer, elektronikvaror och optik	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 26 i Nace Rev. 2
	c) Tillverkning av elapparatur	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 27 i Nace Rev. 2
	d) Tillverkning av övriga maskiner	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 28 i Nace Rev. 2
	e) Tillverkning av motorfordon, släpfordon och påhängsvagnar	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 29 i Nace Rev. 2
	f) Tillverkning av andra transportmedel	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 30 i Nace Rev. 2

Bilaga 1

Sektor	Delsektor	Typ av entitet
6. Digitala leverantörer		— Leverantörer av marknadsplatser online
		— Leverantörer av sökmotorer
		— Leverantörer av plattformar för sociala nätverkstjänster
7. Forskning		Forskningsorganisationer

(1) Europaparlamentets och rådets direktiv 2008/98/EG av den 19 november 2008 om avfall och om upphävande av vissa direktiv (EUT L 312, 22.11.2008, s. 3).

(2) Europaparlamentets och rådets förordning (EG) nr 1907/2006 av den 18 december 2006 om registrering, utvärdering, godkännande och begränsning av kemikalier (Reach), inrättande av en europeisk kemikaliemyndighet, ändring av direktiv 1999/45/EG och upphävande av rådets förordning (EEG) nr 793/93 och kommissionens förordning (EG) nr 1488/94 samt rådets direktiv 76/769/EEG och kommissionens direktiv 91/155/EEG, 93/67/EEG, 93/105/EG och 2000/21/EG (EUT L 396, 30.12.2006, s. 1).

(3) Europaparlamentets och rådets förordning (EG) nr 178/2002 av den 28 januari 2002 om allmänna principer och krav för livsmedelslagstiftning, om inrättande av Europeiska myndigheten för livsmedelssäkerhet och om förfaranden i frågor som gäller livsmedelssäkerhet (EGT L 31, 1.2.2002, s. 1).

(4) 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).

(5) 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).

BILAGA III

JÄMFÖRELSETABELL

Direktiv (EU) 2016/1148	Detta direktiv
Artikel 1.1	Artikel 1.1
Artikel 1.2	Artikel 1.2
Artikel 1.3	–
Artikel 1.4	Artikel 2.12
Artikel 1.5	Artikel 2.13
Artikel 1.6	Artikel 2.6 och 2.11
Artikel 1.7	Artikel 4
Artikel 2	Artikel 2.14
Artikel 3	Artikel 5
Artikel 4	Artikel 6
Artikel 5	–
Artikel 6	–
Artikel 7.1	Artikel 7.1 och 7.2
Artikel 7.2	Artikel 7.4
Artikel 7.3	Artikel 7.3
Artikel 8.1–8.5	Artikel 8.1–8.5
Artikel 8.6	Artikel 13.4
Artikel 8.7	Artikel 8.6
Artikel 9.1, 9.2 och 9.3	Artikel 10.1, 10.2 och 10.3
Artikel 9.4	Artikel 10.9
Artikel 9.5	Artikel 10.10
Artikel 10.1, 10.2 och 10.3 första stycket	Artikel 13.1, 13.2 och 13.3
Artikel 10.3 andra stycket	Artikel 23.9
Artikel 11.1	Artikel 14.1 och 14.2
Artikel 11.2	Artikel 14.3
Artikel 11.3	Artikel 14.4 första stycket leden a–q och led s och 14.7
Artikel 11.4	Artikel 14.4 första stycket led r och andra stycket
Artikel 11.5	Artikel 14.8
Artikel 12.1–12.5	Artikel 15.1–15.5
Artikel 13	Artikel 17
Artikel 14.1 och 14.2	Artikel 21.1–21.4
Artikel 14.3	Artikel 23.1
Artikel 14.4	Artikel 23.3
Artikel 14.5	Artikel 23.5, 23.6 och 23.8

Direktiv (EU) 2016/1148	Detta direktiv
Artikel 14.6	Artikel 23.7
Artikel 14.7	Artikel 23.11
Artikel 15.1	Artikel 31.1
Artikel 15.2 första stycket a	Artikel 32.2 e
Artikel 15.2 första stycket b	Artikel 32.2 g
Artikel 15.2 andra stycket	Artikel 32.3
Artikel 15.3	Artikel 32.4 b
Artikel 15.4	Artikel 31.3
Artikel 16.1 och 16.2	Artikel 21.1–21.4
Artikel 16.3	Artikel 23.1
Artikel 16.4	Artikel 23.3
Artikel 16.5	–
Artikel 16.6	Artikel 23.6
Artikel 16.7	Artikel 23.7
Artikel 16.8 och 16.9	Artiklarna 21.5 och 23.11
Artikel 16.10	–
Artikel 16.11	Artikel 2.1, 2.2 och 2.3
Artikel 17.1	Artikel 33.1
Artikel 17.2 a	Artikel 32.2 e
Artikel 17.2 b	Artikel 32.4 b
Artikel 17.3	Artikel 37.1 a och b
Artikel 18.1	Artikel 26.1 b och 26.2
Artikel 18.2	Artikel 26.3
Artikel 18.3	Artikel 26.4
Artikel 19	Artikel 25
Artikel 20	Artikel 30
Artikel 21	Artikel 36
Artikel 22	Artikel 39
Artikel 23	Artikel 40
Artikel 24	–
Artikel 25	Artikel 41
Artikel 26	Artikel 45
Artikel 27	Artikel 46
Bilaga I punkt 1	Artikel 11.1
Bilaga I punkt 2 a i–iv	Artikel 11.2 a–d

Direktiv (EU) 2016/1148	Detta direktiv
Bilaga I punkt 2 a v	Artikel 11.2 f
Bilaga I punkt 2 b	Artikel 11.4
Bilaga I punkt 2 c i och ii	Artikel 11.5 a
Bilaga II	Bilaga I
Bilaga III punkterna 1 och 2	Bilaga II punkt 6
Bilaga III punkt 3	Bilaga I punkt 8

Sammanfattning av delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)

Direktivet

Europaparlamentet och rådet antog den 14 december 2022 två nya EU-direktiv, NIS2-direktivet, se bilaga 3 och CER-direktivet. Utredningen redovisar i detta delbetänkande förslag om införlivning av NIS2-direktivet och kommer att i sitt slutbetänkande i september 2024 att lämna förslag om införlivning av CER-direktivet.

NIS2-direktivet ställer krav på säkerhet i nätverks- och informationssystem. Det ersätter det tidigare NIS-direktivet från 2016, som genomfördes i svensk rätt genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Utredningen föreslår att NIS2-direktivet i huvudsak införlivas genom en ny lag, cybersäkerhetslagen och att den tidigare lagen upphävs.

NIS2-direktivet skärper kraven jämfört med det tidigare direktivet för verksamhetsutövare och innehåller bestämmelser om ett mer långtgående samarbete inom unionen. Syftet är att uppnå en högre cybersäkerhet. Det är ett minimidirektiv med innebörd att den svenska lagstiftningen skulle kunna innehålla längre gående skyldigheter. Utredningen föreslår med något undantag inte några skyldigheter utöver vad som följer av direktivet.

Vem omfattas av cybersäkerhetsregleringen?

Det finns två viktiga skillnader mellan gällande lagstiftning och förslaget till cybersäkerhetsreglering. Den första är att cybersäkerhetslagen föreslås omfatta betydligt fler aktörer, eftersom antalet sektorer utökas från sju till 18. Den andra viktiga skillnaden är att kraven kommer att gälla för hela verksamheten inte bara för samhällsviktiga och digitala tjänster.

De sektorer som kommer att omfattas är:

- Energi
- Transporter
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvårdssektorn
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- Förvaltning av IKT-tjänster (mellan företag)
- Offentlig förvaltning
- Rymden
- Post- och budtjänster
- Avfallshantering
- Tillverkning, produktion och distribution av kemikalier
- Produktion, bearbetning och distribution av livsmedel
- Tillverkning
- Digitala leverantörer

Innebörden är att den som bedriver verksamhet inom någon av sektorerna som utgångspunkt omfattas av kraven i cybersäkerhetsregleringen. Det gäller för såväl offentliga som enskilda verksamhetsutövare.

Som framgår av uppräkningen av sektorer är offentlig förvaltning en egen sektor. Det får till följd att nästan hela den offentliga sektorn omfattas av lagens krav. Utredningen föreslår att cybersäkerhetslagen ska gälla för de flesta statliga myndigheter i Sverige. De som är undantagna är regeringen, Regeringskansliet, myndigheter som lyder under Riksdagen, och domstolar. Detsamma gäller för sammanlagt 16 myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpning.

Vidare omfattas samtliga regioner och kommuner av lagens krav. Undantag gäller enbart för region- eller kommunfullmäktige. Utredningen föreslår också att lärosäten med examenstillstånd ska omfattas av regleringen.

För enskilda verksamhetsutövare gäller som huvudregel ett storlekskrav med innebörd att verksamheten måste sysselsätta minst 50 personer eller ha en årsomsättning som överstiger 10 miljoner euro för att omfattas av lagen. Det betyder att små företag som utgångspunkt inte kommer att beröras. Vissa särskilt utpekade enskilda verksamhetsutövare omfattas dock oavsett storlek. Myndigheten för samhällsskydd och beredskap (MSB) kommer också att ha möjlighet att peka ut vissa särskilt kritiska mindre verksamheter. Enskilda verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet, brottsbekämpning eller erbjuder tjänster till myndigheter som gör det, är undantagna.

Därutöver kommer lagen att gälla i begränsad utsträckning för offentliga verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller brottsbekämpning, men där den delen inte utgör en väsentlig andel. Motsvarande kommer att gälla för enskilda verksamhetsutövare som bedriver annan verksamhet tillsammans med säkerhetskänslig verksamhet eller brottsbekämpning. För den säkerhetskänsliga delen av verksamheten eller den delen av verksamheten som avser brottsbekämpning kommer det endast att gälla en anmälnings- och uppgiftsskyldighet. Detsamma gäller för verksamheter som redan omfattas av skyldigheter med motsvarande verkan som kraven i cybersäkerhetslagen. Så kommer vara fallet för exempelvis finansiella verksamhetsutövare som omfattas av Dora-förordningen.

Kraven i direktivet

Den nya regleringen ställer krav på verksamhetsutövarna. En verksamhetsutövare som omfattas av lagen ska anmäla sig till sin tillsynsmyndighet och lämna uppgifter om bland annat identitet, kontaktuppgift och verksamhet.

Därutöver ska verksamhetsutövare vidta riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från en riskanalys, vara proportionella i förhållande till risken och de ska utvärderas. Det ställs också krav på att

verksamhetsutövaren ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete samt krav på att verksamhetens ledning ska genomgå utbildning och att anställda ska erbjudas utbildning.

