

Effektivare gränsöverskridande inhämtning av elektroniska bevis

Betänkande av E-bevisningsutredningen

Stockholm 2024



STATENS OFFENTLIGA
UTREDNINGAR

SOU 2024:85

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

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

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

Layout: Kommittéservice, Regeringskansliet

Omslag: Elanders Sverige AB

Tryck och remisshantering: Elanders Sverige AB, Stockholm 2024

ISBN 978-91-525-1077-3 (tryck)

ISBN 978-91-525-1078-0 (pdf)

ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

Regeringen beslutade vid regeringssammanträde den 15 juni 2023 att ge en särskild utredare i uppdrag att se över regleringen om gränsöverskridande åtkomst till elektroniska bevis med anledning av nya internationella instrument.

Hovrättsrådet Ulf Wallentheim förordnades samma dag att vara särskild utredare.

Till experter i utredningen utsågs den 13 september 2023 rådmannen Sonja Ahlgren (Södertörns tingsrätt), advokaten Karl-Fredrik Björklund (Sveriges Advokatsamfund) verksjuristen Isa Blom (Tullverket), juristen Elisabeth Hedborg (Integritetsskyddsmyndigheten), rättssakkunniga Karin Henriksson (Justitiedepartementet), verksamhetsutvecklaren Ingmarie Olsson (Polismyndigheten), verksjuristen Maria Sertcanli (Säkerhetspolisen), vice chefsåklagaren Peter Svedén (Ekobrottsmyndigheten), verksjuristen Sofia Wirlée, (Post- och telestyrelsen), och seniora åklagaren Christoffer Östlind, (Åklagarmyndigheten). Ingmarie Olsson entledigades den 11 januari 2024 och ersattes samma dag som expert av juristen Anna Olander Selldén (Polismyndigheten). Sofia Wirlée entledigades den 6 februari 2024. Samma dag förordnades i hennes ställe juristen Maria Wiberg (Post- och telestyrelsen) som expert i utredningen. Maria Sertcanli entledigades den 13 februari 2024 och ersattes samma dag som expert av seniora verksjuristen Fredrik Hugo (Säkerhetspolisen). Elisabeth Hedborg entledigades den 28 juni 2024. Samma dag förordnades i hennes ställe juristen Mika Kortzon (Integritetsskyddsmyndigheten) som expert i utredningen.

Hovrättsassessorn Sara Vinnefors anställdes som sekreterare i utredningen den 15 juli 2023.

Utredningen har antagit namnet E-bevisningsutredningen.

Utredningen är formellt ett uppdrag för Ulf Wallentheim som särskild utredare. Arbetet har emellertid bedrivits i nära samråd med experterna. Experterna har ställt sig bakom utredningens överväganden och förslag. Betänkandet har därför avfattats med användning av vi-form.

Härmed överlämnas betänkandet *Effektivare gränsöverskridande inhämtning av elektroniska bevis* (SOU 2024:85). Utredningens uppdrag är med detta slutfört.

Stockholm i december 2024

Ulf Wallentheim

Sara Vinnefors

Innehåll

Sammanfattning	17
Summary	27
1 Författningsförslag	37
1.1 Förslag till tillfällig lag (2026:000) om utseende av verksamhetsställen eller rättsliga ombud	37
1.2 Förslag till lag (2026:000) om inhämtande av elektronisk bevisning inom Europeiska unionen	39
1.3 Förslag till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål	45
1.4 Förslag till lag om ändring i lagen (2003:1174) om vissa former av internationellt samarbete i brottmålsutredningar	47
1.5 Förslag till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder	52
1.6 Förslag till lag om ändring i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder.....	54
1.7 Förslag till förordning (2026:000) med kompletterande bestämmelser om inhämtande av elektronisk bevisning inom Europeiska unionen	55
1.8 Förslag till förordning om ändring i förordningen (2000:704) om internationell rättslig hjälp i brottmål	57

1.9	Förslag till förordning om ändring i förordningen (2003:1176) om vissa former av internationellt samarbete i brottsutredningar.....	58
2	Utredningens uppdrag och arbete	63
2.1	Utredningens uppdrag	63
2.2	Utredningens arbete.....	64
2.3	Betänkandets disposition	65
3	Förordning (EU) 2023/1543	67
3.1	Inledning.....	67
3.2	EU-förordningens innehåll och allmänna tillämpningsområde	68
3.2.1	Innehåll	68
3.2.2	Tillämpningsområde	69
3.3	Förordningens definitioner.....	70
3.4	Behöriga myndigheter	71
3.5	Utfärdande av en europeisk utlämnande- eller bevarandeorder	71
3.5.1	Villkoren för utfärdande av en order	71
3.5.2	Förfarandet vid utfärdandet av en order.....	72
3.6	Verkställigheten av en europeisk utlämnande- eller bevarandeorder	73
3.6.1	Mottagarens skyldigheter	73
3.6.2	Verkställande myndighetens huvudsakliga uppgifter	74
3.7	Sanktioner	75
3.8	Rättsmedel	76
3.9	Lagkonflikter	76
3.10	Användarinformation och sekretess.....	77
3.11	Det decentraliserade it-systemet	78

3.12	Övriga bestämmelser och om ikraftträdande	78
4	Nationella bestämmelser om inhämtning av elektronisk bevisning	81
4.1	Inledning.....	81
4.2	Lagen om elektronisk kommunikation	81
4.2.1	Kort om lagens bakgrund och syfte	81
4.2.2	Allmänt om elektronisk kommunikation	82
4.2.3	Säkerhet i nät och tjänster.....	84
4.2.4	Lagringsskyldighet	84
4.2.5	Anpassningsskyldighet.....	86
4.2.6	Förslag om utökad lagringsskyldighet och moderniserad anpassningsskyldighet	87
4.3	Inhämtande av bevisning i en förundersökning	89
4.3.1	Allmänt om bevisinhämtning	89
4.3.2	Särskilt om hemliga tvångsmedel.....	90
4.3.3	Hemliga tvångsmedel och skyddet för den personliga integriteten.....	92
4.3.4	Principerna om ändamål, behov och proportionalitet vid tvångsmedelsanvändning.....	93
4.4	Bevarande och inhämtning av elektronisk bevisning	95
4.4.1	Bevarande av lagrade elektroniska uppgifter.....	95
4.4.2	Inhämtande av uppgifter om abonnemang	96
4.4.3	Inhämtande av innehållsdata samt trafik- och lokaliseringssuppgifter	100
4.4.4	Användning av straffprocessuella tvångsmedel i syfte att verkställa frihetsberövanden.....	108
4.5	Internationellt straffrättsligt samarbete	110
4.5.1	Lagen om internationell rättslig hjälp i brottmål.....	110
4.5.2	Lagen om en europeisk utredningsorder	113
4.5.3	Lagen om vissa former av internationellt samarbete i brottsutredningar	115

5	Allmänna överväganden.....	117
5.1	Inledning.....	117
5.2	Allmänna utgångspunkter för våra överväganden.....	117
5.3	En ny lag ska komplettera EU-förordningen.....	120
5.4	Hänvisningsteknik.....	121
5.5	Termer och uttryck.....	122
6	Behovet av kompletterande nationella bestämmelser om bevisinhämtning	123
6.1	Inledning.....	123
6.2	Aktörer som omfattas av EU-förordningens bestämmelser	124
6.2.1	Inledning.....	124
6.2.2	Tjänsteleverantörer som omfattas av EU-förordningen.....	124
6.2.3	Aktörer som omfattas av punkten a i artikel 3.3.....	125
6.2.4	Aktörer som omfattas av punkten b i artikel 3.3.....	130
6.2.5	Aktörer som omfattas av punkten c i artikel 3.3.....	133
6.2.6	Tjänsteleverantörer som erbjuder tjänster i unionen	134
6.3	Villkoren för utfärdande av en europeisk utlämnandeorder respektive bevarandeorder.....	135
6.3.1	Allmänna förutsättningar för utfärdande av europeisk utlämnande- eller bevarandeorder..	135
6.3.2	Villkoren för utfärdande av en europeisk utlämnandeorder	138
6.3.3	Villkoren för utfärdande av en europeisk bevarandeorder	146
6.4	Allmänna utgångspunkter för våra överväganden och förslag.....	146

6.5	Kretsen av tjänsteleverantörer och skyldigheten att lämna ut uppgifter följer direkt av EU-förordningen ...	148
6.5.1	Kompletteringar i svensk lag behövs inte i fråga om kretsen av tjänsteleverantörer.....	148
6.5.2	Den rättsliga grunden för utlämnande av uppgifter följer direkt av EU-förordningen	148
6.6	Straffrättsliga förfaranden enligt EU-förordningen	152
6.7	Elektronisk bevisning kan inhämtas hos de tjänsteleverantörer som omfattas av EU-förordningen	155
6.8	Utfärdande av en europeisk utlämnandeorder för att inhämta abonnentuppgifter eller andra användaruppgifter	160
6.9	Begreppen trafikuppgifter och innehållsdata och tillämpliga tvångsmedel enligt nationell rätt	164
6.10	Utfärdande av en europeisk utlämnandeorder för att inhämta trafikuppgifter och innehållsdata	168
6.10.1	Inledning	168
6.10.2	Förutsättningar enligt 27 kap. 18 a § rättegångsbalken för inhämtande av innehållsdata.....	168
6.10.3	Förutsättningar enligt 27 kap. 18 b § rättegångsbalken för inhämtande av innehållsdata.....	175
6.10.4	Förutsättningar enligt 27 kap. 19 a § rättegångsbalken för inhämtande av trafikuppgifter	177
6.10.5	Förutsättningar enligt 27 kap. 19 b § rättegångsbalken för inhämtande av trafikuppgifter	180
6.10.6	Nationella bestämmelser bör inte ändras för att kunna utfärda en europeisk utlämnandeorder i fler fall.....	180
6.11	Inhämtande av trafikuppgifter och innehållsdata för verkställighet av fängelsestraff	183

6.12	Utfärdande av en europeisk bevarandeorder	184
6.12.1	Bevarande av uppgifter vid misstanke om brott	184
6.12.2	En möjlighet att förelägga om bevarande av uppgifter i verkställighetssyfte bör införas i svensk rätt.....	186
7	Utfärdande och verkställande myndigheter och dess uppgifter	191
7.1	Inledning	191
7.2	Utfärdande myndigheter.....	192
7.2.1	Myndigheter som är behöriga att utfärda en europeisk utlämnande- eller bevarandeorder	192
7.2.2	Den utfärdande myndighetens uppgifter	194
7.3	Verkställande myndighet och dess uppgifter.....	196
7.3.1	Myndigheter som kan vara verkställande myndighet.....	196
7.3.2	Den verkställande myndighetens uppgifter.....	196
7.4	Behörig domstol	200
7.5	Överväganden och förslag.....	203
7.5.1	Behörig utfärdande myndighet	203
7.5.2	Skyldigheten att följa de regler som följer direkt av EU-förordningen behöver inte regleras i lag	208
7.5.3	Förfaranderegler för domstols godkännande av en europeisk utlämnandeorder.....	209
7.5.4	Behörig verkställande myndighet.....	211
7.5.5	Den verkställande myndighetens prövning.....	214
7.5.6	Centralmyndighet	216
7.5.7	Behörig domstol.....	217
8	Direktivet (EU) 2023/1544	223
8.1	Inledning	223
8.2	EU-direktivets innehåll	224
8.2.1	Tillämpningsområde och definitioner	224

8.2.2	Skyldigheten att utse verksamhetsställen och rättsliga ombud	226
8.2.3	Övriga bestämmelser.....	229
8.3	Utsedda verksamhetsställen och rättsliga ombud.....	230
8.3.1	Skyldigheten att utse verksamhetsställen och rättsliga ombud	230
8.3.2	Erbjudande av tjänster på en medlemsstats territorium	235
8.4	Skyldigheten att motta förelägganden och beslut samt tillhandahålla resurser och befogenheter	236
8.5	Underrättelser och språk.....	238
8.6	Centralmyndighet.....	239
8.6.1	Endast en myndighet ska utses till centralmyndighet	239
8.6.2	Post- och telestyrelsen bör utses till centralmyndighet	240
8.6.3	Centralmyndighetens befogenheter och rätt att besluta om sanktioner	244
9	Sanktioner	251
9.1	Inledning.....	251
9.2	Allmänt om sanktioner och sanktionsavgifter	251
9.3	Sanktionsavgifter vid överträdelser av EU-förordningens bestämmelser	253
9.3.1	Utgångspunkterna i EU-förordningen	253
9.3.2	Utformningen av sanktionsavgiftssystemet	254
9.4	Sanktioner vid överträdelser av de bestämmelser som genomför EU-direktivet.....	264
9.4.1	Utgångspunkter i EU-direktivet	264
9.4.2	Val av sanktioner vid överträdelser av de bestämmelser som genomför EU-direktivet	265
9.4.3	Utformningen av ett sanktionsavgiftssystem utifrån EU-direktivets bestämmelser	270

9.5	Gemensamma förfaranderegler avseende sanktionsavgifter	274
10	Övriga frågor	279
10.1	Inledning	279
10.2	Intyg och språk	280
10.3	Ersättning för kostnader	284
10.4	Effektiva rättsmedel	286
10.4.1	Innehållet i artikel 18	286
10.4.2	Utgångspunkter för våra överväganden.....	288
10.4.3	Effektiva rättsmedel – en översikt	288
10.4.4	Effektiva rättsmedel i fråga om hemliga tvångsmedel i svensk rätt.....	291
10.4.5	Inhämtning av uppgifter om abonnemang och effektiva rättsmedel.....	297
10.4.6	Effektiva rättsmedel i fråga om en europeisk utlämnandeorder.....	299
10.4.7	Kraven på rätten till försvar och rättvist förfarande	302
10.5	Metoder för kommunikation.....	303
10.6	Insamling av statistik.....	305
10.7	Förhållandet till dataskyddsregleringen	308
10.7.1	Utgångspunkter i EU-förordningen.....	308
10.7.2	Gällande rätt	309
10.7.3	Det finns inget behov av ändringar i dataskyddsregleringen.....	311
10.8	Uppgiftslämnande och sekretess	317
11	Säkrande av elektroniska bevis enligt Budapestkonventionen	321
11.1	Inledning	321
11.2	Närmare om Budapestkonventionens reglering om skyndsamt säkrande av lagrade uppgifter	323

11.3	Genomförandet av artiklarna 16 och 29 i Budapestkonventionen i svensk rätt	324
11.3.1	Rättegångsbalkens reglering	324
11.3.2	Det gränsöverskridande samarbetet	326
11.4	Åklagarmyndighetens framställan	329
11.5	Överväganden och förslag	331
11.5.1	Tillämpliga regler vid en begäran enligt artikel 29 i Budapestkonventionen	331
11.5.2	Åklagare ska alltjämt besluta i ett ärende enligt artikel 29 i Budapestkonventionen.....	337
12	Det andra tilläggsprotokollet till Budapestkonventionen	339
12.1	Inledning.....	339
12.2	Kort om innehållet i det andra tilläggsprotokollet	340
12.3	Sverige ska tillträda det andra tilläggsprotokollet till Budapestkonventionen.....	342
12.4	Inhämtande av information om domännamn (artikel 6)	343
12.4.1	Det närmare innehållet i artikel 6	343
12.4.2	Gällande rätt	345
12.4.3	Föreslagna ändringar i toppdomänlagen	348
12.4.4	En möjlighet att inhämta information om domännamn utomlands ska införas	349
12.4.5	Svenska aktörers skyldighet att lämna ut information om domännamn.....	351
12.4.6	I vilket regelverk bör bestämmelserna föras in....	354
12.5	Inhämtande av abonnemangsuppgifter (artikel 7).....	356
12.5.1	Det närmare innehållet i artikel 7	356
12.5.2	Gällande rätt	359
12.5.3	En möjlighet att inhämta abonnemangsuppgifter utomlands ska införas	360
12.5.4	Svenska tjänsteleverantörers skyldighet att lämna ut uppgifter om abonnemang	363
12.5.5	I vilket regelverk bör bestämmelserna föras in....	370

12.6	Skyndsamt framtagande av abonnemangs- och trafikuppgifter (artikel 8)	370
12.6.1	Det närmare innehållet i artikel 8.....	370
12.6.2	Gällande rätt	372
12.6.3	Inhämtande av abonnemangs- och trafikuppgifter utomlands.....	373
12.6.4	Verkställighet i Sverige av en order om inhämtande av abonnemangs- och trafikuppgifter	375
12.6.5	Partiellt förbehåll beträffande historiska trafikuppgifter	381
12.7	Utlämnande av uppgifter i nödsituationer (artiklarna 9 och 10)	382
12.7.1	Det närmare innehållet i artiklarna 9 och 10	382
12.7.2	Gällande rätt	387
12.7.3	Översändande av framställningar enligt artikel 9 och dess innehåll	388
12.7.4	Skyndsamhetskravet i artiklarna 9 och 10	391
12.7.5	Lagstiftningsbehovet beträffande övriga bestämmelser i artikel 10	392
12.8	Förfarandet för internationellt samarbete i avsaknad av avtal (artiklarna 11 och 12)	395
12.8.1	Innehållet i artiklarna 11 och 12.....	395
12.8.2	Gällande rätt	396
12.8.3	Lagstiftningsbehovet beträffande artiklarna 11 och 12.....	398
12.9	Skydd för personuppgifter (artikel 14)	399
12.9.1	Innehållet i artikel 14	399
12.9.2	Gällande rätt	401
12.9.3	Svensk rätt uppfyller de krav som följer av artikel 14.....	405
12.10	Övriga artiklar.....	408
12.11	Förklaringar och underrättelser.....	409
12.11.1	Förklaringar till det andra tilläggsprotokollet.....	409
12.11.2	Underrättelser till kommissionen	412

13	Konsekvenser av utredningens förslag.....	415
13.1	Inledning.....	415
13.2	Konsekvenser för brottsbekämpande myndigheter.....	416
13.2.1	Förslag avseende EU-förordningen som berör brottsbekämpande myndigheter.....	416
13.2.2	Förslag avseende det andra tilläggsprotokollet till Budapestkonventionen samt artikel 29 i konventionen som berör brottsbekämpande myndigheter	417
13.2.3	Konsekvenser för Åklagarmyndigheten och Ekobrottsmyndigheten	418
13.2.4	Konsekvenser för övriga behöriga myndigheter	421
13.3	Konsekvenser för domstolarna och övriga myndigheter....	423
13.4	Konsekvenser för den utsedda centralmyndigheten.....	424
13.5	Konsekvenser för företagen	426
13.6	Konsekvenser för brottsligheten och det brottsförebyggande arbetet.....	428
13.7	Övriga konsekvenser	428
14	Ikraftträdande- och övergångsbestämmelser	429
14.1	Ikraftträdande	429
14.2	Övergångsbestämmelser.....	430
15	Författningskommentar	431
15.1	Förslaget till tillfällig lag (2026:000) om utseende av verksamhetsställen eller rättsliga ombud	431
15.2	Förslaget till lag (2026:000) om inhämtande av elektronisk bevisning inom Europeiska unionen	433
15.3	Förslaget till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål	456

15.4	Förslaget till lag om ändring i lagen (2003:1174) om vissa former av internationellt samarbete i brottmålsutredningar	459
15.5	Förslaget till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder	466
15.6	Förslaget till lag om ändring i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder	467

Bilagor

Bilaga 1	Kommittédirektiv 2023:84.....	471
Bilaga 2	Europaparlamentets och rådets förordning (EU) 2023/1543.....	483
Bilaga 3	Europaparlamentets och rådets direktiv (EU) 2023/1544.....	547
Bilaga 4	Andra tilläggsprotokollet till konventionen om it-brottslighet om utökat samarbete och utlämnande av elektroniska bevis.....	559

Sammanfattning

Uppdraget

Vi har haft i uppdrag att se över regleringen om gränsöverskridande åtkomst till elektroniska bevis med anledning av nya internationella instrument, vilka är

- förordning (EU) 2023/1543 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden (EU-förordningen),
- direktiv (EU) 2023/1544 om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden (EU-direktivet), och
- det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet (Budapestkonventionen).

Vi har också haft i uppdrag att se över regleringen om gränsöverskridande hantering av förelägganden om bevarande av uppgifter.

Syftet med uppdraget är att säkerställa att svenska brottsbekämpande myndigheter på ett effektivt och rättssäkert sätt kan använda de gränsöverskridande verktyg som ovan nämnda instrument erbjuder. Därutöver innebär uppdraget att även brottsbekämpande myndigheter inom EU på ett effektivt och rättssäkert sätt kan få tillgång till elektroniska bevis som kan finnas tillgängliga hos svenska aktörer.

EU-förordningen och EU-direktivet

EU-förordningen syftar till att effektivisera gränsöverskridande inhämtning av elektronisk bevisning. EU-förordningen innebär att en behörig myndighet i en medlemsstat kan vända sig till en tjänsteleverantör som är etablerad eller representerad i en annan medlemsstat, med ett beslut om att elektroniska bevis ska bevaras (bevarandeorder) eller lämnas ut (utlämnandeorder). Det spelar ingen roll i vilket land de elektroniska uppgifterna finns lagrade. Med elektroniska bevis avses abonnentuppgifter, trafikuppgifter och innehållsdata. EU-förordningen omfattar enbart lagrade uppgifter och innebär ingen skyldighet att lagra uppgifter.

Om en order inte följs, kan den utfärdande myndigheten begära verkställighet av ordern av behörig verkställande myndighet i den stat i vilken tjänsteleverantören finns representerad. Efterlevs inte ordern trots detta kan det bli aktuellt att besluta om sanktionsavgifter.

EU-direktivet innehåller bestämmelser om att vissa tjänsteleverantörer är skyldiga att utse utsedda verksamhetsställen eller rättsliga ombud inom unionen. Det är de utsedda verksamhetsställena eller de rättsliga ombuden som ska ta emot europeiska bevarande- och utlämnandeorder för tjänsteleverantörernas räkning samt ansvara för att de fullföljs.

Förordningen överlämnar vissa frågor till medlemsstaterna att reglera i nationell rätt. Enligt EU-förordningen är medlemsstaterna också skyldiga att utse en eller flera behöriga myndigheter som bland annat ska ha befogenhet att utfärda, sända och verkställa europeiska bevarande- och utlämnandeorder. Vi föreslår att sådana bestämmelser samlas i en kompletterande lag; lagen om inhämtande av elektronisk bevisning inom Europeiska unionen. I samma lag ska de bestämmelser som genomför EU-direktivet införas.

Behovet av kompletteringar av nationella bestämmelser om bevisinhämtning

Vi gör bedömningen att det inte behövs några kompletterande bestämmelser i svensk lag angående EU-förordningens bestämmelser om vilka tjänsteleverantörer som omfattas av förordningen. Något behov finns inte heller att ändra i bestämmelserna om lag-

rings- och anpassningsskyldigheten i lagen (2022:482) om elektronisk kommunikation.

Den rättsliga grunden för utlämnande eller bevarande av elektronisk bevisning följer direkt av EU-förordningen. Tjänsteleverantörer samt utsedda verksamhetsställen och rättsliga ombud ska vidare följa de skyldigheter som åvilar dem enligt de bestämmelser som följer direkt av EU-förordningen, utan att det behövs några kompletterande bestämmelser i svensk lag.

Det behövs vidare inte några kompletterande nationella bestämmelser för att det ska vara möjligt för svensk behörig myndighet att utfärda en europeisk utlämnandeorder i syfte att inhämta abonnentuppgifter eller andra användaruppgifter i fråga om de tjänsteleverantörer som omfattas av EU-förordningen. Detsamma gäller inhämtande av trafikuppgifter och innehållsdata enligt EU-förordningen.

De svenska bestämmelserna om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kommer i allt väsentligt kunna tillämpas i samband med utfärdande av en europeisk utlämnandeorder avseende trafikuppgifter och innehållsdata. En viss diskrepans med brottskatalogerna i 27 kap. 18 a, 18 b, 19 a och 19 b §§ rättegångsbalken finns dock, men vi anser inte att katalogerna bör utvidgas till att omfatta ytterligare brott som har ett maximistraff om fängelse i minst tre år, men som inte har ett minimistraff som anges i nämnda bestämmelser. En höjning av maximistraffen bör inte heller ske för de brott för vilka hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation kan användas, men som inte har ett maximistraff om fängelse i minst tre år.

Några ändringar behövs inte i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder för att det ska vara möjligt att utfärda en europeisk utlämnandeorder beträffande trafikuppgifter för att lokalisera en person som är dömd till fängelse, sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning. Nämnda lag bör inte heller utvidgas till att även avse hemlig avlyssning av elektronisk kommunikation för att möjliggöra en europeisk utlämnandeorder avseende innehållsdata. Det krävs inte några ändringar eller kompletteringar av svensk rätt för att en europeisk bevarandeorder ska kunna utfärdas vid misstanke om brott. Däremot föreslår vi att det med stöd av lagen ska kunna beslutas om ett föreläggande om att

bevara lagrade uppgifter för att lokalisera en person som är dömd till fängelse, sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning, vilket får till följd att det även kommer att vara möjligt att utfärda en europeisk bevarandeorder för detta syfte.

Utfärdande och verkställande myndigheter och dess uppgifter

Vi föreslår att åklagare ska vara behöriga att utfärda en europeisk utlämnandeorder respektive europeisk bevarandeorder i Sverige.

Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som ska ingripa mot brott eller brottslig verksamhet ska enligt vårt förslag också vara behöriga att besluta om utfärdande av en europeisk utlämnandeorder avseende inhämtning av abonnentuppgifter och andra användaruppgifter samt om en europeisk bevarandeorder. En sådan order ska dock godkännas av åklagare.

Det krävs enligt artikel 4.2 b i EU-förordningen att domstol godkänner en europeisk utlämnandeorder för inhämtning av trafikuppgifter respektive innehållsdata innan den sänds över till mottagaren. Vi föreslår att vid ett sådant godkännande ska i tillämpliga delar gälla vad som är föreskrivet i rättegångsbalken. Vidare föreslår vi att bestämmelserna i 27 kap. 22–24, 31–33 samt 35 §§ rättegångsbalken också ska gälla vid ett sådant förfarande.

Åklagarmyndigheten ska vara behörig verkställande myndighet enligt EU-förordningen.

Vi föreslår att Stockholms tingsrätt ska vara behörig domstol enligt artikel 17 i EU-förordningen att pröva en fråga om lagkonflikt. Reglerna i rättegångsbalken om domstols handläggning och överklagande av domstols beslut ska enligt förslaget vara tillämpliga vid handläggningen.

Det finns enligt vår mening inte några skäl att utse en centralmyndighet för den administrativa hanteringen av en europeisk utlämnande- eller bevarandeorder.

Genomförande av EU-direktivet

Vi föreslår att en tjänsteleverantör som är etablerad i Sverige ska utse ett verksamhetsställe i Sverige för mottagande, efterlevnad och verkställighet av beslut och förelägganden som omfattas av EU-förordningen och övriga rättsakter som omfattas av tillämpningsområdet i artikel 1.2 i EU-direktivet. Denna skyldighet ska inte gälla om tjänsteleverantören har utsett ett verksamhetsställe i en annan medlemsstat där tjänsteleverantören också erbjuder tjänster eller om tjänsteleverantören endast är etablerad i Sverige och enbart erbjuder tjänster inom Sveriges territorium.

En tjänsteleverantör som inte är etablerad i någon av unionens medlemsstater, men som erbjuder tjänster i Sverige, ska utse ett rättsligt ombud som har sin hemvist i Sverige för mottagande, efterlevnad och verkställighet av beslut och förelägganden som omfattas av EU-förordningen. Denna skyldighet gäller inte om tjänsteleverantören har utsett ett rättsligt ombud som har sin hemvist i någon annan medlemsstat där denne erbjuder tjänster.

Skyldigheten att utse ett verksamhetsställe eller rättsligt ombud ska följa av den kompletterande lagen. Av lagen ska det också följa att tjänsteleverantören ska ge det verksamhetsställe eller rättsliga ombud som har utsetts av leverantören de befogenheter och resurser som krävs för att besvara beslut och förelägganden som omfattas av EU-förordningen och övriga rättsakter som omfattas av tillämpningsområdet anges i artikel 1.2 i EU-direktivet.

Vi föreslår att Post- och telestyrelsen utses till centralmyndighet.

Centralmyndigheten ska utöva tillsyn över att tjänsteleverantörerna utser verksamhetsställen eller rättsliga ombud och att de ges tillräckliga resurser och befogenheter. För detta ändamål ska centralmyndigheten ha rätt att få ta del av handlingar och upplysningar samt ha tillträdesrätt till utrymmen och för dessa ändamål kunna begära biträde från Kronofogdemyndigheten för att kontrollera efterlevnaden av de bestämmelser som genomför artikel 3 i EU-direktivet. Ett föreläggande att lämna ut handlingar och upplysningar ska kunna förenas med vite.

Sanktioner

Sanktionsavgifter ska enligt EU-förordningen följa vid överträdelser av vissa av dess bestämmelser. Sanktioner ska också aktualiseras vid överträdelser av EU-direktivets bestämmelser. Sanktionerna ska vara effektiva, proportionella och avskräckande. Det är både tjänsteleverantörerna och deras utsedda verksamhetsställen eller rättsliga ombud som kan bli föremål för sanktioner.

Det är den verkställande myndigheten, dvs. Åklagarmyndigheten enligt vårt förslag, som ska besluta om sanktionsavgifter vid överträdelser av bestämmelser i EU-förordningen, av ett utsett verksamhetsställe eller rättsligt ombud i Sverige som åsidosätter någon av sina skyldigheter enligt artiklarna 10, 11 och 13.4 i EU-förordningen. Tjänsteleverantören ska svara solidariskt för betalningen av avgiften tillsammans med det i Sverige utsedda verksamhetsstället eller rättsliga ombudet.

Centralmyndigheten ska kunna besluta om vitesföreläggande respektive sanktionsavgifter vid överträdelser av de bestämmelser som genomför EU-direktivet gentemot en tjänsteleverantör. Sanktionsavgifter vid överträdelser av EU-förordningen respektive de nationella bestämmelser som genomför EU-direktivet ska bestämmas till lägst 10 000 kronor och högst till två procent av tjänsteleverantörens totala globala årsomsättning föregående räkenskapsår.

Vid bedömningen av om någon sanktionsavgift ska tas ut och när storleken på avgiften ska bestämmas, ska enligt förslaget särskild hänsyn tas till om överträdelser varit uppsåtlig eller berott på oaktsamhet, den skada, fara eller kränkning som överträdelser innebär samt till överträdelsernas karaktär, svårhetsgrad och varaktighet, om den tjänsteleverantör som har begått överträdelser tidigare begått en liknande överträdelser samt den berörda tjänsteleverantörens finansiella ställning.

Sanktionsavgiften får sättas ned helt eller delvis om överträdelserna är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgift.

Säkrande av elektroniska bevis enligt Budapestkonventionen

För att efterleva artikel 16 i Budapestkonventionen infördes i svensk rätt ett nytt tvångsmedel i 27 kap. 16 § rättegångsbalken om förelägganden om att bevara uppgifter i elektronisk form. När det gäller konventionens krav i artikel 29 om internationellt samarbete gjordes vissa tillägg i lagen (2000:562) om internationell rättslig hjälp i brottmål och lagen (2017:1000) om en europeisk utredningsorder så att samarbetet enligt dessa två lagar även omfattade en åtgärd enligt 27 kap. 16 § rättegångsbalken.

År 2022 lämnade Åklagarmyndigheten in en framställan om förtydliganden i regleringen om det gränsöverskridande samarbetet beträffande förelägganden om att bevara uppgifter i elektronisk form. I framställan anges bl.a. att andra EU-stater inte anser att en europeisk utredningsorder ska användas vid förelägganden enligt artikel 29 i Budapestkonventionen och att det medför problem i det rättsliga samarbetet som kan behöva åtgärdas genom lagändringar.

Vi föreslår med anledning härav att lagen om en europeisk utredningsorder inte ska gälla vid skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter enligt artikel 29 i Budapestkonventionen. I stället ska lagen om internationell rättslig hjälp i brottmål tillämpas vid en sådan begäran.

En ansökan om rättslig hjälp med ett föreläggande att bevara en viss lagrad uppgift enligt artikel 29 i Budapestkonventionen ska enligt vår bedömning även fortsättningsvis handläggas av en åklagare.

Det andra tillägsprotokollet till Budapestkonventionen

I november 2021 antog Europarådets ministerkommitté det andra tillägsprotokollet till Budapestkonventionen. Sverige undertecknade protokollet den 12 maj 2022. Genom ett beslut av rådet den 14 februari 2023 bemyndigades medlemsstaterna att i unionens intresse ratificera protokollet.

Det andra tillägsprotokollet innehåller bestämmelser som syftar till att ge de brottsbekämpande myndigheterna nya och mera effektiva verktyg för gränsöverskridande åtkomst till elektroniska bevis. Det handlar om möjligheter för behöriga myndigheter i en stat att i

brottsutredande syfte dels vända sig till privata aktörer i en annan stat för att få ut domän- och abonnemangsuppgifter, dels vända sig till behöriga myndigheter i den andra staten för verkställighet av en order om utlämnade av abonnemangs- och trafikuppgifter.

Vi föreslår att riksdagen godkänner att Sverige tillträder det andra tilläggsprotokollet till Budapestkonventionen.

För att genomföra det andra tilläggsprotokollet i svensk rätt föreslår vi att åklagare och övriga brottsbekämpande myndigheter ska ha rätt att från en registreringsenhet för toppdomäner eller återförsäljare av domännamn respektive från en tjänsteleverantör i en annan stat som tillträtt det andra tilläggsprotokollet till Budapestkonventionen begära ut uppgifter för att identifiera eller kontakta innehavaren av ett domännamn respektive uppgifter om abonnemang som skäligen kan antas ha betydelse för utredningen om ett brott.

Vidare föreslår vi att en registreringsenhet för toppdomäner eller återförsäljare av domännamn som erbjuder tjänster för domännamnsregistrering i Sverige ska på begäran till en behörig myndighet i en annan stat som tillträtt det andra tilläggsprotokollet till Budapestkonventionen lämna ut uppgifter för att identifiera eller kontakta innehavaren av ett domännamn om uppgifterna rör brottslig verksamhet eller misstanke om brott. Vi föreslår också en motsvarande skyldighet för en tjänsteleverantör som omfattas av regleringen i 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation att lämna ut uppgifter om abonnemang.

Det föreslås också att det av 2 kap. 10 § lagen om internationell rättslig hjälp i brottmål ska följa att i fråga om skyndsamhetskravet särskild hänsyn ska tas till att om det föreligger en omedelbar fara för liv, hälsa eller egendom. Motsvarande bestämmelse föreslås föras in i 3 kap. 23 § lagen om en europeisk utredningsorder.