Slutligen gäller en skyldighet för verksamhetsutövare att rapportera betydande incidenter till MSB i egenskap av CSIRT-enhet (se nedan) inom bestämda tidsgränser. Det betyder att en varning ska lämnas inom 24 timmar efter det att verksamhetsutövaren fått kännedom om den betydande incidenten. Vidare ska en incidentanmälan göras inom 72 timmar och en slutrapport inom en månad.

De uppgifter verksamhetsutövarna lämnar till sin tillsynsmyndighet ovan ska myndigheten använda för att klassificera verksamhetsutövarna som väsentliga eller viktiga och registrera dem.

Det ska också finnas ett särskilt register för gränsöverskridande verksamhetsutövare. Registret ska sedan vidarebefordras till MSB i egenskap av gemensam kontaktpunkt (se nedan) som i sin tur ska informera kommissionen.

Tillsyn

I kommittédirektivet anges att systemet för tillsyn bör utgå från den struktur som finns enligt dagens regelverk. Enligt den nu gällande NIS-lagen finns det för varje sektor och för de digitala tjänster som omfattas av lagen en utpekad tillsynsmyndighet som utövar tillsyn över att regelverket följs. Utredningen föreslår att det även fortsatt ska finnas en tillsynsmyndighet för varje sektor. I de sektorer som är oförändrade i förhållande till det första NIS-direktivet är utredningens förslag att befintliga tillsynsmyndigheter fortsätter att ansvara för dessa. Den kompetens som finns hos befintliga tillsynsmyndigheter bör så långt möjligt även nyttjas för de nya sektorer som omfattas av reglering. Flera tillsynsmyndigheter föreslås därför få utökade ansvarsområden. Utredningen föreslår också fem nya tillsynsmyndigheter. Dessa är länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län samt Läkemedelsverket.

Tillsynsmyndigheten ska utöva tillsyn över att cybersäkerhetslagen och föreskrifter som meddelats i anslutning till lagen följs. Tillsynsåtgärder för viktiga verksamhetsutövare får vidtas endast när tillsynsmyndigheten har befogad anledning att anta att regleringen inte följs.

Verksamhetsutövarna ska tillhandahålla tillsynsmyndigheten den information som behövs för tillsynen. Tillsynsmyndigheten får om det finns särskilda skäl ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att redovisa resultatet för tillsynsmyndigheten. Tillsynsmyndigheten får också låta genomföra säkerhetsskanningar hos verksamhetsutövare som omfattas av cybersäkerhetslagen.

MSB ska även fortsättningsvis leda ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

För att säkerställa gränsöverskridande samarbete ska varje medlemsstat utse en gemensam kontaktpunkt. Den gemensamma kontaktpunkten ska utöva en sambandsfunktion och bland annat lämna sammanfattande rapporter om betydande incidenter, cyberhot och tillbud till Enisa samt underrätta kommissionen och samarbetsgruppen om antalet verksamhetsutövare i Sverige.

Mot bakgrund av att MSB i dag fullgör de uppgifter som följer av att vara gemensam kontaktpunkt samt myndighetens uppgift att stödja och samordna arbetet med samhällets informationssäkerhet anser utredningen att MSB även fortsatt ska vara gemensam kontaktpunkt i Sverige.

Varje medlemsstat ska också utse eller inrätta en eller flera CSIRT-enheter (Computer Security Incident Response Team). CSIRT-enheten ska bland annat övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå och tillhandahålla varningar och information. Vidare ska varje medlemsstat utse eller inrätta en eller flera myndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser (cyberkrishanteringsmyndigheter).

Mot bakgrund av de uppdrag MSB har i dag och den kompetens som finns inom myndigheten bedömer utredningen att MSB även fortsatt ska vara CSIRT-enhet samt vara cyberkrishanteringsmyndighet i Sverige.

Varje medlemsstat ska anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser. Planen ska bland annat innehålla cyberkrishanteringsmyndighetens uppgifter och ansvarsområden. Utformningen av den nationella planen ingår inte i utredningens uppdrag.

Ingripanden och sanktioner

Nuvarande ingripanden och sanktioner

Enligt NIS-lagen får en tillsynsmyndighet ingripa mot överträdelser av vissa skyldigheter i lagen. Tillsynsmyndighetens möjligheter att ingripa beror på vilken skyldighet som har överträtts, men består av förelägganden som kan förenas med vite, eller sanktionsavgifter. Sanktionsavgifterna ska bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor. Tillsynsmyndigheten ska ta särskild hänsyn till vissa omständigheter vid bestämmandet av sanktionsavgiftens storlek.

De nuvarande ingripandena och sanktionerna behålls och kompletteras

Tillsynsmyndighetens möjligheter att besluta om förelägganden (vid vite) och sanktionsavgifter behålls. Tillsynsmyndigheten ska även kunna förelägga en verksamhetsutövare att (1) offentliggöra information om överträdelser av lagens bestämmelser, och att (2) informera användare som kan påverkas av ett betydande cyberhot.

Vidare föreslås tillsynsmyndigheten få ansöka hos allmän förvaltningsdomstol om att en person med ledningsansvar hos en väsentlig

verksamhetsutövare ska förbjudas att utöva ledningsfunktioner där. Det krävs särskilda omständigheter för att sådant förbud ska kunna meddelas.

Anmärkning införs som sanktion och ska alltid beslutas vid överträdelser om ingen annan sanktion har använts av tillsynsmyndigheten.

Sanktionsavgifternas maximinivå ska höjas

Lägstanivåerna för sanktionsavgifter behålls på 5 000 kronor. Högstanivåerna höjs väsentligt i jämförelse med gällande nivåer och uppgår:

För väsentliga verksamhetsutövare till det högsta av:

1. Två procent av den väsentliga verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 10 000 000 euro.

För viktiga verksamhetsutövare till det högsta av:

1. 1,4 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 7 000 000 euro.

För offentliga verksamhetsutövare till 10 000 000 kronor.

Tillsynsmyndigheten ska ingripa mot alla överträdelser och beakta fler omständigheter vid val och utformning av sanktioner

Utredningen föreslår att tillsynsmyndigheten ska ingripa mot alla överträdelser av lagen. Den ska i vissa särskilda fall ha möjlighet att avstå från att ingripa, till exempel för att inte bryta mot det s.k. dubbelprövningsförbudet.

Om tillsynsmyndigheten inte avstår från att ingripa ska den åtminstone meddela en anmärkning. Om den ingriper med någon annan sanktion behöver den inte meddela anmärkning.

När tillsynsmyndigheten ingriper ska den alltid beakta alla relevanta omständigheter, men fler omständigheter görs obligatoriska att beakta än vad som tidigare gällt.

Ekonomiska konsekvenser

Utredningens förslag medför ekonomiska konsekvenser för tillsynsmyndigheterna, MSB och verksamhetsutövarna. För tillsynsmyndigheterna handlar det om att betydligt fler verksamhetsutövare kommer att omfattas av lagen. Tillsynsmyndigheterna är enligt utredningens förslag elva. Sex av dem bedriver redan tillsyn enligt gällande lagstiftning, men fem myndigheter är som framgår ovan nya. Utredningen har som underlag för konsekvensanalysen inhämtat en rapport från Sweco Aktiebolag, som intervjuat de föreslagna tillsynsmyndigheterna och MSB. Av rapporten följer att det varit förenat med svårigheter för myndigheterna att uppskatta de framtida kostnaderna.

Utredningen föreslår att de tillsynsmyndigheter som redan bedriver tillsyn med undantag av Finansinspektionen får ett förstärkt anslag med två miljoner kronor vardera för 2025 avseende löpande kostnader. Skälet är att tillsynsmyndigheterna bör ha utökade resurser för att kunna identifiera vilka verksamhetsutövare som omfattas av den nya lagen, utfärda nya föreskrifter och nya vägledningar utan att samtidigt behöva minska ambitionen med tillsyn. Även MSB bör tillföras motsvarande belopp. De myndigheter som inte redan har tillsynsuppdrag bör få ett förstärkt anslag med fem miljoner kronor vardera för 2025 för att bygga upp tillsynsverksamheten.

Samtidigt föreslår utredningen att regeringen ger Statskontoret i uppdrag att vidare utreda de ekonomiska konsekvenserna för tillsynsmyndigheterna och MSB samt att det för de första åren införs ett återrapporteringskrav för myndigheterna.

För de offentliga verksamhetsutövarna föreslår utredningen att kostnaderna ska finansieras inom befintlig ram. Skälen är att det är rimligt att offentliga verksamhetsutövare vidtar grundläggande säkerhetsåtgärder. Genom förslagen erhåller verksamhetsutövarna också stöd. Vidare kan åtgärder för att förebygga incidenter medföra besparingar.

Förslagen medför även kostnader för enskilda verksamhetsutövare, men även dessa får stöd genom förslagen och det förebyggande arbetet kan medföra besparingar. Som framgått omfattas som huvudregel inte små företag. Kraven kommer att gälla inom hela unionen. Utredningen bedömer därför att regleringen inte får effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt.

Ikraftträdande

Utredningen föreslår att förslagen ska träda i kraft den 1 januari 2025.

Delbetänkandets lagförslag

Förslag till lag om cybersäkerhet

Härigenom föreskrivs följande.

1 kap. Inledande bestämmelser

Lagens syfte

1 § Syftet med denna lag är att uppnå en hög cybersäkerhetsnivå.

Uttryck i lagen

2 § I lagen avses med

1. allmän 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,

2. allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster: begreppen har samma innebörd som i lagen (2022:482) om elektronisk kommunikation,

3. betrodda tjänster: begreppet har samma innebörd som i 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,

4. betydande cyberhot: ett cyberhot som, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på en verksamhetsutövares nätverks- och informationssystem eller användarna av verksamhetsutövarens tjänster genom att vålla betydande materiell eller immateriell skada,

5. cyberhot: ett cyberhot enligt definitionen i artikel 2.8 i Cybersäkerhetsakten,

6. cybersäkerhet: cybersäkerhet enligt definitionen i artikel 2.1 i Cybersäkerhetsakten,

7. Cybersäkerhetsakten: 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,

8. datacentraltjänst: en tjänst som omfattar strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och dataöverföringstjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll,

9. domännamnsregistreringstjänster: registrar eller en annan verksamhetsutövare som verkar som ombud eller återförsäljare av domännamn,

10. domännamnssystem (DNS): ett hierarkiskt distribuerat namnsystem som möjliggör identifieringen av tjänster och resurser på internet,

11. domännamnssystemtjänster (DNS-tjänster): allmänna rekursiva tjänster för att lösa domännamnsfrågor till internetslutanvändare, eller auktoritativa tjänster för att lösa domännamnsfrågor för användning av tredje part, med undantag för rotnamnsservrar,

12. Dora-förordning: 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,

13. EES: Europeiska ekonomiska samarbetsområdet,

14. enskilda verksamhetsutövare: fysiska och juridiska personer som inte är en myndighet, region eller en kommun och som bedriver verksamhet,

15. forskningsorganisation: en verksamhetsutövare vars främsta mål är att bedriva tillämpad forskning i kommersiellt syfte, men som inte inbegriper utbildningsinstitutioner,

16. hanterade säkerhetstjänster: en verksamhet som utför eller tillhandahåller stöd för annan verksamhet gällande hantering av tjänster som hanterar cybersäkerhetsrisker,

17. hanterade tjänster: en verksamhet som erbjuder tjänster som rör installation, förvaltning, drift eller underhåll av IKT-produkter, IKT-nät, IKT-infrastruktur, IKT-tillämpningar eller andra nätverks- och informationssystem, via bistånd eller aktiv administration antingen i kundernas lokaler eller på distans,

18. IKT-produkt, IKT-tjänst och IKT-process: enligt begreppens definitioner i artiklarna 2.12, 2.13 och 2.14 i Cybersäkerhetsakten,

19. incident: en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom nätverks- och informationssystem,

20. kommissionens rekommendation 2003/361/EG: bilagan till kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag,

21. kvalificerade tillhandahållare av betrodda tjänster: begreppet har samma innebörd som i 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,

22. marknadsplatser online: en marknadsplats online enligt definitionen i artikel 2 n i Europaparlamentets och rådets direktiv 2005/29/EG av den 11 maj 2005 om otillbörliga affärsmetoder som tillämpas av näringsidkare gentemot konsumenter på den inre marknaden och om ändring av rådets direktiv 84/450/EEG och Europaparlamentets och rådets direktiv 97/7/EG, 98/27/EG och 2002/65/EG samt Europaparlamentets och rådets förordning (EG) nr 2006/2004 (direktiv om otillbörliga affärsmetoder),

23. molntjänst: en digital tjänst som möjliggör administration på begäran och bred fjärråtkomst till en skalbar och elastisk pool av gemensamma beräkningstjänster, inbegripet när sådana resurser är distribuerade på flera platser,

24. NIS2-direktivet: Europaparlamentets och rådets direktiv 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,

25. nätverk för leverans av innehåll: ett nätverk av geografiskt spridda servrar vars syfte är att säkerställa hög tillgänglighet för tillgång till eller snabb leverans av digitalt innehåll och digitala tjänster till internetanvändare för innehålls- och tjänsteleverantörers räkning.

26. nätverks- och informationssystem:

1. ett elektroniskt kommunikationsnät enligt 1 kap. 7 § lagen (2022:482) om elektronisk kommunikation,

2. en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter, eller

3. digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av 1 och 2 för att de ska kunna driftas, användas, skyddas och underhållas,

27. partnerföretag och anknutna företag: begreppen har samma innebörd som i artikel 3 i rekommendation 2003/361/EG,

28. plattformar för sociala nätverkstjänster: en plattform som gör det möjligt för slutanvändare att interagera, dela och upptäcka innehåll, finna andra användare och kommunicera med andra via flera enheter, särskilt genom chattar, inlägg, videor och rekommendationer.

29. registreringsenhet för toppdomäner: en verksamhet som har delegerats en specifik toppdomän och som ansvarar för att administrera, förvalta, sköta teknisk drift samt registrering av domännamn under en specifik toppdomän, dock inte om toppdomänen endast avses för eget bruk,

30. risk: 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 en sådan incident inträffar,

31. sökmotor: en sökmotor enligt definitionen i artikel 2.5 i Europaparlamentets och rådets förordning (EU) 2019/1150 av den 20 juni 2019 om främjande av rättvisa villkor och transparens för företagsanvändare av online baserade förmedlingstjänster,

32. tillbud: en händelse som kunde ha undergrävt tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem, men som framgångsrikt hindrades från att utvecklas eller som inte uppstod,

33. verksamhetsutövare: juridisk eller fysisk person som bedriver verksamhet. Samlingsterm i denna lag för bland annat leverantör, producent, vårdgivare, leverantör eller tillhandahållare.

Lagens tillämpningsområde

Offentliga verksamhetsutövare

3 § Denna lag gäller för

1. statliga myndigheter i Sverige med undantag för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, Riks-

revisionen, Riksdagens ombudsmän, Sveriges Riksbank, Riksdagsförvaltningen och Sveriges domstolar,

2. regioner i Sverige med undantag för regionfullmäktige, och
3. kommuner i Sverige med undantag för kommunfullmäktige.

Enskilda verksamhetsutövare

4 § Denna lag gäller för enskilda verksamhetsutövare om

1. verksamheten omfattas av bilaga 1 eller 2 i NIS2-direktivet eller är ett lärosäte med examenstillstånd,
2. inte annat följer av 5 och 6 §§, verksamheten är etablerad i Sverige, och
3. inte annat följer av 7 och 8 §§, verksamheten uppfyller kraven för medelstort företag enligt artikel 2 och 3.1–3.3 i bilagan till kommissionens rekommendation 2003/361/EG.

Regeringen eller den myndighet regeringen bestämmer får i föreskrifter meddela undantag för 3 avseende partnerföretag eller anknutna företag som inte i sig uppfyller storlekskravet.

5 § Verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster behöver inte vara etablerade i Sverige för att omfattas av lagen utan det är tillräckligt att verksamhetsutövaren erbjuder tjänster i Sverige.

6 § Gränsöverskridande verksamhetsutövare är verksamhetsutövare som erbjuder:

1. DNS-tjänster,
2. registreringsenheter för toppdomäner,
3. domännamnsregistrering,
4. molntjänster,
5. datacentraltjänster,
6. nätverk för leverans av innehåll,
7. hanterade tjänster,
8. hanterade säkerhetstjänster, eller
9. marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster.

Gränsöverskridande verksamhetsutövare som erbjuder tjänster inom EES, men saknar etablering där ska utse en företrädare med etablering i något av de länder där tjänster erbjuds.

För gränsöverskridande verksamhetsutövare krävs det i stället för etablering att Sverige är huvudsakligt etableringsställe eller att företrädaren är etablerad i Sverige för att verksamhetsutövaren ska omfattas av lagen.

För gränsöverskridande verksamhetsutövare som erbjuder tjänster i Sverige, men inte utser en företrädare gäller kap. 5.

Regeringen får meddela föreskrifter om vad som utgör huvudsakligt etableringsställe.

7 § Verksamhetsutövare som uppfyller kraven i 4 § med undantag för storlekskravet i 3 och som erbjuder allmänna elektroniska

kommunikationsnät, allmänt tillgängliga elektroniska kommunikationstjänster, betrodda tjänster, registreringsenhet för toppdomäner, DNS-tjänster eller domännamnsregistrering omfattas av lagen.

8 § Verksamhetsutövare som uppfyller kraven i 4 § med undantag för storlekskravet i 3 omfattas också av lagen om,

1. verksamheten är väsentlig för att upprätthålla kritiska funktioner i samhället och ekonomiska funktioner,
2. en störning kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet, folkhälsa eller medföra betydande systemrisker särskilt om det får gränsöverskridande konsekvenser, eller
3. verksamheten är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer som är beroende av denna verksamhet.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter.

Undantag från lagens tillämpningsområde

Krav i andra författningar

9 § Om annan författning innehåller bestämmelser om krav på riskhanteringsåtgärder eller incidentrapportering för en verksamhetsutövare med motsvarande verkan gäller inte kraven i 3 kap. för verksamhetsutövaren.

Vid jämförelsen av verkan mellan författningarna ska hänsyn tas till bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till bestämmelserna.

Regeringen får i föreskrifter ange vilka andra bestämmelser om riskhanteringsåtgärder och incidentrapportering som har motsvarande verkan.

10 § Lagen ska inte tillämpas på verksamheter som undantagits enligt artikel 2.4 i Dora-förordningen.

Sveriges säkerhet eller brottsbekämpning

11 § Lagen gäller inte statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585) eller brottsbekämpning.

Regeringen får i föreskrifter ange vilka statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpning.

12 § För andra statliga myndigheter som utövar säkerhetskänslig verksamhet eller brottsbekämpning än de som avses i 11 § gäller inte kraven i 6 § andra och fjärde stycket samt kap. 3 för den del av verksamheten som är säkerhetskänslig eller utgör brottsbekämpning. För den övriga delen av verksamheten gäller lagen i dess helhet.

Vad som anförs i första stycket gäller även regioner och kommuner.

13 § Lagen gäller inte för enskilda verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet, brottsbekämpning eller som enbart erbjuder tjänster till statliga myndigheter som avses i 11 §.

Om en enskild verksamhetsutövare bedriver även annan verksamhet gäller för den säkerhetskänsliga verksamheten, brottsbekämpningen och verksamheten som avser tjänster till statliga myndigheter enligt 11 § inte kraven i 6 § andra och fjärde stycket samt kap. 3. För den övriga delen av verksamheten gäller lagen i dess helhet.

Vad som anförs ovan i andra stycket gäller inte om verksamhetsutövaren är en tillhandahållare av betrodda tjänster. För dessa verksamhetsutövare gäller lagen i dess helhet.

14 § Skyldighet att lämna uppgifter enligt denna lag gäller inte uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen (2018:585).

2 kap. Klassificering och registrering

1 § Följande verksamhetsutövare är väsentliga:

1. Statliga myndigheter,
2. verksamhetsutövare som bedriver verksamhet enligt bilaga 1 till NIS2-direktivet, är en kommun eller ett lärosäte med examenstillstånd och vars verksamhet överstiger trösklarna för medelstora företag enligt artikel 2 och 3.1–3 i bilagan till kommissionens rekommendation 2003/361/EG,
3. verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster och vars verksamhet är medelstora företag enligt artikel 2 och 3.1–3 i bilagan till kommissionens rekommendation 2003/361/EG,
4. kvalificerade tillhandahållare av betrodda tjänster,
5. registreringsenheter för toppdomäner,
6. verksamhetsutövare som erbjuder DNS-tjänster och
7. verksamhetsutövare som anges i 1 kap. 8 § och identifierats som väsentliga enligt 33 § förordning om cybersäkerhet.

Verksamhetsutövare som inte är väsentliga är viktiga verksamhetsutövare.

2 § Verksamhetsutövare ska i en anmälan till tillsynsmyndigheten lämna uppgift om identitet, kontaktuppgift, IP-adressintervall, verksamhet och uppgift om i vilka länder verksamheten bedrivs. Gränsöverskridande verksamhetsutövare ska även lämna uppgift om huvudsakligt etableringsställe och i förekommande fall kontaktuppgift till företrädaren.

Ändras uppgifterna ska verksamhetsutövaren anmäla förändringen inom 14 dagar.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om uppgifterna.