Ikraftträdande- och övergångsbestämmelser

Lagen om inhämtande av elektronisk bevisning inom Europeiska unionen föreslås träda i kraft den 18 augusti 2026. Mellan den 18 februari 2026 och den 18 augusti 2026 ska enligt vårt förslag en tillfällig lag gälla som reglerar tjänsteleverantörernas skyldighet att utse verksamhetsställen eller rättsliga ombud. Övriga bestämmelser

föreslås träda i kraft den 1 juli 2026. De föreslagna lagändringarna kräver enligt vår bedömning inte några särskilda övergångsbestämmelser.

Summary

The remit

We have been tasked with reviewing regulation of cross-border access to electronic evidence in relation to the following new international instruments:

- Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (“the EU Regulation”);
- Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (“the EU Directive”); and
- the Second Additional Protocol to the Council of Europe’s Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (“the Budapest Convention”).

We have also been instructed to review regulation of cross-border management of orders for the preservation of data.

The aim of the remit is to ensure that Swedish law enforcement authorities can use the cross-border tools offered by the above-mentioned instruments in an efficient and legally secure manner. In addition, the remit also involves ensuring that law enforcement authorities in the EU can gain access to electronic evidence that may be available from Swedish actors in an efficient and legally secure manner.

The EU Regulation and the EU Directive

The aim of the EU Regulation is to make cross-border gathering of electronic evidence more efficient. Under the EU Regulation, a competent authority in one Member State can contact a service provider established or represented in another Member State with a decision to preserve electronic evidence (preservation order) or to produce it (production order). It makes no difference which country the electronic data is stored in. 'Electronic evidence' refers to subscriber data, traffic data and content data. The EU Regulation only covers stored data and does not impose an obligation to store data.

If an order is not complied with, the issuing authority may request the enforcement of the order by the competent enforcing authority of the State in which the service provider is represented. If, despite this, the order is not complied with, it may be necessary to impose pecuniary penalties.

The EU Directive contains provisions whereby certain service providers are required to designate designated establishments or legal representatives within the European Union. The designated establishments or legal representatives receive European Preservation Orders and European Production Orders on behalf of the service providers and are responsible for ensuring that they are complied with.

The Regulation leaves certain issues to the Member States to regulate in national legislation. Under the EU Regulation, Member States are also required to designate one or more competent authorities that have the power to issue, transmit and execute European Preservation Orders and European Production Orders. We propose that such provisions be brought together in a supplementary act, the Act on gathering electronic evidence within the European Union. The provisions implementing the EU Directive should be included in the same Act.

The need to supplement national provisions on the gathering of evidence

In our view, there is no need for any supplementary provisions in Swedish law regarding the provisions of the EU Regulation specifying which service providers are covered by the Regulation. Nor is

there any need to amend the provisions on the storage and adaptation obligation in the Electronic Communications Act (2022:482).

The legal basis for the production or preservation of electronic evidence is derived directly from the EU Regulation. Service providers and designated establishments and legal representatives must also comply with the obligations incumbent on them under the provisions derived directly from the EU Regulation, without the need for any supplementary provisions in Swedish law.

Furthermore, no supplementary national provisions are necessary for the Swedish competent authority to be able to issue a European Production Order with the aim of obtaining subscriber data or other user data as regards the service providers covered by the EU Regulation. The same applies to obtaining traffic data and content data under the EU Regulation.

In essence, it will be possible to apply the Swedish provisions on secret interception of electronic communications and secret surveillance of electronic communications in connection with issuing a European Production Order regarding traffic data and content data. Although there are certain discrepancies with the catalogue of offences listed in Chapter 27, Sections 18a, 18b, 19a and 19b of the Swedish Code of Judicial Procedure, we do not consider that the catalogue should be expanded to include additional offences that have a maximum penalty of imprisonment of at least three years, but for which the relevant provisions do not specify a minimum penalty. Nor should the maximum penalties be increased for offences for which secret interception of electronic communications or secret surveillance of electronic communications may be used, but which do not have a maximum penalty of imprisonment of at least three years.

No amendments are needed to the Act on secret coercive measures for the purpose of enforcing custodial penalties (2024:326) to enable European Production Orders to be issued regarding traffic data to locate a person who is sentenced to imprisonment, institutional youth care or forensic mental care with special assessment for discharge. Nor should the abovementioned Act be expanded to also cover secret interception of electronic communications to enable European Production Orders to be issued regarding content data. No amendments or additions to Swedish law are needed for European Preservation Orders to be issued when a criminal offence

is suspected. However, we do propose that the Act should allow issuing an order on preserving stored data to locate a person who is sentenced to imprisonment, institutional youth care or forensic mental care with special assessment for discharge since it will also be possible to issue a European Preservation Order for this purpose.

Issuing and enforcing authorities and their responsibilities

We propose that prosecutors should be competent to issue European Production Orders and European Preservation Orders in Sweden.

Under our proposal, the Swedish Police Authority, the Swedish Security Service, Swedish Customs or another public authority that is to intervene against criminal offences or activities should also be competent to decide on issuing European Production Orders for gathering subscriber data and other user data, and on issuing European Preservation Orders. However, such orders must be approved by a prosecutor.

Under Article 4(2)(b) of the EU Regulation, a court must approve a European Production Order for the gathering of traffic data and content data before it is transmitted to the recipient. We propose that in the event of such approval, the applicable parts of what is prescribed in the Swedish Code of Judicial Procedure should apply. Furthermore, we propose that the provisions of Chapter 27, Sections 22–24, 31–33 and 35 of the Swedish Code of Judicial Procedure should also apply in such proceedings.

Under the EU Regulation, the Swedish Prosecution Authority is to be the enforcing authority.

We propose that, pursuant to Article 17 of the EU Regulation, Stockholm District Court should be the competent court for considering matters concerning conflicts of law. Under the proposal, the rules on court proceedings and appeals against court decisions would apply during the proceedings.

We consider that there is no reason to designate a central authority for the administrative management of European Production Orders or European Preservation Orders.

Implementation of the EU Directive

We propose that a service provider established in Sweden should designate an establishment in Sweden for the receipt of, compliance with and enforcement of decisions and orders covered by the EU Regulation and other legal acts falling within the scope of Article 1(2) of the EU Directive. This obligation will not apply if the service provider has designated an establishment in another Member State where the service provider also offers services or if the service provider is only established in Sweden and only offers services within Swedish territory.

A service provider that is not established in any of the EU Member States but that offers services in Sweden must designate a legal representative residing in Sweden for the receipt of, compliance with and enforcement of decisions and orders covered by the EU Regulation. This obligation does not apply if the service provider has designated a legal representative residing in another Member State in which they offer services.

The obligation to designate an establishment or legal representative should follow from the supplementary Act. It should also follow from the Act that the service provider must give the establishment or legal representative designated by the provider the powers and resources necessary to respond to decisions and orders covered by the EU Regulation and other legal acts falling within the scope specified in Article 1(2) of the EU Directive.

We propose that the Swedish Post and Telecom Authority be designated as the central authority.

The central authority is to ensure that service providers designate establishments or legal representatives and that adequate resources and powers are allocated to them. To this end, the central authority is to be entitled to access documents and data and have access rights to premises and, for these purposes, be able to request assistance from the Swedish Enforcement Authority to monitor compliance with the provisions implementing Article 3 of the EU Directive. It should be possible to impose a fine in connection with an order to produce documents and data.

Penalties

Under the EU Regulation, infringements of some of its provisions will result in pecuniary penalties. Penalties will also be imposed for infringements of provisions of the EU Directive. The penalties should be effective, proportionate and dissuasive. Penalties may be imposed both on service providers and their designated establishments or legal representatives.

It is the enforcing authority – under our proposal the Swedish Prosecution Authority – that will take decisions on pecuniary penalties in the event of infringements of the provisions in the EU Regulation by a designated establishment or legal representative in Sweden that neglects any of its obligations under Articles 10, 11 and 13(4) of the EU Regulation. The service provider is jointly and severally liable for payment of the penalty, together with the designated establishment or legal representative in Sweden.

The central authority must be able to take decisions on imposing conditional fines and pecuniary penalties in the event of infringements of the provisions implementing the EU Directive by a service provider. Pecuniary penalties in the event of infringements of the EU Regulation or the national provisions implementing the EU Directive should be set at a minimum of SEK 10 000 and a maximum of two per cent of the service provider's total global annual turnover in the previous financial year.

When assessing whether a pecuniary penalty should be imposed and determining its size, we propose that particular consideration should be given to whether the infringement was intentional or due to negligence, the damage, danger or violation the infringement involved, the nature, severity and duration of the infringement, whether the service provider who committed the infringement has previously committed a similar infringement and the financial position of the service provider concerned.

A pecuniary penalty may be reduced or waived if the infringement is excusable or if, in view of the circumstances, it would be unreasonable to impose a penalty.

Securing electronic evidence under the Budapest Convention

To comply with Article 16 of the Budapest Convention, a new coercive measure was introduced in Swedish law in Chapter 27, Section 16 of the Swedish Code of Judicial Procedure concerning orders to preserve data in electronic form. Regarding the Convention's requirement concerning international cooperation in Article 29, certain amendments were made to the International Legal Assistance in Criminal Matters Act (2000:562) and the European Investigation Order Act (2017:1000) so that cooperation under these two Acts also includes measures taken in accordance with Chapter 27, Section 16 of the Swedish Code of Judicial Procedure.

In 2022, the Swedish Prosecution Authority submitted a request for clarification concerning regulation of cross-border cooperation regarding orders to preserve data in electronic form. The request states that other EU Member States do not consider that European Investigation Orders should be used for orders under Article 29 of the Budapest Convention, and that this causes problems in judicial cooperation that may need to be addressed through legislative amendments.

In view of this, we propose that the European Investigation Order Act should not apply to the expeditious securing of data stored by means of a computer system pursuant to Article 29 of the Budapest Convention. Instead, the International Legal Assistance in Criminal Matters Act should apply to such requests.

We consider that handling a request for legal assistance in connection with an order to preserve certain stored data under Article 29 of the Budapest Convention should remain the responsibility of a prosecutor.

The Second Additional Protocol to the Budapest Convention

In November 2021, the Committee of Ministers of the Council of Europe adopted the Second Additional Protocol to the Budapest Convention. Sweden signed the Protocol on 12 May 2022. By means of a decision of the Council on 14 February 2023, EU Member

States were authorised to ratify the Protocol in the interest of the European Union.

The Second Additional Protocol contains provisions aimed at providing law enforcement authorities with new and more effective tools for cross-border access to electronic evidence. This includes the possibility for competent authorities in one State – for the purpose of a criminal investigation – to apply to private actors in another State to obtain domain and subscription data, and to contact competent authorities in the other State to enforce orders on the disclosure of subscription and traffic data.

We propose that the Riksdag approve Sweden's accession to the Second Additional Protocol to the Budapest Convention.

In order to implement the Second Additional Protocol in Swedish law, we propose that prosecutors and other law enforcement authorities should have the right to request – from top-level domain registrars or domain name resellers, or from service providers in another State that has acceded to the Second Additional Protocol to the Budapest Convention – data to identify or contact the holder of a domain name, or data about subscriptions that can reasonably be assumed to be of importance for the investigation of a criminal offence.

Furthermore, we propose that top-level domain registrars or domain name resellers offering services for domain name registration in Sweden must, upon request, provide data to a competent authority in another State that has acceded to the Second Additional Protocol to the Budapest Convention to identify or contact the holder of a domain name if that data relates to criminal activities or a criminal offence is suspected. We also propose a corresponding obligation for service providers covered by the regulations in Chapter 9, Section 33, first paragraph, point 2 of the Electronic Communications Act to produce subscription data.

It is also proposed that it should follow from Chapter 2, Section 10 of the International Legal Assistance in Criminal Matters Act that in matters concerning the requirement to deal with requests expeditiously, particular attention must be given to whether there is immediate danger to life, health or property. It is proposed that a corresponding provision be introduced in Chapter 3, Section 23 of the European Investigation Order Act.

Entry into force and transitional provisions

It is proposed that the Act on obtaining electronic evidence within the European Union enter into force on 18 August 2026. Under our proposal, a temporary act regulating the obligation of service providers to appoint establishments or legal representatives will apply between 18 February 2026 and 18 August 2026. It is proposed that the remaining provisions enter into force on 1 July 2026. In our assessment, the proposed legislative amendments do not require any special transitional provisions.

1 Författningsförslag

1.1 Förslag till tillfällig lag (2026:000) om utseende av verksamhetsställen eller rättsliga ombud

Härigenom föreskrivs följande.

1 § Denna lag genomför vissa bestämmelser i Europaparlamentets och rådets direktiv (EU) 2023/1544 av den 12 juli 2023 om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden, i denna lag kallat EU-direktivet.

Lagen innehåller tillfälliga bestämmelser om en skyldighet för tjänsteleverantörer att utse ett verksamhetsställe eller rättsligt ombud i enlighet med EU-direktivet.

2 § I lagen avses med tjänsteleverantör en juridisk person som tillhandahåller en tjänst i enlighet med artikel 2.1 i EU-direktivet.

3 § En tjänsteleverantör som är etablerad i Sverige ska utse ett verksamhetsställe i Sverige eller i en annan medlemsstat för mottagande, efterlevnad och verkställighet av beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet.

Om tjänsteleverantören utser ett verksamhetsställe i en annan medlemsstat är tjänsteleverantören inte skyldig att utse ett verksamhetsställe i Sverige under förutsättning att verksamhetsstället är etablerat i en medlemsstat där tjänsteleverantören erbjuder sina tjänster och att den staten tillämpar en av de rättsakter som anges i artikel 1.2.

Skyldigheten att utse ett verksamhetsställe gäller inte om tjänsteleverantören endast är etablerad i Sverige och enbart erbjuder tjänster inom Sveriges territorium.

4 § En tjänsteleverantör som inte är etablerad i någon medlemsstat, men som erbjuder tjänster i Sverige, ska utse ett rättsligt ombud med hemvist i Sverige för mottagande, efterlevnad och verkställighet av beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet.

Första stycket gäller inte om tjänsteleverantören har utsett ett rättsligt ombud med hemvist i en annan medlemsstat i vilken tjänsteleverantören erbjuder sina tjänster och att den staten tillämpar en av de rättsakter som anges i artikel 1.2.

Denna lag träder i kraft den 18 februari 2026 och gäller till den 18 augusti 2026.

1.2 Förslag till lag (2026:000) om inhämtande av elektronisk bevisning inom Europeiska unionen

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

1 § Denna lag innehåller bestämmelser som kompletterar Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden, i denna lag kallad EU-förordningen.

Denna lag genomför också Europaparlamentets och rådets direktiv (EU) 2023/1544 av den 12 juli 2023 om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden, i denna lag kallat EU-direktivet.

2 § Termer och uttryck i bestämmelser i denna lag som kompletterar EU-förordningen har samma betydelse som i EU-förordningen.

2 kap. Bestämmelser som kompletterar EU-förordningen

Utfärdande i Sverige av en europeisk utlämnandeorder eller bevarandeorder

1 § Åklagare är behörig enligt EU-förordningen att utfärda en europeisk utlämnandeorder och en europeisk bevarandeorder.

Polismyndigheten, Säkerhetspolisen, Tullverket, eller någon annan myndighet som ska ingripa mot brott eller brottslig verksamhet är behörig enligt EU-förordningen att utfärda en europeisk utlämnandeorder för att inhämta abonnentuppgifter och uppgifter som begärs med det enda syftet att identifiera användaren samt en europeisk bevarandeorder.

En order som har utfärdats enligt andra stycket ska godkännas av åklagare.

2 § För domstolens handläggning av ett godkännande av en europeisk utlämnandeorder för inhämtning av trafikuppgifter eller innehållsdata enligt artikel 4.2 b i EU-förordningen gäller det som föreskrivs i rättegångsbalken vid rättens lämnande av tillstånd till hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation. Vid utfärdande av en sådan order ska även 27 kap. 22, 23–24, 31–33 och 35 §§ rättegångsbalken tillämpas.

3 § Bestämmelserna i 9 kap. 29 a § lagen (2022:482) om elektronisk kommunikation ska tillämpas i de fall en motsvarande tjänsteleverantör i en annan medlemsstat lämnar ut elektronisk bevisning till en myndighet som med stöd av 1 § har utfärdat en europeisk utlämnandeorder.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om ersättningen och schablonberäkningen.

Verkställighet i Sverige av en europeisk utlämnandeorder eller bevarandeorder

4 § Åklagarmyndigheten är verkställande myndighet enligt EU-förordningen.

5 § Ett beslut av åklagare att en europeisk utlämnandeorder ska vägras enligt artikel 12.1 i EU-förordningen eller att verkställighet av en europeisk utlämnande- eller bevarandeorder inte ska ske enligt artikel 16 i EU-förordningen ska innehålla skälen för beslutet.

6 § Ett intyg om en europeisk utlämnandeorder eller en europeisk bevarandeorder ska vara skrivet på svenska eller engelska eller åtföljas av en översättning till något av dessa språk.

Förfarandet enligt artikel 17 i EU-förordningen

7 § Stockholms tingsrätt är behörig domstol enligt artikel 17 i EU-förordningen.

8 § Vid rättens handläggning av ett ärende enligt artikel 17 i EU-förordningen tillämpas reglerna om domstols handläggning i brottmål, om inte annat sägs i denna lag.

Handläggningen ska ske skriftligen. Sammanträde ska hållas endast om mottagaren av ordern begär det, om det inte är uppenbart att den europeiska utlämnandeordern ska upphävas.

Domstolen ska avgöra ett ärende inom 30 dagar efter det att den myndighet som har utfärdat den europeiska utlämnandeordern har begärt domstolens prövning. Endast om det finns särskilda skäl får denna tidsfrist överskridas.

3 kap. Bestämmelser som genomför EU-direktivet

Centralmyndighet

1 § Den myndighet regeringen bestämmer är centralmyndighet enligt EU-direktivet.

Skyldighet att utse verksamhetsställe eller rättsligt ombud

2 § En tjänsteleverantör som är etablerad i Sverige ska utse ett verksamhetsställe i Sverige eller i en annan medlemsstat för mottagande, efterlevnad och verkställighet av beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet.

Om tjänsteleverantören utser ett verksamhetsställe i en annan medlemsstat är tjänsteleverantören inte skyldig att utse ett verksamhetsställe i Sverige under förutsättning att verksamhetsstället är etablerat i en medlemsstat där tjänsteleverantören erbjuder sina tjänster och att den staten tillämpar en av de rättsakter som anges i artikel 1.2.

Skyldigheten att utse ett verksamhetsställe gäller inte om tjänsteleverantören endast är etablerad i Sverige och enbart erbjuder tjänster inom Sveriges territorium.

3 § En tjänsteleverantör som inte är etablerad i någon medlemsstat, men som erbjuder tjänster i Sverige ska utse ett rättsligt ombud med hemvist i Sverige för mottagande, efterlevnad och verkställighet av

beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet.

Första stycket gäller inte om tjänsteleverantören har utsett ett rättsligt ombud med hemvist i en annan medlemsstat i vilken tjänsteleverantören erbjuder sina tjänster och att den staten tillämpar en av de rättsakter som anges i artikel 1.2.

4 § De verksamhetsställen och rättsliga ombud som har utsetts i Sverige ska ta emot sådana beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet.

5 § En tjänsteleverantör som utser ett verksamhetsställe enligt 2 § ska ge verksamhetsstället de befogenheter och resurser som krävs för att svara på sådana beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet.

Ett verksamhetsställe, som inte har utsetts enligt 2 §, eller ett rättsligt ombud i Sverige ska ha de befogenheter och resurser som krävs för att svara på sådana beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet.

Tillsyn

6 § Centralmyndigheten ska ha tillsyn över att 2–5 §§ och de föreskrifter som har meddelats i anslutning till lagen följs.

7 § Centralmyndigheten har rätt att för tillsynen få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som omfattas av denna lag bedrivs.

8 § Centralmyndigheten får förelägga den som bedriver verksamhet som omfattas av denna lag att tillhandahålla myndigheten de upplysningar eller handlingar som behövs för tillsynen.

Ett föreläggande enligt första stycket får förenas med vite.

9 § Centralmyndighetens beslut som avser åtgärder som krävs för tillsynen enligt denna lag får verkställas av Kronofogdemyndigheten. Då gäller bestämmelserna i utskökningsbalken om verkställighet av för-

pliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

10 § Centralmyndigheten får meddela de förelägganden som behövs för att 2–5 §§ eller de föreskrifter som har meddelats i anslutning till lagen ska följas.

Ett föreläggande enligt första stycket får förenas med vite.

4 kap. Gemensamma bestämmelser om sanktionsavgifter

1 § Åklagarmyndigheten ska besluta att ta ut en sanktionsavgift av ett utsett verksamhetsställe eller rättsligt ombud i Sverige som åsidosätter någon av sina skyldigheter enligt artikel 10, 11 eller 13.4 i EU-förordningen, i den ursprungliga lydelsen.

Åklagarmyndigheten får besluta att den tjänsteleverantör som har utsett det verksamhetsställe eller rättsliga ombudet som ska betala en sanktionsavgift enligt första stycket ska ha ett solidariskt betalningsansvar för avgiften.

2 § Centralmyndigheten ska besluta att ta ut en sanktionsavgift av den tjänsteleverantör som åsidosätter någon av sina skyldigheter enligt 3 kap. 2–5 §§.

3 § Sanktionsavgiften enligt 1 och 2 §§ ska bestämmas till lägst 10 000 kronor och högst till ett sådant högre belopp som följer av artikel 15.1 i EU-förordningen, i den ursprungliga lydelsen.

4 § När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till

1. om överträdelsen varit uppsåtlig eller berott på oaktsamhet,
2. den skada, fara eller kränkning som överträdelsen inneburit,
3. överträdelsens karaktär, svårhetsgrad och varaktighet,
4. om den tjänsteleverantör som har begått överträdelsen tidigare begått en överträdelse, och
5. den berörda tjänsteleverantörens finansiella ställning.

5 § Sanktionsavgiften får sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut en avgift.

6 § En sanktionsavgift får inte beslutas enligt 2 § om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

En sanktionsavgift får inte beslutas enligt 1 § om överträdelsen omfattas av ett beslut om sanktionsavgift enligt 2 §.

7 § 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.

8 § En sanktionsavgift ska betalas till Åklagarmyndigheten eller Centralmyndigheten 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 tid, ska myndigheten lämna den obetalda avgiften för indrivning enligt lagen (1993:891) om indrivning av statliga fordringar m.m.

Sanktionsavgiften tillfaller staten.

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

10 § Beslut om sanktionsavgift får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Denna lag träder i kraft den 18 augusti 2026.

1.3 Förslag till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål

Härigenom föreskrivs i fråga om lagen (2000:562) om internationell rättslig hjälp i brottmål att 1 kap. 7 a §, 2 kap. 10 § och 3 kap. 1 § ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

1 kap. 7a §¹

Denna lag gäller inte om lagen (2017:1000) om en europeisk utredningsorder är tillämplig.

Denna lag gäller inte om lagen (2017:1000) om en europeisk utredningsorder är tillämplig.

Att lagen gäller vid skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter enligt artikel 29 i Europarådets konvention om it-relaterad brottslighet följer av 1 kap. 5 a § lagen (2017:1000) om en europeisk utredningsorder.

2 kap. 10 §

Ansökningar om rättslig hjälp skall behandlas skyndsamt. Om inte annat föreskrivs i denna lag tillämpas samma förfarande som när en motsvarande åtgärd vidtas vid en svensk förundersökning eller rättegång. Domstol kan bestämma att handläggningen helt eller delvis skall ske på ett främmande språk, om det är lämpligt.

Ansökningar om rättslig hjälp ska behandlas skyndsamt. Om det föreligger en omedelbar fara för liv, hälsa eller egendom, ska särskild hänsyn tas till kravet om skyndsamhet vid handläggningen av en ansökan.

Om inte annat föreskrivs i denna lag tillämpas samma förfarande som när en motsvarande åtgärd vidtas

¹ Senaste lydelse 2017:1005.

vid en svensk förundersökning eller rättegång.

Domstol kan bestämma att handläggningen helt eller delvis ska ske på ett främmande språk, om det är lämpligt.

3 kap.

1 §²

Bestämmelserna i 2 kap. 4 § första och tredje styckena ska tillämpas vid ansökan om rättslig hjälp utomlands, om inte annat följer av en internationell överenskommelse som är bindande för Sverige eller av krav från den mottagande staten.

I 4 kap. 9, 10, 13, 24 b, 26, 26 c och 31 a §§ finns särskilda bestämmelser om vad en ansökan ytterligare ska innehålla vid vissa slag av åtgärder.

En order enligt artikel 8 i det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet om inhämtande av abonnemangsuppgifter och lagrade trafikuppgifter ska jämföras med en ansökan om rättslig hjälp.

Denna lag träder i kraft den 1 juli 2026.

² Senaste lydelse 2013:836.

1.4 Förslag till lag om ändring i lagen (2003:1174) om vissa former av internationellt samarbete i brottmålsutredningar

Härigenom föreskrivs i fråga om lagen (2003:1174) om vissa former av internationellt samarbete i brottmålsutredningar

dels att 1 § ska ha följande lydelse,

dels att det ska införas sex nya paragrafer, 18–23 §§, och närmast före 18 och 19 §§, nya rubriker av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

1 §¹

Bestämmelserna i 2–9 §§ gäller för sådana gemensamma utredningsgrupper för brottmålsutredningar som inrättas mellanmyndigheter i Sverige och myndigheter i en eller flera stater med stöd av

1. rådets rambeslut 2002/465/RIF av den 13 juni 2002 om gemensamma utredningsgrupper,

2. konventionen av den 29 maj 2000 om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater,

3. avtalet av den 19 december 2003 mellan Europeiska unionen och Republiken Island och Konungariket Norge om tillämpningen av vissa bestämmelser i konventionen av den 29 maj 2000 om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater och 2001 års protokoll till denna, *eller*

4. det andra tilläggsprotokollet till den europeiska konventionen av den 20 april 1959 om ömsesidig rättslig hjälp i brottmål.

3. avtalet av den 19 december 2003 mellan Europeiska unionen och Republiken Island och Konungariket Norge om tillämpningen av vissa bestämmelser i konventionen av den 29 maj 2000 om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater och 2001 års protokoll till denna,

4. det andra tilläggsprotokollet till den europeiska konventionen av den 20 april 1959 om ömsesidig rättslig hjälp i brottmål, *eller*

5. *det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet.*

¹ Senaste lydelse 2013:837.

I 10–14 §§ finns bestämmelser om internationellt samarbete med kontrollerade leveranser.

Bestämmelserna i 15–17 §§ gäller överenskommelser mellan myndigheter i Sverige och myndigheter i en annan stat om samarbete som avser åtgärder i en brottsutredning som utförs av tjänstemän med skyddsidentitet.

I 18–23 §§ finns bestämmelser om inhämtande av uppgifter om domännamnsregistrering och abonnemang.

Inhämtande av uppgifter om domännamnsregistrering och abonnemang utomlands

18 §

Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott eller brottslig verksamhet får i en stat som har tillträtt det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet begära ut uppgifter från

1. en registreringsenhet för toppdomäner eller återförsäljare av domännamn för att identifiera eller kontakta innehavaren av ett domännamn, eller

2. en tjänsteleverantör om abonnemang.

En begäran får endast ske om uppgifterna rör brottslig verksamhet eller misstanke om brott.

Om en begäran enligt första stycket 2 inte har gjorts av en åklagare ska den godkännas av en

åklagare om den andra staten kräver det.

Inhämtande av uppgifter om domännamnsregistrering och abonnemang i Sverige

19 §

En registreringsenhet för toppdomäner eller återförsäljare av domännamn som erbjuder tjänster för domännamnsregistrering i Sverige ska på begäran till en behörig myndighet i en annan stat som tillträtt det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet lämna ut uppgifter för att identifiera eller kontakta innehavaren av ett domännamn om uppgifterna rör brottslig verksamhet eller misstanke om brott.

20 §

En tjänsteleverantör som är skyldig att lämna ut uppgifter om abonnemang enligt 9 kap. 33 § första stycket 2 lagen (2022:482) om elektronisk kommunikation, ska på begäran av behörig myndighet i en stat som har tillträtt det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet lämna ut motsvarande uppgifter om uppgifterna rör brottslig verksamhet eller misstanke om brott.

Uppgifterna ska lämnas ut senast 30 dagar från mottagandet

av begäran eller inom den tidsfrist som anges i begäran om fristen är längre än 30 dagar.

En begäran enligt första stycket ska vara beslutad av en åklagare eller annan rättslig myndighet eller på annat sätt vara utfärdad under oberoende tillsyn.

21 §

Uppgifterna som begärts enligt 19 och 20 §§ ska lämnas ut om inte begäran är så bristfällig att den inte utan väsentlig olägenhet kan läggas till grund för ett utlämnande. Om mottagaren inte följer begäran ska den ange skälen för detta.

En begäran enligt 19 och 20 §§ ska vara skriven på eller översatt till svenska eller engelska eller det språk som godtas av mottagaren.

22 §

Den underrättelse som den behöriga myndigheten i den andra staten ska lämna enligt artikel 7.5 a i det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet om att en begäran har gjorts enligt 20 § ska vara skriven på eller översatt till svenska, danska, norska eller engelska.

23 §

En tjänsteleverantör ska vid behov samråda med Åklagarmyndigheten innan de uppgifter som

begärts enligt 20 § första stycket lämnas ut.

Åklagarmyndigheten får besluta att tjänsteleverantören inte får lämna ut uppgifterna om det finns skäl att anta att ett utlämnande kan skada en pågående utredning om brott eller om det finns förutsättningar att vägra att lämna ut motsvarande uppgifter om de hade begärts ut enligt lagen (2000:562) om internationell rättslig hjälp i brottmål.

Denna lag träder i kraft den 1 juli 2026.

1.5 Förslag till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder

Härigenom föreskrivs i fråga om lagen (2017:1000) om en europeisk utredningsorder att det ska införas en ny paragraf, 1 kap. 5 a §, av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

1 kap.

5 a §

Lagen gäller inte vid skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter enligt artikel 29 i Europarådets konvention om it-relaterad brottslighet. För sådant säkrande gäller i stället lagen (2000:562) om internationell rättslig hjälp i brottmål.

3 kap.

23 §

En utredningsåtgärd ska verkställas skyndsamt och inom 90 dagar efter det att verkställbarhetsförklaringen meddelades enligt 19 §. Om det inte är praktiskt möjligt, får verkställigheten ske vid en senare tidpunkt.

En utredningsåtgärd ska verkställas skyndsamt och inom 90 dagar efter det att verkställbarhetsförklaringen meddelades enligt 19 §. Om det inte är praktiskt möjligt, får verkställigheten ske vid en senare tidpunkt. *Om det föreligger en omedelbar fara för liv, hälsa eller egendom, ska särskild hänsyn tas till kravet om skyndsamhet vid verkställigheten av en utredningsåtgärd.*

Om en utredningsorder översänds enligt artikel 32 i Europaparlamentets och rådets direktiv 2014/41/EU, i den ursprungliga lydelsen, ska verkställighet om möjligt ske inom 24 timmar efter det att verkställbarhetsförklaringen meddelades enligt 19 §.

Denna lag träder i kraft den 1 juli 2026.

1.6 Förslag till lag om ändring i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder

Härigenom föreskrivs i fråga om lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder

dels att 1 § ska ha följande lydelse,

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

Nuvarande lydelse

Denna lag innehåller bestämmelser om användning av hemliga tvångsmedel för att lokalisera personer i syfte att möjliggöra verkställighet av frihetsberövande påföljder.

Föreslagen lydelse

1 §

Denna lag innehåller bestämmelser om *bevarande av vissa lagrade uppgifter i elektronisk form* och om användning av hemliga tvångsmedel för att lokalisera personer i syfte att möjliggöra verkställighet av frihetsberövande påföljder.

4 a §

Den som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för att lokalisera en person för verkställighet av en frihetsberövande påföljd och som kan inhämtas med stöd av 3 § eller 9 kap. 33 § första stycket 1 lagen (2022:482) om elektronisk kommunikation får föreläggas att bevara uppgiften.

För ett föreläggande enligt första stycket tillämpas 27 kap. 16 § andra och tredje styckena och 16 a § rättegångsbalken.

Denna lag träder i kraft den 1 juli 2026.

1.7 Förslag till förordning (2026:000) med kompletterande bestämmelser om inhämtande av elektronisk bevisning inom Europeiska unionen

Härigenom föreskrivs följande.

1 § Denna förordning innehåller kompletterande bestämmelser till Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden, i denna förordning kallad EU-förordningen.

Denna förordning genomför också Europaparlamentets och rådets direktiv (EU) 2023/1544 av den 12 juli 2023 om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden, i denna förordning kallat EU-direktivet.

Förordningen är meddelad med stöd av 8 kap. 7 § regeringsformen.

2 § Termer och uttryck i bestämmelser i denna förordning som kompletterar EU-förordningen har samma betydelse som i EU-förordningen.

3 § Riksåklagaren bestämmer vilka åklagare inom åklagarväsendet som, i förekommande fall, enligt lagen (2026:000) om inhämtande av elektronisk bevisning inom Europeiska unionen är behöriga att utfärda eller godkänna en europeisk utlämnandeorder eller en europeisk bevarandeorder.

En svensk europeisk delegerad åklagare och den svenska europeiska åklagaren är som särskilda åklagare behöriga att utfärda en europeisk utlämnandeorder och europeisk bevarandeorder när de fullgör uppgifter för Europeiska åklagarmyndigheten.

4 § Post- och telestyrelsen är centralmyndighet enligt EU-direktivet.

5 § Post- och telestyrelsen får efter samråd med Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket och Åklagarmyndigheten meddela ytterligare föreskrifter om ersättning och scha-

blonberäkning enligt 2 kap. 3 § lagen (2026:000) om inhämtande av elektronisk bevisning inom Europeiska unionen.

6 § En tjänsteleverantör som har utsett ett verksamhetsställe eller rättsligt ombud i Sverige enligt 3 kap. 2–3 §§ lagen (2026:000) om inhämtande av elektronisk bevisning inom Europeiska unionen ska underrätta centralmyndigheten om

1. kontaktuppgifterna till det utsedda verksamhetsstället eller rättsliga ombudet samt eventuella ändringar av dessa uppgifter,

2. vilket eller vilka av Europeiska unionens officiella språk som en framställning till det utsedda verksamhetsstället eller rättsliga ombudet ska vara skriven på eller översatt till, och

3. det territoriella tillämpningsområdet för varje verksamhetsställe eller rättsliga ombud, om tjänsteleverantören utsett verksamhetsställen eller rättsliga ombud i fler medlemsstater än Sverige, samt vilket eller vilka av Europeiska unionens officiella språk som en framställning till vart och ett av dessa verksamhetsställen eller rättsliga ombud ska vara skriven på eller översatt till.