3 kap. Riskanteringsåtgärder och incidentrapportering

1 § Verksamhetsutövaren ska vidta tekniska, driftsrelaterade och organisatoriska riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från ett allriskperspektiv och en riskanalys och vara proportionella i förhållande till risken. De ska utvärderas och särskilt innefatta följande:

1. Incidenthantering,
2. kontinuitetshantering,
3. säkerhet i leveranskedjan,
4. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinformation,
5. strategier och förfaranden för användning av kryptografi och kryptering,
6. personalsäkerhet,
7. strategier för åtkomstkontroll och tillgångsförvaltning,
8. säkrade lösningar för kommunikation, och
9. lösningar för autentisering.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om riskhanteringsåtgärder.

2 § Verksamhetsutövare ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om systematiskt och riskbaserat informationssäkerhetsarbete.

3 § Ledningen i enskilda och offentliga verksamheter ska genomgå utbildning om riskhanteringsåtgärder och anställda ska erbjudas sådan utbildning.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om utbildning.

4 § Med betydande incident avses

1. En incident som orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller
2. en incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om vad som utgör en betydande incident.

5 § Verksamhetsutövaren ska som en varning underrätta CSIRT-enheten om betydande incidenter inom 24 timmar efter det att verksamhetsutövaren fått kännedom om den. Det ska anges om att det finns misstanke om incidenten orsakats uppsåtligen och om incidenten kan ha gränsöverskridande effekter.

6 § Verksamhetsutövaren ska också inom 72 timmar från tidpunkten från kännedom göra en incidentanmälan till CSIRT-enheten om betydande incidenter. Den ska innehålla en inledande bedömning av hur allvarlig den betydande incidenten är, konsekvenserna av den och förekomsten av angreppsindikatorer. Vidare ska tidigare varning enligt 5 § uppdateras.

För verksamhetsutövare som erbjuder betrodda tjänster ska en incidentanmälan göras inom 24 timmar.

CSIRT-enheten får begära ytterligare information av verksamhetsutövaren.

Verksamhetsutövaren ska samtidigt även informera kunder som kan antas påverkas av den betydande incidenten. Kunderna ska vid behov informeras om avhjälpande åtgärder. Detsamma gäller betydande cyberhot.

7 § Verksamhetsutövaren ska inom en månad från incidentanmälan i 5 § lämna en slutrapport till CSIRT-enheten. Om incidenten fortfarande är pågående ska i stället en lägesrapport lämnas som ska kompletteras med en slutrapport en månad efter det att incidenten har hanterats. Slutrapporten eller lägesrapporten ska innehålla en beskrivning av

1. Incidenten och dess konsekvenser,
2. hur allvarlig incidenten bedöms vara,
3. vad som sannolikt utlöst incidenten,
4. åtgärderna för att begränsa incidenten, och
5. incidentens möjliga gränsöverskridande effekter.

8 § Regeringen eller den myndigheten regeringen bestämmer får meddela föreskrifter om incidentrapporteringen enligt 5–7 §§.

4 kap. Tillsyn

Tillsynsmyndighet

1 § Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet.

Tillsynsmyndighetens uppdrag

2 § Tillsynsmyndigheten ska utöva tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs.

3 § Tillsynsåtgärder för viktiga verksamhetsutövare får vidtas endast när tillsynsmyndigheten har befogad anledning att anta att denna lag eller föreskrifter som meddelats i anslutning till lagen inte följs.

Tillsynsmyndighetens undersökningsbefogenheter

4 § Den som står under tillsyn ska på begäran tillhandahålla tillsynsmyndigheten den information som behövs för tillsyn.

5 § Tillsynsmyndigheten har i den omfattning det behövs för tillsynen rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamheten.

6 § Tillsynsmyndigheten får förelägga den som står under tillsyn att tillhandahålla information och ge tillträde enligt 4 och 5 §§.

Ett sådant föreläggande får förenas med vite.

7 § Tillsynsmyndigheten får begära handräckning av Kronofogdemyndigheten för att genomföra de åtgärder som avses i 4 och 5 §§. Vid handräckning gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

Säkerhetsrevision

8 § Tillsynsmyndigheten får om det finns särskilda skäl ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att redovisa resultatet för tillsynsmyndigheten.

Tillsynsmyndigheten får även anlita ett oberoende organ för att utföra regelbundna säkerhetsrevisioner av väsentliga verksamhetsutövare.

Regeringen får meddela föreskrifter om säkerhetsrevisioner.

Säkerhetsskanning

9 § Tillsynsmyndigheten får låta genomföra säkerhetsskanningar hos verksamhetsutövare som omfattas av denna lag.

En säkerhetsskanning ska ske i samarbete med verksamhetsutövaren.

5 kap. Ingripanden och sanktioner

Inledande bestämmelser

1 § Tillsynsmyndigheten ska ingripa om en verksamhetsutövare har åsidosatt sina skyldigheter enligt denna lag, eller föreskrifter som har meddelats med stöd av bestämmelserna om

1. skyldighet att utse företrädare enligt 1 kap. 6 §,
2. anmälningsskyldighet enligt 2 kap. 2 §,
3. riskhanteringsåtgärder enligt 3 kap. 1 §,
4. utbildning enligt 3 kap. 3 §, eller
5. incidentrapportering enligt 3 kap. 5–7 §§.

2 § Ingripanden sker genom att tillsynsmyndigheten

1. meddelar föreläggande enligt 6 §,
2. ansöker om förbud att utöva ledningsfunktion enligt 7 §, eller
3. meddelar sanktionsavgift enligt 11 §.

Om tillsynsmyndigheten inte finner skäl att ingripa enligt första stycket ska den i stället meddela verksamhetsutövaren en anmärkning.

Tillsynsmyndigheten får avstå från att ingripa enligt första och andra stycket om någon annan tillsynsmyndighet har vidtagit åtgärder mot

verksamhetsutövaren eller den fysiska personen med anledning av överträdelsen, och tillsynsmyndigheten bedömer att dessa åtgärder är tillräckliga.

Omständigheter som ska beaktas vid ett ingripande

3 § Vid val och utformning av ingripandeåtgärder enligt 2 § ska hänsyn tas till hur allvarlig överträdelsen är, hur länge den har pågått, samt den skada eller risk för skada som uppstått till följd av överträdelsen.

Vid bedömningen ska särskilt beaktas

1. de åtgärder verksamhetsutövaren vidtagit för att förhindra eller minska skadan,
2. verksamhetsutövarens samarbete med tillsynsmyndigheten,
3. om överträdelsen begåtts med uppsåt eller oaktsamhet, och
4. den ekonomiska fördel som verksamhetsutövaren fått till följd av överträdelsen.

4 § Utöver vad som anges i 3 § ska det beaktas som försvårande om verksamhetsutövaren tidigare har begått en överträdelse.

I förmildrande riktning ska beaktas om verksamhetsutövaren har följt godkända uppförandekoder eller godkända certifieringsmekanismer.

5 § En överträdelse ska betraktas som allvarlig om verksamhetsutövaren

1. har begått upprepade överträdelser,
2. inte har rapporterat eller avhjälpt en betydande incident,
3. inte har följt ett tidigare föreläggande från en tillsynsmyndighet,
4. har hindrat säkerhetsrevisioner eller tillsynsåtgärder som tillsynsmyndigheten beslutat om, eller
5. har lämnat oriktiga uppgifter avseende riskhanteringsåtgärder eller rapporteringsskyldigheter enligt 3 kap. 1 eller 5–7 §§.

Förelägganden

6 § Tillsynsmyndigheten får meddela de förelägganden som behövs för att verksamhetsutövare ska uppfylla skyldigheterna som följer av 1 §.

Förelägganden enligt denna paragraf får förenas med vite.

7 § Tillsynsmyndigheten får förelägga en verksamhetsutövare att offentliggöra information på det sätt som tillsynsmyndigheten beslutar rörande överträdelser av denna lag och föreskrifter som har meddelats med stöd av lagen.

Tillsynsmyndigheten får förelägga en verksamhetsutövare att informera de användare som kan påverkas av ett betydande cyberhot om hotet och vilka skydds- eller motåtgärder de kan vidta.

Förelägganden enligt denna paragraf får förenas med vite.

Förbud att utöva ledningsfunktion

8 § Om ett föreläggande enligt 6 § inte följts får tillsynsmyndigheten ingripa mot en person som ingår i verksamhetsutövarens ledning. Ingripande sker genom att tillsynsmyndigheten ansöker hos allmän

förvaltningsdomstol om att en person inte ska få vara befattningshavare hos en viss verksamhetsutövare (förbud).

Ett sådant ingripande får riktas mot den som är befattningshavare enligt 3 § andra stycket lagen (2014:836) om näringsförbud.

Ett ingripande får endast göras om överträdelsen som ligger till grund för föreläggandet är allvarlig och om personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

9 § Ett beslut om förbud enligt 8 § fattas av förvaltningsrätten på ansökan från tillsynsmyndigheten. En ansökan ska innehålla uppgifter om

1. den person som ansökan avser,
2. verksamhetsutövaren,
3. överträdelsen och de omständigheter som behövs för att kännetecknа den, och
4. de bestämmelser som är tillämpliga på överträdelsen.

Ett förbud ska tidsbegränsas till lägst ett år och högst tre år och ska upphävas omedelbart när föreläggandet har följts.

Förbud får inte riktas mot offentliga verksamhetsutövare.

Ansökan ska prövas skyndsamt av domstolen.

10 § Ett beslut om förbud ska upphävas om det inte längre finns förutsättningar för förbudet.

11 § Förvaltningsrätten ska pröva om ett beslutat förbud ska upphävas om tillsynsmyndigheten eller den enskilde begär det, eller om det annars finns skäl för det. Den enskilde ska upplysas om sin rätt att begära att ett förbud ska upphävas.

Om tillsynsmyndigheten bedömer att det inte längre finns förutsättningar för förbudet ska den omedelbart begära att förvaltningsrätten ska upphäva förbudet.

Sanktionsavgift

12 § Tillsynsmyndigheten får besluta att en verksamhetsutövare ska betala en sanktionsavgift till följd av en överträdelse enligt 1 §.

Sanktionsavgiftens storlek

13 § Sanktionsavgiften ska för väsentliga verksamhetsutövare bestämmas till lägst 5 000 kr och högst till det högsta av:

1. Två procent av den väsentliga verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 10 000 000 euro.

14 § Sanktionsavgiften ska för viktiga verksamhetsutövare bestämmas till lägst 5 000 kr och högst till det högsta av:

1. 1,4 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 7 000 000 euro.

15 § Sanktionsavgiften ska för offentliga verksamhetsutövare bestämmas till lägst 5 000 kr och högst 10 000 000 kr.

Hur sanktionsavgiften ska bestämmas

16 § När sanktionsavgiftens storlek bestäms ska tillsynsmyndigheten särskilt beakta de omständigheter som följer av 3–5 §§.

Hinder mot att ta ut sanktionsavgift

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

En sanktionsavgift får inte heller beslutas för samma överträdelse som lett till att verksamhetsutövaren har påförts en sanktionsavgift enligt Allmänna dataskyddsförordningen.

Betalning, verkställighet och preskription

18 § En sanktionsavgift får endast tas ut om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Beslut om sanktionsavgift ska delges.

19 § Sanktionsavgiften ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas i rätt tid, ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning ska verkställighet få ske enligt utsökningsbalken.

Sanktionsavgift tillfaller staten.

20 § 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.

Förordnande om att beslut ska gälla omedelbart

21 § Tillsynsmyndigheten får bestämma att ett beslut om föreläggande enligt denna lag ska gälla omedelbart.

6 kap. Överklagande

1 § Tillsynsmyndighetens beslut enligt denna lag eller anslutande föreskrifter får överklagas till allmän förvaltningsdomstol. När ett sådant beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

---

1. Denna lag träder i kraft den 1 januari 2025.

2. Genom lagen upphävs lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Lagen ska dock fortfarande gälla för överträdelser som har skett före ikraftträdandet.

Förslag till lag om ändring i lagen (2006:24) om nationella toppdomäner för Sverige på internet

Härigenom föreskrivs att rubriken till lag (2006:24) om nationella toppdomäner för Sverige på internet samt 1, 2 och 6 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
Lag om *nationella* toppdomäner *för Sverige* på internet	**Lag om toppdomäner på internet**
1 §	
Denna lag gäller teknisk drift av *nationella* toppdomäner *för* Sverige på *I*nternet *samt* tilldelning och registrering av domännamn under dessa toppdomäner.	Denna lag gäller teknisk drift av toppdomäner *med huvudsakligt etableringsställe i* Sverige på *i*nternet. *Vidare omfattar lagen* tilldelning och registrering av domännamn under dessa toppdomäner.
2 §	
I denna lag avses med	
domännamnssystemet: det internationella hierarkiska system som för befordringsändamål på Internet används för att tilldela domännamn,	
domän: nivå i domännamnssystemet och del av domännamn,	
domännamn: unikt namn sammansatt av domäner, där en i domännamnssystemet lägre placerad domän står före en domän som är högre placerad i systemet,	
toppdomän: den domän som återfinns sist i ett domännamn,	
nationell toppdomän: toppdomän som betecknar en nation eller en region,	
administration: teknisk drift av en toppdomän samt tilldelning och registrering av domännamn under denna,	
domänadministratör: den som ansvarar för administration av en *nationell* toppdomän *för* Sverige,	domänadministratör: den som ansvarar för administration av en toppdomän,
namnserver: dator i ett elektroniskt kommunikationsnät som programmerats så att den lagrar och distribuerar information om domännamn samt tar emot och svarar på frågor om domännamn.	
6 §	
En domänadministratör *skall* föra ett register över tilldelade domännamn under toppdomänen och löpande upprätta	En domänadministratör *ska* föra ett register över tilldelade domännamn under toppdomänen och löpande upprätta

Bilaga 3

säkerhetskopior av registeruppgifterna	säkerhetskopior av registeruppgifterna
Registret *skall* innehålla	Registret *ska* innehålla
1. domännamnet,	
2. namnet på domännamnsinnehavaren och dennes postadress, telefonnummer och adress för elektronisk post,	
3. namnet på den som tekniskt administrerar domännamnet och dennes postadress, telefonnummer och adress för elektronisk post,	
4. uppgifter om de namnservrar som är knutna till domännamnet, *samt*	4. uppgifter om de namnservrar som är knutna till domännamnet,
5. övrig teknisk information som behövs för att administrera domännamnet.	5. övrig teknisk information som behövs för att administrera domännamnet, *och*
	6. registreringsdatum.
Uppgifterna i registret *skall* kunna hämtas utan avgift via *I*nternet.	Uppgifterna i registret *ska* kunna hämtas utan avgift via *i*nternet. *Därutöver ska uppgifter även på begäran lämnas ut skyndsamt till myndigheter och andra med offentligrättsliga uppgifter inom EES.*
Personuppgifter får *dock* göras tillgängliga på *detta sätt endast* om den registrerade har samtyckt till det.	Personuppgifter får *endast* göras tillgängliga på *internet* om den registrerade har samtyckt till det.
Domänadministratören är personuppgiftsansvarig för behandling av personuppgifter i registret.	

Denna lag träder i kraft den 1 januari 2025.

Förslag till lag om ändring i lagen (2022:482) om elektronisk kommunikation

Härigenom föreskrivs i fråga om lagen (2022:482) om elektronisk kommunikation

dels att 8 kap. 1–4 §§ ska upphöra att gälla,
dels att 12 kap. 1 § ska ha följande lydelse,
dels att rubriken närmast före 8 kap. 1 § ska utgå.

Nuvarande lydelse	*Föreslagen lydelse*
12 kap.	
1 §[1]	
Tillsynsmyndigheten ska besluta att ta ut en sanktionsavgift av den som	
1. inte tillhandahåller en sammanfattning av avtalet i enlighet med 7 kap. 1 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 102.3 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,	
2. inte tillämpar villkor om bindningstid eller uppsägningstid i enlighet med 7 kap. 8, 13 eller 14 §,	
3. inte uppfyller kraven på nummerportabilitet i enlighet med 7 kap. 19 och 20 §§ eller föreskrifter om nummerportabilitet som har meddelats med stöd av 7 kap. 21 § första stycket,	
4. inte vidtar åtgärder för att hantera risker som hotar säkerheten i nät och tjänster i enlighet med 8 kap. 1 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,	
5. inte rapporterar om säkerhetsincidenter i enlighet med 8 kap. 3 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,	
6. inte informerar om hot om säkerhetsincidenter i enlighet med 8 kap. 4 §, föreskrifter som har	

[1] Senaste lydelse 2023:411.

meddelats med stöd av den paragrafen eller genomförande-akter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,	
7. inte vidtar skyddsåtgärder i enlighet med 8 kap. 5 § eller föreskrifter som har meddelats med stöd av den paragrafen,	*4*. inte vidtar skyddsåtgärder i enlighet med 8 kap. 5 § eller föreskrifter som har meddelats med stöd av den paragrafen,
8. inte vidtar åtgärder för att säkerställa skydd av uppgifter som behandlas i samband med tillhandahållandet av en tjänst i enlighet med 8 kap. 6 § eller föreskrifter som har meddelats med stöd av den paragrafen,	*5*. inte vidtar åtgärder för att säkerställa skydd av uppgifter som behandlas i samband med tillhandahållandet av en tjänst i enlighet med 8 kap. 6 § eller föreskrifter som har meddelats med stöd av den paragrafen,
9. inte informerar abonnenten om särskilda risker för bristande skydd av behandlade uppgifter i enlighet med 8 kap. 7 §,	*6*. inte informerar abonnenten om särskilda risker för bristande skydd av behandlade uppgifter i enlighet med 8 kap. 7 §,
10. inte underrättar om integritetsincidenter i enlighet med 8 kap. 8 § eller 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,	*7*. inte underrättar om integritetsincidenter i enlighet med 8 kap. 8 § eller 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,
11. inte behandlar uppgifter i ett elektroniskt meddelande eller trafikuppgifter som hör till detta meddelande i enlighet med 9 kap. 27 §,	*8*. inte behandlar uppgifter i ett elektroniskt meddelande eller trafikuppgifter som hör till detta meddelande i enlighet med 9 kap. 27 §,
12. inte bedriver sin verksamhet så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs i enlighet med 9 kap. 29 § första stycket eller föreskrifter som har meddelats i anslutning till det stycket,	*9*. inte bedriver sin verksamhet så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs i enlighet med 9 kap. 29 § första stycket eller föreskrifter som har meddelats i anslutning till det stycket,
13. inte ordnar uppgifter och gör dem tillgängliga i ett format som gör att de enkelt kan tas om hand i	*10*. inte ordnar uppgifter och gör dem tillgängliga i ett format som gör att de enkelt kan tas om hand i

enlighet med 9 kap. 29 b § andra stycket eller föreskrifter som har meddelats i anslutning till det stycket,	enlighet med 9 kap. 29 b § andra stycket eller föreskrifter som har meddelats i anslutning till det stycket,
14. inte överför signaler till samverkanspunkter i enlighet med 9 kap. 30 § eller föreskrifter som har meddelats med stöd av den paragrafen, eller	*11*. inte överför signaler till samverkanspunkter i enlighet med 9 kap. 30 § eller föreskrifter som har meddelats med stöd av den paragrafen, eller
15. inte lämnar ut en uppgift i enlighet med 9 kap. 33 §.	*12*. inte lämnar ut en uppgift i enlighet med 9 kap. 33 §.

En sanktionsavgift enligt första stycket 2 ska, när det är fråga om ett paket enligt 7 kap. 26 §, tas ut endast om överträdelsen avser en allmänt tillgänglig elektronisk kommunikationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst eller en överföringstjänst som används för tillhandahållande av maskin-till-maskin-tjänster.

---

1. Denna lag träder i kraft den 1 januari 2025.
2. Äldre bestämmelser gäller fortfarande för överträdelser som skett före ikraftträdandet.