7 § Åklagarmyndigheten och Post- och telestyrelsen ska samråda med och informera varandra om de åtgärder som myndigheterna avser att vidta i ett ärende om påförande av sanktionsavgift enligt 4 kap. lagen (2026:000) om inhämtande av elektronisk bevisning inom Europeiska unionen.

8 § Post- och telestyrelsen ska i sin tillsyn enligt 3 kap. lagen (2026:000) om inhämtande av elektronisk bevisning inom Europeiska unionen vid behov samråda med centralmyndigheter i andra medlemsstater.

9 § Handlingar får skickas till Sverige på det sätt som parterna i det enskilda fallet överenskommer om.

10 § Ekobrottsmyndigheten, Kustbevakningen, Polismyndigheten, Säkerhetspolisen, Tullverket eller Åklagarmyndigheten ska till Europeiska kommissionen lämna de statistikuppgifter och andra uppgifter som avses i artikel 28 i EU-förordningen och som finns tillgängliga hos respektive myndighet.

Denna förordning träder i kraft den 18 augusti 2026.

1.8 Förslag till förordning om ändring i förordningen (2000:704) om internationell rättslig hjälp i brottmål

Härigenom föreskrivs i fråga om förordningen (2000:704) om internationell rättslig hjälp i brottmål att det ska införas två nya paragrafer, 4 a och 14 b §§, av följande lydelse.

4 a §

Om en begäran om ett visst förfarande enligt 2 kap. 11 § lagen (2000:562) om internationell rättslig hjälp i brottmål inte kan följas, ska den utländska myndigheten underrättas om detta.

14 b §

Om den utländska myndigheten har angett villkor för verkställighet av en ansökan om rättslig hjälp ska den myndigheten underrättas skyndsamt om villkoret kan godtas.

Denna förordning träder i kraft den 1 juli 2026.

1.9 Förslag till förordning om ändring i förordningen (2003:1176) om vissa former av internationellt samarbete i brottsutredningar

Härigenom föreskrivs i fråga om förordningen (2003:1176) om vissa former av internationellt samarbete i brottsutredningar

dels att det närmast efter 1 § ska införas en ny rubrik som ska lyda ”Gemensamma utredningsgrupper”,

dels att det ska införas åtta nya paragrafer, 7–14 §§,

dels att det närmast före de nya 7 och 12 §§ ska införas nya rubriker av följande lydelse.

Inhämtande av uppgifter om domännamnsregistrering och abonnemang utomlands

7 §

En begäran av en svensk myndighet enligt 18 § första stycket 1 lagen (2003:1174) om vissa former av internationellt samarbete i brottmålsutredningar ska innehålla uppgifter om

1. namn på den myndighet och, den person på myndigheten som kan kontaktas,

2. adress, telefonnummer och e-postadress till myndigheten,

3. datum för utfärdande av begäran,

4. det domännamn som begäran avser och en detaljerad redogörelse för den information som begärs,

5. den tid inom vilken uppgifterna ska lämnas ut samt hur uppgifterna ska lämnas ut, och

6. att begäran görs enligt andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet.

8 §

En begäran enligt 18 § första stycket 2 lagen (2003:1174) om vissa former av internationellt samarbete i brottnålsutredningar ska, utöver vad som anges 7 § 1–3 samt 5 och 6, innehålla uppgifter om

- 1. namn och adress till den tjänsteleverantör till vilken begäran riktas,*
- 2. det eller de brott som den brottsliga verksamheten eller brottsmiss-tanken avser och tillämplig påföljd för brottet eller brotten,*
- 3. annan myndighet än den utfärdande myndigheten eftersöker uppgifterna,*
- 4. den rättsliga grunden för den utfärdande myndighetens befogenhet att utfärda begäran,*
- 5. en detaljerad beskrivning av de uppgifter om abonnemang som begäran avser,*
- 6. andra uppgifter som underlättar inhämtandet av uppgifterna.*

9 §

Om den andra staten kräver samtidig underrättelse om en begäran enligt 18 § första stycket 2 lagen (2003:1174) om vissa former av internationellt samarbete i brottnålsutredningar ska en sådan underrättelse skickas samtidigt med begäran till den myndighet som utsetts av den andra staten.

En underrättelse enligt första stycket ska innehålla den information som anges i 8 §.

10 §

Den myndighet som skickar en begäran enligt 18 § första stycket lagen (2003:1174) om vissa former av internationellt samarbete i brottmålsutredningar ansvarar för att begäran översätts till ett språk som mottagaren godtar.

11 §

En begäran enligt 18 § första stycket lagen (2003:1174) om vissa former av internationellt samarbete i brottmålsutredningar får översändas i elektronisk form om mottagaren godtar det.

Inhämtande av uppgifter om domännamnsregistrering och abonnemang i Sverige

12 §

En begäran som riktas mot en registreringsenhet för toppdomäner eller återförsäljare av domännamn i Sverige enligt 19 § lagen (2003:1174) om vissa former av internationellt samarbete i brottmålsutredningar ska innehålla de uppgifter som anges i 7 §. En sådan begäran får översändas i elektronisk form.

13 §

En begäran som riktas mot en tjänsteleverantör i Sverige enligt 20 § lagen (2003:1174) om vissa former av internationellt samarbete i brottmålsutredningar ska innehålla de upp-

gifter som anges i 8 §. En sådan begäran får översändas i elektronisk form.

14 §

Åklagarmyndigheten får begära kompletterande information från den myndighet som utfärdat en begäran enligt 20 § lagen (2003:1174) om vissa former av internationellt samarbete i brottmålsutredningar. Den kompletterande informationen får inte lämnas ut till tjänsteleverantören utan den utfärdande myndighetens samtycke.

Denna förordning träder i kraft den 1 juli 2026.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

Regeringen beslutade den 15 juni 2023 att ge en särskild utredare i uppdrag att se över regleringen om gränsöverskridande åtkomst till elektroniska bevis med anledning av nya internationella instrument, vilka är

- förordning (EU) 2023/1543 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden (EU-förordningen),
- direktiv (EU) 2023/1544 om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden (EU-direktivet), och
- det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet (Budapestkonventionen).

Syftet med uppdraget är, enligt kommittédirektiven, att säkerställa att svenska brottsbekämpande myndigheter på ett effektivt och rättssäkert sätt kan använda de gränsöverskridande verktyg som ovan nämnda instrument erbjuder. Därutöver innebär uppdraget att även brottsbekämpande myndigheter inom EU på ett effektivt och rättssäkert sätt kan få tillgång till elektroniska bevis som kan finnas tillgängliga hos svenska aktörer.

I uppdraget ingår bl.a. att

- kartlägga vilka svenska bestämmelser som berörs av EU-förordningens bestämmelser om europeiska utlämnande- och bevarandeborder samt analysera om de svenska bestämmelserna bör ändras eller kompletteras,
- ta ställning till vilken eller vilka myndigheter som bör utses till behöriga myndigheter enligt EU-förordningen,
- analysera hur EU-direktivet om utsedda verksamhetsställen och rättsliga ombud bör genomföras i svensk rätt,
- kartlägga och analysera vilka sanktioner som bör aktualiseras vid överträdelse av EU-förordningen och relevanta nationella bestämmelser som genomför EU-direktivet,
- kartlägga vilka svenska bestämmelser som berörs av det andra tilläggsprotokollet till Budapestkonventionen och analysera om de svenska bestämmelserna bör ändras eller kompletteras, och
- lämna nödvändiga författningsförslag.

Utredningens direktiv finns i bilaga 1 till betänkandet, tillsammans med EU-förordningen (bilaga 2), EU-direktivet (bilaga 3) och det andra tilläggsprotokollet till Budapestkonventionen (bilaga 4). Översättningen av tilläggsprotokollet är inte en officiell översättning.

2.2 Utredningens arbete

Utredningens arbete har bedrivits på sedvanligt sätt med regelbundna sammanträden med förordnade experter. Sedan oktober 2023 har utredningen hållit sammanlagt åtta sammanträden, varav ett tvådagars slutsammanträde i internatform. Därutöver har utredningen haft kontakter med de olika experterna för att diskutera specifika frågor.

Enligt direktiven ska vi i den utsträckning det behövs samråda med berörda myndigheter och organisationer. Vi ska också hålla oss informerade om sådant arbete inom Regeringskansliet och utredningsväsendet samt inom EU och andra internationella forum som är relevant för uppdraget.

Under utredningsarbetet har vi därför haft möten med företrädare för Åklagarmyndigheten, Post- och telestyrelsen samt Polismyndigheten. Vi har också haft möte med organisationen TechSverige tillsammans med representanter från några av dess medlemsföretag; Microsoft, Telenor Sverige, Tele2 Sverige, Telia Sverige och Hi3G Access. Vidare har vi haft möte med Stiftelsen för Internetinfrastruktur (Internetstiftelsen).

Sekretariatet och experten Karin Henriksson har deltagit vid möten som Europeiska kommissionen anordnat för EU:s medlemsstater med anledning av tillämpningen av EU-förordningen respektive möten arrangerade av Europarådet avseende genomförandet av det andra tilläggsprotokollet till Budapestkonventionen. Relevant arbete inom Regeringskansliet och på EU-nivå har följts främst genom Karin Henrikssons försorg.

2.3 Betänkandets disposition

I avsnitt 1 redovisas våra författningsförslag. Därefter behandlas i detta avsnitt vårt uppdrag och arbete. Avsnitt 3 innehåller en redogörelse för innehållet i EU-förordningen. Avsnitt 4 innehåller en redogörelse för gällande rätt i fråga om inhämtning av elektronisk bevisning. I avsnitt 5 redovisas de allmänna utgångspunkterna för vårt arbete. I avsnitt 6–12 redovisas i huvudsak våra överväganden och förslag. Avsnitt 6 rör behovet av kompletteringar av befintliga nationella bestämmelser om bevisinhämtning. I avsnitt 7 behandlar vi frågor om behöriga utfärdande och verkställande myndigheter enligt EU-förordningen. Avsnitt 8 behandlar genomförandet av EU-direktivet. Frågor om sanktioner vid överträdelser av vissa bestämmelser i EU-förordningen respektive de föreslagna nationella bestämmelserna som genomför EU-direktivet behandlar vi i avsnitt 9. Avsnitt 10 rör övriga frågor i förhållande till EU-förordningen. Skyndsamt säkrande av elektronisk bevisning enligt artikel 29 i Budapestkonventionen hanterar vi i avsnitt 11. Avsnitt 12 rör det andra tilläggsprotokollet till Budapestkonventionen och våra förslag för att kunna ratificera protokollet. Konsekvenserna av våra förslag hanteras i avsnitt 13. Ikraftträdande och övergångsbestämmelser behandlas i avsnitt 14 och författningskommentaren till föreslagna lagregler finns i avsnitt 15.

3 Förordning (EU) 2023/1543

3.1 Inledning

Det övergripande syftet med förordning (EU) 2023/1543¹ är att skapa ett nytt ändamålsenligt regelverk som kompletterar befintlig lagstiftning och effektiviserar gränsöverskridande inhämtning av elektronisk bevisning (se även skäl 9 och 10). Hädanefter i betänkandet EU-förordningen. EU-förordningen gör det möjligt för en myndighet i en medlemsstat att beordra en tjänsteleverantör som är etablerad i en annan medlemsstat och oaktat var uppgifterna finns lagrade att lämna ut eller bevara elektronisk bevisning. En order ska i första hand översändas till den rättsliga företrädare som tjänsteleverantören enligt direktiv (EU) 2023/1544² ska utse. Hädanefter i betänkandet EU-direktivet. I avsnitt 8 redogörs närmare för EU-direktivet. Kort kan dock sägas att EU-direktivet syftar till att säkerställa att medlemsstaterna ser till att de tjänsteleverantörer som omfattas av EU-förordningens regelverk utser verksamhetsställen eller rättsliga ombud som ansvarar för att en order om att lämna ut eller bevara elektronisk bevisning verkställs.

En grundläggande förutsättning enligt EU-förordningen är att en order om att lämna ut eller bevara elektronisk bevisning görs inom ramen för ett straffrättsligt förfarande eller för verkställighet av en frihetsberövande påföljd. En annan viktig förutsättning är att den tjänsteleverantör som ordern riktas mot erbjuder sina tjänster inom EU. De tjänsteleverantörer som omfattas är i huvudsak företag som erbjuder elektroniska kommunikations- och informations-

¹ Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden.

² Europaparlamentets och rådets direktiv (EU) 2023/1544 av den 12 juli 2023 om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden.

tjänster samt it-infrastruktur tjänster som t.ex. ip-adresser och domännamn. Elektroniska bevis kan enligt EU-förordningen vara t.ex. namn- och adressuppgifter, kontonummer och telefonnummer å ena sidan och det faktiska innehållet i skriftlig eller muntlig kommunikation å andra sidan. EU-förordningen omfattar enbart lagrade uppgifter och innebär ingen skyldighet att lagra uppgifter.

Om tjänsteleverantören eller dess rättsliga företrädare inte efterlever ordern, kan den utfärdande myndigheten, enligt EU-förordningen, vända sig till en behörig myndighet i den verkställande staten och be myndigheten att erkänna ordern och vidta åtgärder för att se till att den blir verkställd. Efterlevs inte ordern trots detta kan det bli aktuellt med sanktionsavgifter.

3.2 EU-förordningens innehåll och allmänna tillämpningsområde

3.2.1 Innehåll

EU-förordningen reglerar under vilka förutsättningar en myndighet i en medlemsstat – i straffrättsliga förfaranden – får utfärda en europeisk utlämnande- eller bevarandeorder och därigenom beordra en tjänsteleverantör i en annan medlemsstat att lämna ut eller att bevara elektroniska bevis, oavsett var uppgifterna finns lagrade (artikel 1.1 första stycket). Ett viktigt undantag är att EU-förordningen inte påverkar de nationella myndigheternas befogenheter att rikta sig till tjänsteleverantörer som har ett verksamhetsställe eller är representerade på deras territorium i syfte att säkerställa att dessa följer nationella åtgärder liknande dem som avses i förordningen (artikel 1.1 andra stycket). Se även skäl 18 i EU-förordningen.

Även om det i huvudsak kommer att vara myndigheter som initierar ett utfärdande av en europeisk utlämnande- eller bevarandeorder kan en sådan order också utfärdas på begäran av en misstänkt eller tilltalad, eller av dennes försvarare om det är förenligt med nationell straffprocessrätt (artikel 1.2).

I artikel 1.3 anges att EU-förordningen inte ändrar medlemsstaternas eller dess myndigheters skyldigheter att respektera de grundläggande rättigheter och rättsprinciper som återges i Europeiska unionens stadga om de grundläggande rättigheterna (EU:s rättighetsstadga) och artikel 6 i Fördraget om Europeiska unionen

(EU-fördraget). Vidare anges i samma bestämmelse att EU-förordningen ska tillämpas utan att det påverkar tillämpningen av grundläggande principer, särskilt yttrande- och informationsfriheten, vilket innefattar mediernas frihet och mångfald, respekten för privatlivet och familjelivet, skyddet av personuppgifter och rätten till ett effektivt rättsligt skydd. I skäl 10 och 11 redogörs närmare om dessa rättigheter.

3.2.2 Tillämpningsområde

I artikel 2 finns allmänna begränsningar av EU-förordningens tillämpningsområde.

EU-förordningen är tillämplig på tjänsteleverantörer som erbjuder tjänster i unionen (artikel 2.1). En europeisk utlämnande- eller bevarandeorder får endast utfärdas för uppgifter som hänförs till de tjänster som avses i artikel 3.3 (artikel 2.3). EU-förordningen är inte tillämplig för att ge en annan medlemsstat eller ett tredjeland ömsesidig rättslig hjälp (artikel 2.4).

Vidare får en europeisk utlämnande- eller bevarandeorder enligt artikel 2.2 utfärdas endast inom ramen för straffrättsliga förfaranden, vilket inkluderar förfaranden avseende brott för vilka en juridisk person kan ställas till ansvar eller bestraffas i den utfärdande staten. En order får också enligt samma bestämmelse utfärdas för verkställighet av en frihetsberövande påföljd på minst fyra månader om den dömda personen undandragit sig verkställighet av den utdömda påföljden (se även skäl 25)³. I sistnämnda fallet undantas domar som beslutats efter en förhandling där personen inte var personligen närvarande (s.k. utevarodomar).

När vi i betänkandet behandlar frågor om EU-förordningen kommer begreppet ”straffrättsliga förfaranden” att inkludera förfaranden som rör verkställighet av en frihetsberövande påföljd om minst fyra månader, om inte annat särskilt anges.

³ I den svenska översättningen har ”absconded from justice” översatts ”undandragit sig lagföring”. Den korrekta innebörden torde dock – med hänsyn till att det är fråga om verkställighet av påföljd och till den engelska lydelsen av artikeltexten – vara att personen ska ha undandragit sig från verkställighet av den utdömda påföljden.

3.3 Förordningens definitioner

Artikel 3 innehåller definitioner av begrepp som används i EU-förordningen. I detta avsnitt redogörs översiktligt för dessa definitioner.

I artiklarna 3.1 och 3.2 definieras en europeisk utlämnandeorder respektive en europeisk bevarandeorder. Den förra syftar till att en tjänsteleverantör ska lämna ut elektronisk bevisning till den utfärdande myndigheten, medan den andra avser ett beslut varigenom en tjänsteleverantör ska bevara nämnda bevis i avvaktan på en utlämnandeorder. Närmare om innehållet i definitionerna av och förutsättningarna för att utfärda en europeisk utlämnande- eller bevarandeorder redogörs för i avsnitt 6.3.

I artiklarna 3.3 och 3.4 anges vilka tjänsteleverantörer som omfattas av regelverket samt vad som avses med att ”erbjuda tjänster i unionen”. Dessa frågor behandlas utförligt i avsnitt 6.2. En tjänsteleverantör ska enligt EU-direktivet utse ett verksamhetsställe eller rättsligt ombud som ska ta emot och verkställa en europeisk utlämnande- eller bevarandeorder. Verksamhetsställe och rättsligt ombud definieras i artikel 3.5–3.7 och behandlas i avsnitt 8.2.1.

Med elektroniska bevis avses enligt artikel 3.8 abonnentuppgifter, trafikuppgifter eller innehållsdata som lagras i elektronisk form av en tjänsteleverantör eller på en tjänsteleverantörs vägnar vid tidpunkten för mottagandet av ett intyg om en europeisk utlämnande- eller bevarandeorder. I artikel 3.9–3.12 definieras närmare vad som avses med abonnentuppgifter, uppgifter som har begärts med det enda syftet att identifiera användaren, trafikuppgifter och innehållsdata. Den närmare innebörden av dessa definitioner behandlas i avsnitt 6.3.1. När det gäller ”uppgifter som har begärts med det enda syftet att identifiera användaren” kommer begreppet ”andra användaruppgifter” användas i betänkandet.

En definition av informationssystem finns i artikel 3.13. I artikel 3.14–3.17 definieras begreppen utfärdande stat, utfärdande myndighet, verkställande stat och verkställande myndighet. Vad som avses med nödsituationer anges i artikel 3.18 (se närmare om detta i avsnitt 7.2.1). Slutligen anges i artikel 3.21 vad som avses med decentraliserat it-system (se avsnitten 3.11 och 10.5).

3.4 Behöriga myndigheter

I artikel 4.1–4.4 finns bestämmelser om vilka nationella myndigheter som är behöriga att utfärda en europeisk utlämnandeorder respektive en europeisk bevarandeorder. I korthet kan nämnas att en europeisk utlämnande- eller bevarandeorder får som huvudregel utfärdas av en domare, en domstol, en undersökningsdomare eller en allmän åklagare som är behörig i det berörda ärendet. En åklagare får dock inte utfärda en europeisk utlämnandeorder om den avser inhämtning av trafikuppgifter eller innehållsdata.

För att EU-förordningen ska bli mer anpasslig till medlemsstaternas nationella system får en europeisk utlämnande- eller bevarandeorder utfärdas av en annan myndighet än vad som följer av huvudregeln om den myndigheten har behörighet att utfärda en motsvarande order enligt nationell rätt. I dessa fall ska dock ordern godkännas av en domare, domstol, undersökningsdomare eller allmän åklagare i den utfärdande staten eller av en domare, en domstol eller en undersökningsdomare om det rör sig om en europeisk utlämnandeorder avseende trafikuppgifter eller innehållsdata. I nödsituationer görs vissa undantag (artikel 4.5).

Varje medlemsstat får utse en eller flera centralmyndigheter som bl.a. ska ansvara för det administrativa översändandet av intyg om europeiska utlämnande- eller bevarandeorder samt annan officiell kommunikation (artikel 4.6).

EU-förordningens bestämmelser om behöriga myndigheter och centralmyndigheter behandlas närmare i avsnitt 7.

3.5 Utfärdande av en europeisk utlämnande- eller bevarandeorder

3.5.1 Villkoren för utfärdande av en order

Artiklarna 5 och 6 anger de närmare villkoren för utfärdande av en europeisk utlämnande- eller bevarandeorder. Generellt kan sägas att kraven för att utfärda en europeisk utlämnandeorder är högre ställda än de som gäller för att utfärda en europeisk bevarandeorder, vilket förklaras av att en utlämnandeorder är mer ingripande än en bevarandeorder. I båda fallen krävs emellertid att åtgärden är nödvändig och proportionell med beaktande av den misstänktes

eller tilltalades rättigheter, och en order får utfärdas endast om en liknande order skulle ha kunnat utfärdas på samma villkor i ett liknande inhemskt ärende.

En europeisk utlämnandeorder för inhämtning av abonnent-uppgifter eller andra användaruppgifter och en europeisk bevarandeorder får utfärdas för alla brott och för verkställighet av en frihetsberövande påföljd om minst fyra månader. Beträffande en europeisk utlämnandeorder för inhämtning av trafikuppgifter eller innehållsdata ställs krav på strafftrösklar eller att det ska röra sig om vissa i artikeln särskilt angivna brott, under förutsättning att brotten har begåtts helt eller delvis med hjälp av ett informationssystem.

I båda artiklarna anges vilken information en europeisk utlämnande- eller bevarandeorder ska innehålla (se även bilaga I och II till EU-förordningen).

När det gäller utfärdande av en europeisk utlämnandeorder finns ytterligare bestämmelser om bl.a. till vilken tjänsteleverantör en order ska riktas mot, sekretess och om att den utfärdande myndigheten ska rådgöra med den verkställande myndigheten om trafikuppgifter eller innehållsdata som begärs ut hänför sig till tryck- och yttrandefrihet.

Villkoren för utfärdande av en europeisk utlämnandeorder respektive europeisk bevarandeorder behandlas närmare i avsnitt 6.3. Övriga frågor behandlas i avsnitt 10.

3.5.2 Förfarandet vid utfärdandet av en order

Enligt artikel 7.1 ska en europeisk utlämnande- eller bevarandeorder som huvudregel ställas direkt till ett utsett verksamhetsställe eller till ett rättsligt ombud för den berörda tjänsteleverantören.

Om en europeisk utlämnandeorder utfärdas för att inhämta trafikuppgifter eller innehållsdata, ska den utfärdande myndigheten enligt artikel 8.1 som utgångspunkt anmäla detta till den verkställande myndigheten.

En europeisk utlämnande- eller bevarandeorder översänds genom att den utfärdande myndigheten fyller i ett intyg om en europeisk utlämnande- eller bevarandeorder (artikel 9.1). Intygen återfinns i bilaga I och II till EU-förordningen.

Enligt artikel 9.2–9.3 ska en ett intyg innehålla den information som följer av artiklarna 5.5 respektive 6.4. I artikel 9.4 finns bestämmelser om vilket ett språk ett intyg ska vara upprättat på eller översatt till.

Bestämmelserna i artiklarna 7–9 berörs mer i avsnitt 7.2 och 7.3.

3.6 Verkställigheten av en europeisk utlämnande- eller bevarandeorder

3.6.1 Mottagarens skyldigheter

Artikel 10 reglerar de skyldigheter som åvilar det verksamhetsställe eller rättsliga ombud som mottar en europeisk utlämnandeorder. I EU-förordningen anges emellanåt ”mottagaren”, vilket begrepp inkluderar det utsedda verksamhetsstället eller det rättsliga ombudet men även tjänsteleverantören.

Till att börja med ska verksamhetsstället eller det rättsliga ombudet skyndsamt se till att bevara de uppgifter som ska lämnas ut. I artikel 10.2–10.4 regleras inom vilka tidsfrister uppgifterna ska lämnas ut, vilket enligt huvudregeln är tio dagar. I de fall en anmälan har gjorts enligt artikel 8.1 gäller samma tidsfrister för den verkställande myndigheten att ta ställning till om ett utlämnande ska vägras. I nödsituationer är tidsfristerna mycket kortare och uppgifterna ska lämnas ut av mottagaren inom åtta timmar. I anmälningsfallen (enligt artikel 8.1) har dock den verkställande myndigheten 96 timmar på sig för att ta ställning till om de uppgifter som har lämnats över får användas eller inte, dvs. den myndighetens ställningstagande kommer i huvudsak ske efter det att uppgifterna har lämnats ut till den utfärdande myndigheten.

Motsvarande bestämmelser beträffande verksamhetsställets och det rättsliga ombudets skyldigheter när europeisk bevarandeorder har utfärdats finns i artikel 11. Verksamhetsstället eller det rättsliga ombudet ska se till att utan onödigt dröjsmål bevara de begärda uppgifterna. Skyldigheten att bevara uppgifterna upphör efter 60 dagar om inte den utfärdande myndigheten bekräftar att en efterföljande utlämnandeorder har utfärdats (artikel 11.1). Under denna period får den utfärdande myndigheten förlänga tidsfristen för skyldigheten att bevara uppgifterna med ytterligare 30 dagar, om det är nödvändigt för att en efterföljande utlämnandeorder ska

kunna utfärdas. Om den utfärdande myndigheten under den tidsperiod uppgifterna är bevarade, bekräftar att en efterföljande utlämnandeorder har utfärdats ska mottagaren bevara uppgifterna så länge som krävs för att lämna ut uppgifterna när framställan om utlämnande mottas (artikel 11.2).

Om verksamhetsstället eller det rättsliga ombudet anser att ett utlämnande eller bevarande av uppgifterna skulle kunna inkräkta på immunitet eller privilegier, eller på regler om fastställande eller begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet eller yttrandefrihet i andra medier enligt den verkställande statens rätt, ska verksamhetsstället eller det rättsliga ombudet enligt artiklarna 10.5 respektive 11.4 informera den utfärdande och verkställande myndigheten, vilka myndigheter kan eller ska vidta vissa åtgärder.

I de fall verksamhetsstället eller det rättsliga ombudet inte kan fullgöra sin skyldighet att lämna ut eller bevara uppgifterna inom de tidsfrister som anges i artiklarna 10.6 och 10.7 respektive 11.5 och 11.6 ska den utfärdande myndigheten underrättas.

Av artikel 14 framgår att tjänsteleverantören får kräva ersättning för sina kostnader från den utfärdande staten. Det får dock endast ske om sådan rätt till ersättning föreskrivs i den utfärdande statens nationella rätt.

Bestämmelserna i artiklarna 10 och 11 behandlas i avsnitt 6.5.2, medan artikel 14 behandlas i avsnitt 10.3.

3.6.2 Verkställande myndighetens huvudsakliga uppgifter

Om den verkställande myndigheten har mottagit en sådan anmälan som avses i artikel 8.1 ska myndigheten enligt artikel 12.1, inom de tidsfrister som anges i artikeln, ta ställning till om det kan finnas skäl att åberopa en av de vägransgrunder som anges i artikel 12.1.

Om mottagaren av en europeisk utlämnande- eller bevarandeorder inte efterlever en begäran utan godtagbara skäl får enligt artikel 16.1 den myndighet som utfärdat ordern begära att den verkställande myndigheten verkställer orden om den myndigheten i tillämpliga fall inte efter en anmälan enligt artikel 8.1 redan har åberopat några av vägransgrunderna i artikel 12.1.

Den verkställande myndigheten ska som huvudregel erkänna och vidta de åtgärder som krävs för att verkställa ordern (artikel 16.2). Ett sådant beslut behöver dock inte fattas om den verkställande myndigheten anser att skäl finns att vägra verkställighet med stöd av de vägransgrunder som anges i artiklarna 16.4 respektive 16.5.

Om den verkställande myndigheten beslutar att erkänna ordern ska den enligt artikel 16.3 kräva att mottagaren fullgör sina skyldigheter. Samtidigt ska mottagaren informeras om möjligheten att invända mot fullföljandet av den berörda ordern med stöd av artikel 16.4 a–f respektive artikel 16.5 a–e. Vidare ska den verkställande myndigheten informera mottagaren om de tillämpliga sanktionerna vid bristande efterlevnad samt tidsfristen för efterlevnad eller invändningar.

I avsnitt 7.5.4 behandlas frågan om vilken eller vilka nationella myndigheter som bör utses till verkställande myndighet. En närmare redogörelse för vägransgrunderna i artiklarna 12 och 16 och den prövning som den utsedda verkställande myndigheten ska vidta görs i avsnitten 7.3.2 och 7.5.4–5.

3.7 Sanktioner

Enligt artikel 15.1 ska medlemsstaterna fastställa regler om sanktionsavgifter som är tillämpliga på överträdelse av artiklarna 10, 11 och 13.4, i enlighet med artikel 16.

Sanktionsavgifterna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska säkerställa att sanktionsavgifter på upp till två procent av tjänsteleverantörens totala globala årsomsättning föregående räkenskapsår kan åläggas. Utan att det påverkar deras skyldigheter vad avser dataskydd ska tjänsteleverantörer inte hållas ansvariga för olägenheter som orsakas av deras användare eller tredje parter utslutande till följd av att de i god tro rättar sig efter ett intyg om en europeisk utlämnandeorder eller ett intyg om en europeisk bevarandeorder (artikel 15.2).

I avsnitt 9 behandlas frågan om sanktionsavgifter.

3.8 Rättsmedel

I artikel 18 regleras frågor om rättsmedel. Den person vars uppgifter har begärts genom en europeisk utlämnandeorder ska ha rätt till effektiva rättsmedel mot ordern. Om personen är en misstänkt eller en tilltalad, ska den ha rätt till effektiva rättsmedel under det straffrättsliga förfarande där uppgifterna användes. Rätten till effektiva rättsmedel ska utövas vid en domstol i den utfärdande staten i enlighet med dess nationella rätt och ska innefatta möjligheten att bestrida åtgärdens lagenlighet, inklusive dess nödvändighet och proportionalitet, utan att det påverkar garantierna för de grundläggande rättigheterna i den verkställande staten. Vid tillämpningen av artikel 13.1 (se avsnitt 3.10) ska information ges i god tid om möjligheterna enligt nationell rätt att utnyttja rättsmedel, och det ska säkerställas att de kan utövas på ett effektivt sätt.

Samma tidsfrister eller andra villkor för att utnyttja rättsmedel ska gälla vid tillämpning av EU-förordningen som i liknande inhemska ärenden och på ett sätt som garanterar att de berörda personerna kan utöva sin rätt till dessa rättsmedel på ett effektivt sätt.

Utan att det påverkar nationella förfaranderegler ska den utfärdande staten och varje annan medlemsstat till vilken elektroniska bevis har överförts enligt EU-förordningen säkerställa att rätten till försvar och ett rättvist förfarande vid bedömningen av de bevis som inhämtats genom den europeiska utlämnandeordern respekteras.

I avsnitt 10.4 behandlas frågan om effektiva rättsmedel närmare.

3.9 Lagkonflikter

Artikel 17 innehåller bestämmelser om motstridiga skyldigheter i förhållande till tredje land.

Om ett verksamhetsställe eller ett rättsligt ombud anser att efterlevnaden av en europeisk utlämnandeorder skulle strida mot en skyldighet enligt ett tredjelands tillämpliga rätt, ska den senast tio dagar efter mottagandet av intyget om ordern informera den utfärdande myndigheten och den verkställande myndigheten om sina skäl till att inte fullfölja ordern (artikel 17.1–17.2). Den utfärdande myndigheten ska ompröva om huruvida den europeiska utlämnandeordern ska fullföljas. Om den myndigheten har för avsikt

att upprätthålla den europeiska utlämnandeordern ska den begära prövning av en domstol i den utfärdande staten.

Domstolens prövning om den europeiska utlämnandeordern ska fullföljas eller om uppgifterna inte får röjas, ska baseras på vissa i artikeln angivna faktorer, bl.a. det intresse som skyddas genom tredje-landets relevanta rätt, inklusive grundläggande rättigheter samt andra grundläggande intressen som förhindrar röjande av uppgifterna.

Frågor om behörig domstol samt hur ett ärende enligt artikel 17 ska handläggas i svensk domstol behandlas i avsnitt 7.4 och 7.5.7.

3.10 Användarinformation och sekretess

Av artikel 13.1 följer att den utfärdande myndigheten utan onödigt dröjsmål ska informera den person vars uppgifter begärs genom en europeisk utlämnandeorder, bl.a. om tillgängliga rättsmedel. Den utfärdande myndigheten får dock enligt artikel 13.2 i enlighet med den utfärdande statens nationella rätt skjuta upp eller begränsa informationen till, eller underlåta att informera den person vars uppgifter begärs, i den mån och så länge som villkoren i artikel 13.3 i direktiv 2016/680⁴ är uppfyllda. I sådant fall ska den utfärdande myndigheten ange skälen till uppskjutandet, begränsningen eller underlåtelser. Även en kort motivering ska läggas till i intyget om en europeisk utlämnandeorder.

Verksamhetsstället eller det rättsliga ombudet ska vidta de operativa och tekniska åtgärder som krävs för att säkerställa konfidentialitet, sekretess och integritet i fråga om en europeisk utlämnande- eller bevarandeorder och för de uppgifter som lämnas ut eller bevaras (artikel 13.4).

Frågan om användarinformation behandlas i avsnitt 10.4. Bestämmelserna i artikel 13.4 om sekretess behandlas närmare i avsnitt 6.5.2. I avsnitt 10.8 behandlas frågor om sekretess beträffande det informationsutbyte som sker mellan myndigheter till följd av EU-förordningens bestämmelser.

⁴ 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.

3.11 Det decentraliserade it-systemet

EU-förordningen innehåller bestämmelser om ett decentraliserat it-system (artiklarna 19–26).

All skriftlig kommunikation mellan behöriga myndigheter och utsedda verksamhetsställen eller rättsliga ombud ska ske genom ett säkert och tillförlitligt decentraliserat it-system. Varje medlemsstat och tjänsteleverantör ska säkerställa att de utsedda verksamhetsställena eller rättsliga ombuden i den medlemsstaten ges åtkomst till det decentraliserade it-systemet via sina respektive nationella it-system.

Skriftlig kommunikation mellan behöriga myndigheter samt skriftlig kommunikation med behöriga unionsbyråer eller unionsorgan, ska också ske via det decentraliserade it-systemet.

I avsnitt 10.5 behandlas närmare det decentraliserade it-systemet och frågan om kommunikation.

3.12 Övriga bestämmelser och om ikraftträdande

Enligt artikel 27 får varje medlemsstat när som helst besluta att den kommer att godta översättningar av en europeisk utlämnande- eller bevarandeorder till ett eller flera av unionens officiella språk utöver deras officiella språk (se även avsnitt 10.2).

Artikel 28 innehåller bestämmelser om övervakning av effekterna av EU-förordningen samt rapportering av statistik (se avsnitt 10.6).

Artiklarna 29–31 innehåller bestämmelser om ändringar av intyg och formulär, delegering till kommissionen samt skyldighet för medlemsstaterna att rapportera bl.a. behöriga myndigheter till kommissionen.

Av artikel 32.1 följer att EU-förordningen inte påverkar unionens instrument eller andra internationella instrument, avtal och överenskommelser beträffande bevisinhämtning som omfattas av förordningens tillämpningsområde. Enligt artikel 32.2 ska medlemsstaterna meddela kommissionen senast den 18 augusti 2026 om eventuella befintliga instrument, avtal och överenskommelser som avses i artikel 32.1 och som de kommer att fortsätta att tillämpa. Medlemsstaterna ska också inom tre månader efter det att de har undertecknat nya avtal eller överenskommelser enligt artikel 32.1

meddela kommissionen om detta. I avsnitten 11.5.1 och 12.11.2 behandlas underrättelser till kommissionen.

Artikel 33 reglerar frågor om utvärdering av EU-förordningen och riktar sig till kommissionen.

Artikel 34 innehåller bestämmelser om ikraftträdande och tillämpning. Av artikel 34.1 följer att EU-förordningen träder i kraft den 18 augusti 2023 och ska enligt artikel 34.2 tillämpas från och med den 18 augusti 2026. Skyldigheten för behöriga myndigheter och tjänsteleverantörer enligt artikel 19 att använda det decentraliserade it-systemet ska dock tillämpas med början ett år efter antagandet av de genomförandeakter som avses i artikel 25.

4 Nationella bestämmelser om inhämtning av elektronisk bevisning

4.1 Inledning

Som har behandlats i avsnitt 3 innehåller EU-förordningen bestämmelser om inhämtande av elektronisk bevisning. Elektroniska bevis är enligt EU-förordningen abonnentuppgifter, trafikuppgifter eller innehållsdata som lagras i elektronisk form av en tjänsteleverantör eller på en tjänsteleverantörs vägnar vid tidpunkten för mottagandet av en europeisk utlämnande- eller bevarandeorder.

I detta avsnitt behandlas de nationella bestämmelserna som omfattar utlämnande och bevarande av sådana elektroniska uppgifter som omfattas av EU-förordningens bestämmelser. Avsnittet utgör en bakgrund till våra överväganden och förslag i avsnitt 6–12.

Avsnittet inleds med en redogörelse för lagen (2022:482) om elektronisk kommunikation. Därefter behandlas de nationella bestämmelserna om bevisinhämtning i allmänhet, vilket följs av en redogörelse för regleringen som särskilt rör inhämtning av elektronisk bevisning. Slutligen finns en beskrivning av det internationella rättsliga samarbetet som rör bevisinhämtning.

4.2 Lagen om elektronisk kommunikation

4.2.1 Kort om lagens bakgrund och syfte

I december 2018 antogs Europaparlamentets och rådets direktiv (EU) 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation (direktiv 2018/1972). Direktivet trädde i kraft den 21 december 2018. Direktivet har genomförts genom lagen om

elektronisk kommunikation, som trädde i kraft i juni 2022 och ersatte den tidigare lagen med samma namn.

Lagen syftar till dels att enskilda och myndigheter ska få tillgång till säkra och effektiva elektroniska kommunikationer, dels största möjliga utbyte för alla elektroniska kommunikationstjänster sett till urvalet och till deras pris, kvalitet och kapacitet. Syftet ska uppnås främst genom att konkurrens, innovation, internationell harmonisering samt att säkerhet i nät och tjänster främjas. Samhällsomsfattande tjänster ska därutöver alltid finnas tillgängliga på för alla likvärdiga villkor i hela landet till överkomliga priser. Vid tillämpningen av lagen ska särskilt Sveriges säkerhet liksom elektroniska kommunikationers betydelse för yttrandefrihet och informationsfrihet beaktas (1 kap. 1 §).

Lagen gäller elektroniska kommunikationsnät och elektroniska kommunikationstjänster med tillhörande faciliteter och tjänster samt annan radioanvändning (1 kap. 2 §).

4.2.2 Allmänt om elektronisk kommunikation

Elektronisk kommunikation innebär överföring av signaler i elektronisk form. Elektronisk kommunikation omfattar telefoni, datakommunikation och utsändningar till allmänheten via radio eller tv. Den tekniska utvecklingen har medfört att dessa delar gradvis vuxit samman. Dessutom har de tjänster som används i kommunikationssyfte utvecklats på så sätt att traditionell taltelefoni, sms och e-posttjänster har ersatts med funktionsmässigt likvärdiga onlinetjänster, där överföring av signaler inte ingår i tjänsten.

Uppgifter om elektronisk kommunikation har i svensk rätt delats in i tre olika och delvis överlappande grupper, nämligen

- uppgifter om abonnemang,
- trafikuppgifter, och
- lokaliseringssuppgifter.

Det finns inte någon definition av begreppet *uppgift om abonnemang* varken i EU-rätten eller i svensk rätt. Regeringen har uttalat att uppgifter om abonnemang, som utgångspunkt, är uppgifter som identifierar abonnenten eller den registrerade användaren bakom

ett visst nummer eller en viss adress, i motsats till uppgifter som redogör för hur numret eller adressen har använts.¹ Med uppgifter om abonnemang avses främst uppgifter om abonnentens nummer, namn, titel och adress, men även uppgifter om exempelvis avtal och fakturering. Vidare innefattas uppgift om vem som använt en fast eller dynamisk ip-adress (ett nummer som används som adress på internet) eller ett IMSI-nummer (International Mobile Subscriber Identity, ett nummer som är kopplat till abonnentens sim-kort och telefonnummer).² Även IMEI-nummer (International Mobile Equipment Identity, ett nummer som är kopplat till själva kommunikationsenheten) kan vara uppgift om abonnemang. Post- och telestyrelsen (PTS) har inom ramen för sin tillsyn över bestämmelserna i lagen om elektronisk kommunikation bedömt att uppgifter om IMEI-nummer är att anse som uppgift om abonnemang, när det tydligt framgår av begäran att syftet är att identifiera ett abonnemang eller en abonnent.³

En *trafikuppgift* definieras i 1 kap. 7 § lagen om elektronisk kommunikation som en uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande. De trafikuppgifter som genereras vid elektronisk kommunikation kan ge information om t.ex. vilken typ av kommunikation som förekommit (telefoni, sms, etc.), vilken utrustning som använts, vilka nummer eller adresser som kommunicerat med varandra samt när och hur länge kommunikationen har pågått. Utanför begreppet trafikuppgifter faller information som avslöjar meddelandets innehåll.⁴

En *lokaliseringssuppgift* definieras i samma bestämmelse i lagen om elektronisk kommunikation som en uppgift som behandlas i ett allmänt mobilt elektroniskt kommunikationsnät och som anger den geografiska positionen för en slutanvändares terminalutrustning eller en uppgift i ett allmänt fast elektroniskt kommunikationsnät om nätanslutningspunktens fysiska adress. Det kan t.ex. vara fråga om vilken cell (antenn på basstation) som utrustningen kopplat upp sig mot, eller en gps-position.⁵

¹ Prop. 2018/19:86 s. 93. Jfr med prop. 2011/12:55 s. 101–102.

² Prop. 2018/19: 86 s.12 och 93 samt SOU 2023:22 s. 104 och 171.

³ PTS beslut den 17 mars 2021 i ärende dnr 20-3144.

⁴ SOU 2017:75 s. 100.

⁵ SOU 2017:75 s. 100.

Uppgifter om abonnemang anses typiskt sett vara mindre integritetskänsliga än trafik- och lokaliseringssuppgifter.

I 1 kap. 7 § lagen om elektronisk kommunikation finns andra definitioner som anger vilka tjänsteleverantörer som omfattas av lagens tillämpningsområde och direktivet 2018/1972. Det rör sig främst om vad som avses med begreppet *elektronisk kommunikationstjänst*. I avsnitt 6.2 redogörs ingående för dessa definitioner.

4.2.3 Säkerhet i nät och tjänster

Bestämmelser om säkerhet i nät och tjänster finns i 8 kap. 1–5 §§ lagen om elektronisk kommunikation. Här anges bl.a. att den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att på lämpligt sätt hantera risker som hotar säkerheten i nät och tjänster.

Av 8 kap. 5 § följer att den som är skyldig att lagra uppgifter enligt 9 kap. 19 § ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling. Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § och som har förelagts enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift ska avseende den uppgiften vidta samma åtgärder för att skydda uppgiften. Om lagringsskyldighet, se avsnitt 4.2.4. I avsnitt 4.4.1 behandlas föreläggande enligt 27 kap. 16 § rättegångsbalken.

Vidare finns bestämmelser om skydd av uppgifter vid tillhandahållande av tjänster i 8 kap. 6–9 §§ lagen om elektronisk kommunikation. Den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst ska bl.a. vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas.

4.2.4 Lagringsskyldighet

Uppgifter om elektronisk kommunikation är mycket viktiga för brottsbekämpningen. Det finns därför regler i lagen om elektronisk kommunikation som har till syfte att säkerställa att dessa uppgifter

lagras av tjänsteleverantörer som tillhandahåller elektroniska kommunikationstjänster och att de brottsbekämpande myndigheterna under vissa förutsättningar kan få tillgång till uppgifterna. Operatörerna är även skyldiga att bedriva sin verksamhet så att beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs (mer om dessa tvångsmedel, se avsnitten 4.3.2 och 4.4.3).

I 9 kap. 1–10 §§ lagen om elektronisk kommunikation finns regler om under vilka förutsättningar trafik- och lokaliseringssuppgifter får behandlas. Generellt gäller att trafikuppgifter, och däribland uppgifter som behandlas för att fakturera elektroniska meddelanden, ska utplånas eller avidentifieras så snart de inte längre behövs. En leverantör får dock lagra sådana uppgifter för vissa specifika ändamål. Så är fallet t.ex. för abonnentfakturerings- och – om den som uppgifterna gäller har samtyckt till det – för marknadsföring.

Den centrala bestämmelsen om lagringsskyldighet finns i 9 kap. 19 § lagen om elektronisk kommunikation. Lagringsskyldiga enligt den bestämmelsen är de som bedriver verksamhet som ska anmälas enligt 2 kap. 1 §. Allmänna elektroniska kommunikationsnät som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster är typiskt sett sådana verksamheter som får tillhandahållas endast efter anmälan till tillsynsmyndigheten. Någon skyldighet att anmäla verksamheten gäller dock inte för tillhandahållare av en nummeroberoende interpersonell kommunikationstjänst (Noik) eller för verksamhet som består enbart i överföring av signaler via tråd för utsändning till allmänheten av program som avses i 1 kap. 2 § yttrandefrihetsgrundlagen. Sådana aktörer omfattas alltså inte av lagringsskyldigheten (se dock avsnitt 4.2.6).

Lagringsskyldigheten omfattar enligt 9 kap. 19 § första stycket lagen om elektronisk kommunikation uppgift om abonnemang eller annan uppgift som angår ett särskilt elektroniskt meddelande som anges som nödvändiga för vissa preciserade syften. Dessa är formulerade som uppgifter som är nödvändiga för att spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut.

Skyldigheten att lagra uppgifter omfattar uppgifter som genereras eller behandlas i leverantörens verksamhet. Det innebär att leverantören inte har någon skyldighet att införskaffa uppgifter som inte genereras eller behandlas i verksamheten. Däremot ska en uppgift lagras så fort den har funnits hos leverantören, även om det bara rör sig om en ytterst kort tid.⁶

Uppgifter som har lagrats enligt 9 kap. 19 § får enligt 9 kap. 21 § behandlas endast för att lämnas ut för brottsbekämpande ändamål enligt 9 kap. 33 § första stycket 2 och 5, 27 kap. 19 § rättegångsbalken eller lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Lagringsskyldighetens längd regleras i 9 kap. 22 § lagen om elektronisk kommunikation och varierar från två månader upp till tio månader beroende på uppgiftsslag. Lagringstiden räknas från den dag kommunikationen avslutades. I 9 kap. 7 och 8 §§ förordningen (2022:511) om elektronisk kommunikation anges på en mer detaljerad nivå vilka uppgifter som ska lagras när det gäller telefonitjänst och meddelandehantering via mobil nätanslutningspunkt samt internetåtkomst.

När lagringstiden har löpt ut ska uppgifterna omedelbart utplånas enligt 9 kap. 22 § tredje stycket lagen om elektronisk kommunikation. Om däremot en begäran om utlämnande har kommit in eller ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken har meddelats innan lagringstiden löpt ut, ska den lagringsskyldige fortsätta att lagra uppgifterna till dess de har lämnats ut respektive när tiden för bevarande har löpt ut. Därefter ska uppgifterna genast utplånas.

4.2.5 Anpassningsskyldighet

Anpassningsskyldigheten innebär enligt 9 kap. 29 § lagen om elektronisk kommunikation att vissa verksamheter ska bedrivas så att beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation kan verkställas under sådana former att verkställandet inte röjs.

⁶ Prop. 2010/11 :46 s. 77.

Anpassningsskyldigheten gäller endast för verksamhet som innefattar tillhandahållande av

1. ett allmänt elektroniskt kommunikationsnät som inte enbart är avsett för utsändning till allmänheten av program som avses i 1 kap. 2 § yttrandefrihetsgrundlagen, eller
2. tjänster inom ett allmänt elektroniskt kommunikationsnät som består av
 - en allmänt tillgänglig telefonitjänst till en fast nätanslutningspunkt som medger överföring av lokala, nationella och internationella samtal, telefax och datakommunikation med en viss angiven lägsta datahastighet som medger funktionell tillgång till internet, eller
 - en allmänt tillgänglig elektronisk kommunikationstjänst till mobil nätanslutningspunkt.

Anpassningsskyldigheten innebär också enligt 9 kap. 29 b och 29 c §§ lagen om elektronisk kommunikation ett krav på skyndsamhet och format vid utlämnandet av uppgifter. Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § har enligt 9 kap. 29 a § rätt till ersättning för kostnader som uppstår när uppgifter lämnas ut till brottsbekämpande myndigheter. I de fall det är särskilt föreskrivet ska ersättningen beräknas enligt schablon. Ersättningen ska betalas av den myndighet som har begärt uppgifterna.

I sammanhanget kan nämnas att leverantörer av Noik inte omfattas av bestämmelserna om anpassningsskyldighet.⁷

4.2.6 Förslag om utökad lagringsskyldighet och moderniserad anpassningsskyldighet

I betänkandet *Datalagring och åtkomst till elektronisk information* (SOU 2023:22) har 2021 års datalagringsutredning lämnat flera förslag som är relevanta för vårt uppdrag bl.a. om utökad lagringsskyldighet vad gäller elektronisk kommunikation samt leverantörers anpassningsskyldighet. Betänkandet bereds i skrivande stund inom Regeringskansliet. Det kan noteras att regeringen den 22 november

⁷ Prop. 2021/22:136 s. 329.

2024 remitterat ett utkast till lagrådsremiss *Datalagring och tillgång till elektronisk kommunikation*. I utkastet föreslås bl.a. att tillhandahållare av Noik ska omfattas av regler om lagringsskyldighet och ska anpassa sin verksamhet så att hemliga tvångsmedel kan verkställas. Med hänsyn till tidpunkten för remittering har vi inte haft möjlighet att beakta utkastet till lagrådsremiss närmare än så i vårt betänkande.

Förslag avseende lagringsskyldigheten

I betänkandet föreslås regler som innebär dels att skyldigheten att lagra i sig utökas, dels att ytterligare tjänsteleverantörer ska omfattas av lagringsskyldigheten.

I betänkandet finns till att börja med förslag på två former av riktad lagring i syfte att bekämpa grov brottslighet: geografiskt riktad lagring och utökad riktad lagring.

Geografiskt riktad lagring ska ske i områden där det utifrån objektiva kriterier går att konstatera att det finns en jämförelsevis större sannolikhet för förekomst av grov brottslighet än i andra områden. *Utökad riktad lagring* ska komplettera den geografiskt riktade lagringen och kan avse ett begränsat geografiskt område där grov brottslighet har förekommit eller där det är sannolikt att grov brottslighet kommer att äga rum. Lagringen kan även avse en skyddsvärd plats, en person som dömts för grova brott, en person som har varit föremål för hemliga tvångsmedel, eller en utrustnings- eller abonnemangsidentitet som använts vid eller skäligen kan antas komma till användning vid ett grovt brott eller vid grov brottslig verksamhet.

I betänkandet föreslås även en *nationell säkerhetslagring* som ska användas om det bedöms vara absolut nödvändig för att bekämpa ett allvarligt hot mot nationell säkerhet som är verkligt och aktuellt eller förutsebart. De uppgifter som lagrats får endast användas för brott som rör allvarliga hot mot Sveriges säkerhet.

När det gäller tillhandahållare av Noik föreslås det i betänkandet att den lagringsskyldighet som i dag gäller enligt 9 kap. 19 § lagen om elektronisk kommunikation för andra tjänsteleverantörer även ska omfatta dessa tillhandahållare. Lagringsskyldigheten ska omfatta kommunikation som till någon del sker i Sverige.

Förslag avseende anpassningsskyldigheten

I betänkandet SOU 2023:22 konstateras att det är svårt att tydligt klargöra vilka verksamheter som omfattas av anpassningsskyldigheten samt att denna skyldighet och den nu gällande lagringsskyldigheten till vissa delar träffar olika verksamheter.

Det föreslås därför att anpassningsskyldigheten ska omfatta samma aktörer som enligt betänkandets förslag ska omfattas av lagringsskyldighet enligt lagen om elektronisk kommunikation. Den som bedriver verksamhet som ska anmälas enligt lagen om elektronisk kommunikation samt tillhandahållare av Noik ska enligt förslaget således vara skyldiga att bedriva sin verksamhet så att beslut om hemliga tvångsmedel kan verkställas och så att verkställandet inte röjs, även i de fall en tillhandahållare för sina kunder möjliggör totalsträckskryptering, dvs. när bara sändare och mottagare har tillgång till meddelandena i läsbar form.

Undantag görs för s.k. maskin-till-maskintjänster (tjänster som omfattar automatisk överföring av data mellan enheter eller mellan mjukvarubaserade tillämpningar, med liten eller ingen mänsklig medverkan).

4.3 Inhämtande av bevisning i en förundersökning

4.3.1 Allmänt om bevisinhämtning

De åtgärder som de brottsbekämpande myndigheterna kan vidta vid utredningen av brott regleras företrädesvis i 23–28 kap. rättegångsbalken.

Om det finns anledning att anta att ett brott som hör under allmänt åtal har begåtts ska enligt 23 kap. 1 § rättegångsbalken en förundersökning inledas. Syftet med förundersökningen är enligt 23 kap. 2 § att utreda vem som skäligen kan misstänkas för brottet och om tillräckliga skäl föreligger för åtal samt att bereda målet så att bevisningen kan förebringas i ett sammanhang vid en huvudförhandling i domstol.

Förundersökningen leds i huvudsak av åklagare, men kan även ledas av Polismyndigheten eller Säkerhetspolisen om saken är av enkel beskaffenhet och så länge någon inte skäligen kan misstänkas för brottet (23 kap. 3 §). Med stöd av särskild lagstiftning får även

Tullverket och Kustbevakningen leda förundersökningar beträffande vissa brott. I enlighet med Åklagarmyndighetens egna föreskrifter ska åklagare överta ledningen av förundersökningen om det kan bli aktuellt att begära bistånd i en annan stat (7 § 2 ÅFS 2005:9).

Under förundersökningen kan olika åtgärder vidtas för att inhämta sådant som senare kan komma att användas som bevis. Det kan t.ex. handla om att hålla förhör med någon som kan antas kunna lämna upplysningar av betydelse för utredningen (23 kap. 6 § rättegångsbalken) eller att inhämta yttrande från sakkunnig (23 kap. 14 §). Föremål och handlingar som kan få betydelse som bevisning kan också hämtas in med hjälp av olika tvångsåtgärder.

Av intresse för våra överväganden och förslag är bestämmelserna i 27 kap. rättegångsbalken om straffprocessuella tvångsmedel för inhämtande av bevisning och då särskilt reglerna om föreläggande om bevarande av lagrad uppgift samt hemlig avlyssning och hemlig övervakning av elektronisk kommunikation.

4.3.2 Särskilt om hemliga tvångsmedel

Tvångsmedelsanvändningen enligt rättegångsbalken förutsätter att det finns en konkret brottsmisstanke som är föremål för förundersökning. Hemliga tvångsmedel kan även används preventivt men då vi gör bedömningen att EU-förordningen inte omfattar underrättelseverksamhet berörs dessa regler inte närmare (se avsnitt 6.6).

Regleringen om de hemliga tvångsmedlen finns huvudsakligen i 27 kap. rättegångsbalken. Därutöver finns bestämmelser om hemlig dataavläsning i lagen (2020:62) om hemlig dataavläsning.

När hemliga tvångsmedel används känner inte den som är föremål för tvångsmedlet av naturliga skäl till åtgärden och kan därför inte överklaga ett beslut som fattas i frågan, eller på annat sätt bevaka sina intressen, i vart fall fram till dess åtal har väckts. Dessa förutsättningar medför att särskilda krav måste ställas på såväl beslutsordning som övriga rättssäkerhetsgarantier.

Flertalet av de hemliga tvångsmedlen prövas därför av en domstol efter ansökan av en åklagare (se t.ex. 27 kap. 9 och 21 §§ rättegångsbalken). Under vissa förutsättningar får en åklagare i brådsakande fall interimistiskt besluta om tillstånd till hemliga tvångsmedel (se t.ex. 27 kap. 9 a och 21 a §§ rättegångsbalken). Ett sådant

beslut ska utan dröjsmål anmälas till rätten som skyndsamt ska pröva ärendet.

När det gäller flertalet av de hemliga tvångsmedlen ska ett offentligt ombud utses för att bevaka enskildas intressen i ärenden i domstol. Endast den som är eller har varit advokat eller ordinarie domare kan förordnas som offentligt ombud. Domstolsprövningen sker i dessa fall efter ett sammanträde där åklagaren och det offentliga ombudet har varit närvarande (se t.ex. 27 kap. 26–30 §§ rättegångsbalken).

För att hemliga tvångsmedel ska få användas ställs det vidare upp vissa kvalifikationskrav som tar sikte på behovet av åtgärden i det enskilda fallet. I de fall en förundersökning pågår krävs att åtgärden är av synnerlig vikt för utredningen (se t.ex. 27 kap. 20 § rättegångsbalken).

Säkerhets- och integritetsskyddsnämnden utövar med stöd av lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel. Nämnden är även skyldig att på begäran av en enskild person kontrollera om han eller hon har varit utsatt för hemliga tvångsmedel och om denna användning har varit författningens enlig.

Förutom Säkerhets- och integritetsskyddsnämnden utövar både Riksdagens ombudsmän (JO) och Justitiekanslern tillsyn över de brottsbekämpande myndigheternas verksamhet och kan inom ramen för sin respektive tillsyn uttala sig i frågor om användningen av hemliga tvångsmedel.

Vidare redovisar regeringen årligen till riksdagen hur de hemliga tvångsmedlen, med undantag för kvarhållande av försändelse, har använts. Redovisningen innehåller information om antal ärenden och meddelade tillstånd, brottstyper samt bedömningar av den nytta som åtgärderna anses ha medfört.⁸

⁸ Se t.ex. regeringens skrivelse 2023/24:47 Redovisning av användningen av hemliga tvångsmedel under 2022.

4.3.3 Hemliga tvångsmedel och skyddet för den personliga integriteten

Användning av hemliga tvångsmedel innebär en risk för intrång i enskildas personliga integritet. I 2 kap. regeringsformen finns föreskrifter om grundläggande fri- och rättigheter. Föreskrifterna innebär bl.a. att var och en gentemot det allmänna är skyddad mot kroppsvisitation, husrannsakan och liknande intrång, mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande (6 § första stycket). Var och en är också skyddad gentemot det allmänna mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden (6 § andra stycket). Dessa grundläggande rättigheter får begränsas bara genom lag och endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna får aldrig gå utöver vad som är nödvändigt eller utgöra ett hot mot den fria åsiktsbildningen (20 och 21 §§).

Enligt artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Denna rätt omfattar bl.a. skydd mot övervakning i olika former. Offentliga myndigheter får inte inskränka dessa rättigheter annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt bl.a. med hänsyn till statens säkerhet och den allmänna säkerheten, till förebyggande av oordning och brott eller till skydd för andra personers fri- och rättigheter. Konventionen gäller som svensk lag, se lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna. Lag eller annan föreskrift får inte meddelas i strid med Sveriges åtaganden på grund av Europakonventionen (2 kap. 19 § regeringsformen). Artikel 8 i Europakonventionen ger inte bara upphov till förpliktelser för det allmänna att avhålla sig från omotiverade inskränkningar i enskildas rättigheter, utan även skyldigheter att se till att enskilda tillförsäkras skydd för sina rättigheter gentemot andra enskilda. Det innebär t.ex. att staten i vissa fall kan vara skyldig att införa straffrättslig reglering för att skydda enskilda mot intrång i

deras rättigheter från andra enskilda. Det innebär också att staten för sådana fall behöver säkerställa att brott kan utredas effektivt.

En bestämmelse om rätt till respekt för bl.a. privatliv finns också i artikel 7 i EU:s rättighetsstadga. Varje begränsning i utövandet av de fri- och rättigheter som erkänns i EU:s rättighetsstadga måste vara föreskriven i lag och förenlig med innehållet i dessa fri- och rättigheter. Begränsningar får, med beaktande av proportionalitetsprincipen, göras endast om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors fri- och rättigheter (artikel 52.1). I den mån stadgan omfattar rättigheter som motsvarar sådana som garanteras av Europakonventionen, ska de ha samma innebörd och räckvidd som enligt konventionen, eller ett mer långtgående skydd (artikel 52.3). Rättighetsstadgan riktar sig till medlemsstaterna när de tillämpar unionsrätten (artikel 51.1). Det innebär att rättigheterna i stadgan måste iaktas vid tillämpningen av nationell lagstiftning som genomför EU-rätt och nationell lagstiftning som omfattas av unionens tillämpningsområde (se bl.a. EU-domstolens dom i mål C-617/10, Åkerberg Fransson, punkt 21).

Vidare innehåller Förenta nationernas konvention om barnets rättigheter (barnkonventionen) bestämmelser om barns rätt till privatliv. Av artikel 16 följer att inget barn får utsättas för godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv. Vidare framgår av artikel 3 att vid alla åtgärder som rör barn ska i första hand beaktas vad som bedöms vara barnets bästa. I artikel 40 uppställs även vissa krav i fråga om barn som misstänks för brott. Sedan den 1 januari 2020 gäller barnkonventionen som svensk lag, se lagen (2018:1197) om Förenta nationernas konvention om barnets rättigheter. All lagstiftning som rör barn ska utformas i överensstämmelse med barnkonventionens bestämmelser.⁹

4.3.4 Principerna om ändamål, behov och proportionalitet vid tvångsmedelsanvändning

För all användning av tvångsmedel gäller tre allmänna principer. Dessa principer är ändamålsprincipen, behovsprincipen och proportionalitetsprincipen.

⁹ Prop. 2017/18:186 s. 94.

Enligt ändamålsprincipen får ett tvångsmedel användas endast för det ändamål som framgår av lagstiftningen. En ändamålsprövning bör ske före behovs- och proportionalitetsprövningen. Om tvångsmedlet inte ska användas för det ändamål det är till för, saknar det betydelse om det finns ett påtagligt behov och åtgärden framstår som proportionerlig. I reglerna om hemliga tvångsmedel anges dock inte uttryckligen för vilket specifikt ändamål tvångsmedlen får användas. Ändamålet får i stället sökas i de allmänna ändamålen med förundersökning.¹⁰

Behovsprincipen innebär att en myndighet får använda ett tvångsmedel bara när det finns ett påtagligt behov av det och en mindre ingripande åtgärd inte är tillräcklig. När det inte längre finns skäl för åtgärden ska den upphävas.

Proportionalitetsprincipen finns lagstadgad i t.ex. 27 kap. 1 § rättegångsbalken, men anses gälla vid all tvångsanvändning även utan lagstöd. Proportionalitetsprincipen innebär att ett tvångsmedel får tillgripas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller något annat motstående intresse. Härmed inbegrips, förutom direkta följder för den som utsätts för tvångsmedlet, även indirekta verkningar av tvångsmedelsanvändningen. Det kan t.ex. röra sig om intrång i tredje mans rättsligt skyddade intressen. Det ska alltid ske en prövning huruvida tvångsmedlet över huvud taget är påkallat med hänsyn till förhållandena i det enskilda fallet och om syftet kan tillgodoses genom någon mindre ingripande åtgärd. Utgångspunkten bör vara att pröva om alternativa spaningsåtgärder kan användas och om det kan räcka med att exempelvis tillgripa hemlig övervakning av elektronisk kommunikation i stället för hemlig avlyssning. Personlig frihet och integritet ska också beaktas. Ingrepp i dessa intressen är till sin art allvarligare än ingrepp mot egendom eller andra ekonomiska intressen.¹¹

¹⁰ Lindberg, *Straffprocessuella tvångsmedel* (2022, version 5, JUNO) s. 569 och SOU 2017:75 s. 90–92.

¹¹ SOU 1979:6 s. 294 och SOU 1984:54 s. 78.

4.4 Bevarande och inhämtning av elektronisk bevisning

4.4.1 Bevarande av lagrade elektroniska uppgifter

I 27 kap. 16 § rättegångsbalken finns bestämmelser som gör det möjligt för brottsutredande myndigheter att skyndsamt säkra och bevara lagrade elektroniska uppgifter som kan antas ha betydelse för utredningen om ett brott. Ett föreläggande enligt paragrafen är ett straffprocessuellt tvångsmedel.¹²

Av 27 kap. 16 § första stycket rättegångsbalken följer att den som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för utredningen om ett brott får föreläggas att bevara uppgiften.

De uppgifter som avses kan vara av vilket slag som helst, t.ex. en digitalt lagrad bild, innehållet i ett meddelande eller uppgifter om ett meddelandes ursprung och adressat. Att uppgiften ska vara lagrad innebär att den ska finnas bevarad elektroniskt. Både sådana uppgifter som finns lagrade på grund av regler om datalagring och sådana som lagrats av annan anledning omfattas, t.ex. uppgifter som hos tillhandahållare av elektroniska kommunikationsnät eller kommunikationstjänster behandlats för fakturahantering eller liknande. Uppgiften måste finnas lagrad när föreläggandet meddelas. Det är inte möjligt att med stöd av paragrafen förelägga någon att lagra eller spara eventuella framtida uppgifter.¹³

Syftet med ett föreläggande är att skydda uppgifterna från att raderas eller förändras på något sätt eller att göras oåtkomliga. Ett föreläggande innebär alltså en ”frysning” av uppgifterna i syfte att säkerställa att de förvaras på ett betryggande sätt fram till dess de eventuellt ska lämnas ut.¹⁴

Av bestämmelsens andra stycke följer att i föreläggandet ska det anges hur länge uppgiften ska bevaras. Tiden får inte bestämmas till längre än nödvändigt och får inte överstiga 90 dagar från dagen för beslutet. Om det finns särskilda skäl får enligt tredje stycket tiden för bevarande förlängas med högst 90 dagar.

Ett föreläggande om bevarande får enligt 27 kap. 16 a § första stycket rättegångsbalken beslutas av undersökningsledaren eller en

¹² Prop. 2020/21:72 s. 24.

¹³ Prop. 2020/21:72 s. 68.

¹⁴ Prop. 2020/21:72 s. 23–27.

åklagare. Den som har förelagts att bevara en uppgift kan begära rättens prövning av föreläggandet.

Ett bevarandeföreläggande innebär inte att uppgifterna ska lämnas ut till den som har utfärdat föreläggandet. Om föreläggandet har riktats mot en tillhandahållare av en elektronisk kommunikationstjänst eller ett elektroniskt kommunikationsnät får uppgifterna inhämtas med stöd av beslut om hemliga tvångsmedel eller ett beslut enligt lagen om elektronisk kommunikation.

4.4.2 Inhämtande av uppgifter om abonnemang

Tystnadsplikt

I 9 kap. 31 § lagen om elektronisk kommunikation föreskrivs att den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av eller tillgång till vissa närmare angivna uppgifter inte obehörigen får föra vidare eller utnyttja det han eller hon har fått del av eller tillgång till. Bestämmelsen omfattar inte tillhandahållare av Noik. Tystnadsplikten omfattar uppgift om abonnemang, innehållet i ett elektroniskt meddelande eller annan uppgift som angår ett särskilt elektroniskt meddelande.¹⁵ Dessutom föreskrivs i 9 kap. 32 § en tystnadsplikt som hänför sig till användning av vissa hemliga tvångsmedel, bl.a. för uppgift som hänför sig till en begäran om utlämnande av uppgifter för brottsbekämpande verksamhet enligt 9 kap. 33 § första stycket 2 och 5. Ett obehörigt röjande eller utnyttjande av sådana uppgifter i strid med aktuella bestämmelser är straffsanktionerat som brott mot tystnadsplikten enligt 20 kap. 3 § brottsbalken.