Förteckning över remissinstanserna

Efter remiss har yttranden över delbetänkandet inkommit från Affärsverket svenska kraftnät, Bankgirocentralen BGC AB, Bolagsverket, Brottsförebyggande rådet, Brottsoffermyndigheten, Certezza AB, Chalmers tekniska högskola, Domstolsverket, Drivkraft Sverige, E-hälsomyndigheten, Ekobrottsmyndigheten, Energiföretagen Sverige, Energimarknadsinspektionen, Euroclear Sweden AB, Finansbolagens Förening, Finansiell ID-Teknik BID AB, Finansinspektionen, Flens kommun, Fortifikationsverket, Företagarna, Försvarets materielverk, Försvarets radioanstalt, Försvarshögskolan, Försvarsmakten, Försvarsunderrättelsedomstolen, Försäkringskassan, Förvaltningsrätten i Malmö, Gentekniknämnden, Gotlands kommun, Gymnastik- och idrottshögskolan, Gävle kommun, Göteborgs kommun, Hi3G Access AB, IKEM Innovations- och kemiindustrierna i Sverige, Inspektionen för strategiska produkter, Inspektionen för vård och omsorg, Integritetsskyddsmyndigheten, Jönköpings kommun, Kalmar kommun, Kammarrätten i Stockholm, Karlskrona kommun, Karlstads kommun, Karolinska institutet, Kemikalieinspektionen, Kommerskollegium, Konkurrensverket, Kriminalvården, Kronofogdemyndigheten, Kungl. Tekniska högskolan, Kustbevakningen, Lantbrukarnas riksförbund, Lantmännen, Lantmäteriet, Linköpings kommun, Livsmedelsföretagen, Livsmedelsverket, Luftfartsverket, Luleå kommun, Lunds universitet, Läkemedelsindustriföreningen, Läkemedelsverket, Länsstyrelsen i Blekinge län, Länsstyrelsen i Dalarnas län, Länsstyrelsen i Gotlands län, Länsstyrelsen i Gävleborgs län, Länsstyrelsen i Hallands län, Länsstyrelsen i Jämtlands län, Länsstyrelsen i Jönköpings län, Länsstyrelsen i Kalmar län, Länsstyrelsen i Kronobergs län, Länsstyrelsen i Norrbottens län, Länsstyrelsen i Skåne län, Länsstyrelsen i Stockholms län, Länsstyrelsen i Södermanlands län, Länsstyrelsen i Uppsala län, Länsstyrelsen i Värmlands län, Länsstyrelsen i Västerbottens län, Länsstyrelsen i Västernorrlands län, Länsstyrelsen i Västmanlands län, Länsstyrelsen i Västra Götalands län, Länsstyrelsen i Örebro län, Länsstyrelsen i Östergötlands län, Malmö kommun, Mittuniversitetet, Myndigheten för digital förvaltning, Myndigheten för psykologiskt försvar, Myndigheten för samhällsskydd och beredskap, Myndigheten för totalförsvarsanalys, Naturvårdsverket, Netnod AB, Nynäshamns kommun, Patent- och registreringsverket, Pensionsmyndigheten, Polismyndigheten, Post- och telestyrelsen, Regelrådet, Region Jönköpings län, Region Skåne, Region Stockholm, Region Sörmland, Riksgäldskontoret, Rymdstyrelsen, Rättsmedicinalverket, Salems kommun, Scrive AB, SJ AB, Sjöfartsverket, Skatteverket, Socialstyrelsen, Sparbankernas Riksförbund, Statens energimyndighet, Statens haverikommission, Statens jordbruksverk, Statens inspektion för försvarsunderrättelseverksamhet, Statens servicecenter, Statens veterinärmedicinska anstalt, Statistiska centralbyrån, Statskontoret, Stiftelsen för internetinfrastruktur, Stockholm Vatten och Avfall AB, Stockholms kommun, Stockholms universitet, Strålsäkerhetsmyndigheten, Strängnäs kommun, Svensk Elektronik, Svensk Handel, Svensk Sjöfart, Svenska Bankföreningen, Svenska Stadsnätsföreningen, Svenskt Näringsliv, Svenskt Vatten, Sveriges Kommuner och Regioner, Swedish Medtech, Säkerhets- och försvarsföretagen, Säkerhets- och integritetsskydds-

nämnden, Säkerhetspolisen, Tech Sverige, Teknikföretagen, Tele2 Sverige AB, Telefonaktiebolaget LM Ericsson, Telenor Sverige AB, Teracom Group AB, Tillväxtverket, Totalförsvarets forskningsinstitut, Totalförsvarets plikt- och prövningsverk, Trafikverket, Transportföretagen, Transportstyrelsen, Trelleborgs kommun, Tullverket, Tågföretagen, Umeå kommun, Uppsala universitet, Utbetalningsmyndigheten, Valmyndigheten, Verket för innovationssystem (Vinnova), Vetenskapsrådet, Växjö kommun, Åklagarmyndigheten, Östersunds kommun och Östhammars kommun.

Därutöver har yttranden inkommit från Advokatfirman Kahn Pedersen, AMF Fastigheter, Castellum AB, CreativityWorks!, Eskilstuna Kommunfastigheter AB, Fastighetsägarna, Föreningen för Digitala Fri- och Rättigheter, Förvaltningsrätten i Stockholm, GovSec Sweden AB, Hufvudstaden AB, Högskolan i Borås, ICANN Business Constituency, Ifpi Sverige, ISACA Sweden Chapter, Kollegiet för svensk bolagsstyrning, Kungl. Musikhögskolan, LawSec Sweden AB, Linköpings universitet, M^{3}AAWG, Marie Cederschiöld högskola, MTR, Mälardalens universitet, Nacka kommun, Orange Cyberdefense Sweden AB, Prolegia Research AB, Rättighetsalliansen, Skellefteå kommun, Sophiahemmet Högskola, Stiftelsen Högskolan i Jönköping, Styrelseakademien, Styrelsen för ackreditering och teknisk kontroll (Swedac), Svensk Dagligvaruhandel, Svenska Föreningen mot Piratkopiering, Sveriges advokatsamfund, Sveriges Allmännytta, Sveriges universitets- och högskoleförbund, Swedsoft, Södertörns högskola, The Swedish Association of Small and Medium Size Enterprises in Defense and Security (SME-D), TV4, Örebro universitet, en arbetsgrupp inom Cybernoden samt tre privatpersoner.

Följande remissinstanser har inte svarat eller angett att de avstår från att lämna några synpunkter: AB Volvo, ACR Aviation Capacity Resources AB, Apple Aktiebolag, Arelion Sweden AB, Avfall Sverige, Bring Mail Nordic AB, CGI Sverige AB, COWI AB, Dataskydd.net, Energigas Sverige, Enköpings kommun, Facebook Sweden AB, Falkenbergs kommun, Falu kommun, Getswish AB, GlobalConnect AB, Google Sweden AB, Hexagon AB, Inera AB, Kalix kommun, Karlskoga kommun, Leksands kommun, Lilla Edets kommun, Livsmedelsgrossisterna, Loopia Group AB, Nasdaq Clearing AB, Nasdaq Stockholm AB, Nordic Growth Market NGM AB, On Tower Sweden AB/Cellnex Sverige, PostNord Sverige AB, Region Norrbotten, Region Östergötland, Riksdagens ombudsmän, Riksrevisionen, RISE Research Institutes of Sweden, Scania AB, Spotlight Group AB, Sundsvalls kommun, Svensk Torv, Svenska rymdaktiebolaget (SSC), Sveriges Hamnar, Sveriges riksbank, Swedavia AB, Swedegas AB, Swedish FinTech Association, Säffle kommun, Telia Company AB, Tietoevry AB, Truesec AB, Volvo Car AB, Vårdföretagarna och Västerås kommun.

Sammanfattning av slutbetänkandet Motståndskraft i samhällsviktiga tjänster (SOU 2024:64)

CER-direktivet

Europaparlamentet och rådet antog den 14 december 2022 CER-direktivet[1]. Direktivets syfte är att stärka kritiska verksamhetsutövares motståndskraft och förmåga att tillhandahålla samhälls-viktiga tjänster på den inre marknaden.

Enligt direktivet ska medlemsstaterna senast den 17 juli 2026 identifiera verksamhetsutövare som erbjuder samhällsviktiga tjänster inom sektorerna energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, offentlig förvaltning, rymden samt produktion, bearbetning och distribution av livsmedel. Medlemsstaterna ska senast den 17 januari 2026 ta fram en nationell riskbedömning och en strategi för kritiska verksamhetsutövares motståndskraft.

Direktivet ställer krav på kritiska verksamhetsutövare, de ska göra en riskbedömning och vidta åtgärder för motståndskraft inklusive bakgrundskontroller i syfte att stärka motståndskraften samt rapportera incidenter. Riskbedömningen ska göras inom nio månader från mottagandet av underrättelsen om identifiering. Kravet på åtgärder för motståndskraft ska tillämpas först tio månader efter att den kritiska verksamhetsutövaren har underrättats om identifieringen. I direktivet finns också bestämmelser om kritiska verksamhetsutövare av särskild europeisk betydelse.

Direktivet innehåller vidare bestämmelser om tillsyn och sanktioner samt en ram för samarbete mellan medlemsstaterna.

Direktivet är ett minimidirektiv med innebörd att den svenska lagstiftningen skulle kunna innehålla mer långtgående skyldigheter. Medlemsstaterna ska senast den 17 oktober 2024 anta och offentliggöra de bestämmelser som är nödvändiga för att följa direktivet. Bestämmelserna ska tillämpas från och med den 18 oktober 2024.

Direktivet ersätter rådets direktiv 2008/114/EG om identifiering av, klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna som upphör att gälla med verkan från och med den 18 oktober 2024. Hänvisningar i det upphävda direktivet ska anses som hänvisningar till det här direktivet.

Utredningens uppdrag

Utredningen redovisar i detta slutbetänkande förslag om införlivning av CER-direktivet i svensk rätt samt förslag till ändring i offentlighets- och sekretessbestämmelserna, ändring i säkerhetsskyddslagen samt i lagen om

[1] 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.

cybersäkerhet. Utredningen redovisade i delbetänkandet Nya regler om cybersäkerhet, SOU 2024:18 förslag om införlivning av NIS2-direktivet[2].

Utredningens uppdrag har varit att föreslå de anpassningar av svensk rätt som är nödvändiga för att CER-direktivet ska kunna genomföras. Det har innefattat att föreslå hur identifiering och krav på verksamhetsutövare som omfattas av direktivet ska regleras samt rollfördelningen mellan svenska myndigheter med avseende på de olika uppgifter och ansvarsområden som föreskrivs i CER-direktivet.

I utredningens uppdrag har även ingått att ta ställning till om bestämmelserna i offentlighets- och sekretesslagen (2009:400) innebär ett tillräckligt skydd för sådana uppgifter som kan komma att behandlas enligt NIS2- och CER-direktiven, föreslå de ändringar som behövs för en mer sammanhållen systematik mellan säkerhetsskyddslagen, lagen om cybersäkerhet och lagen om motståndskraft hos kritiska verksamhetsutövare, särskilt vad gäller tillsynsmyndigheternas befogenheter och sanktionsavgifternas storlek.

Utredningen ska vidare beakta de frågor som är gemensamma för NIS2- och CER-direktiven i den mån dessa är hänförliga till genomförandet av CER-direktivet.

Utredningens förslag

Lagen om motståndskraft hos kritiska verksamhetsutövare

Utredningen föreslår att CER-direktivet införlivas genom en ny lag, lagen om motståndskraft hos kritiska verksamhetsutövare. Utredningen föreslår inte några skyldigheter utöver vad som följer av direktivet.

Vem omfattas av reglerna om motståndskraft hos kritiska verksamhetsutövare?

Regelverket ska tillämpas på enskilda och offentliga verksamhetsutövare som tillhandahåller en samhällsviktig tjänst som omfattas av bilagan till direktivet. Vidare krävs att verksamhetsutövaren har identifierats som kritisk av tillsynsmyndigheten. För kritiska verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur gäller endast vissa begränsade delar av regelverket.