Om en fysisk person har samtyckt till att uppgifter om honom eller henne tas in i en allmänt tillgänglig abonnentförteckning omfattas uppgifterna, på grund av abonnentens samtycke, i praktiken inte av tystnadsplikten (9 kap. 17 och 18 §§ lagen om elektronisk kommunikation). Bestämmelserna om skyldighet att lämna ut uppgifter om abonnemang som redogörs för nedan får därför betydelse

¹⁵ Med detta begrepp avses bl.a. uppgift om mellan vilka abonnemang som ett telefonsamtal har förmedlats (prop. 1992/93:200 s. 162 f. och 310 och. prop. 2002/03:110 s. 269 och 397). 2021 års datalagringsutredning har bedömt att begreppet har samma innebörd som begreppet trafikuppgift i lagen om elektronisk kommunikation, och har därför föreslagit att begreppet trafikuppgift ska ersätta detta begrepp (se SOU 2023:22 s. 174–177).

i första hand i fråga om uppgifter som rör abonnenter som inte har lämnat sitt samtycke till att uppgifterna offentliggörs och när det gäller sådana uppgifter som normalt inte offentliggörs, såsom t.ex. ip-adresser.¹⁶

Allmänt om inhämtande av abonnemangsuppgifter

Eftersom inhämtning av abonnemangsuppgifter inte ses som ett hemligt tvångsmedel och ingreppet i privatlivet är begränsat i jämförelse med tillgång till trafik- och lokaliseringssuppgifter, finns det inte något krav på förhandskontroll av domstol eller annan oberoende myndighet, eller på underrättelse till de berörda. Det saknas vidare närmare regler om vem inom de brottsbekämpande myndigheterna som har rätt att hämta in abonnemangsuppgifterna och formen för hur uppgifterna ska hämtas in.

Inhämtande av abonnemangsuppgifter omfattar inte innehållet i meddelanden eller uppgifter som karaktäriseras som trafik- eller lokaliseringssuppgifter. Sådana uppgifter kräver tillstånd till hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation enligt regleringen i 27 kap. rättegångsbalken. Skyldigheten gäller inte heller sådana uppgifter som inte redan vid begäran finns hos den uppgiftsskyldige. Om myndigheten behöver tillgång till sådana uppgifter krävs tillstånd till sådan avlyssning eller övervakning i realtid enligt bestämmelserna i 27 kap. rättegångsbalken (se avsnitt 4.4.3).

Bestämmelserna om inhämtande av abonnemangsuppgifter omfattar inte tillhandahållare av Noik. I betänkandet *Datalagring och åtkomst till elektronisk information* (SOU 2023:22) har emellertid föreslagits att bl.a. tystnadsplikten i 9 kap. 31 § lagen om elektronisk kommunikation samt skyldigheterna att lämna ut uppgifter om abonnemang m.m. med stöd av 9 kap. 33 § samma lag ska gälla för samtliga tillhandahållare av elektroniska kommunikationsnät och elektroniska kommunikationstjänster, dvs. även för tillhandahållare av Noik.

¹⁶ Prop. 2018/19:86 s. 94.

Inhämtande av abonnemangsuppgifter i brottsbekämpande syfte

I 9 kap. 33 § lagen om elektronisk kommunikation regleras frågan om utlämnande av abonnemangsuppgifter till myndigheter, bl.a. i fråga om brottsbekämpande verksamhet. Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst ska enligt 9 kap. 33 § första stycket 2 på begäran lämna ut en uppgift om abonnemang som gäller brottslig verksamhet eller misstanke om brott till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brottet eller den brottsliga verksamheten. Regleringen innebär att de brottsbekämpande myndigheterna i princip har rätt att hämta in abonnemangsuppgifter för att beivra alla typer av brott utom sådana som åtalas enbart av målsäganden.¹⁷ Bestämmelsen är tillämplig både vid brottsutredningar och underrättelseverksamhet.¹⁸

Det krävs således inte att brottet är av en viss svårhetsgrad för att utlämnande av uppgifter om abonnemang ska kunna ske i brottsbekämpande syfte. När tillgångsbestämmelserna i 9 kap 33 § första stycket 2 lagen om elektronisk kommunikation utökades till att avse alla slags brott gjordes övervägandena bl.a. utifrån att trakasserier över internet och vuxnas kontakter med barn i sexuellt syfte blivit ett allt vanligare fenomen och att det integritetsintrång som ett utlämnande av abonnemangsuppgifter, vilket innefattade information om ip-adresser, ansågs inte väga upp mot den stora betydelse uppgifterna ofta kan ha för Polisens möjlighet att över huvud taget utreda brott som begås på internet.¹⁹

¹⁷ Se t.ex. SOU 2015:31 s. 198 f. och SOU 2017:75 s. 101. I avgörande RK 2018:1 konstaterade kammarrätten att det ingrepp i de grundläggande rättigheterna i artiklarna 7 och 8 i EU:s rättighetsstadga som bestämmelsen innebär inte är av allvarlig art. Något krav på att tillgången begränsas till utredning av allvarliga brott eller förhandskontroll av domstol eller en oberoende förvaltningsmyndighet kunde därför inte anses gälla. Bestämmelsen ansågs förenlig med artikel 15.1 i direktiv 2002/58/EG jämförd med artiklarna 7, 8 och 52.1 i EU:s rättighetsstadga.

¹⁸ Prop. 2021/22 :183 s. 61 och s. 76.

¹⁹ Prop. 2011/12:55 s. 102–103.

Inhämtande av abonnemangsuppgifter i syfte att lokalisera dömda

Bestämmelserna i 9 kap. 33 § första stycket lagen om elektronisk kommunikation omfattar även skyldigheter för leverantörerna att lämna ut uppgifter till vissa andra myndigheter och till regionala alarmeringscentraler i annat än brottsbekämpande syfte.

Sedan den 1 juli 2024 är tillhandahållare av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst enligt 9 kap. 33 § första stycket 1, skyldiga att på begäran lämna ut uppgifter om abonnemang till Polismyndigheten om myndigheten bedömer att uppgiften behövs i ett särskilt fall för att lokalisera en person som är dömd till fängelse, rättspsykiatrisk vård eller sluten ungdomsvård i syfte att möjliggöra verkställighet av påföljden (punkt i). Regeringen anförde i förarbetena till bestämmelsen att abonnemangsuppgifter ger de brottsutredande myndigheterna värdefulla pusselbitar i arbetet med att lokalisera eftersökta personer och bidrar till att arbetet blir mer effektivt.²⁰

Information om andra tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster

I 9 kap. 33 § första stycket 5 lagen om elektronisk kommunikation föreskrivs en skyldighet för den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, som inte är en Noik, att lämna ut uppgifter om vilka övriga tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster som har deltagit vid överföringen av ett meddelande som omfattas av ett föreläggande enligt 27 kap. 16 § rättegångsbalken (se avsnitt 4.4.1). Det är genom bestämmelsen möjligt att ta reda på från vilken tillhandahållare som meddelandet sändes och, för det fall det har vidare sänts, till vilken tillhandahållare det vidare sändes. Det ankommer på tillhandahållaren att ta fram de uppgifter som begärs. Om leverantören inte har någon uppgift om vilka de övriga aktörerna är kan någon information inte lämnas ut. Bestämmelsen innebär inte heller något krav på att spara eller lagra uppgifter.²¹

²⁰ Prop. 2023/24:108 s. 70.

²¹ Prop. 2020/21:72 s. 38.

4.4.3 Inhämtande av innehållsdata samt trafik- och lokaliseringssuppgifter

Hemlig avlyssning av elektronisk kommunikation

Allmänt om tvångsmedlet

Hemlig avlyssning av elektronisk kommunikation innebär att meddelanden, som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress, i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet (27 kap. 18 § första stycket rättegångsbalken).

Avlyssning kan således ske i realtid eller tas upp med ett tekniskt hjälpmedel för senare återgivning av meddelandet. Lagtekniskt görs ingen skillnad mellan direkt avlyssning och senare avlyssning. Avlyssningen får även avse meddelanden som tidigare har överförts, dvs. historiska uppgifter som finns kvar hos en operatör trots att meddelandena har överförts till mottagaren. Det är då som regel fråga om uppgifter som finns i en röstbrevlåda eller motsvarande funktion hos en operatör.²²

Avlyssningen kan omfatta alla former av kommunikation genom elektroniska kommunikationsnät, såväl muntlig som skriftlig, och avse t.ex. telefontrafik, e-posttrafik och överföring av datafiler. Avlyssning kan, med vissa begränsningar, ske även utanför allmänt tillgängliga telenät, t.ex. inom större företagsnät.²³

Enligt 27 kap. 21 b § rättegångsbalken får hemlig avlyssning av elektronisk kommunikation inte avse meddelanden som endast överförs eller har överförts i ett elektroniskt kommunikationsnät som med hänsyn till sin begränsade omfattning och omständigheterna i övrigt får anses vara av mindre betydelse från allmän kommunikationssynpunkt, t.ex. system för snabbtelefoner, porttelefoner och liknande utrustning inom eller intill en bostad samt hörselslingor för hörselskadade. Även interna kommunikationsnät på mindre arbetsplatser, via t.ex. pc-nät, utgör nät av mindre betydelse.²⁴

Ett tillstånd till hemlig avlyssning av elektronisk kommunikation ger enligt 27 kap. 18 § andra stycket rättegångsbalken också

²² Lindberg, Rättegångsbalk (1942:740) 27 kap. 16 §, Lexino (JUNO).

²³ Se t.ex. Ds 2020:12 s. 41 och SOU 2023:22 s. 120.

²⁴ Prop. 1994/95:227 s. 27 och 31.

rätt till att vidta sådana åtgärder som omfattas av regleringen om hemlig övervakning av elektronisk kommunikation (se vidare nedan).

I 27 kap. 22 § första stycket rättegångsbalken finns begränsningar vad den hemliga avlyssningen kan avse. Den får inte avse samtal eller tal där någon som yttrar sig är undantagen från vittnesplikt på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken. Det råder således ett absolut förbud mot att avlyssna dels samtal där en försvarare deltar vid utövandet av sitt uppdrag, dels samtal som avser bikt eller enskild själavård om en präst eller annan själasörjare deltar i samtalet. Därtill får avlyssning som huvudregel inte ske vid samtal med personer som tillhör vissa andra yrkeskategorier, om samtalet har samband med deras yrkesutövning. De yrkeskategorier som avses är bl.a. advokater, läkare, sjuksköterskor och psykologer. Vidare omfattas i vissa avseenden de som är verksamma inom andra verksamheter.²⁵

De brottsbekämpande myndigheternas tillgång till innehållet i ett särskilt elektroniskt meddelande som finns hos en teleoperatör som omfattas av anmälningsskyldigheten i lagen om elektronisk kommunikation regleras exklusivt av reglerna om hemlig avlyssning av elektronisk kommunikation. Husrannsakan och beslag eller editionsföreläggande får inte användas för att inhämta sådana uppgifter. När ett meddelande har nått fram till mottagaren är det däremot åtkomligt med stöd av reglerna om husrannsakan och beslag. Är t.ex. e-post lagrad i den misstänkes dator eller telefon kan den kommunikationsutrustning där meddelandet har lagrats tas i beslag.²⁶

Användning vid skäligen misstanke om brott

Hemlig avlyssning av elektronisk kommunikation får enligt 27 kap. 18 a § första stycket rättegångsbalken användas om någon är skäligen misstänkt för brott som avses i paragrafens andra stycke och åtgärden är av synnerlig vikt för utredningen. I det andra stycket anges 22 punkter för vilka brott hemlig avlyssning av elektronisk kommunikation får användas under förundersökningen.

Tvångsmedlet får som huvudregel användas vid förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fäng-

²⁵ Prop. 2013/14:237 s. 131–132.

²⁶ Prop. 2002/03:74 s. 45–46, SOU 2023:22 s. 116 och Lindberg, Straffprocessuella tvångsmedel (2022, version 5, JUNO), s. 600–601.

else i två år (punkt 1). I de övriga punkter anges brott som inte föreskriver ett minimistraff om fängelse i två år, men som ändå har ansetts vara så pass allvarliga att hemlig avlyssning ska kunna användas. Det rör sig om vissa brottsbalksbrott och brott enligt annan specialstraffrättslig lagstiftning. Ofta krävs det att det rör sig om ett grovt brott eller att brottet har visst straffvärde.

I uppräknningen inkluderas även försök, förberedelse eller stämpling beträffande vissa av de fullbordade brott som omfattas i uppräknningen eller andra brott om straffvärdet överstiger fängelse i två år. Slutligen anges i andra stycket att avlyssning kan ske om det rör sig om flera brott och det sammanlagda straffvärdet överstiger fängelse i två år samt att vissa andra förutsättningar är uppfyllda.

I 27 kap. 18 a § tredje stycket rättegångsbalken finns vissa ytterligare begränsningar. Avlyssningen får endast avse en adress eller en viss utrustning som innehas eller har innehafts av den misstänkte eller annars kan antas ha använts eller komma att användas av honom eller henne, t.ex. ett telefonnummer till den misstänktes sambo eller arbetsplats eller en viss mobiltelefon med ett visst identifikationsnummer.²⁷ Avlyssning får enligt samma bestämmelse också avse en adress eller utrustning som det finns synnerlig anledning att anta att den misstänkte har kontaktat eller kommer att kontakta. Möjligheten till avlyssning ska i dessa fall tillämpas restriktivt. Enligt förarbetena innebär det att det ska finnas tillförlitliga uppgifter som medför att man kan vara så gott som säker på att den misstänkte kommer att kontakta den uppgivna adressen.²⁸

Användning av tvångsmedlet för att utreda vem som skäligen kan misstänkas för brott

Av 27 kap. 18 b § första stycket rättegångsbalken följer att hemlig avlyssning av elektronisk kommunikation även får användas för att utreda vem som skäligen kan misstänkas för brott. Avlyssningen ska vidare vara av synnerlig vikt för utredningen. I det andra stycket anges 19 punkter för vilka brott som kan leda till hemlig avlyssning i dessa fall.

Systematiken är densamma som den i 27 kap. 18 a §, men med den skillnaden de brott som räknas upp i 27 kap. 18 b § är av all-

²⁷ Se t.ex. Ds 2007:2 s. 58 och prop. 2011/12:55 s. 129.

²⁸ Prop. 2002/03:74 s. 38 f och 49 och prop. 2022/23:126 s. 206.

varligare slag. Huvudregel enligt punkt 1 i det andra stycket är att avlyssning får användas för ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i fyra år. De brott som räknas upp i punkterna 2–15 motsvarar flera av de brott som räknas upp i 27 kap. 18 a § andra stycket, men med i vissa fall ett krav på att brottets straffvärde ska vara högre. I listan i 27 kap. 18 b § andra stycket har lagts till ytterligare brott som har ett minimistraff om fängelse i två år (men inte fyra år).

Även i denna uppräkninɡ inkluderas dels försök, förberedelse eller stämpling beträffande vissa av de fullbordade brott som omfattas av andra stycket eller andra brott om straffvärdet överstiger fängelse i fyra år, dels om det rör sig om flera brott och det sammanlagda straffvärdet överstiger fängelse i fyra år samt att vissa andra förutsättningar är uppfyllda.

I 27 kap. 18 b § tredje stycket rättegångsbalken föreskrivs, på samma sätt som i 27 kap. 18 a §, vissa begränsningar. Avlyssning får endast avse en adress eller viss utrustning som det finns särskild anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har använt eller kommer att använda. Det krävs förvisso inte att gärningsmannen är identifierad, men det ska dock inte enbart vara fråga om ett allmänt antagande om att gärningsmannen har använt eller kommer att använda adressen eller utrustningen, tvärtom krävs en faktisk omständighet som med viss styrka talar för att så är fallet. Ett exempel kan vara en utredning om människorov där det är känt att kidnapparna kontaktar målsägandens anhöriga från ett visst telefonnummer.²⁹ Avlyssning får också avse en adress eller viss utrustning om det finns synnerlig anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har kontaktat eller kommer att kontakta. Synnerliga skäl är för handen om det på grund av tillförlitliga uppgifter är så gott som säkert att gärningsmannen har kontaktat eller kommer att kontakta adressen eller utrustningen.³⁰

²⁹ Prop. 2022/23:126 s. 210.

³⁰ Prop. 2022/23:126 s. 211.

Hemlig övervakning av elektronisk kommunikation

De allmänna bestämmelserna om hemlig övervakning av elektronisk kommunikation finns i 27 kap. 19 § rättegångsbalken. Hemlig övervakning innebär enligt bestämmelsen att uppgifter i hemlighet hämtas in om samtal och skriftliga meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller en annan adress. Även uppgifter om vilka elektroniska kommunikationsutrustningar som finns eller har funnits inom ett visst geografiskt område (s.k. basstationstömning) kan hämtas in med stöd av hemlig övervakning. Tvångsmedlet kan även användas för att hindra meddelanden som överförs i ett elektroniskt kommunikationsnät från att nå fram. De uppgifter som kan hämtas in är trafik- och lokaliseringssuppgifter, med däremot inte innehållet i ett meddelande.

Hemlig övervakning får enligt 27 kap. 19 a § rättegångsbalken användas om någon är skäligen misstänkt för brott som avses i bestämmelsens andra stycke och åtgärden är av synnerlig vikt för utredningen. Den systematik som föreskrivs för hemlig avlyssning av elektronisk kommunikation om vilka brott som omfattas gäller även för hemlig övervakning elektronisk kommunikation, med den skillnaden att det för hemlig övervakning rör mindre allvarligare brott. Huvudregeln är enligt bestämmelsens andra stycke att hemlig övervakning får användas vid en förundersökning om det rör ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader. Därutöver får övervakning användas för brott som räknas upp i bestämmelsen. Det ska framhållas att hemlig övervakning får användas vid brott som kan leda till hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 18 a § andra stycket.

I 27 kap. 19 a § tredje stycket begränsas vilka telefonnummer eller en annan adress eller viss elektronisk kommunikationsutrustning en hemlig övervakning får avse. Bestämmelsen har samma lydelse som den i 27 kap. 18 a § tredje stycket (se ovan).

I likhet med hemlig avlyssning av elektronisk kommunikation får inte hemlig övervakning av elektronisk kommunikation avse meddelande som överförs eller har överförts i ett elektroniskt kommunikationsnät som med hänsyn till sin begränsade omfattning och omständigheterna i övrigt får anses vara av mindre betydelse från allmän kommunikationssynpunkt (27 kap. 21 b §).

Hemlig övervakning av elektronisk kommunikation får även enligt 27 kap. 19 b § första stycket rättegångsbalken användas i syfte att utreda vem som skäligen kan misstänkas för brott som avses i andra stycket, om åtgärden är av synnerlig vikt för utredningen. Övervakning får enligt andra stycket användas vid en förundersökning som avser brott som anges 27 kap. 18 a § andra stycket 1–21 eller vid förundersökning om flera brott flera brott och det sammanlagda straffvärdet överstiger fängelse i två år samt att vissa andra förutsättningar är uppfyllda.

I likhet med vad som är fallet beträffande hemlig avlyssning av elektronisk kommunikation är det inte möjligt att använda husrannsakan och beslag eller editionsföreläggande som substitut för hemlig övervakning av elektronisk kommunikation. Det finns dock inte något hinder mot att tvångsmedlen används för att få fram övervakningsuppgifter som finns hos den misstänkte eller någon annan (t.ex. specificerade uppgifter om telefonsamtal på en räkning), om förutsättningarna i övrigt för att använda tvångsmedlen är uppfyllda.³¹

Hemlig dataavläsning

I lagen (2020:62) om hemlig dataavläsning finns bestämmelser om det relativt nya tvångsmedlet hemlig dataavläsning. Hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling, i hemlighet och med ett tekniskt hjälpmedel läses av eller tas upp i ett avläsningsbart informationssystem (1 §).

Hemlig dataavläsning är ett självständigt tvångsmedel men kan även användas som ett komplement för att kunna genomföra andra hemliga tvångsmedel som hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation.

I 2 § första stycket anges i sju punkter vilka typer av uppgifter som får läsas av eller tas upp efter ett tillstånd om hemlig dataavläsning. Uppräkningen är uttömmande. Det rör sig bl.a. om kommunikationsavlyssningsuppgifter, kommunikationsövervakningsuppgifter och platsuppgifter.

³¹ Prop. 2002/03:74 s 45–46 och Lindberg, *Straffprocessuella tvångsmedel* (2022, version 5 JUNO), s. 617.

Det som skiljer hemlig dataavläsning från andra hemliga tvångsmedel är hur verkställigheten sker. Verkställighet av traditionella hemliga tvångsmedel sker genom inhämtning av uppgifter från operatörer alternativt genom kamera- eller avlyssningsutrustning som tillhör de brottsbekämpande myndigheterna. Vid verkställighet av hemlig dataavläsning hämtas uppgifterna i stället in från den berördes egna kommunikationsutrustning, t.ex. en dator eller en mobiltelefon.³²

Metoden för hemlig dataavläsning kan sägas innebära två delar, dels att den brottsbekämpande myndigheten bereder sig tillgång till teknisk utrustning som kan användas för kommunikation, dels att myndigheten tar del av uppgifter som finns i utrustningen. De uppgifter som hemlig dataavläsning är tänkta att komma åt finns alltså i den tekniska utrustningen, t.ex. i en mobiltelefon eller en dator. Det skiljer sig således från vad som är fallet vid hemlig avlyssning eller övervakning av elektronisk kommunikation, där uppgifterna hämtas in på väg till eller från någons tekniska utrustning.³³

Med stöd av tvångsmedlet kan myndigheterna i hemlighet installera mjuk- eller hårdvara i en teknisk utrustning (t.ex. en dator eller mobiltelefon) och med hjälp av mjuk- eller hårdvaran läsa av uppgifter som finns i utrustningen. Det kan t.ex. handla om att installera ett program för att läsa av meddelanden och avlyssna samtal i krypterade program och appar eller skaffa sig tillgång till ett konto i sociala medier. Myndigheterna kan också med tillgång till inloggningsuppgifter logga in från sina egna datorer på ett användarkonto för att t.ex. ta del av e-postmeddelanden. Om hårdvara behöver installeras i t.ex. någons dator, kan myndigheterna få tillstånd att i hemlighet ta sig in i utrymmet där utrustningen finns för att installera hårdvaran.³⁴

I lagen om hemlig dataavläsning ställs krav på att det ska vara fråga om viss allvarlig brottslighet. Enligt 4 § kan alla de brott som kan leda till hemlig avlyssning av elektronisk kommunikation också leda till hemlig dataavläsning. Detta gäller med undantag för hemlig dataavläsning som avser rumsavlyssningsuppgifter. Åtgärden får i detta avseende endast enligt 6 § tillåtas vid förundersökning om sådana brott som kan föranleda hemlig rumsavlyssning.

³² SOU 2023:78 s. 62.

³³ Prop. 2019/20:64 s. 55.

³⁴ SOU 2023:22 s. 126–127.

Frågor om hemlig dataavläsning prövas av domstol.

Lagen om hemlig dataavläsning är tidsbegränsad och upphör att gälla vid utgången av mars 2025. I en lagrådsremiss av den 10 oktober 2024 föreslås att hemlig dataavläsning ska införas som ett permanent tvångsmedel. Vidare föreslås bl.a. att tvångsmedlet ska få användas i fler fall i syfte att utreda vem som skäligen kan misstänkas för ett brott samt att reglerna för vilka typer av uppgifter som får hämtas in och för utformningen av ett tillstånd till hemlig dataavläsning ska förtydligas.

Genomsökning på distans

Bestämmelserna om genomsökning på distans finns i 28 kap. 10 a–10 i §§ rättegångsbalken. Tvångsmedlet innebär en möjlighet för de brottsbekämpande myndigheterna att söka efter handlingar som finns lagrade i ett avläsningsbart informationssystem utanför den elektroniska kommunikationsutrustning som används för att utföra genomsökningen (28 kap. 10 a §). Med avläsningsbart informationssystem menas både en fysisk elektronisk kommunikationsutrustning och andra mer immateriella tjänster, såsom kommunikationstjänster och lagringstjänster. Genomsökning på distans ska inte användas för att identifiera och hämta in lokalt lagrade uppgifter eftersom det är tillåtet att leta efter lokalt lagrade uppgifter i en elektronisk kommunikationsutrustning som tagits i beslag eller påträffats vid en husrannsakan. Det som kan bli föremål för genomsökning på distans är de handlingar som finns lagrade på andra platser än t.ex. i den enskilda mobiltelefonen, såsom i internetbaserade kommunikations- eller lagringstjänster.³⁵

Genomsökning på distans får ske endast i syfte att söka efter handlingar som kan ha betydelse för utredning av brott eller om förverkande av utbyte av brottslig verksamhet enligt 36 kap. 1 b § brottsbalken. För att genomsökning på distans ska få utföras krävs att det finns anledning att anta att brott har begåtts på vilket fängelse kan följa. Vidare krävs att det informationssystem som genomsökningen ska utföras i kan ha använts av den som skäligen kan misstänkas för brottet eller, i annat fall, om det finns synnerlig anledning att anta att det går att påträffa handlingar som kan vara av

³⁵ Prop. 2021/22:119 s. 77.

betydelse för utredning av brottet eller om förverkande av utbyte av brottslig verksamhet.

Till skillnad mot hemlig dataavläsning får genomsökningen endast utföras genom autentisering i det informationssystem som åtgärden avser (28 kap. 10 b § rättegångsbalken).

Om det finns anledning att anta att någon har möjlighet att öppna informationssystemet genom biometrisk autentisering, är han eller hon skyldig att på tillsägelse av en polisman medverka till detta under förutsättning att genomsökningen annars försvåras. Vid vägran att medverka vid sådan autentisering får en polisman genomföra autentiseringen (27 kap. 17 f § rättegångsbalken). Vad som nu sagts gäller även för tjänstemän vid Tullverket eller Kustbevakningen i fråga om vissa brott, se 26 och 29 a §§ lagen (2000:1225) om straff för smuggling.

Genomsökning på distans beslutas av undersökningsledaren, åklagaren eller rätten. En polisman får vidta åtgärden utan ett sådant beslut om det är fara i dröjsmål och genomsökningen inte kan antas bli av stor omfattning eller medföra synnerlig olägenhet för den som drabbas av åtgärden (28 kap. 10 d § rättegångsbalken). Genomsökning på distans får beslutas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller något annat motstående intresse (28 kap. 10 i §).

4.4.4 Användning av straffprocessuella tvångsmedel i syfte att verkställa frihetsberövanden

Den 1 juli 2024 trädde lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder i kraft. Lagen gör det möjligt att använda vissa hemliga tvångsmedel i syfte att lokalisera personer för att se till att en frihetsberövande påföljd kan verkställas. De hemliga tvångsmedel som är tillgängliga är hemlig övervakning av elektronisk kommunikation samt hemlig dataavläsning som gäller kommunikationsövervaknings- och platsuppgifter.

Ett tillstånd till nämnda tvångsmedel får meddelas om åtgärden är av synnerlig vikt för att kunna lokalisera en person som är dömd till fängelse, rättspsykiatrisk vård eller slutna ungdomsvård och om åtgärden sker i syfte att möjliggöra verkställighet av påföljden. Tillståndet får endast meddelas om den dom som ska verkställas omfattar brott som avses i 27 kap. 19 a § andra stycket rättegångsbalken re-

spektive 4 § lagen om hemlig dataavläsning, dvs. brott som kan motivera att åtgärden vidtas under en förundersökning, eller om domen avser rättspsykiatrisk vård med särskild utskrivningsprövning (3 och 4 §§ lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder). Kravet på synnerlig vikt innebär att andra möjligheter att lokalisera den eftersökte har uttömts eller att sådana åtgärder skulle vara utsiktslösa eller medföra en orimligt stor arbetsinsats. Det måste också finnas skäl att räkna med att tvångsmedlet – ensam eller tillsammans med andra åtgärder – verkligen kan leda till att den eftersökte anträffas.³⁶

Frågor om tillstånd enligt 3 eller 4 § nämnda lag prövas som huvudregel av den tingsrätt som har meddelat den dom som ska verkställas. Om domen har meddelats av högre rätt prövas frågan av den tingsrätt som har dömt i målet. Frågan tas upp på ansökan av åklagaren (5 § första stycket). Om det är fara i dröjsmål, får tillstånd meddelas av åklagaren i avvaktan på rättens beslut (6 § första och andra stycket).

Enligt 7 § aktuell lag ska rättegångsbalkens regler om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut tillämpas om inte något annat anges i förstnämnda lag. Enligt 8 och 9 §§ ska vissa bestämmelser som gäller vid hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt rättegångsbalken respektive lagen om hemlig dataavläsning även tillämpas när dessa tvångsmedel används för att göra det möjligt att verkställa en frihetsberövande påföljd.

Den som har varit utsatt för en åtgärd enligt lagen ska enligt 12 och 13 §§ som huvudregel underrättas om åtgärden så snart det kan ske efter det att det ärende som åtgärden vidtogs i avslutades. Om åtgärden har avsett ett telefonnummer eller en annan adress, en viss elektronisk kommunikationsutrustning eller ett avläsningsbart informationssystem som innehas av någon annan än den eftersökte, ska även han eller hon underrättas. En underrättelse ska innehålla uppgifter om vilket tvångsmedel som har använts och om tiden för åtgärden.

Nämnda hemliga tvångsmedel kan också användas i syfte att lokalisera en person som är anhållen eller häktad för ett brott (27 kap. 19 c § rättegångsbalken respektive 6 b § lagen om hemlig dataavläsning).

³⁶ Prop. 2023/24:108 s. 51.

4.5 Internationellt straffrättsligt samarbete

Svenska brottsbekämpande myndigheter saknar jurisdiktion för att verkställa beslut om utredningsåtgärder i en annan stat. I stället får de begära hjälp från den aktuella staten för att få åtgärden utförd.

Straffrättsligt samarbete innebär att stater bistår varandra med åtgärder för att kunna utreda brott och lagföra den som är misstänkt. Samarbetet avser även verkställighet av domar och slutliga beslut.

Samarbetet baserar sig i huvudsak på internationella överenskommelser genom vilka staterna åtar sig att bistå varandra inom ramen för den specifika överenskommelsens tillämpningsområde. Dessa överenskommelser har Sverige i huvudsak tillträtt och genomfört genom olika lagar.

När det gäller samarbetet mellan EU:s medlemsstater har särskilda rättsakter antagits som avser att utveckla och effektivisera det straffrättsliga samarbetet.

En viktig del av samarbetet rör bevisinhämtning under pågående brottsutredningar, t.ex. förhör under förundersökning, husrannsakan och beslag eller användande av hemliga tvångsmedel. Nedan redogörs översiktligt för dels lagen (2000:562) om internationell rättslig hjälp i brottmål, dels lagen (2017:1000) om en europeisk utredningsorder som tillsammans utgör de centrala regelverken när det gäller gränsöverskridande bevisinhämtning under en pågående förundersökning eller rättegång i brottmål. Slutligen redovisas kortfattat innehållet i lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar, som reglerar vissa samarbetsformer som används inom ramen för internationell rättslig hjälp, men även i det internationella polissamarbetet.

4.5.1 Lagen om internationell rättslig hjälp i brottmål

Lagen om internationell rättslig hjälp i brottmål reglerar rättslig hjälp som svenska åklagare och domstolar kan begära utomlands eller lämna på utländsk begäran. Den gäller i förhållande till samtliga stater, utom EU:s medlemsstater. I förhållande till sistnämnda stater (utom Danmark och Irland) tillämpas lagen om en europeisk utredningsorder.

Lagen om internationell rättslig hjälp i brottmål är tillämplig oavsett om Sverige har ett avtal om rättslig hjälp i brottmål med den andra staten eller inte.

Rättslig hjälp enligt lagen omfattar enligt 1 kap. 2 § första stycket samtliga de åtgärder som är möjliga att vidta i en inhemsk förundersökning eller rättegång i Sverige, bl.a. förhör under förundersökning och husrannsakan och beslag samt andra åtgärder som avses i 28 kap. rättegångsbalken. Vidare omfattar lagen föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken samt de hemliga tvångsmedel som regleras i 27 kap. rättegångsbalken och lagen om hemlig dataavläsning. Uppräkningen av vilka åtgärder som avses med rättslig hjälp är uttömmande.³⁷ Lagen om internationell rättslig hjälp i brottmål hindrar dock inte att hjälp lämnas med annan åtgärd än sådan som anges i första stycket om det kan ske utan tvångsmedel eller annan tvångsåtgärd (1 kap. 2 § andra stycket).

Rättslig hjälp lämnas i första hand av åklagare eller domstol (1 kap. 4 §) med vissa undantag.

I lagens andra kapitel finns allmänna bestämmelser om rättslig hjälp i Sverige. En utgångspunkt är att rättslig hjälp i Sverige lämnas under de förutsättningar som gäller för motsvarande åtgärd i en svensk förundersökning eller rättegång enligt rättegångsbalken eller annan lag eller författning (2 kap. 1 §). När det gäller hemliga tvångsmedel ställs därutöver upp ett krav på dubbel straffbarhet, dvs. att den gärning som biståndet avser även ska vara en straffbar gärning i Sverige (2 kap. 2 §).

Bestämmelserna i 2 kap. 3–13 §§ innehåller föreskrifter om bl.a. hur en framställning om internationell rättslig hjälp som inges i Sverige ska utformas, ansökningsförfarandet och rätten till juridiskt biträde.

I 2 kap. 14 § stadgas om hinder mot att lämna rättslig hjälp. Det är här fråga framför allt om hänsyn till svenska rättsprinciper eller andra väsentliga intressen. En ansökan ska enligt bestämmelsens första stycke avslås om ett bifall till ansökan skulle kränka Sveriges suveränitet, medföra fara för rikets säkerhet eller strida mot svenska allmänna rättsprinciper eller andra väsentliga intressen. Ansökan får vidare avslås bl.a. om gärningen har karaktär av ett politiskt eller militärt brott, eller omständigheterna annars är sådana att ansökan inte bör bifallas (andra stycket). Om åklagaren eller domstolen

³⁷ Prop. 1999/2000:61 s. 188.

finner att ansökan bör avslås på någon av de nu angivna grunderna ska ansökan överlämnas till regeringen som beslutar i frågan (2 kap. 15 § första stycket). Övriga förutsättningar prövas av den handläggande myndigheten, t.ex. om kravet på dubbel straffbarhet är uppfyllt (2 kap. 15 § andra stycket).

I 3 kap. i lagen finns allmänna bestämmelser om rättslig hjälp utomlands. De formella kraven för rättslig hjälp utomlands är generellt lägre än vad som gäller för rättsligt bistånd i Sverige. Skälet för detta är att möjligheterna till svenskt bistånd utomlands styrs av lagstiftningen i det aktuella landet och vilka internationella åtaganden som landet gjort i förhållande till Sverige.³⁸

Särskilda bestämmelser om olika former av rättslig hjälp finns i 4 kap. I dessa anges närmare om vad t.ex. en ansökan ska innehålla avseende en viss typ av åtgärd, vem som prövar om åtgärden ska bifallas, närmare om förutsättningarna för att vidta åtgärden och om hur åtgärden verkställs.