I förslaget görs vissa undantag från lagens tillämpningsområde. Lagen gäller inte för sådant som regleras i förslaget till lag om cybersäkerhet och inte heller om det i annan författning finns bestämmelser om krav på riskbedömning, åtgärder för motståndskraft, bakgrundskontroll och incidentrapportering om kraven har minst motsvarande verkan. Lagen gäller inte heller för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, Riksrevisionen, Riksdagens ombudsmän, Sveriges Riksbank, Riksdagsförvaltningen eller Sveriges domstolar.

Lagen gäller inte för statliga myndigheter som till övervägande del bedriver brottsbekämpning eller säkerhetskänslig verksamhet. För övriga

[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)

verksamhetsutövare gäller inte 3–6 kap. i lagen för den del av den samhällsviktiga tjänsten som är säkerhetskänslig. Det innebär att dessa verksamhetsutövare bland annat omfattas av bestämmelserna om identifiering i 2 kap. i den föreslagna lagen.

Identifiering av kritiska verksamhetsutövare

Tillsynsmyndigheterna ska genom beslut identifiera kritiska verksamhetsutövare inom sina tillsynsområden. För att en verksamhetsutövare ska identifieras som kritisk enligt direktivet ska tre kriterier vara uppfyllda. För det första ska verksamhetsutövaren tillhandahålla en eller flera samhällsviktiga tjänster inom någon av sektorerna som finns i bilagan till direktivet, för det andra ska verksamhetsutövaren ha en kritisk infrastruktur belägen i Sverige och för det tredje ska en incident få betydande störande effekter för tillhandahållandet av den samhällsviktiga tjänsten. Myndigheten för samhällsskydd och beredskap ska meddela föreskrifter om när en störande effekt är betydande.

Vid identifieringen ska tillsynsmyndigheten beakta den nationella riskbedömningen och strategin för kritiska verksamhetsutövares motståndskraft.

Tillsynsmyndigheten ska upprätta en förteckning över kritiska verksamhetsutövare inom sitt tillsynsområde. Myndigheten för samhällsskydd och beredskap ska upprätta en samlad förteckning över samtliga kritiska verksamhetsutövare.

Kritiska verksamhetsutövare av särskild europeisk betydelse

Kritiska verksamhetsutövare som tillhandahåller en samhällsviktig tjänst till eller i minst sex medlemsstater ska anmäla detta till tillsynsmyndigheten. Dessa verksamhetsutövare ska delta i kommissionens samråd. På grundval av samrådet fastställer kommissionen om den kritiska verksamhetsutövaren är av särskild europeisk betydelse.

Myndigheten för samhällsskydd och beredskap tar emot kommissionens underrättelse om att en kritisk verksamhetsutövare är av särskild europeisk betydelse och vidarebefordrar den till tillsynsmyndigheten. Tillsynsmyndigheten underrättar den kritiska verksamhetsutövaren.

Kommissionen anordnar rådgivande uppdrag för att bedöma de åtgärder som den kritiska verksamhetsutövaren har infört för att uppfylla sina skyldigheter. Ett rådgivande uppdrag får endast genomföras om MSB efter samråd med den kritiska verksamhetsutövaren och dennas tillsynsmyndighet, lämnat samtycke.

Krav på riskbedömning, åtgärder för motståndskraft och incidentrapportering

Utredningen föreslår att Myndigheten för samhällsskydd och beredskap ska göra en nationell riskbedömning.

En kritisk verksamhetsutövare ska göra en riskbedömning nio månader efter att den fått del av beslutet om identifiering. Riskbedömningen ska

innehålla en redogörelse för alla relevanta risker som skulle kunna leda till en incident.

Verksamhetsutövaren ska vidare vidta tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft. Åtgärderna ska vidtas på grundval av riskbedömningen, utgå från ett allriskperspektiv och vara proportionella i förhållande till risken. Det ska finnas en plan som beskriver åtgärder som vidtagits eller ska vidtas. Tillsynsmyndigheterna får meddela föreskrifter om riskbedömning, åtgärder och planer för motståndskraft. Myndigheten för samhällsskydd och beredskap får meddela föreskrifter för sektorn offentlig förvaltning.

Kritiska verksamhetsutövare ska utan dröjsmål rapportera incidenter som medför eller kan medföra en betydande störning i tillhandahållandet av den samhällsviktiga tjänsten till Myndigheten för samhällsskydd och beredskap. En första rapport ska lämnas inom 24 timmar. Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om vad som utgör en betydande störning och om incidentrapportering.

Skyldigheterna avseende åtgärder och incidentrapportering börjar gälla först tio månader efter den dag verksamhetsutövaren fått del av tillsynsmyndighetens beslut om identifiering.

Kritiska verksamhetsutövare ska också utse en samverkansansvarig som utgör kontaktpunkt för berörda myndigheter.

Bakgrundskontroll

Syftet med en bakgrundskontroll är att endast den som bedöms lämplig ska få vara anställd eller på annat sätt delta i befattningar där deltagandet kan orsaka mer än ringa skada på den samhällsviktiga tjänsten.
Utredningen föreslår att kritiska verksamhetsutövare ska göra en befattningsanalys där det framgår för vilka befattningar det finns ett krav på bakgrundskontroll. Analysen ska dokumenteras.

Den kritiska verksamhetsutövaren ska genomföra bakgrundskontrollen och bedöma om personen som kontrollen avser är lämplig. En bakgrundskontroll innebär att den som kontrolleras ska styrka sin identitet och visa upp ett särskilt utdrag från belastningsregistret. Av förordningen (1999:1134) om belastningsregister framgår vilka uppgifter ett utdrag ska innehålla.

Det ska dokumenteras att en bakgrundskontroll genomförts och anteckningen ska bevaras i två år.

Tillsyn

Utredningen föreslår att den tillsynsmyndighet som är tillsynsmyndighet enligt den föreslagna lagen om cybersäkerhet även blir tillsynsmyndighet enligt lagen om motståndskraft hos kritiska verksamhetsutövare. Ett fåtal tillsynsmyndigheter har fått ny undersektor eller kategori av entitet. Vidare ingår i sektorn offentlig förvaltning endast statliga myndigheter. Följande tillsynsmyndigheter föreslås.

Tillsynsmyndighet	**Sektor**
Statens energimyndighet	Energi
Transportstyrelsen	Transport
Finansinspektionen	Bankverksamhet

Tillsynsmyndighet	Sektor
	Finansmarknadsinfrastruktur
Inspektionen för vård och omsorg	Vårdgivare[3] i Hälso- och sjukvårdssektorn
Läkemedelsverket	Hälso- och sjukvårdssektorn, med undantag för vårdgivare
Livsmedelsverket	Avloppsvatten Dricksvatten Produktion, bearbetning och distribution av livsmedel
Post- och telestyrelsen	Digital infrastruktur
	Rymden
Länsstyrelserna i Norrbottens, Skåne, Stockholms och Västra Götalands län	Offentlig förvaltning

Tillsynsmyndigheten ska utöva tillsyn över att lagen och föreskrifter som meddelats i anslutning till lagen följs.

Kritiska verksamhetsutövare ska tillhandahålla tillsynsmyndigheten den information som behövs för tillsynen och den nationella riskbedömningen. Tillsynsmyndigheten har också rätt att få tillträde till områden, lokaler och andra utrymmen i den omfattning som behövs för tillsynen. Undantag görs för uppgifter som är säkerhetsskyddsklassificerade och tillträde till verksamhet där säkerhetskänslig verksamhet bedrivs.

MSB ska leda ett samarbetsforum där tillsynsmyndigheterna ingår för att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

Inom ramen för tillsyn ska tillsynsmyndigheten även genomföra rådgivande uppdrag som anordnas av kommissionen avseende kritiska verksamhetsutövare av särskild europeisk betydelse.

Tillsynsmyndigheten ska även bidra med underlag till den nationella riskbedömningen.

Gemensam kontaktpunkt

Myndigheten för samhällsskydd och beredskap ska vara gemensam kontaktpunkt. Den gemensamma kontaktpunkten ska ha en sambandsfunktion för att säkerställa det gränsöverskridande samarbetet med gemensamma kontaktpunkter i andra medlemsstater och med kommissionen.

Ingripande och sanktioner

Utredningen föreslår att ingripande sker genom att tillsynsmyndigheten beslutar om föreläggande, sanktionsavgift eller anmärkning. Tillsynsmyndigheten ska ingripa mot den som åsidosatt skyldigheten att anmäla att man tillhandahåller tjänsten till minst sex medlemsstater, göra en riskbedömning, vidta åtgärder och plan för motståndskraft, utse

[3] Vårdgivare enligt definitionen i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård.

samverkansansvarig, rapportera incidenter, göra en befattningsanalys, genomföra en bakgrundskontroll och bevara viss information.

Nivåerna på sanktionsavgiften föreslås vara desamma som för väsentliga verksamhetsutövare i lagen om cybersäkerhet. Det innebär att sanktionsavgiften för enskilda kritiska verksamhetsutövare ska bestämmas till lägst 5 000 kronor och högst till det högsta av:

1. 2 procent av den kritiska verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 10 000 000 euro.

För offentliga kritiska verksamhetsutövare ska avgiften bestämmas till lägst 5 000 kronor och högst till 10 000 000 kronor.

Vid bedömning av sanktionsavgiftens storlek ska särskild hänsyn tas till den skada eller risk för skada som uppstått till följd av överträdelsen, om den kritiska verksamhetsutövaren tidigare har begått en överträdelse och de kostnader som verksamhetsutövaren har undvikit till följd av överträdelsen.

Om tillsynsmyndigheten inte finner skäl att ingripa med föreläggande eller sanktionsavgift ska den i stället meddela en anmärkning. Tillsynsmyndigheten får i vissa fall avstå från att ingripa.

Lagen om cybersäkerhet

Den som identifierats som en kritisk verksamhetsutövare enligt lagen om motståndskraft hos kritiska verksamhetsutövare ska oavsett storlek omfattas av lagen om cybersäkerhet om verksamheten omfattas av bilaga 1 eller 2 i NIS2-direktivet och verksamhetsutövaren är etablerad i Sverige.

Sekretess och tystnadsplikt

För att MSB och tillsynsmyndigheterna ska kunna lämna ut uppgifter som härrör från andra medlemsstater och EU:s institutioner och som omfattas av sekretess enligt 15 kap. 1 a § offentlighets- och sekretesslagen (2009:400), OSL, till varandra, föreslår utredningen en ny sekretessbrytande bestämmelse i 15 kap.

Utredningen föreslår vidare att sekretesskyddet ska stärkas och föreslår att en ny bestämmelse om sekretess införs i 18 kap. OSL för uppgift i incidentrapporter enligt lagen om cybersäkerhet och lagen om motståndskraft hos kritiska verksamhetsutövare samt för uppgift om åtgärd som följer av en sådan incident. Bestämmelsen förslås få ett omvänt skaderekvisit och rätten att meddela och offentliggöra uppgifterna begränsas. Vidare föreslås att diarium över incidenter hos rapporterande myndigheter, tillsynsmyndigheter och MSB ska kunna omfattas av sekretess.