I nämnda kapitel finns också ett flertal bestämmelser som i huvudsak endast ska tillämpas gentemot EU:s medlemsstater samt Island och Norge. Bestämmelserna infördes främst mot bakgrund av Sveriges genomförande av Europeiska unionens konvention om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater från 2000 (SÖ 2005:42). Det gäller bl.a. användning av vissa hemliga tvångsmedel. Mot bakgrund av lagen om en europeisk utredningsorder torde flertalet av dessa bestämmelser inte längre tillämpas gentemot medlemsstaterna förutom Danmark och Irland som inte deltar i samarbetet om en europeisk utredningsorder. Särregleringen rör i huvudsak hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation i realtid och berörs inte närmare.

I 5 kap. 1–4 §§ finns bestämmelser om användningsbegränsningar, dvs. hur inhämtad bevisning får användas för andra syften än vad som avsågs med ansökan. Det kan bl.a. röra sig om villkor som gäller om hur avlyssnat eller övervakat material får användas efter det att materialet har överlämnats till den ansökande staten.³⁹ I 5 kap. finns därutöver regler om bl.a. immunitet, sekretess, uppgiftsskyldighet, delning av förverkad egendom och återkrav av kostnader.

³⁸ Se t.ex. prop. 1999/2000:61 s. 82.

³⁹ Prop. 1999/2000:61 s. 147.

4.5.2 Lagen om en europeisk utredningsorder

Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området ersätter i allt väsentligt samarbetet mellan EU:s medlemsstater som tidigare skedde enligt bestämmelserna om internationell rättslig hjälp i brottmål. Direktivet har genomförts i huvudsak genom lagen om en europeisk utredningsorder. Lagen gäller i förhållande till alla EU-medlemsstater utom Danmark och Irland (1 kap. 2 §). Gentemot dessa två stater tillämpas lagen om internationell rättslig hjälp i brottmål.

I 1 kap. 3 § definieras vad som avses med en europeisk utredningsorder. I korthet kan sägas att en europeisk utredningsorder ska avse bevisinhämtning i en annan stat och ska ha utfärdats av en domare, domstol, undersökningsdomare eller allmän åklagare i ett straffrättsligt förfarande. Andra myndigheter kan under vissa förutsättningar utfärda en sådan order. Vidare kan en order utfärdas i vissa andra förfaranden.

I 1 kap. 4 § anges vad en utredningsåtgärd enligt lagen ska avse eller motsvara. Sammanfattningsvis kan sägas att det rör sig om samma åtgärder som är möjliga att ansöka om i Sverige eller utomlands enligt lagen om internationell rättslig hjälp i brottmål, t.ex. förhör under förundersökning, husrannsakan och beslag samt hemliga tvångsmedel.

En europeisk utredningsorder får enligt 2 kap. 1 och 3–4 §§ utfärdas i Sverige av åklagare om de förutsättningar som gäller för att vidta utredningsåtgärden under en svensk förundersökning är uppfyllda och åtgärden är proportionerlig. Dessutom krävs, när det är fråga om hemliga tvångsmedel, enligt 2 kap. 5 § att domstol har lämnat tillstånd att utfärda ordern. I avvaktan på domstolens beslut får åklagaren under vissa förutsättningar fatta interimistiskt beslut.

När det gäller erkännande och verkställighet i Sverige av en europeisk utredningsorder gäller enligt 3 kap. 1 § att en utredningsorder som sänds över från en annan medlemsstat ska erkännas och verkställas i Sverige om vissa särskilda förutsättningar enligt lagen är uppfyllda och inte annat följer av lagen. För hemliga tvångsmedel ställs i 3 kap. 4 § som en särskild förutsättning upp att en utredningsorder får erkännas och verkställas endast om den gärning som avses i utredningsordern motsvarar ett brott enligt svensk lag och

om övriga förutsättningar som gäller för en motsvarande åtgärd i en svensk förundersökning är uppfyllda.

Enligt de obligatoriska vägransgrunderna i 3 kap. 5 § får en order inte erkännas och verkställas bl.a. om det skulle medföra fara för Sveriges säkerhet, äventyra enskilda personers säkerhet eller medföra risk för röjande av uppgifter som rör underrättelseverksamhet. Även att utredningsåtgärden inte motsvarar en åtgärd som anges i 1 kap. 4 § utgör en obligatorisk vägransgrund, dock inte om en annan utredningsåtgärd kan vidtas som ger motsvarande resultat som den åtgärd som utredningsordern avser.

I 3 kap. 6 och 7 §§ finns några fakultativa vägransgrunder. Av 6 § följer att en verkställighet av en utredningsorder får vägras om det för samma gärning som avses i utredningsordern har meddelats dom i Sverige eller i en annan stat och domen har fått laga kraft samt. Enligt 7 § får en verkställighet av en order vägras för vissa i paragrafen angivna utredningsåtgärder, däribland föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken, bl.a. om den gärning som avses i utredningsordern inte motsvarar ett brott enligt svensk lag och det inte är fråga om en sådan gärning som finns angiven i bilagan till lagen och för vilken det i den andra medlemsstatens lagstiftning är föreskrivet en frihetsberövande påföljd i tre år eller mer.

En utredningsorder avseende bevisinhämtning under en pågående brottsutredning handläggs i huvudsak av åklagaren. Beträffande hemliga tvångsmedel ska dock domstol pröva om utredningsordern ska erkännas och verkställas (3 kap. 8 och 9 §§ lagen om en europeisk utredningsorder). Åklagaren har viss möjlighet att fatta interimistiska beslut om erkännande och verkställighet (3 kap. 10 §). Om utredningsordern kan erkännas och verkställas i Sverige, ska beslut meddelas om att verkställighet ska äga rum, en s.k. verkställbarhetsförklaring (3 kap. 19 §).

För verkställigheten av en utredningsorder ska samma bestämmelser som gäller vid verkställighet av en motsvarande åtgärd i ett inhemskt förfarande tillämpas. För hemliga tvångsmedel finns särskilda bestämmelser i 3 kap. 34–37 §§.

I 4 kap. finns bestämmelser om bl.a. användningsbegränsningar.

4.5.3 Lagen om vissa former av internationellt samarbete i brottsutredningar

I lagen regleras vissa former av samarbete som används inom ramen för internationell rättslig hjälp och i det internationella polissamarbetet. De samarbetsformer som regleras i lagen är gemensamma utredningsgrupper, kontrollerade leveranser och brottsutredningar med användning av skyddsidentitet. Lagen gäller inte om lagen om en europeisk utredningsorder är tillämplig.

Syftet med att inrätta en gemensam utredningsgrupp är att samordna och effektivisera en eller flera brottsutredningar som har kopplingar till flera stater.

En gemensam utredningsgrupp inrättas för ett särskilt syfte, dvs. utredning av viss konkret brottslighet, och för en begränsad tid (2 §). Om en förundersökning pågår i Sverige avseende den brottslighet som den gemensamma utredningsgruppen ska utreda är det åklagaren eller den myndighet som leder förundersökningen som kommer överens med de andra staterna om att inrätta gruppen (3 § första stycket). I övriga fall får sådana överenskommelser ingås av Åklagarmyndigheten, Polismyndigheten, Tullverket eller Kustbevakningen. I lagen finns bestämmelser om vilka förutsättningar som gäller för de utredningsåtgärder som kan behöva vidtas i Sverige (4 §). I 5 § finns bestämmelser om användningsbegränsningar.

En kontrollerad leverans innebär i huvudsak att de brottsutredande myndigheterna avvaktar eller underlåter att ingripa mot en leverans av exempelvis narkotika i syfte att under övervakning följa leveransen och avslöja mottagaren för att bättre kunna kartlägga vem eller vilka som ligger bakom brottsligheten. I lagen regleras de fall då leveransen sker in på eller ut från svenskt territorium. En ansökan om biträde med en kontrollerad leverans i Sverige handläggs av åklagare (10 §). En ansökan om att en kontrollerad leverans ska genomföras utomlands får göras av åklagare eller, sedan åklagare har lämnat sitt tillstånd till åtgärden, av Polismyndigheten, Tullverket eller Kustbevakningen (11 §).

Brottsutredning med användning av skyddsidentitet innebär att tjänstemän med skyddsidentitet tillåts att i en konkret brottsutredning verka i den stat som lämnar tillstånd till ett sådant samarbete. De närmare villkoren för hur ett sådant samarbete ska ske bestäms av den nationella lagstiftningen i den stat i vilken utred-

ningen avser att äga rum. Om en förundersökning pågår i Sverige avseende den brottslighet som åtgärden avser är det åklagaren eller den myndighet som leder förundersökningen som kommer överens med de andra staterna om sådant bistånd. I övriga fall får sådana överenskommelser ingås av Åklagarmyndigheten eller Polismyndigheten (15 §).

5 Allmänna överväganden

5.1 Inledning

Vi har i uppdrag att se över regleringen om gränsöverskridande åtkomst till elektroniska bevis med anledning av nya internationella instrument; EU-förordningen, EU-direktivet och det andra tilläggsprotokollet till Budapestkonventionen. I detta avsnitt redogör vi för vissa allmänna utgångspunkter i våra överväganden.

5.2 Allmänna utgångspunkter för våra överväganden

EU-förordningar och förhållandet till nationell rätt

EU-förordningar har allmän giltighet och är till alla delar bindande och direkt tillämpliga i varje medlemsstat (artikel 288 Fördraget om Europeiska unionens funktionssätt, FEUF).

En EU-förordning får därför inte införlivas i eller transformeras till nationell rätt. Att införliva bestämmelserna i nationell normgivning kan skapa oklarhet om reglernas ursprung och medföra att innehållet förändras. Något genomförande av en EU-förordning ska således inte ske, till skillnad mot vad som är fallet beträffande ett EU-direktiv.

En EU-förordning får inte heller, om det inte särskilt anges, fyllas ut eller kompletteras med mer detaljerade materiella regler inom samma område. En medlemsstat får vidare inte utfärda föreskrifter om hur en EU-förordning ska tolkas.

Särskilda nationella bestämmelser får dock finnas för sådana frågor som faller utanför det område som EU-förordningen reglerar och som kräver en nationell författningsreglering. Även om EU-förordningar är direkt tillämpliga innehåller dessa förordningen ofta bestämmelser som förutsätter eller ger utrymme för komplett-

erande nationell reglering av olika slag. En EU-förordning kan t.ex. innehålla bestämmelser som anger att medlemsstaterna i vissa fall ska eller får meddela regler för att fylla ut förordningen, göra undantag från den eller på annat sätt komplettera den. I dessa avseenden kan sägas att EU-förordningarna innehåller bestämmelser av direktivliknande karaktär.

När det gäller EU-förordningar är medlemsstaterna skyldiga att se till att det finns bestämmelser som gör att de kan tillämpas i praktiken och få effektivt genomslag. Det kan alltså vara nödvändigt med nationella tillämpningsföreskrifter till vissa bestämmelser i EU-förordningar. Det kan t.ex. behöva införas processuella och administrativa regler samt regler om sanktioner vid överträdelser av bestämmelser i en förordning för att bestämmelserna i en EU-förordning ska kunna tillämpas effektivt. Vidare kan en EU-förordning kräva bestämmelser av verkställande karaktär. Exempelvis kan det behövas nationella regler om vilken myndighet som ska svara för tillämpningen. Även i andra fall än då nationella tillämpningsföreskrifter är nödvändiga, kan det under vissa förutsättningar vara tillåtet med nationella tillämpningsföreskrifter.

Genomförande av EU-direktiv i svensk rätt

Ett EU-direktiv är bindande med avseende på det resultat som ska uppnås men överlåter åt de nationella myndigheterna att bestämma form och tillvägagångssätt för genomförandet (artikel 288 FEUF).

En medlemsstat behöver vid genomförandet inte använda sig av samma terminologi och systematik som i direktivet så länge det avsedda resultatet uppnås. Om direktivet är ett minimidirektiv har medlemsstaterna möjlighet att införa strängare regler än vad som följer av direktivet. Om bestämmelserna däremot är fullharmoniserade (eller maximiharmoniserande) har medlemsstaterna inte rätt att införa kompletterande regler.

För att ett direktiv ska bli gällande i svensk rätt måste det genomföras, dvs. införlivas i den svenska rättsordningen. Det är regeringen som ansvarar för att EU-rättsliga direktiv genomförs korrekt och i rätt tid. I den utsträckning det krävs lagändringar för att genomföra hela eller delar av ett direktiv sker det i enlighet med den ordinarie lagstiftningsprocessen. Om det i svensk rätt redan finns bestäm-

melser som motsvarar bestämmelserna i ett direktiv uppfylls kraven i direktivet och några lagstiftningsåtgärder behöver då inte vidtas.

EU-kommissionen bevakar att medlemsstaterna följer och i rätt tid genomför de regler som EU har beslutat om. Om kommissionen anser att svensk lagstiftning eller beslut från svenska myndigheter inte följer EU:s regler kan den inleda ett så kallat överträdelseförfarande mot Sverige. Ett sådant förfarande kan ytterst leda till böter eller vite för fördragsbrott.

Genomförande av internationella överenskommelser i svensk rätt

Enligt 10 kap. 1 § regeringsformen är behörigheten att ingå internationella överenskommelser förbehållen regeringen. I vissa fall krävs emellertid att riksdagen godkänner överenskommelsen. Det gäller bl.a. om den förutsätter att en lag ändras eller upphävs eller att en ny lag stiftas eller om överenskommelsen är av större vikt (10 kap. 3 § regeringsformen).

När regeringen ingår en internationell överenskommelse av offentligrättslig natur är det Sverige som stat som bär det folkrättsliga ansvaret för att förpliktelserna uppfylls i lagstiftning och rätts-tillämpning. Internationella överenskommelser med normativt innehåll blir i Sverige inte automatiskt en del av den nationella rätten, utan måste på något sätt införlivas med svensk rätt för att bli gällande för svenska domstolar och myndigheter.

En överenskommelse kan t.ex. införlivas genom transformering eller konstaterande av normharmoni. Transformering innebär att, i den utsträckning det anses behövligt, införa eller ändra svenska bestämmelser så att de överensstämmer med överenskommelsens krav. Konstateras i stället normharmoni, dvs. att svensk rätt redan överensstämmer med överenskommelsen, behövs inte några lag-ändringar.

5.3 En ny lag ska komplettera EU-förordningen

Förslag: Kompletterande bestämmelser till EU-förordningen ska tas in i en särskild lag. I samma lag ska de bestämmelser som genomför EU-direktivet införas.

Skälen för förslaget: EU-förordningen förutsätter i ett flertal avseenden att medlemsstaterna inför kompletterande bestämmelser för att möjliggöra dess tillämpning. Detta främst mot bakgrund av att det i förordningen i förhållandevis stor utsträckning föreskrivs uttryckligen eller i vart fall är underförstått att olika frågor ska regleras av medlemsstaternas nationella rätt. Bland annat förutsätts att medlemsstaterna inför regler om vilka myndigheter som är behöriga att agera enligt förordningen, om vilka förfaranderegler som ska tillämpas och hur beslut ska få överklagas samt om hur ett system med sanktionsavgifter ska vara konstruerat. Vidare kan kompletteringar behövas för att svenska myndigheter ska kunna använda sig av EU-förordningen så långt som möjligt.

Som framgår i detta betänkande gör vi bedömningen att det behöver införas flera kompletterande bestämmelser till EU-förordningen. Att föra in de kompletterande reglerna till EU-förordningen i redan befintliga lagar framstår mot denna bakgrund inte som en ändamålsenlig lösning. De kompletterande lagbestämmelserna till EU-förordningen bör i stället tas in i en särskild lag.

EU-direktivet reglerar bl.a. tjänsteleverantörers skyldighet att utse verksamhetsställen eller rättsliga ombud, vilka ska kunna ta emot en sådan europeisk utlämnande- eller bevarandeorder som omfattas av EU-förordningens bestämmelser. EU-direktivets bestämmelser bör, eftersom direktivet är så starkt kopplat till EU-förordningen, genomföras genom att införa bestämmelser i den särskilda lagen.

Behovet av eventuella följdändringar i andra författningar behandlas i anslutning till respektive rättsakt.

I avsnitt 14 analyserar vi behovet av en tillfällig lag som genomför vissa delar av EU-direktivet.

5.4 Hänvisningsteknik

Förslag: Hänvisningar till EU-förordningen i de bestämmelser som föreslås, ska som huvudregel vara dynamiska, dvs. avse förordningen i den vid varje tidpunkt gällande lydelsen.

Statisk hänvisning, dvs. hänvisning till EU-förordningens ursprungliga lydelse, ska dock användas när det gäller påförande av sanktionsavgift.

Skälen för förslaget: Hänvisningar i svensk författning till en EU-rättsakt kan göras antingen statiska eller dynamiska. En statisk hänvisning innebär att hänvisningen avser EU-rättsakten i en viss angiven lydelse. En dynamisk hänvisning innebär att hänvisningen avser EU-rättsakten i den vid varje tidpunkt gällande lydelsen.

I den nya lagen föreslås ett flertal bestämmelser i vilka en hänvisning till EU-förordningen görs. Några är av upplysande karaktär och andra är av sådant slag att EU-förordningen förutsätter att det finns bestämmelser om det i svensk rätt för att Sverige ska uppfylla sina unionsrättsliga åtaganden. Till sistnämnda kategori hör bestämmelser om bl.a. utseende av behöriga myndigheter, förfaranderegler, ett system med sanktionsavgifter samt regler om domstolsprövning. Statiska hänvisningar till sådana bestämmelser skulle kunna leda till oklarheter och brister om EU-förordningen skulle ändras. För att säkerställa att eventuella ändringar som görs i förordningen får omedelbart genomslag är det därför lämpligt att som huvudregel låta hänvisningarna till förordningen vara dynamiska.

Den nya lagen föreslås innehålla bestämmelser om sanktionsavgifter. Då sanktionsavgifter har en straffliknande karaktär bör statisk hänvisning användas när det gäller påförande av sanktionsavgift för överträdelse av EU-förordningens bestämmelser. Om EU-förordningens bestämmelser om sanktioner skulle ändras, får nya kompletteringar föras in i lag.

5.5 Termer och uttryck

Förslag: Termer och uttryck i bestämmelser i den nya föreslagna lagen som kompletterar EU-förordningen ska ha samma betydelse som i EU-förordningen.

Skälen för förslaget: I artikel 3 i EU-förordningen finns ett antal definitioner av centrala begrepp, bl.a. vad avser europeisk utlämnandeorder och europeisk bevarandeorder, tjänsteleverantör, samt elektroniska bevis. Det är inte möjligt att i svensk rätt ange hur begrepp i en EU-förordning ska förstås. Eftersom den nya lagens syfte är bl.a. att komplettera EU-förordningen får termer och begrepp i lagen inte ges en annan innebörd än den som gäller enligt förordningen. Det är också EU-domstolen som är den yttersta uttolkaren av en EU-förordning och av de termer och uttryck som används i den.

I vissa lagar som kompletterar en EU-förordning har det införts förtydligande bestämmelser om att de termer och uttryck som används i lagen ska ha samma betydelse som i den aktuella EU-förordningen, se t.ex. 1 kap. 1 § andra stycket lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. En motsvarande upplysningsbestämmelse bör tas in i den nya lagen. Detta särskilt mot bakgrund av att flera begrepp som används i lagen inte har en vedertagen definition i svensk rätt (t.ex. tjänsteleverantör) samt att definitionen av ett begrepp i EU-förordningen kan skilja sig från hur begreppet definieras enligt svensk rätt (t.ex. trafikuppgifter). Det ska noteras att bestämmelsen avser endast termer och uttryck i lagen som genomför EU-förordningen.

6 Behovet av kompletterande nationella bestämmelser om bevisinhämtning

6.1 Inledning

EU-förordningens övergripande syfte är att skapa ett ändamålsenligt regelverk som kompletterar befintlig lagstiftning och effektiviserar gränsöverskridande inhämtning av elektronisk bevisning. EU-förordningen gör det möjligt för en myndighet i en medlemsstat att begära ut eller begära bevarande av elektronisk bevisning direkt hos en tjänsteleverantör som är etablerad i en annan medlemsstat och oavsett var uppgifterna finns lagrade (artikel 1.1).

Som följer av våra direktiv är det angeläget att säkerställa en effektiv och rättssäker hantering av en europeisk utlämnande- och bevarandeorder samt att svenska brottsbekämpande myndigheter fullt ut kan använda de möjligheter som EU-förordningen tillhandahåller.

Vårt uppdrag i denna del är att dels kartlägga vilka svenska bestämmelser som berörs av EU-förordningens bestämmelser om europeiska utlämnande- och bevarandeorder, dels analysera om de svenska bestämmelserna bör ändras eller kompletteras och i så fall lämna nödvändiga författningsförslag.

I detta kapitel redogörs i avsnitt 6.2 för de aktörer som omfattas av EU-förordningens bestämmelser. Därefter redovisas i avsnitt 6.3 villkoren för utfärdande av en europeisk utlämnande- och bevarandeorder. I avsnitt 6.4–6.12 finns våra överväganden och förslag.

6.2 Aktörer som omfattas av EU-förordningens bestämmelser

6.2.1 Inledning

I artikel 2.1 anges att EU-förordningen gäller för tjänsteleverantörer som erbjuder tjänster inom unionen. Vilka tjänsteleverantörer som närmare omfattas av EU-förordningen och direktivet klargörs i artikel 3 i EU-förordningen. Detsamma gäller begreppet ”erbjuda tjänster i unionen”. Eftersom dessa begrepp är grundläggande för EU-förordningens tillämpningsområde redogörs för dessa mer ingående.

6.2.2 Tjänsteleverantörer som omfattas av EU-förordningen

En tjänsteleverantör definieras i artikel 3.3 i EU-förordningen som en fysisk eller juridisk person som tillhandahåller en eller flera av följande kategorier av tjänster:

- a) Elektroniska kommunikationstjänster enligt definitionen i artikel 2.4 i direktiv 2018/1972¹.
- b) Tjänster för internetdomännamn och IP-numrering, såsom tjänster för tilldelning av IP-adresser, tjänster för domännamnsregister, tjänster för domännamnsregistratorer och domännamnsrelaterade integritets- och proxytjänster.
- c) Andra av informationssamhällets tjänster enligt artikel 1.1 b i direktiv 2015/1535² som
 - i. gör det möjligt för användarna att kommunicera med varandra, eller
 - ii. gör det möjligt att lagra eller på annat sätt behandla uppgifter på uppdrag av de användare till vilka tjänsten tillhandahålls, förutsatt att datalagringen är en väsentlig del av den tjänst som tillhandahålls användaren.

¹ Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation.

² Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (kodifiering).

Finansiella tjänster som avses i artikel 2.2 b i direktiv 2006/123³ är undantagna från förordningens tillämpningsområde. Sådana finansiella tjänster är enligt den nämnda artikeln banktjänster och tjänster som avser krediter, försäkringar och återförsäkringar, tjänstepensioner och individuellt pensionssparande, värdepapper, investeringsfonder, betalningar och investeringsrådgivning, inbegripet tjänster som förtecknas i bilaga I till direktiv 2006/48⁴.

6.2.3 Aktörer som omfattas av punkten a i artikel 3.3

Punkten a i artikel 3.3 avser leverantörer av elektroniska kommunikationstjänster såsom de tjänsterna är definierade i artikel 2.4 i direktiv 2018/1972. Av den artikeln följer att en elektronisk kommunikationstjänst är en tjänst som vanligen tillhandahålls mot ersättning via elektroniska kommunikationsnät och som omfattar följande typer av tjänster:

- internetanslutningstjänst enligt definitionen i artikel 2.2 förordning 2015/2120⁵,
- interpersonell kommunikationstjänst, och
- tjänster som helt eller huvudsakligen utgörs av överföring av signaler, såsom överföringstjänster som används för tillhandahållande av maskin till maskin-tjänster och för utsändningstjänster.

Från artikel 2.4 i direktiv 2018/1972 undantas tjänster i form av tillhandahållande av innehåll som överförs med hjälp av elektroniska kommunikationsnät och kommunikationstjänster eller tjänster som innebär utövande av redaktionellt ansvar över sådant innehåll. Rena innehållstjänster, som programverksamheten hos vissa programföretag för radio och tv och innehållstjänster som tillhandahålls via

³ Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden.

⁴ Europaparlamentets och rådets direktiv 2006/48/EG av den 14 juni 2006 om rätten att starta och driva verksamhet i kreditinstitut.

⁵ 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.

internet, och tjänster som innebär utövande av redaktionellt ansvar över sådant innehåll faller således utanför definitionen.⁶

Bestämmelserna i direktiv 2018/1972 har genomförts i svensk rätt genom lagen (2022:482) om elektronisk kommunikation. I 1 kap. 7 § tydliggörs innebörden av ett antal begrepp som i väsentligt överensstämmer med motsvarande definitioner i nämnda direktiv.

Tre olika slag av elektroniska kommunikationstjänster anges i artikel 2.4 i direktiv 2018/1972, vilka delvis kan överlappa varandra. Dessa är internetanslutningstjänster, interpersonella kommunikationstjänster och tjänster som helt eller huvudsakligen utgörs av överföring av signaler. En grundläggande förutsättning är att tjänsten vanligen tillhandahålls mot ersättning. Tjänsten ska alltså tillhandahållas kommersiellt. Sker tillhandahållandet på rent ideell basis omfattas tjänsten inte av definitionen, t.ex. forskarnät eller andra nät inom universitetsvärlden. I vissa fall tillhandahålls kommersiella tjänster gratis till slutkunden. Det kommersiella inslaget manifesteras då på något annat sätt, t.ex. genom att tjänsten är reklamfinansierad. Kravet på tillhandahållande mot ersättning bör anses vara uppfyllt även i andra fall när tillhandahållaren får betalt av tredje part och inte av slutkunden, t.ex. om tillhandahållaren tjänar pengar på personuppgifter eller andra data som samlas in vid användningen av tjänsten.⁷

En annan förutsättning är att den elektroniska kommunikationstjänsten tillhandahålls via ett elektroniskt kommunikationsnät. I artikel 2.1 i direktiv 2018/1972 definieras ett sådant nät som 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. I 1 kap. 7 § lagen om elektronisk kommunikation finns en motsvarande definition.⁸

⁶ Prop. 2021/22:136 s. 406.

⁷ Prop. 2021/22:136 s. 406, se även skäl 16 i direktiv 2018/1972.

⁸ Se även prop. 2021/22:136 s. 407.

Internetanslutningstjänst

I artikel 2.2 i förordningen 2015/2120 definieras internetanslutningstjänst som en allmänt tillgänglig elektronisk kommunikationstjänst som erbjuder anslutning till internet och därigenom möjlighet till anslutning mellan praktiskt taget alla ändpunkter på internet, oberoende av vilken nätteknik och terminalutrustning som används.

I skäl 4 till nämnda förordning anges beträffande tillgång till i princip till alla internets ändpunkter att av orsaker som leverantörer av internetanslutningstjänster inte har kontroll över är vissa slutpunkter på internet kanske inte alltid tillgängliga. En leverantör av internetanslutningstjänster ska ansetts ha uppfyllt sina skyldigheter rörande tillhandahållande av en internetanslutningstjänst i den mening som avses i förordningen när tjänsten erbjuder anslutning till praktiskt taget alla ändpunkter på internet.

Interpersonell kommunikationstjänst

Allmänt om begreppet

Begreppet *interpersonell kommunikationstjänst* definieras i artikel 2.5 i direktiv 2018/1972, med en motsvarande definition i 1 kap. 7 § lagen om elektronisk kommunikation.

En interpersonell kommunikationstjänst är en tjänst som vanligen tillhandahålls mot ersättning och som möjliggör direkt interpersonellt och interaktivt informationsutbyte via elektroniska kommunikationsnät mellan ett begränsat antal personer som bestäms av kommunikationens avsändare eller deltagare.

I skäl 17 i direktivet anges att begreppet omfattar tjänster som traditionella röstsamtal mellan två fysiska personer, men även t.ex. e-posttjänster, meddelandetjänster och gruppchattar. I skäl 27 i EU-förordningen nämns också VoIP (Voice over Internet Protocol, eller IP-telefoni) som exempel på en interpersonell kommunikationstjänst.

I skäl 17 i direktiv 2018/1972 preciseras begreppet ytterligare. Kommunikation som involverar juridiska personer omfattas i de fall då fysiska personer agerar för dessa juridiska personers räkning eller är involverade på minst en sida av kommunikationen. Interaktiv kommunikation innebär att tjänsten gör det möjligt för mot-

tagaren av informationen att svara. Tjänster som inte uppfyller dessa krav omfattas inte av definitionen. Det kan exempelvis gälla linjära sändningstjänster för radio och tv, beställvideo, webbplatser, sociala nätverk, bloggar och informationsutbyte mellan maskiner. Sådana tjänster kan dock erbjudas på samma plattform som en tjänst som uppfyller kraven för en interpersonell kommunikationstjänst.⁹

Det finns inget krav på att interpersonella kommunikationstjänster helt eller huvudsakligen ska utgöras av överföring av signaler. Därmed omfattas t.ex. mjukvarutjänster för direkt kommunikation mellan slutanvändares datorer där tjänstetillhandahållaren inte har inflytande eller rådighet över själva överföringen av kommunikationen.¹⁰

En tjänst anses enligt aktuell definitionen inte som en interpersonell kommunikationstjänst om funktionen enbart är en extrafunktion av mindre betydelse. För att undantas från direktivets tillämpningsområde ska vidare en sådan tjänst vara direkt kopplad till en annan tjänst och inte av tekniska skäl kunna användas utan den huvudtjänsten. I skäl 17 i direktiv 2018/1972 anges att integreringen av tjänsten inte får vara ett sätt att kringgå tillämpningen av bestämmelserna för elektroniska kommunikationstjänster. Begreppen mindre och extrafunktion bör tolkas restriktivt och ur ett objektivt slutanvändarperspektiv. Ett exempel på en funktion som skulle kunna anses falla utanför definitionen är en kommunikationskanal i online-spel.

Nummerbaserade eller nummeroberoende interpersonella kommunikationstjänster

En interpersonell kommunikationstjänst kan vara nummerbaserad eller nummeroberoende. Begreppen definieras i artikel 2.6–2.7 i direktiv 2018/1972. En motsvarande definition finns i 1 kap. 7 § lagen om elektronisk kommunikation.

En *nummerbaserad interpersonell kommunikationstjänst* möjliggör enligt definitionen kommunikation med nummer i nationella eller internationella nummerplaner. Det rör sig om nummer som är tilldelade, t.ex. traditionella telefonnummer. Nummerbaserade inter-

⁹ Prop. 2021/22:136 s. 407.

¹⁰ Prop. 2021/22:136 s. 408.

personella kommunikationstjänster är exempelvis taltjänster via fast telefoni och video-, tal- och meddelandetjänster via mobiltelefoni.¹¹ I skäl 18 i direktiv 2018/1972 preciseras begreppet ytterligare. Nummerbaserade interpersonella kommunikationer omfattar både tjänster till vilka telefonnummer tilldelas för att säkerställa att slutanvändare kan nå varandra och tjänster som gör det möjligt för slutanvändare att nå personer som har tilldelats sådana nummer. Enbart användningen av ett nummer för att identifiera t.ex. en slutanvändare, är inte tillräckligt för att en tjänst ska anses vara nummerbaserad.

En *nummeroberoende interpersonell kommunikationstjänst*, eller Noik, använder inte allmänt tilldelade nummerresurser (dvs. nummer i nationella eller internationella nummerplaner) och möjliggör inte heller kommunikation mellan sådana nummer. Nummeroberoende interpersonella kommunikationstjänster kan använda traditionella telefonnummer för att identifiera slutanvändare så att de ska kunna nå varandra, men möjliggör inte kommunikation med sådana nummer. Tillhandahållare av en Noik kan i och för sig ställa krav på att ett telefonnummer anges vid registreringen av ett konto i tjänsten, men telefonnumret har ingen betydelse för hur kommunikationen etableras eller förmedlas genom tjänsten. Däremot kan telefonnumret ibland användas för att slutanvändare ska kunna nå varandra i tjänsten.¹²

Ibland används begreppet OTT-tjänster i stället för Noik. OTT är en förkortning för engelskans *over the top*. OTT-tjänster är operatörsoberoende tjänster i form av TV, video, ljud eller meddelanden som sänds ut till användare via data-, tele- eller kabelnätet av en fristående distributör. Benämningen *over the top* används på grund av att signalerna förekommer utöver – ovanpå – de vanliga sändningarna. Den fristående tjänsten tar normalt inte betalt för datakommunikationen; denna betalar användarna för genom sitt internetabonnemang. Internetleverantören ansvarar i sin tur inte för innehållet utan ser enbart till att materialet kommer fram.

Exempel på OTT-tjänster är Apple Imessage och Facetime, Discord, Google Messages, Kik Messenger, Line, Messenger from Meta, Skype, Slack, Telegram, Viber och Whatsapp.¹³ Andra tjänster

¹¹ Prop. 2021/22:136 s. 408.

¹² Prop. 2021/22:136 s. 408–409.

¹³ SOU 2023:22 s. 325–326.

är Instagram (chatt och meddelandedelarna), Snapchat, Microsoft Teams, Zoom, LinkedIn (chatt och meddelandedelarna), Tiktok (chatt och meddelandedelarna), Google Meet. Vidare omfattas ett stort antal tillhandahållare av e-post, t.ex. Gmail, Apple Mail, Outlook (tidigare MSN, Hotmail), Yahoo! Mail.¹⁴

Tjänster som helt eller huvudsakligen utgörs av överföring av signaler

Slutligen ingår i begreppet elektronisk kommunikationstjänst tjänster som helt eller huvudsakligen utgörs av överföring av signaler såsom överföringstjänster som används för tillhandahållande av maskin till maskin-tjänster och för utsändningstjänster.

Vad som avses med en tjänst som helt eller huvudsakligen utgörs av överföring av signaler är inte alltid lätt att avgöra i praktiken.¹⁵ Tjänster som innebär överföring av signaler kan ske t.ex. via tråd, fiber, radiovågor, satellit, kabel eller andra elektromagnetiska överföringsmedier samt via egen eller annans infrastruktur (om tjänsten innebär ett åtagande att sköta överföringen av signaler).

Med maskin-till-maskin-tjänster avses tjänster som omfattar automatisk överföring av data och information mellan enheter och mjukvarubaserade tillämpningar med liten eller ingen mänsklig medverkan. Enligt praxis från EU-domstolen omfattas bl.a. tjänster som huvudsakligen omfattar överföring av kabel-tv-sändningar till slutanvändares mottagare, om tillhandahållaren är ansvarig gentemot slutanvändarna för den överföring av signalen som säkerställer att användarna tillhandahålls den tjänst som de abonnerar på.¹⁶

6.2.4 Aktörer som omfattas av punkten b i artikel 3.3

Punkt b i artikel 3.3 avser leverantörer av tjänster för internetdomännamn och IP-numrering. Som exempel i bestämmelsen anges i punkten b i artikel 3.3 tjänster för tilldelning av IP-adresser, regi-

¹⁴ SOU 2023:22 s. 330.

¹⁵ Prop. 2021/22:136 s. 123.

¹⁶ Prop. 2021/22:136 s. 123 och 407.

streringsenheter för toppdomäner¹⁷, registrarer (dvs. återförsäljare) av domännamn och domännamnsrelaterade integritets- och proxy-tjänster.

I skäl 28 till EU-förordningen anges betydelsen av att dessa aktörer omfattas av EU-förordningen för att göra det möjligt att identifiera en person eller enhet som ligger bakom en webbplats som används för brottslig verksamhet, eller offret för en brottslig verksamhet.

Särskilt om IP-adresser

I betänkandet *Datalagring och åtkomst till elektronisk kommunikation* (SOU 2023:22) beskrivs IP-adresser enligt följande.

IP-adresser kan förenklat beskrivas som en länk mellan å ena sidan en användares enhet (exempelvis en dator eller mobiltelefon) och å andra sidan den som vill kommunicera med enheten. IP-adressen fyller två huvudsakliga funktioner. Den första funktionen är att identifiera en enhet inom ett nätverk, vilket är förutsättning för att kunna tillhandahålla tjänsten och ta betalt för den från den som äger enheten eller låter andra bruka den. Den andra funktionen är att återge enhetens placering inom ett nätverk för att enheten ska kunna kommunicera med andra enheter, vilket är en förutsättning för internet-trafik. En internetleverantör utgör i praktiken en länk mellan en användares privata nätverk och interna IP-adresser (ofta i form av en router som genererar IP-adresser för enheterna i ett hem) och internet. Extern kommunikation blir möjligt genom att användaren får en extern IP-adress av sin internetleverantör. I de flesta fall ändras IP-adressen från gång till annan när enheten kopplar upp sig mot internetleverantörens infrastruktur (dynamiska IP-adresser) och i andra fall, i regel mot extra avgift, kan enheten få en fast IP-adress.¹⁸

Det är vanligen slutanvändarens internetleverantör som tilldelar en IP-adress till slutanvändaren och oftast är det en dynamisk IP-adress som tilldelas, dvs. en tillfällig adress som ändras över tid. Om slutanvändaren behöver en fast IP-adress, såsom vid egen webbserver eller e-postserver, kan en sådan tilldelas av internetleverantören, som slutanvändaren får konfigurera i sina nätverksinställningar.

¹⁷ I svenska översättningen av EU-förordningen har begreppen ”domain name registry” och ”domain name registrar” översatts till ”tjänster för domännamnsregister” respektive ”tjänster för domännamnsregistratorer”. En mer ändamålsenlig översättning torde dock vara ”en registreringsenhet för toppdomäner” samt ”registrar av domännamn”. Se även avsnitt 12.4.1.

¹⁸ SOU 2023:22 s. 169.

Domännamn

Ett domännamn kan sägas utgöra en blandning av en adress och en identitet på internet. Bakom varje domännamn döljer sig en IP-adress, som används av enheter när de kommunicerar med varandra. IP-adressen utgörs av en rad siffror, och domännamnet kan sägas utgöra en översättning av siffrorna till bokstäver. Bokstäverna efter den sista punkten i ett domännamn kallas för toppdomän. Varje land har en egen toppdomän. Om ett domännamn slutar på ".se" innebär det att det ligger under den svenska landstoppdomänen.¹⁹

I Sverige ansvarar Stiftelsen för Internetinfrastruktur (Internetstiftelsen) i egenskap av domänadministratör för den svenska toppdomänen ".se" för registrering av domännamn, samt administration och teknisk drift av det nationella domännamnsregistret. Det nationella begreppet domänadministratör är att likställa med begreppet registreringsenhet för toppdomäner som används i EU-förordningen. Internetstiftelsen ska avseende toppdomänen ".se" föra register över tilldelade domännamn under toppdomänen enligt 6 § lagen (2006:24) om nationella toppdomäner för Sverige på internet. Registret ska innehålla uppgifter om bl.a. domännamnet och namnet på domännamnsinnehavaren och dennes postadress, telefonnummer och adress för elektronisk post (mer om nämnda lag och registret, se avsnitt 12.4). Internetstiftelsen sköter också drift och administration av toppdomänen ".nu".

Återförsäljare av domännamn kallas ombud eller registrar. För registrering av en ny domän krävs alltså kontakt med en återförsäljare av domännamn (se även avsnitt 12.4).

Domännamnsrelaterade integritets- och proxytjänster möjliggör för en person eller företag att genom någon annan (proxy) registrera ett domännamn, alternativt att kontaktuppgifterna för domännamnsinnehavet är någon annans. Det kan t.ex. förhålla sig så att ett företag som innan lansering av en ny produkt vill registrera samtliga domännamn med produktens kommande namn så att ingen annan kan köpa dem, men utan att visa sitt namn då det kan röja den kommande produktens lansering. Ett annat exempel är att en köpare i vissa fall måste vara medborgare i det land i vilket man vill registrera en domän. Om köparen saknar sådant medborgarskap kan ett ombud registrera domännamnet mot ersättning.

¹⁹ <https://internetstiftelsen.se/domaner/domannamn-vad-ar-det/>.

6.2.5 Aktörer som omfattas av punkten c i artikel 3.3

EU-förordningen är tillämplig på leverantörer av andra informations-samhällets tjänster i den mening som avses i artikel 1.1 b i direktiv 2015/1535 och som gör det möjligt

- för användarna att kommunicera med varandra, eller
- att lagra eller på annat sätt behandla uppgifter på uppdrag av de användare till vilka tjänsten tillhandahålls, förutsatt att data-lagringen är en väsentlig del av den tjänst som tillhandahålls användaren.

I artikel 1.1 b i direktiv 2015/1535 definieras tjänst som alla informationssamhällets tjänster, dvs. tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare. I samma bestämmelse avse med

- *på distans*: tjänster som tillhandahålls utan att parterna är närvarande samtidigt,
- *på elektronisk väg*: en tjänst som sänds vid utgångspunkten och tas emot vid slutpunkten med hjälp av utrustning för elektronisk behandling (inbegripet digital signalkomprimering) och lagring av uppgifter, och som i sin helhet sänds, befordras och tas emot genom tråd, radio, optiska medel eller andra elektromagnetiska medel,
- *på individuell begäran av en tjänstemottagare*: en tjänst som tillhandahålls genom överföring av uppgifter på individuell begäran.

I bilaga till direktivet finns en vägledande förteckning över tjänster som inte omfattas av denna definition.

I skäl 27 i EU-förordningen sägs att den bör vara tillämplig på leverantörer av informations-samhällets tjänster i den mening som avses med direktiv 2015/1535 som inte kan klassas som leverantörer av elektroniska kommunikationstjänster men som erbjuder sina användare möjligheten att kommunicera med varandra eller tjänster som kan användas för att lagra eller på annat sätt behandla uppgifter för användarnas räkning. Uppgiftsbehandling bör enligt skäl 27 förstås i teknisk mening, som skapande eller manipulation av uppgifter, dvs. teknisk bearbetning för att framställa eller ändra

uppgifter med hjälp av datorernas bearbetningskapacitet. I samma skäl preciseras ytterligare vilka leverantörer som omfattas av artikel 3.3 c. Exempel på tjänster som nämns är rättsliga tjänster, dataarkitektur-tjänster och bokföringstjänster som tillhandahålls online på distans.

6.2.6 Tjänsteleverantörer som erbjuder tjänster i unionen

En viktig och förklarlig avgränsning av EU-förordningen är att endast tjänsteleverantörer som erbjuder tjänster i unionen omfattas av regleringen. Detta betonas i skäl 26 till EU-förordningen där det anges att tjänster som erbjuds uteslutande utanför unionen inte bör omfattas av förordningens tillämpningsområde, även om tjänsteleverantören har ett verksamhetsställe i unionen. Förordningen ska således enligt nämnda skäl inte avse åtkomst till andra uppgifter än uppgifter som rör de tjänster som erbjuds användaren i unionen av dessa tjänsteleverantörer.

Med begreppet *erbjuda tjänster i unionen* avses enligt artikel 3.4

- a) att göra det möjligt för fysiska eller juridiska personer i en medlemsstat att använda de tjänster som i anges i artikel 3.3, och
- b) att ha en betydande anknytning baserad på specifika faktiska kriterier till den medlemsstat som avses i punkten a.

Vidare anges i artikel 3.4 b att en sådan betydande anknytning ska anses föreligga om tjänsteleverantören har ett verksamhetsställe i en medlemsstat eller, om ett sådant verksamhetsställe saknas, ska en betydande anknytning anses vara för handen om det finns ett betydande antal användare i en eller flera medlemsstater eller om verksamheten är inriktad på en eller flera medlemsstater.

Ett verksamhetsställe definieras i artikel 3.5 som en enhet som de facto utövar en ekonomisk verksamhet under en obegränsad tid genom en stabil infrastruktur varifrån tillhandahållandet av tjänster genomförs eller verksamheten förvaltas.

När det gäller bedömningen av om tjänsteleverantören gör det möjligt för fysiska eller juridiska personer i en eller flera medlemsstater att använda dess tjänster framhålls i skäl 29 i EU-förordningen att enbart det förhållande att ett online-gränssnitt är tillgängligt i unionen, exempelvis genom en tjänsteleverantörs eller en mellanhands webbplats eller en e-postadress eller andra kontakt-

uppgifter, bör inte i sig anses vara tillräckligt för att fastställa att en tjänsteleverantör erbjuder tjänster i unionen i den mening som avses i förordningen.

Bedömningen om en tjänsteleverantörs verksamhet enligt artikel 3.4 b är inriktad på en eller flera medlemsstater bör enligt skäl 30 i förordningen göras med hänsyn till samtliga relevanta förhållanden. Detta innefattar bl.a. omständigheter som användningen av ett språk eller en valuta som allmänt används i den medlemsstaten, eller möjligheten att beställa varor eller tjänster. Ytterligare omständigheter som talar för att verksamheten är inriktad på en medlemsstat kan enligt nämnda skäl vara förekomsten av en app i den berörda nationella appbutiken, att lokal marknadsföring eller reklam görs på det språk som allmänt används i den medlemsstaten eller att kundkontakter, t.ex. kundtjänst, sköts på det språk som allmänt används i den medlemsstaten. En betydande anknytning bör också enligt skälet anses föreligga när en tjänsteleverantör riktar sin verksamhet mot en eller flera medlemsstater enligt förordning 2012/1215.²⁰ Däremot bör tillhandahållande av en tjänst enbart i syfte att efterleva det förbud mot diskriminering som fastställs i förordning (EU) 2018/302²¹ i sig inte anses innebära att verksamheten är inriktad på ett visst territorium inom unionen.

6.3 Villkoren för utfärdande av en europeisk utlämnandeorder respektive bevarandeorder

6.3.1 Allmänna förutsättningar för utfärdande av europeisk utlämnande- eller bevarandeorder

En europeisk utlämnande- eller bevarandeorder får enligt artikel 2.2 i EU-förordningen utfärdas endast inom ramen för straffrättsliga förfaranden och för verkställighet av en frihetsberövande påföljd om minst fyra månader. I skäl 24 anges att en order får endast utfärdas i förhållande till ett specifikt brott som redan har ägt rum.

²⁰ Europaparlamentets och rådets förordning (EU) nr 1215/2012 av den 12 december 2012 om domstols behörighet och om erkännande och verkställighet av domar på privaträttsens område.

²¹ Europaparlamentets och rådets förordning (EU) 2018/302 av den 28 februari 2018 om åtgärder mot omotiverad geoblockering och andra former av diskriminering på grund av kunders nationalitet, bosättningsort eller etableringsort på den inre marknaden och om ändring av förordningarna (EG) nr 2006/2004 och (EU) 2017/2394 samt direktiv 2009/22/EG.

En utlämnande- eller bevarandeorder får också enligt samma bestämmelser utfärdas i förfaranden som avser brott för vilka en juridisk person skulle kunna ställas till ansvar eller bestraffas i den utfärdande staten. EU-förordningen är däremot enligt artikel 2.4 inte tillämplig på förfaranden som inletts i syfte att ge en annan medlemsstat eller ett tredjeland ömsesidig rättslig hjälp (se även skäl 23).

En europeisk utlämnandeorder definieras i artikel 3.1 som ett beslut som förelägger ett utsett verksamhetsställe eller ett rättsligt ombud för en tjänsteleverantör, som erbjuder tjänster i unionen, att lämna ut elektroniska bevis. Enligt definitionen krävs att en order har utfärdats eller godkänts av en rättslig myndighet enligt artikel 4. Vidare förutsätts att det utsedda verksamhetsstället eller det rättsliga ombudet befinner sig i en annan medlemsstat som är bunden av EU-förordningen.

I avsnitt 6.2 redogörs närmare för vilka tjänsteleverantörer som omfattas av regleringen.

Definitionen av en europeisk bevarandeorder enligt artikel 3.2 är likalydande med definitionen av en europeisk utlämnandeorder med den skillnaden att en bevarandeorder avser bevarande av elektroniska bevis i avvaktan på en efterföljande begäran om utlämnande av bevisningen.

Med elektroniska bevis avses enligt artikel 3.8 *abonmentuppgifter*, *trafikuppgifter* eller *innehållsdata* som lagras i elektronisk form av en tjänsteleverantör eller på en tjänsteleverantörs vägnar vid tidpunkten för mottagandet av ett intyg om en europeisk utlämnandeorder eller en europeisk bevarandeorder. En order innebär således inte någon förpliktelse för en tjänsteleverantör att lagra framtida uppgifter eller att bistå med avlyssning eller övervakning i realtid (skäl 19). Inte heller åläggs tjänsteleverantörerna att dekryptera de uppgifter som begärs utlämnande (skäl 20). Det ska dock noteras att tjänsteleverantörernas skyldighet att lämna ut eller bevara uppgifter gäller oavsett var uppgifterna lagras och inkluderar således även molnbaserade uppgifter (artikel 1.1 och skäl 21).

En *abonmentuppgift* definieras enligt artikel 3.9 som:

- en abonnents eller kunds identitet, såsom angivet namn, födelse-datum, postadress eller geografisk adress, fakturerings- och betalningsuppgifter, telefonnummer eller e-postadress,

- typen av tjänst och dess varaktighet, inbegripet tekniska data och uppgifter om relaterade tekniska åtgärder eller gränssnitt som använts av eller tillhandahållits av abonnenten eller kunden vid tidpunkten för den ursprungliga registreringen eller aktiveringen, samt uppgifter som rör valideringen av tjänsteanvändningen, förutom lösenord eller andra autentiseringsmetoder som används i stället för ett lösenord och som tillhandahålls av användaren eller skapas på dennas begäran.

Trafikuppgifter definieras som uppgifter som rör tillhandahållandet av en tjänst som erbjuds av en tjänsteleverantör och vilka tjänar till att ge kontext eller ytterligare information om tjänsten samt som genereras eller behandlas av tjänsteleverantörens informationssystem, t.ex. källan till eller destinationen för ett meddelande eller en annan typ av interaktion, var utrustningen är belägen, datum, tid, varaktighet, storlek, rutt, format, vilket protokoll som använts och typen av komprimering samt andra metadata från elektronisk kommunikation och uppgifter, med undantag för abonnentuppgifter, som rör inledande och avslutande av en användares åtkomst till en tjänst, såsom datum och tid för användningen, eller inloggning i och utloggning från tjänsten (artikel 3.11).

Med *innehållsdata* avses alla uppgifter i digital form, t.ex. text, röst, video, bilder och ljud, med undantag för abonnentuppgifter och trafikuppgifter (artikel 3.12).

Begreppet *uppgifter som begärts med det enda syftet att identifiera användaren* används också i EU-förordningen. Begreppet definieras som IP-adresser och, vid behov, relevanta källportar och tidsstämpel, dvs. datum och tid, eller tekniska motsvarigheter till dessa identifierare och relaterad information, när brottsbekämpande myndigheter eller rättsliga myndigheter begärt detta med det enda syftet att identifiera användaren i en specifik brottsutredning (artikel 3.10). I betänkandet använder vi termen *andra användaruppgifter*.

I skäl 32 och 33 till EU-förordningen redogörs närmare för de uppgifter som avses i artikel 3.10. Beroende på kontexten bör andra användaruppgifter i vissa fall jämföras med abonnentuppgifter, medan i andra fall med trafikuppgifter. I en viss situation begärs nämnda uppgifter ut med det enda syftet att identifiera användaren innan abonnentuppgifter avseende denna användare kan begäras från tjänsteleverantören. I sådana fall är det enligt skäl 32 lämpligt

att tillämpa samma ordning för dessa uppgifter som för abonnentuppgifter. I andra fall kan samma uppgifter användas för att fastställa en omfattande profil för en berörd person eftersom uppgifterna presenteras i ett strukturerat och standardiserat format. I sådana situationer är det därför enligt skäl 33 viktigt att de uppgifter som avses i artikel 3.10 och som inte begärs med det enda syftet att identifiera användaren i en specifik brottsutredning behandlas som trafikuppgifter.

Som följer av avsnitt 6.2.4 omfattas registreringsenheter för toppdomäner och registrarer (återförsäljare) av domännamn av EU-förordningens bestämmelser. Bakom varje domännamn döljer sig en IP-adress som utgörs av en rad siffror. Domännamnet är enkelt uttryckt en översättning av siffrorna till bokstäver (se avsnitt 6.2.4). Enligt EU-förordningen faller IP-nummer, som angetts ovan, under begreppet andra användaruppgifter. Även uppgifter hänförliga till domännamn bör falla inom denna kategori eftersom uppgifterna alltså i stort motsvarar en IP-adress.

6.3.2 Villkoren för utfärdande av en europeisk utlämnandeorder

Artikel 5 anger villkoren för utfärdande av en europeisk utlämnandeorder. En utfärdande myndighet får utfärda en europeisk utlämnandeorder endast om de villkor som anges i artikeln är uppfyllda (artikel 5.1). En europeisk utlämnandeorder ska enligt artikel 5.2 vara nödvändig och proportionell med beaktande av den miss-tänktes eller tilltalades rättigheter, och får utfärdas endast om en liknande order skulle ha kunnat utfärdas på samma villkor i ett liknande inhemskt ärende (se även skäl 38).

Av artikel 5.3 följer att en europeisk utlämnandeorder för att inhämta *abbonentuppgifter* eller *andra användaruppgifter* får utfärdas för alla brott och för verkställighet av en frihetsberövande påföljd om minst fyra månader.

Enligt artikel 5.4 får en europeisk utlämnandeorder för att inhämta *trafikuppgifter*, med undantag för andra användaruppgifter, eller *innehållsdata* endast utfärdas

- a) för brott för vilka maximistraffet i den utfärdande staten är fängelse eller annan frihetsberövande åtgärd i minst tre år, eller

- b) för följande brott, om de helt eller delvis begås med hjälp av ett informationssystem (som definieras i artikel 3.13)²²:
 - i. brott enligt definitionerna i artiklarna 3–8 i Europaparlamentets och rådets direktiv (EU) 2019/713²³,
 - ii. brott enligt definitionerna i artiklarna 3–7 i direktiv 2011/93/EU²⁴,
 - iii. brott enligt definitionerna i artiklarna 3–8 i direktiv 2013/40/EU²⁵,
- c) för brott enligt definitionerna i artiklarna 3–12 och 14 i direktiv (EU) 2017/541²⁶,
- d) för verkställighet av en frihetsberövande påföljd om minst fyra månader, för brott som avses i leden a, b och c ovan.

De brott som följer av *punkten a* är således samtliga brott i den utfärdande staten där ett fängelsestraff om minst tre år kan dömas ut (se även skäl 40). Det innebär att för de brott i svensk rätt det föreskrivs ett fängelsestraff om tre år eller mer kan en europeisk utlämnandeorder utfärdas enligt artikel 5.4 a i EU-förordningen.

I artikel 5.4 b och c inkluderas brott som har ansetts bör omfattas av EU-förordningen även om det maximistraff som föreskrivs är lägre än tre år (se skäl 41). I avsnitten nedan anges i korthet vilka kriminaliseringsåtaganden som följer av de direktiv som räknas upp i artikel 5.4 b och c samt hur dessa åtaganden har omhändertagits i svensk rätt.

²² I artikel 3.13 hänvisas till definitionen i artikel 2 a i 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.

²³ Europaparlamentets och rådets direktiv (EU) 2019/713 av den 17 april 2019 om bekämpande av bedrägeri och förfalskning som rör andra betalningsmedel än kontanter och om ersättande av rådets rambeslut 2001/413/RIF.

²⁴ 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.

²⁵ 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.

²⁶ Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF.

Brott som faller under punkten b – allmänna utgångspunkter

För samtliga brott som faller under punkten b krävs att brottet helt eller delvis har begåtts med hjälp av ett informationssystem. I artikel 3.13 anges att med informationssystem avses detsamma som framgår av definitionen i artikel 2 a i direktiv 2013/40.

Enligt den definitionen är ett informationssystem en apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program automatiskt behandlar datorbehandlingsbara uppgifter, samt datorbehandlingsbara uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av en apparat eller en grupp av apparater för att de ska kunna drivas, användas, skyddas och underhållas.

Brott som faller under punkten b i

Brott som faller under *punkten b i* är de brott som anges i artiklarna 3–8 i direktiv 2019/713. I direktivet slås fast minimiregler om fastställande av brottsrekvisit och påföljder inom områdena bedrägeri och förfalskning som rör andra betalningsmedel än kontanter (artikel 1).

Artikel 3 innehåller bestämmelser om bedräglig användning av icke-kontanta betalningsinstrument. I artiklarna 4 och 5 regleras brott med anknytning till bedräglig användning av fysiska respektive icke-fysiska icke-kontanta betalningsinstrument. Brott som rör bedrägeri med anknytning till informationssystem behandlas i artikel 6. Artikel 7 innehåller bestämmelser om verktyg som används för att begå brott. Artikel 8 anger i vilka fall anstiftan, medhjälp och försök till brott enligt direktivet ska vara straffbart.

För att möta direktivets kriminaliseringskrav i artiklarna 3–5, 7 och 8 har brotten olovlig befattning med betalningsverktyg och grov olovlig befattning med betalningsverktyg införts i 9 kap. 3 c § brottsbalken. Försök och förberedelse till dessa brott är kriminaliserade (9 kap. 11 § brottsbalken). I övrigt har regeringen ansett att direktivets kriminaliseringskrav motsvaras av bestämmelserna i brottsbalken om egenmäktigt förfarande (8 kap. 8 §), bedrägeri och förberedelse till bedrägeri (9 kap. 1 och 11 §§), häleri (9 kap. 6 §) och urkundsförfalskning (14 kap. 1 §).²⁷

²⁷ Prop. 2020/21:73 s. 8–28.

Brott som faller under punkten b ii

De brott som faller under punkten b ii följer av artiklarna 3–7 i direktiv 2019/713 om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi. I artikel 3 i direktivet behandlas frågan om vilka brott som har samband med sexuella övergrepp och som ska vara straffbara. Artikel 4 rör brott om sexuell exploatering. Artikel 5 behandlar brott som har samband med barnpornografi och artikel 6 behandlar brott som avser kontaktsökning med barn i sexuellt syfte. I artikel 7 stadgas ansvar för anstiftan, medhjälp och försök till brott enligt direktivet.

Vid genomförandet av direktivet ansågs kriminaliseringskraven i de angivna artiklarna uppfyllda genom befintliga straffbestämmelser i 4, 6 och 16 kap. brottsbalken. När det gäller 4 kap. rör det sig bl.a. om människohandel och olaga tvång (1 a och 4 §§). De brott i 6 och 16 kap. som lever upp till kriminaliseringskraven är bl.a. våldtäkt, våldtäkt mot barn, sexuellt utnyttjande av barn, sexuellt övergrepp mot barn, utnyttjande av barn för sexuell posering och köp av sexuell handling av barn samt barnpornografibrott (6 kap. 1, 4, 5, 6, 8 och 9 §§ samt 16 kap. 10 a §). För en fullständig redogörelse hänvisas till förarbetena.²⁸ Även det brott som vid genomförande av direktivet betecknades som sexuellt tvång ansågs genomföra direktivets krav på kriminalisering. Detta brott har ersatts av beteckningarna sexuellt övergrepp (6 kap. 2 §), men också oaktsamt sexuellt övergrepp (6 kap. 3 §).

Brott som faller under punkten b iii

De brott som faller under punkten b iii följer av artiklarna 3–8 i direktiv 2013/40 om angrepp mot informationssystem som anger de gärningar som ska vara straffbelagda enligt direktivet. Artikel 3 reglerar intrång i informationssystem. Enligt artikel 4 ska det vara straffbart att allvarligt hindra eller avbryta driften av ett informationssystem genom att bl.a. mata in, radera eller ändra datorbehandlingsbara uppgifter. Av artikel 5 följer att det ska vara straffbart att radera, skada eller ändra datorbehandlingsbara uppgifter i ett informationssystem. Enligt artikel 6 ska avlyssning med tekniska hjälp-

²⁸ Prop. 2012/13:194 s. 14 och Ds 2012:45 bilaga 2.

medel av icke-offentliga överföringar av datorbehandlingsbara uppgifter vara straffbelagda. Enligt artikel 7 ska det vara straffbart att tillverka, sälja eller anskaffa i syfte att använda vissa uppräknade verktyg om det sker orättmätigt och med uppsåt att begå något av de brott som avses i artiklarna 3–6. De verktyg som avses är datorprogram som utformats eller anpassats i första hand för att begå något av de brott som avses i artiklarna 3–6. I artikel 8 anges att anstiftan av och medhjälp till sådana gärningar som ska utgöra brott enligt direktivet ska straffbeläggas. Där anges även de gärningar för vilka försök ska vara straffbart, nämligen de i artiklarna 4 och 5.

Svensk rätt uppfyller kraven på vad som ska vara straffbelagt enligt direktivet främst genom straffbestämmelserna i brottsbalken om dataintrång och grovt dataintrång i 4 kap. 9 c § brottsbalken, men även brytande av post- eller telehemlighet (4 kap. 8 §), skadegörelse (12 kap. 1 §) och grov skadegörelse (12 kap. 3 §), sabotage (13 kap. 4 §) och grovt sabotage (13 kap. 5 §) samt genom bestämmelserna om försök och förberedelse till dessa brott.²⁹

Brott som faller under punkten c

Under punkten c faller de brott som följer av artiklarna 3–12 och 14 i direktiv 2017/541 om terroristbrott. Av artikel 3 följer ett krav på att medlemsstaterna kriminaliserar terroristbrott. Artikel 4 innebär ett krav på kriminalisering av brott med anknytning till en terroristgrupp. Enligt artikel 5 ska offentlig uppmaning till terroristbrott kriminaliseras. Rekrytering för terrorismsyften ska vara straffbart enligt artikel 6. Artiklarna 7 och 8 innebär ett krav på kriminalisering av tillhandahållande respektive mottagande av utbildning för terrorismsyfte. Ett krav på kriminalisering av resor respektive organiserande eller annat underlättande av resor för terrorismsyften följer av artiklarna 9 och 10. Enligt artikel 11 ska finansiering av terrorism kriminaliseras. Artikel 12 innehåller en uppräknad av vissa gärningar som anses vara särskilt frekventa i samband med utförandet av terroristbrott, som medlemsstaterna under vissa förutsättningar ska betrakta som brott med anknytning

²⁹ Prop. 2013/14:92 s. 11–13.

till terroristverksamhet. Artikel 14 anger i vilka fall medhjälp, anstiftan och försök ska kriminaliseras.

Direktivets krav på kriminalisering av de angivna gärningarna genomfördes – i den mån gärningarna inte redan var straffbelagda i svensk rätt – genom ändringar i de då gällande lagarna (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, (2003:148) om straff för terroristbrott och (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet.³⁰

Sedan den 1 juli 2022 är de tre nämnda lagarna upphävda och ersatta av terroristbrottslagen (2022:666). Terroristbrottslagen reglerar straffansvar för terroristbrott (4 §) och samröre med en terroristorganisation (5 §). Vidare regleras ett straffansvar för, finansiering, offentlig uppmaning, rekrytering, utbildning samt resa för terrorism eller särskilt allvarlig brottslighet (6–10 §§). Straffansvar för försök, förberedelse och stämpling regleras i 11 §. Även deltagande i en terroristorganisation är sedan den 1 juni 2023 straffbelagt i lagen (4 a §). Behovet av ett deltagandebrott var dock inte föranlett av terrorismdirektivets kriminaliseringskrav.³¹

Övriga bestämmelser i artikel 5

I artikel 5.5 anges närmare vilken information som en europeisk utfärdandeorder ska innehålla (punkterna a–j). Det rör sig bl.a. om uppgifter om den utfärdande myndigheten och i förekommande fall den godkännande myndigheten samt orderns mottagare. Utlämnandeordern ska innehålla uppgifter om användaren, utom i de fall syftet med ordern är att identifiera användaren, de uppgifter som begärs ut och, om tillämpligt, tidsintervallet för dessa uppgifter. Vidare ska anges tillämpliga bestämmelserna i den utfärdande statens straffrätt, skälen till att utlämnandeordern uppfyller villkoren för att vara nödvändig och proportionell samt en kortfattad beskrivning av ärendet. I intyget om en europeisk utlämnandeorder anges detaljerat vilka uppgifter som ska anges (se bilaga I till EU-förordningen).

³⁰ Se prop. 2017/18:174.

³¹ Prop. 2022/23:73 s. 33.

Enligt artikel 5.6 ska en utlämnandeorder i normalfallet riktas till den tjänsteleverantör som agerar som personuppgiftsansvarig enligt EU:s dataskyddsförordning³². En personuppgiftsansvarig definieras i artikel 4.7 i dataskyddsförordningen som en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt. I undantagsfall får ordern riktas direkt till den tjänsteleverantör som lagrar eller på annat sätt behandlar uppgifterna på den personuppgiftsansvariges vägnar, om den personuppgiftsansvarige inte kan identifieras trots att rimliga ansträngningar gjorts från den utfärdande myndighetens sida, eller det kan vara till skada för utredningen att rikta sig till den personuppgiftsansvarige (se även skäl 42). Att sistnämnda villkor är uppfyllda ska anges i utlämnandeordern (artikel 5.5 h). Bestämmelsen i artikel 5.6 syftar till att klargöra till vilken tjänsteleverantör en europeisk utlämnande- eller bevarandeorder ska ställas till. När tjänsteleverantören väl är identifierad ska orden enligt huvudregeln i artikel 7 sändas över till det utsedda verksamhetsstället eller rättsliga ombudet.

Det personuppgiftsbiträde som lagrar eller på annat sätt behandlar uppgifterna på den personuppgiftsansvariges vägnar i enlighet med dataskyddsförordningens bestämmelser ska enligt artikel 5.7 informera den personuppgiftsansvarige om utlämnandet av uppgifterna, såvida inte den utfärdande myndigheten har begärt att tjänsteleverantören ska avstå från att informera den personuppgiftsansvarige, under så lång tid som det är nödvändigt och proportionellt, för att inte hindra de straffrättsliga förfarandena i fråga (se även skäl 43). I sådant fall ska den utfärdande myndigheten i ärendet ange skälen till fördröjningen med att informera den personuppgiftsansvarige. En kort motivering ska också läggas till i intyget om en europeisk utlämnandeorder.

³² 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).

Om uppgifterna lagras eller på annat sätt behandlas som en del av en infrastruktur som en tjänsteleverantör tillhandahåller en offentlig myndighet, får en utlämnandeorder enligt artikel 5.8 utfärdas endast om den offentliga myndighet för vilken uppgifterna lagras eller på annat sätt behandlas är belägen i den utfärdande staten.

I de fall där uppgifter som omfattas av sekretess eller tystnadsplikt enligt den utfärdande statens rätt lagras eller på annat sätt behandlas av en tjänsteleverantör som en del av en infrastruktur som tillhandahålls yrkesutövare som omfattas av sekretess eller tystnadsplikt inom ramen för deras verksamhet, får enligt artikel 5.9 en europeisk utlämnandeorder för att inhämta trafikuppgifter eller innehållsdata utfärdas endast om

- den yrkesutövare som omfattas av sekretess eller tystnadsplikt är bosatt i den utfärdande staten,
- det kan vara till skada för utredningen att rikta sig till den yrkesutövare som omfattas av sekretess eller tystnadsplikt, eller
- undantag gjorts från sekretessen eller tystnadsplikten i enlighet med tillämplig rätt.

Om den utfärdande myndigheten har skäl att anta att de trafikuppgifter eller innehållsdata som begärts genom en europeisk utlämnandeorder skyddas av immunitet eller privilegier som beviljas enligt den verkställande statens rätt, eller att dessa uppgifter omfattas av den statens regler om fastställande och begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet eller yttrandefrihet i andra medier, får den utfärdande myndigheten enligt första stycket i artikel 5.10 söka klagöranden före utfärdandet av ordern (se även skälen 47 och 48). En europeisk utlämnandeorder får enligt andra stycket i nämnda artikel inte utfärdas om den utfärdande myndigheten anser att de begärda uppgifterna skyddas på det sätt som anges i första stycket.

6.3.3 Villkoren för utfärdande av en europeisk bevarandeorder

Artikel 6 anger villkoren för utfärdande av en europeisk bevarandeorder. En utfärdande myndighet får enligt artikel 6.1 utfärda en bevarandeorder endast om de villkor som anges i artikeln är uppfyllda (se även skäl 39). Artikel 5.8 ska gälla i tillämpliga delar.

En europeisk bevarandeorder ska enligt artikel 6.2 vara nödvändig och proportionell för ändamålet att förhindra avlägsnande, radering eller ändring av uppgifter i avvaktan på en efterföljande framställan om utlämnande av dessa uppgifter via ömsesidig rättslig hjälp, en europeisk utredningsorder eller en europeisk utlämnandeorder, med beaktande av den misstänkta eller tilltalade personens rättigheter.

Av artikel 6.3 följer att en europeisk bevarandeorder får utfärdas för alla brott, om den skulle kunna ha utfärdats på samma villkor i ett liknande inhemskt ärende, och för verkställighet av en frihetsberövande påföljd om minst fyra månader.

Den information en europeisk bevarandeorder ska innehålla enligt artikel 6.4 motsvarar i huvudsak den information som en europeisk utlämnandeorder ska innehålla, men med vissa undantag. I intyget om en europeisk bevarandeorder anges närmare vilka uppgifter som ska lämnas (se bilaga II till EU-förordningen).