När det gäller bakgrundskontroller föreslås en bestämmelse om tystnadsplikt för uppgifter som förekommer i angelägenheter som avser bakgrundskontroll i den nya lagen. En motsvarande bestämmelse införs i 35 kap. OSL för det allmännas verksamhet.

Sekretesskyddet för uppgifter som tillsynsmyndigheten kommer att hantera behöver kompletteras när det gäller uppgifter som rör enskilds affärs- eller driftsförhållanden. Utredningen föreslår därför att det i bilagan

till offentlighets- och sekretessförordningen (2009:641) införs en bestämmelse om att sekretess gäller för dessa uppgifter i verksamhet som består i tillsyn och utredning enligt lagen om motståndskraft hos enskilda verksamhetsutövare.

Sanktionsavgift enligt säkerhetsskyddslagen med mera

Utredningen föreslår att sanktionsavgifternas storlek i säkerhetsskyddslagen (2018:585) ska höjas för enskilda verksamhetsutövare. Det innebär att sanktionsavgiften ska bestämmas till lägst 25 000 kronor och högst till det högsta av 120 000 000 kronor eller 2 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår.

Utredningen föreslår inga ändringar i säkerhetsskyddslagen avseende tillsynsmyndighetens befogenheter.

Utredningen har bedömt att ingripande genom att ansöka om förbud att utöva ledningsfunktion och att meddela en anmärkning inte ska införas i säkerhetsskyddslagen.

Anger en kritisk verksamhetsutövare att den samhällsviktiga tjänsten till någon del är säkerhetskänslig ska tillsynsmyndigheten enligt säkerhetsskyddslagen underrättas. Tillsynsmyndigheten ska inom fem dagar meddela tillsynsmyndigheten enligt lagen om motståndskraft hos kritiska verksamhetsutövare huruvida den kritiska verksamhetsutövaren har anmält att den bedriver säkerhetskänslig verksamhet.

Konsekvenser

Utredningens förslag medför ekonomiska konsekvenser för tillsynsmyndigheterna, MSB, Polismyndigheten och kritiska verksamhetsutövare.

Utredningen föreslår att

- tillsynsmyndigheterna för år 2025 och 2026 tilldelas ett förstärkt anslag. Kostnader för löpande tillsyn föreslås beräknas när identifieringen av kritiska verksamhetsutövare är genomförd.
- MSB för år 2025 och 2026 får ett förstärkt anslag. Kostnader för stöd vid incidenter får klarläggas när identifieringen av kritiska verksamhetsutövare är genomförd.
- Polismyndighetens kostnader för den löpande hanteringen av utdrag ur belastningsregistret föreslås beräknas när identifieringen av kritiska verksamhetsutövare är genomförd och dessa har gjort den föreskrivna befattningsanalysen.

När det gäller kostnader för offentliga verksamhetsutövare föreslår utredningen att dessa finansieras inom befintlig budgetram. Avseende kostnader för enskilda verksamhetsutövare föreslår utredningen, när antalet kritiska verksamhetsutövare har identifierats och riskbedömningarna har genomförts, att det kan finnas anledning att överväga om det finns behov av att införa statligt stöd.

Ikraftträdande

Utredningen föreslår att lagen om motståndskraft hos kritiska verksamhetsutövare och tillhörande förordning ska träda i kraft den 1 augusti 2025.

Förslagen i offentlighets- och sekretesslagen och offentlighets- och sekretessförordningen som gäller lagen om cybersäkerhet föreslås träda i kraft den 1 januari 2025.

Övriga förslag föreslås träda i kraft den 1 augusti 2025.

Slutbetänkandets lagförslag i relevanta delar

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

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

dels att det ska införas två nya paragrafer, 15 kap. 3 c § och 18 kap. 8 d § av följande lydelse,

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

Nuvarande lydelse	*Föreslagen lydelse*
	15 kap.
	3 c §
	Sekretessen enligt 1 a § hindrar inte att Myndigheten för samhällsskydd och beredskap lämnar en uppgift som avses där till tillsynsmyndigheten enligt lagen (2025:000) om cybersäkerhet och lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag
	Detsamma gäller när en tillsynsmyndighet lämnar sådana uppgifter till Myndigheten för samhällsskydd och beredskap.
	En uppgift får lämnas endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

18 kap.

8 d §

Utöver vad som följer av 8 § gäller sekretess för uppgift i en incidentrapport enligt 3 kap. 5–7 §§ lagen (2025:000) om cybersäkerhet och 5 kap. 1 § lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare samt för uppgift om åtgärd som följer av en sådan incident om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens verksamhet skadas eller de åtgärder som vidtagits motverkas.

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

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.

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.

[1] Senaste lydelse 2024:477.

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.

Denna lag träder i kraft den 1 januari 2025 i fråga om lagen (2025:000) om cybersäkerhet och i övrigt den 1 augusti 2025.

Förteckning över remissinstanserna

Efter remiss har yttrande över slutbetänkandet inkommit från Affärsverket svenska kraftnät, Arbetsgivarverket, Bevakningsbranschens Yrkes- och Arbetsmiljönämnd (BYA), Bolagsverket, Brottsförebyggande rådet, Domstolsverket, Drivkraft Sverige, E-hälsomyndigheten, Energiföretagen Sverige, Energimarknadsinspektionen, Enköpings kommun, Finansiell ID-Teknik BID AB, Finansinspektionen, Fortifikationsverket, Försvarets materielverk, Försvarets radioanstalt, Försvarshögskolan, Försvarsmakten, Försvarsunderrättelsedomstolen, Försäkringskassan, Förvaltningsrätten i Linköping, Förvaltningsrätten i Umeå, Gotlands kommun, Gävle kommun, Göteborgs kommun, IKEM Innovations- och kemiindustrierna i Sverige, Inspektionen för strategiska produkter, Inspektionen för vård och omsorg, Integritetsskyddsmyndigheten, Jönköpings kommun, Kalix kommun, Kammarkollegiet, Kammarrätten i Jönköping, Karlstads kommun, Karolinska institutet, Kemikalieinspektionen, Kommerskollegium, Konkurrensverket, Kriminalvården, Kustbevakningen, Landsorganisationen i Sverige (LO), Lantbrukarnas riksförbund, Linköpings kommun, Livsmedelsverket, Luftfartsverket, Luleå kommun, Läkemedelsindustriföreningen, Läkemedelsverket, Länsstyrelsen i Blekinge län, Länsstyrelsen i Dalarnas län, Länsstyrelsen i Gotlands län, Länsstyrelsen i Gävleborgs län, Länsstyrelsen i Hallands län, Länsstyrelsen i Jönköpings län, Länsstyrelsen i Kalmar län, Länsstyrelsen i Kronobergs län, Länsstyrelsen i Norrbottens län, Länsstyrelsen i Skåne län, Länsstyrelsen i Stockholms län, Länsstyrelsen i Södermanlands län, Länsstyrelsen i Uppsala län, Länsstyrelsen i Värmlands län, Länsstyrelsen i Västerbottens län, Länsstyrelsen i Västernorrlands län, Länsstyrelsen i Västmanlands län, Länsstyrelsen i Västra Götalands län, Länsstyrelsen i Örebro län, Länsstyrelsen i Östergötlands län, Malmö kommun, Myndigheten för digital förvaltning, Myndigheten för psykologiskt försvar, Myndigheten för samhällsskydd och beredskap, Naturvårdsverket, Netnod AB, Nynäshamns kommun, Patent- och registreringsverket, Pensionsmyndigheten, Polismyndigheten, Post- och telestyrelsen, Regelrådet, Region Jönköpings län, Region Norrbotten, Region Stockholm, Region Sörmland, Region Östergötland, Rymdstyrelsen, Salems kommun, Sjöfartsverket, Skatteverket, Socialstyrelsen, Sparbankernas Riksförbund, Statens energimyndighet, Statens inspektion för försvarsunderrättelseverksamheten, Statens jordbruksverk, Statens servicecenter, Statskontoret, Stockholms kommun, Stockholms universitet, Strålsäkerhetsmyndigheten, Svensk Dagligvaruhandel, Svensk Handel, Svenska Bankföreningen, Svenska Journalistförbundet, Svenska stadsnätsföreningen, Svenska Tidningsutgivareföreningen (TU), Svenskt Näringsliv, Svenskt Vatten, Sveriges advokatsamfund, Sveriges akademikers centralorganisation (Saco), Sveriges Kommuner och Regioner, Sveriges meteorologiska och hydrologiska institut (SMHI), Säffle kommun, Säkerhets- och försvarsföretagen, Säkerhets- och integritetsskyddsnämnden, Säkerhetspolisen, Tech Sverige, Teknikföretagen, Tillväxtverket, Totalförsvarets forskningsinstitut, Totalförsvarets plikt- och prövningsverk, Trafikverket, Transportföretagen, Transportstyrelsen, Trelleborgs kommun, Tullverket, Umeå

kommun, Uppsala universitet, Verket för innovationssystem (Vinnova), Vetenskapsrådet, Växjö kommun och Östersunds kommun.

Därutöver har yttranden inkommit från Advokatfirman Kahn Pedersen, Almega Säkerhetsföretagen, Defensify AB, GovSec Sweden AB, LawSec Sweden AB, Prolegia Research AB, Stiftelsen för Internetinfrastruktur, SJ AB, Svenska Transportarbetareförbundet, Sveriges universitets- och högskoleförbund, Sydvatten, SäkerhetsBranschen, Tågföretagen och Vattenfall AB.

Följande remissinstanser har inte svarat eller angett att de avstår från att lämna några synpunkter: Arelion Sweden AB, Chalmers tekniska högskola AB, Energigas Sverige, Falkenbergs kommun, Falu kommun, Finansbolagens Förening, Flens kommun, GlobalConnect AB, Industriarbetsgivarna i Sverige Service AB, Kalmar kommun, Karlskoga kommun, Karlskrona kommun, Kungl. Tekniska högskolan, Lantmännen, Leksands kommun, Lilla Edets kommun, Livsmedelsföretagen, Livsmedelsgrossisterna, Länsstyrelsen i Jämtlands län, Myndigheten för totalförsvarsanalys, On Tower Sweden AB/Cellnex Sverige, Region Skåne, Riksdagens ombudsmän, RISE Research Institutes of Sweden AB, Scrive AB, Stockholm Vatten och Avfall AB, Strängnäs kommun, Sundsvalls kommun, Svenska Regionala Flygplatser AB, Svenska rymdaktiebolaget (SSC), Sveriges Hamnar, Swedavia AB, Tjänstemännens centralorganisation (TCO), Västerås kommun och Östhammars kommun.