6.4 Allmänna utgångspunkter för våra överväganden och förslag

Som utvecklats i avsnitt 5.2 får en EU-förordning inte införlivas i eller transformeras till nationell rätt. Något genomförande av en EU-förordning ska således inte ske. En EU-förordning får inte heller, om det inte särskilt anges, fyllas ut eller kompletteras med mer detaljerade regler inom samma område. En medlemsstat får vidare inte utfärda föreskrifter om hur en EU-förordning ska tolkas. Särskilda nationella bestämmelser får dock finnas för sådana frågor som faller utanför det område som EU-förordningen reglerar men som kräver en nationell författningsreglering.

Utgångspunkten är alltså att de villkor som ställs upp för att utfärda en europeisk utlämnande- eller bevarandeorder uteslutande regleras i förordningen. Det är således inte möjligt att i nationell

rätt införa kompletterande bestämmelser om t.ex. under vilka förutsättningar en sådan order får utfärdas, eftersom detta följer direkt av EU-förordningen. Däremot kan det finnas ett behov av att komplettera nationella bestämmelser på området för att säkerställa att svenska myndigheter kan använda sig av de instrument som EU-förordningen omfattar.

I de följande avsnitten återfinns våra överväganden och förslag. Först övervägs om huruvida några kompletterande bestämmelser behövs när det gäller frågan om vilka tjänsteleverantörer som ska omfattas av samarbetet enligt förordningen (se avsnitt 6.5). I det avsnittet redogörs vidare för den rättsliga grunden att lämna ut uppgifter enligt EU-förordningen. Vidare berörs frågan om lagrings-skyldighet och utlämnande av uppgifter för tjänsteleverantörer i Sverige. Avsnitt 6.5 är främst inriktat på de fall då Sverige är den verkställande staten, dvs. då en order utfärdats gentemot en tjänsteleverantör i Sverige.

I avsnitt 6.6 analyseras innebörden av begreppet straffrättsliga förfaranden i artikel 2.1 i EU-förordningen i syfte att se vid vilka tidpunkter i en svensk brottmålsprocess som en europeisk utlämnande- eller bevarandeorder kan utfärdas. I avsnitt 6.7 redogörs för lagrings- och anpassningsskyldigheten i lagen om elektronisk kommunikation för att se om det finns behov av ändringar med anledning av EU-förordningen. I de efterföljande avsnitten övervägs om det behövs några ändringar i lagen om elektronisk kommunikation, brottsbalken, rättegångsbalken eller annan lag för att svenska myndigheter ska kunna utfärda en europeisk utlämnande- eller bevarandeorder i den omfattning som EU-förordningen tillhandahåller (avsnitten 6.8–6.12). Avsnitten 6.7–6.12 avser det förhållandet att Sverige är utfärdande stat i fråga om en europeisk utlämnande- respektive bevarandeorder.

6.5 Kretsen av tjänsteleverantörer och skyldigheten att lämna ut uppgifter följer direkt av EU-förordningen

6.5.1 Kompletteringar i svensk lag behövs inte i fråga om kretsen av tjänsteleverantörer

Bedömning: Några kompletterande bestämmelser behövs inte i svensk lag angående EU-förordningens bestämmelser om vilka tjänsteleverantörer som omfattas av förordningen.

Skälen för bedömningen: I artikel 3.3 i EU-förordningen finns bestämmelser om vilka tjänsteleverantörer som omfattas av förordningens tillämpningsområde. Vilka dessa tjänsteleverantörer det rör sig om redogörs för utförligt i avsnitt 6.2.

Som konstaterats i avsnitt 5.2 får en EU-förordning inte, om det inte särskilt anges, fyllas ut eller kompletteras med mer detaljerade regler inom samma område. Omfattningen av vilka tjänsteleverantörer som avses i EU-förordningen kan med denna utgångspunkt varken begränsas eller utökas i svensk lag utan denna fråga styrs helt av EU-förordningen och dess status som direkt tillämplig i Sverige.

Det finns därför inte några behov att i nationell rätt införa kompletterande bestämmelser som utvidgar eller begränsar avseende vilka tjänsteleverantörer som omfattas av EU-förordningen.

6.5.2 Den rättsliga grunden för utlämnande av uppgifter följer direkt av EU-förordningen

Bedömning: Den rättsliga grunden för utlämnande eller bevarande av abonnentuppgifter, andra användaruppgifter, trafikuppgifter och innehållsdata följer direkt av EU-förordningen. Tjänsteleverantörer samt utsedda verksamhetsställen och rättsliga ombud ska vidare följa de skyldigheter som åvilar dem enligt de bestämmelser som följer direkt av EU-förordningen, utan att det behövs några kompletterande bestämmelser i svensk lag.

Svenska tjänsteleverantörernas skyldighet att lämna ut uppgifter till behörig myndighet i annan medlemsstat gäller oaktat

att andra förutsättningar för att lämna ut motsvarande uppgifter tillämpas i andra medlemsstater eller på vilka grunder de svenska tjänsteleverantörerna har lagrat uppgifterna.

Skälen för bedömningen

Den rättsliga grunden för utlämnande av uppgifter och andra skyldigheter

Den rättsliga grunden för att ett utsett verksamhetsställe eller rättsligt ombud i Sverige ska lämna ut eller bevara abonnentuppgifter, andra användaruppgifter, trafikuppgifter och innehållsdata följer direkt av artikel 10 och 11 i EU-förordningen. Av det skälet finns det inget behov att i svensk lag föreskriva att ett utlämnande eller bevarande av de aktuella uppgifterna kan eller ska ske med stöd av EU-förordningen, t.ex. genom ett tillägg i lagen om elektronisk kommunikation.

I EU-förordningen regleras vissa andra frågor som ett utsett verksamhetsställe eller ett rättsligt ombud har att förhålla sig till. Det gäller framför allt andra skyldigheter som följer av artiklarna 10 och 11, t.ex. skyldigheten att skyndsamt bevara uppgifter som ska lämnas ut, att lämna ut uppgifterna inom vissa tidsfrister, att bevara uppgifterna under en viss tid och att informera den utfärdande myndigheten när det finns hinder mot att lämna ut eller bevara uppgifterna (se avsnitt 3.6.1). Det ska också noteras att ett utsett verksamhetsställe eller rättsligt ombud kan med stöd av artiklarna 10.5 och 11.4 informera den utfärdande och verkställande myndigheten om ett utlämnande eller bevarande skulle bl.a. inskränka på regler om fastställande eller begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet eller yttrandefrihet i andra medier enligt den verkställande staten rätt.

I detta sammanhang kan även bestämmelserna i artikel 13 tas som exempel på bestämmelser som är direkt tillämpliga för en tjänsteleverantör. Artikeln innehåller bestämmelser om användarinformation och sekretess och riktar sig, utöver till den utfärdande myndigheten, även till tjänsteleverantören. Av artikel 13.4 följer att mottagarna av en order och, om de inte är desamma, tjänsteleverantörerna omfattas av ett krav på tystnadsplikt vad gäller ordern och de uppgifter som lämnas ut eller bevaras. Ett ytterligare exempel

är bestämmelserna i artikel 17 om invändning om lagkonflikt. Artikel 17.2 reglerar hur en mottagare av en europeisk utlämnandeorder ska agera om den anser att ordern strider mot en skyldighet enligt ett tredjelands tillämpliga rätt (se även avsnitt 3.9 och 7.4).

De nämnda skyldigheterna regleras alltså direkt i EU-förordningen och ska därför inte, som utvecklats i avsnitt 5.2, regleras i svensk lag.

Skyldigheten att lämna ut uppgifter gäller även om andra förutsättningar gäller i medlemsstaterna

EU-förordningens bestämmelser innebär, utöver att svenska behöriga myndigheter kan utfärda en europeisk utlämnande- eller bevarandeorder gentemot en tjänsteleverantör i en annan medlemsstat, att en motsvarande order kan riktas mot en tjänsteleverantör i Sverige. Samma förutsättningar gäller även i ett sådant fall, dvs. att en liknande order ska vara möjlig att utfärda i ett inhemskt ärende i den medlemsstat vars behöriga myndighet har utfärdat ordern. En utfärdad order kan endast avse sådana uppgifter som finns lagrade hos den tjänsteleverantör som avses med ordern.

I förhållande till vissa av de tjänsteleverantörer i Sverige som omfattas artikel 3.3 i EU-förordningen gäller lagen om elektronisk kommunikation och den lagringsskyldighet som följer av 9 kap. 19 § i nämnda lag. I 2021 års datalagringsutredning har föreslagits en mer långtgående lagringsskyldighet; geografiskt riktad lagring, utökad riktad lagring och nationell säkerhetslagring. Förslaget beskrivs närmare i avsnitt 4.2.6. Därutöver lagras tjänsteleverantörers uppgifter för egna syften.

Mot dessa svenska tjänsteleverantörer kan beslut om hemliga tvångsmedel riktas för att brottsbekämpande myndigheter ska få ta del av sådana uppgifter som omfattas av begreppet elektronisk bevisning i EU-förordningen. I avsnitt 6.10 redogörs för den nationella regleringen i fråga om användning av hemliga tvångsmedel i detta avseende. Som följer av den redogörelsen är det endast vid förundersökning om brott av viss svårhetsgrad som det kan komma i fråga att använda hemliga tvångsmedel såsom hemlig avlyssning respektive hemlig övervakning av elektronisk kommunikation. Det ska vara fråga om brott med ett visst minimistraff eller vissa i lagtexten angivna brott.

Det får förutsättas att motsvarande reglering i andra medlemsstater ser annorlunda ut och sådana åtgärder som motsvaras av en europeisk utlämnandeorder för inhämtning av trafikuppgifter och innehållsdata kan komma i fråga för mindre allvarliga brott än vad som gäller vid motsvarande användning av hemliga tvångsmedel i Sverige. Detta innebär att tjänsteleverantörer i Sverige kan komma att vara tvungna att lämna ut lagrade trafikuppgifter respektive innehållsdata till behörig myndighet i annan medlemsstat vid förundersökning om sådana brott som inte omfattas av de svenska reglerna om hemliga tvångsmedel och som således inte skulle lämnas ut i en svensk förundersökning för samma brott.

EU-förordningen innebär emellertid ingen harmonisering om under vilka förutsättningar dessa uppgifter kan hämtas in under ett straffrättsligt förfarande och gör inte heller någon skillnad på vilken grund uppgifterna har lagrats för att de ska lämnas ut. Det innebär att de svenska tjänsteleverantörernas skyldighet att lämna ut uppgifter till behörig myndighet i annan medlemsstat inte är avhängig av om uppgifterna har lagrats för att möjliggöra användning av hemliga tvångsmedel enligt svensk rätt.

Den beskrivna asymmetrin är en följd av att lagstiftningen i de olika medlemsstaterna kan skilja sig i fråga om dels under vilka omständigheter sådana åtgärder som motsvaras av en europeisk utlämnandeorder för inhämtning av trafikuppgifter respektive innehållsdata kan komma i fråga, dels vilka uppgifter tjänsteleverantörerna är skyldiga att lagra. Leverantörerna är dock inte under några omständigheter skyldiga att lämna ut uppgifter som inte finns lagrade vid tidpunkten när den utfärdade ordern tas emot (se avsnitt 6.3.1 ovan). Därutöver ska påpekas att en europeisk utlämnandeorder får endast utfärdas om förutsättningarna enligt EU-förordningen är uppfyllda.

Det ska dock poängteras att det omvända också gäller, dvs. utländska tjänsteleverantörer är skyldiga att lämna ut uppgifter till svenska brottsbekämpande myndigheter även om motsvarande uppgifter inte skulle kunnat ha lämnats ut till en myndighet i den stat där tjänsteleverantören finns.

6.6 Straffrättsliga förfaranden enligt EU-förordningen

Bedömning: Några kompletterande bestämmelser i svensk lag behövs inte med hänsyn till begreppet straffrättsligt förfarande i EU-förordningen.

Skälen för bedömningen: En europeisk utlämnande- eller bevarandeorder får enligt artikel 2.1 i EU-förordningen endast utfärdas inom ramen för straffrättsliga förfaranden och för verkställighet av frihetsberövande påföljd om minst fyra månader som har beslutats till följd av ett straffrättsligt förfarande.

Vad som avses med straffrättsliga förfaranden anges inte närmare i EU-förordningen. Eftersom begreppet inte hänvisar till nationell rätt följer det av EU-domstolens fasta praxis att sådana ska ges en självständig unionsrättslig tolkning. Även om begreppet förekommer i andra EU-rättsakter ska den närmare innebörden av begreppet avgöras i förhållande till den rättsakt där begreppet förekommer. EU-domstolen är också den instans som avgör det närmare innebörden av unionsrättsliga begrepp. Även om begreppet straffrättsliga förfaranden är ett EU-autonomt begrepp finns det skäl att närmare analysera när en europeisk utlämnande- eller bevarandeorder kan utfärdas i Sverige.

När det gäller begreppet straffrättsliga förfaranden i EU-förordningen kan inledningsvis konstateras att ett sådant förfarande har en början och ett slut.

I EU-förordningen ges ingen närmare ledning om när ett straffrättsligt förfarande har sin början. Vid genomförandet av direktivet om en europeisk utredningsorder som i artikel 4 använder sig av samma begrepp, har tidpunkten för när ett straffrättsligt förfarande ansetts inträffa då en förundersökning inleds enligt 23 kap. 1 § rättegångsbalken.³³ Vi gör också den bedömningen att den utredning som sker före en förundersökning inte torde omfattas av begreppet straffrättsliga förfaranden. Brottsbekämpande myndigheters underrättelseverksamhet får därför anses falla utanför EU-förordningens tillämpningsområde (se även skäl 24 som anger att straffrättsliga förfaranden avser ett specifikt brott). Artikel 4 som innehåller bestämmelser om vilka myndigheter som får utfärda en

³³ Se prop. 2016/17:218 s. 73. Se även prop. 2012/13:132 s. 15 och SOU 2012:49 s. 49–50.

europaisk utlämnande- eller bevarandeorder indikerar också en sådan begränsning. Informationsutbyte som sker på ett tidigare stadium får exempelvis hanteras via det internationella polisiära samarbetet.³⁴

En snävare tolkning, t.ex. att ett straffrättsligt förfarande förutsätter att ett åtal har väckts, anser vi – å andra sidan – inte vara avsedd eftersom EU-förordningens tillämpningsområde då skulle begränsas avsevärt. Tvärtom syftar EU-förordningen till att inrätta effektiva förfaranden för inhämtande och bevarande av elektroniska bevis i brottsutredningar och åtal (se skäl 2) vilket bör innefatta även brottsutredningar i tiden före det att åtal väcks.

Ett straffrättsligt förfarande har som nämnts ett slut, vilket som huvudregel bör kunna tolkas som den tidpunkt då en meddelad dom eller meddelat slutligt beslut har fått laga kraft. Detsamma får anses gälla om förundersökningen läggs ned eller om den avslutas med att åtal inte väcks. En särskild fråga är dock om en europeisk utlämnande- eller bevarandeorder skulle kunna utfärdas vid användande av särskilda rättsmedel, trots att det finns en dom som fått laga kraft. Tillämpligheten av EU-förordningen är inte uttryckligen begränsad till en viss tidpunkt när det straffrättsliga förfarandet är avslutat. Avgörande bör i stället vara att det förfarande som tillämpas är ett straffrättsligt förfarande avseende en specifik gärning. En rimlig slutsats är därför att en europeisk utlämnande- eller bevarandeorder bör kunna utfärdas i samband med ett förfarande om resning. I ett sådant förfarande kan det bli aktuellt för en åklagare att vidta kompletterande åtgärder (se 58 kap. 6 a och 6 b §§ rättegångsbalken). När det däremot gäller en ansökan om återställande av försutten tid eller klagan över domvillan torde motsvarande åtgärder inte bli aktuella.³⁵

EU-förordningen innehåller inte några krav på att det straffrättsliga förfarandet ska kunna leda till ett visst resultat, t.ex. att en brottspåföljd döms ut. Straffrättsliga förfaranden som leder till andra följder av brott bör också omfattas av EU-förordningens tillämpningsområde, under förutsättning att förfarandet grundar sig på en straffbar gärning. I svensk rätt finns också andra författningsreglerade följder av brott än brottspåföljder. Av 1 kap. 8 § brottsbalken framgår att förutom en påföljd kan brott föranleda

³⁴ 2016/17:218 s. 73.

³⁵ Se prop. 2016/17:218 s. 74.

förverkande av egendom, företagsbot eller annan särskild rättsverkan. Förfaranden avseende dessa andra reglerade följder av brott bör anses omfattas av EU-förordningens tillämpningsområde under förutsättning att den rättsverkan som avses hanteras enligt reglerna om förundersökning och rättegång i brottmål.

En europeisk utlämnande- eller bevarandeorder bör således enligt vår mening kunna utfärdas i Sverige från det att en förundersökning inleds till dess det finns en dom eller slutligt beslut som har fått laga kraft. Detsamma gäller om förundersökningen läggs ned eller om den avslutas med att åtal inte väcks. Vidare bör en sådan order kunna utfärdas i samband med ett resningsförfarande. Vilken svensk myndighet som leder förundersökning påverkar inte vår bedömning, även om artikel 4 kräver att en domare, domstol, undersökningsdomare eller åklagare godkänner en europeisk utlämnande- eller bevarandeorder som har utfärdats av en annan myndighet.

I sammanhanget bör dock framhållas att EU-förordningen är begränsad till åtgärder som avser inhämtning av elektronisk bevisning direkt från den tjänsteleverantör som lagrat uppgiften i fråga. Ett beslut under ett straffrättsligt förfarande ska alltså innebära att en utredningsåtgärd vidtas i syfte att hämta in sådan bevisning. Åtgärder för ett annat syfte eller som riktas mot en annan aktör än en sådan tjänsteleverantör som avses i EU-förordningen faller utanför förordningens tillämpningsområde.

Sammanfattningsvis anser vi att några kompletterande bestämmelser i svensk lag inte behövs med anledning av begreppet straffrättsligt förfarande i EU-förordningen.

6.7 Elektronisk bevisning kan inhämtas hos de tjänsteleverantörer som omfattas av EU-förordningen

Bedömning: Svensk rätt gör det möjligt för brottsbekämpande myndigheter att i ett inhemskt ärende hämta in elektronisk bevisning från de tjänsteleverantörer som omfattas av artikel 3.3 i EU-förordningen. Några behov finns inte att ändra i bestämmelserna om lagrings- och anpassningsskyldigheten i lagen om elektronisk kommunikation. Inte heller finns behov av andra kompletterande bestämmelser för att svenska brottsbekämpande myndigheter ska kunna hämta in uppgifter om elektronisk bevisning.

Skälen för bedömningen

Utgångspunkter i EU-förordningen

En europeisk utlämnandeorder får enligt artikel 5.2 i EU-förordningen endast utfärdas om en liknande order skulle ha kunnat utfärdas på samma villkor i ett liknande inhemskt ärende. En medlemsstat ska således inte kunna använda sig av en europeisk utlämnandeorder på ett sätt som inte överensstämmer med nationell rätt.

Frågan är därför om svensk rätt ger våra brottsbekämpande myndigheter motsvarande möjlighet till att hämta in elektronisk bevisning på sätt som begreppet definieras i EU-förordningen, dvs. abonnentuppgifter, trafikuppgifter eller innehållsdata, vilket inkluderar andra användaruppgifter, som lagras i elektronisk form av en tjänsteleverantör eller på en tjänsteleverantörs vägnar. I detta avsnitt övervägs möjligheterna att *över huvud taget* inhämta elektronisk bevisning som finns hos de tjänsteleverantörer som omfattas av artikel 3.3. I avsnitten 6.8–6.11 övervägs närmare om de närmare villkoren som ställs upp i svensk rätt för att inhämta de olika typer av uppgifter är i överensstämmelse med EU-förordningen.

Ett första steg är att analysera om svensk rätt medger att en motsvarande order utfärdas i ett nationellt ärende, dvs. genom den uppgiftsskyldighet som föreskrivs i lagen om elektronisk kommunikation för vissa tjänsteleverantörer eller genom användning av

tvångsmedel eller andra åtgärder gentemot övriga tjänsteleverantörer som omfattas av EU-förordningen.

Den nationella regleringen och vilka leverantörer som omfattas

Av 9 kap. 19 § lagen om elektronisk kommunikation följer att den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § ska lagra uppgifter om abonnemang samt trafikuppgifter för brottsbekämpande ändamål. Enligt 2 kap. 1 § gäller anmälningsplikten för den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst (se även avsnitt 4.2.4).

Vidare är anpassningsskyldigheten i 9 kap. 29 § lagen om elektronisk kommunikation av central betydelse. Den tjänsteleverantör som omfattas av den bestämmelsen är skyldig att bedriva sin verksamhet på så sätt att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs. Vidare är dessa tjänsteleverantörer skyldiga enligt 9 kap. 33 § att lämna ut abonnentuppgifter.

I avsnitt 6.2 redogörs för vilka tjänsteleverantörer som enligt artikel 3.3 omfattas av EU-förordningens bestämmelser.

Flertalet, men inte alla, tjänsteleverantörer som avses i artikel 3.3 a i EU-förordningen omfattas också av lagen om elektronisk kommunikation. Dessa är enligt nämnda bestämmelser i lagen om elektronisk kommunikation skyldiga att bistå de brottsutredande myndigheterna. Det finns dock andra tjänsteleverantörer som inte omfattas av nämnda lags bestämmelser.

Leverantörer av tjänster för internetdomännamn och IP-numrering (artikel 3.3 b) samt leverantörer av andra av informationssamhällets tjänster enligt artikel 1.1 b i direktiv 2015/1535 (artikel 3.3 c i EU-förordningen) tillhandahåller vare sig ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och är därmed inte anmälningskyldiga enligt 2 kap. 1 § lagen om elektronisk kommunikation. De omfattas således inte av lagringsskyldigheten enligt 9 kap. 19 § lagen om elektronisk kommunikation. Inte heller omfattas de av anpassnings- och uppgiftsskyldigheten enligt 9 kap. 29 och 33 §.

Vidare omfattas inte heller samtliga tjänsteleverantörer som tillhandahåller elektroniska kommunikationstjänster enligt definitionen i artikel 2.4 i direktiv 2018/1972 (artikel 3.3 a i EU-förordningen) av skyldigheterna i lagen om elektronisk kommunikation. Tillhandahållare av Noik faller under artikel 3.3 a men är inte anmälningsskyldiga enligt 2 kap. 1 § lagen om elektronisk kommunikation, varför dessa aktörer är undantagna de krav som följer av nämnda lag.

I fråga om de leverantörer som faller under artikel 3.3 b sker inhämtning i Sverige av uppgifter hänförliga till domännamn genom Internetstiftelsen och det register denna aktör är skyldig att föra över domännamn (mer om inhämtning av sådana uppgifter, se avsnitt 6.8 nedan).

I vilken omfattning information kan inhämtas från en tillhandahållare av Noik i nuläget har behandlats av 2021 års datalagringsutredning som har konstaterat följande³⁶:

De brottsbekämpande myndigheterna kan i vissa fall komma åt uppgifter om elektronisk kommunikation hos tillhandahållare av Noik genom användning av olika straffprocessuella tvångsmedel, såsom husrannsakan med efterföljande beslag. Möjligheten för myndigheterna att på egen hand hitta den eftersökta informationen vid en husrannsakan i exempelvis stora serverhallar är dock mycket begränsad. De brottsbekämpande myndigheterna kan också komma åt uppgifter om elektronisk kommunikation genom tvångsmedlet genomsökning på distans (28 kap. 10 a § RB). Vid en sådan genomsökning får handlingar eftersökas i ett avläsningsbart informationssystem utanför den elektroniska kommunikationsutrustning som används för att utföra genomsökningen. Det kan röra sig om handlingar som finns lagrade på t.ex. externa servrar eller i molntjänster. Detta får dock bara ske genom autentisering eller inloggning i det system åtgärden avser. Det är vid genomsökning på distans nämligen inte tillåtet för myndigheterna att komma åt information genom att utnyttja sårbarheter i informationssystemet.

I teorin kan vidare de brottsbekämpande myndigheter redan i dag komma åt uppgifterna genom att få tillstånd till HÖK hos en tillhandahållare av Noik, eftersom regleringen i 27 kap. 19 § RB är teknikneutral. Tillhandahållarna omfattas dock inte av någon anpassningskyldighet. Möjligheten för de brottsbekämpande myndigheterna att få del av uppgifterna beror alltså i dessa fall till stor del på om tillhandahållaren vill samarbeta med myndigheterna.

Myndigheterna kan också i vissa fall komma åt uppgifter om elektronisk kommunikation som avser kommunikation via Noik genom

³⁶ SOU 2023:22 s. 346–347.

hemlig dataavläsning. Hemlig dataavläsning medför dock ett förhållandevis stort integritetsintrång. För att inhämta kommunikationsövervaknings- eller platsuppgifter får åtgärden vidare användas endast om den är av synnerlig vikt antingen för utredningen av allvarliga brott eller för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som innefattar allvarliga brott. Tillhandahållarna av Noik har inte heller någon skyldighet att medverka i samband med verkställigheten av hemlig dataavläsning och har inte heller tystnadsplikt som teleoperatörerna har enligt lagen om hemlig dataavläsning.

[...]

Det finns visserligen en möjlighet att förelägga den som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för utredningen om ett brott att bevara uppgiften (s.k. bevarandeföreläggande, 27 kap. 16 § RB). Ett sådant föreläggande kan riktas mot en tillhandahållare av Noik. Men skyldigheten i 9 kap. 33 § 5 nya LEK på begäran lämna ut uppgifter till brottsbekämpande myndigheter om vilka övriga tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster som har deltagit vid överföringen av ett meddelande som omfattas av ett bevarandeföreläggande gäller inte för tillhandahållare av Noik.

När det gäller de tjänsteleverantörer som faller inom EU-förordningens tillämpningsområde (artikel 3.3) men inte omfattas av de aktuella skyldigheterna i lagen om elektronisk kommunikation är det alltså ändå möjligt att rikta ett beslut om tvångsmedel mot dem, t.ex. husrannsakan och beslag eller hemliga tvångsmedel (se dock ovan angående uppgifter från Internetstiftelsen). Eftersom de inte omfattas av lagringsskyldigheten enligt lagen om elektronisk kommunikation är det dock inte säkert att de efterfrågade uppgifterna finns kvar hos leverantören, utan endast de uppgifter som leverantören av någon anledning har kvar är möjliga att inhämta. Det kan vidare vara förenat med praktiska svårigheter att sammanställa och utnyttja uppgifterna. Om leverantören tillhandahåller inbyggda funktioner som utför kryptering och saknar möjlighet att dekryptera meddelanden som förmedlas, innebär avsaknaden av anpassningsskyldighet att uppgifterna kommer att överlämnas i krypterad form, vilket i princip innebär att informationen är oåtkomlig för de brottsbekämpande myndigheterna. Möjligheten för myndigheterna att få del av uppgifterna beror då till stor del på om leverantören är villig att samarbeta med dem.³⁷

³⁷ Se t.ex. SOU 2023:22 s. 407.

2021 års datalagringsutredning och dess förslag

2021 års datalagringsutredning har lämnat förslag som innebär att även leverantörer av Noik ska omfattas av lagrings- respektive anpassningsskyldigheten i lagen om elektronisk kommunikation (se avsnitt 4.2.6). Utredningen har vidare föreslagit att dessa leverantörer ska omfattas av skyldigheten att lämna ut uppgifter om abonnemang enligt 9 kap. 33 § första stycket 2, vilket vi återkommer till i följande avsnitt. Vidare har utredningen lämnat förslag om en utökad lagringsskyldighet, som beskrivs i avsnitt 4.2.6.

Det finns inte skäl att utvidga lagen om elektronisk kommunikation till att omfatta samtliga leverantörer

Det finns enligt vår mening inte skäl att föreslå ändringar i regelverket i syfte att låta samtliga leverantörer som faller inom EU-förordningens tillämpningsområde omfattas av de aktuella skyldigheterna i lagen om elektronisk kommunikation. Som konstaterats ovan anses de tjänsteleverantörer som anges i artikel 3.3 b och c inte tillhandahålla vare sig ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, vilket gör att av rent systematiska skäl blir det svårt att utvidga lagen om elektronisk kommunikation till att omfatta dessa tjänsteleverantörer.

Lagrings- respektive anpassningsskyldigheten i lagen om elektronisk kommunikation har vidare varit föremål för en grundlig översyn genom 2021 års datalagringsutredning, som föreslagit att leverantörer av Noik ska omfattas av de nämnda bestämmelserna i lagen om elektronisk kommunikation (se avsnitt 4.2.6). Blir detta förslag verklighet kommer det alltså att vara enklare än i dag att inhämta information från dessa aktörer genom bestämmelserna i lagen om elektronisk kommunikation respektive i rättegångsbalken om hemliga tvångsmedel.

Det ska dock konstateras, som behandlats ovan, att de tvångsmedel som återfinns i bl.a. rättegångsbalken är tillämpliga mot sådana leverantörer som i dag inte omfattas av de nämnda skyldigheterna i lagen om elektronisk kommunikation eftersom bestämmelserna i rättegångsbalken är teknikneutrala. Vi menar således att t.ex. åklagaren kan besluta om tvångsmedel gentemot en sådan leverantör som innebär att uppgifter ska lämnas ut, vilket får anses

vara i överensstämmelse med kravet i artikel 5.2 om att motsvarande uppgifter ska kunna hämtas in i ett inhemskt ärende. En annan sak är dock om uppgifterna finns kvar, men det är inget krav enligt EU-förordningen för att kunna utfärda en europeisk utlämnandeorder. Vidare kan de uppgifter som artikel 3.3 b åsyftar inhämtas från Internetstiftelsen.

Sammanfattningsvis anser vi att svensk rätt gör det möjligt att i ett inhemskt ärende hämta in elektronisk bevisning från de tjänsteleverantörer som omfattas av artikel 3.3. Det är därför som en allmän utgångspunkt möjligt för svenska behöriga myndigheter att utfärda en europeisk utlämnandeorder i fråga om sådan bevisning som omfattas av EU-förordningen. Vi ser vidare inga skäl att ändra bestämmelserna om lagrings- och anpassningsskyldigheten i lagen om elektronisk kommunikation. Inte heller anser vi att några andra kompletterande bestämmelser behövs för att svenska brottsbekämpande myndigheter ska kunna hämta in uppgifter.

6.8 Utfärdande av en europeisk utlämnandeorder för att inhämta abonnentuppgifter eller andra användaruppgifter

Bedömning: Det behövs inte några kompletterande nationella bestämmelser för att det ska vara möjligt för en svensk behörig myndighet att utfärda en europeisk utlämnandeorder i syfte att inhämta abonnentuppgifter eller andra användaruppgifter i fråga om de tjänsteleverantörer som omfattas av EU-förordningen.

Skälen för bedömningen

Inhämtande av abonnentuppgifter och andra användaruppgifter enligt nationell rätt

En europeisk utlämnandeorder som utfärdas för att inhämta abonnentuppgifter eller andra användaruppgifter får enligt artikel 5.3 utfärdas för alla brott och för verkställighet av en frihetsberövande påföljd om minst fyra månader. Ett krav är att motsvarande uppgifter skulle ha kunnat inhämtas in i ett inhemskt ärende.

Definitionen av abonnentuppgifter i artikel 3.8 avser uppgifter om en abonnents eller kunds identitet, såsom angivet namn, födelse-datum, postadress eller geografisk adress, fakturerings- och betalningsuppgifter, telefonnummer eller e-postadress (se även avsnitt 6.3.1). Definitionen innefattar även typen av tjänst och dess varaktighet samt uppgifter som rör valideringen av tjänsteanvändningen.

Definitionen av abonnentuppgifter enligt EU-förordningen får anses omfatta de uppgifter som innefattas i begreppet uppgifter om abonnemang i svensk rätt (avsnitt 4.2.2). Uppgifter om abonnemang enligt nationell rätt anses emellertid ha en vidare innebörd än begreppet abonnentuppgifter enligt EU-förordningen, eftersom det förra begreppet även innefattar uppgifter om t.ex. IP-adresser. IP-adresser faller i stället enligt EU-förordningen under begreppet andra användaruppgifter (artikel 3.10). I de fall dessa uppgifter syftar till att identifiera användaren ska samma ordning för dessa uppgifter tillämpas som för abonnentuppgifter.

Som redogjorts för i avsnitt 4.4.2 föreskrivs i 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation en skyldighet för den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, som inte är en Noik, att på begäran lämna ut uppgifter om abonnemang till brottsbekämpande myndigheter. Denna bestämmelse utgör således ett undantag från den tystnadsplikt som gäller för de operatörer som omfattas av bestämmelserna.

De brottsbekämpande myndigheterna har enligt regleringen i lagen om elektronisk kommunikation rätt att hämta in abonnemangsuppgifter för att beivra i princip alla typer av brott, dvs. det ställs inte krav på att brottet ska vara av en viss svårhetsgrad för att skyldigheten att lämna ut abonnemangsuppgifter för en aktör som omfattas av bestämmelsen ska aktualiseras.

Uppgifter hänförliga till domännamn omfattas enligt vår bedömning av begreppet andra användaruppgifter i EU-förordningen. Inhämtning av sådana uppgifter sker genom en förfrågan till Internetstiftelsen, som är ansvarig för att föra register över uppgifter om domännamn (se avsnitt 6.2.4). Internetstiftelsen, i dess egenskap av personuppgiftsansvarig för uppgifterna enligt dataskyddsförordningen, lämnar ut uppgifter ur registret efter en prövning om det finns en rättslig grund för utlämnande av personuppgifter enligt

bestämmelserna i dataskyddsförordningen. Utlämnande av uppgifter till brottsbekämpande myndigheter sker med stöd av den rättsliga grunden berättigat intresse. Vissa utredande och verkställande myndigheter kan förplikta Internetstiftelsen att lämna ut uppgifter. I dessa fall har Internetstiftelsen en skyldighet att tillhandahålla myndigheten de uppgifter som efterfrågas. Det görs ingen bedömning av det misstänkta brottets allvar vid utlämnandet av uppgifter.

Sammanfattningsvis kan brottsbekämpande myndigheter enligt den nationella regleringen i lagen om elektronisk kommunikation inhämta sådana abonnentuppgifter och andra användaruppgifter som omfattas av EU-förordningen från tjänsteleverantörer som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, med undantag för en Noik. Vidare kan motsvarande uppgifter om domännamn inhämtas av brottsbekämpande myndigheter från Internetstiftelsen på det ovan beskrivna sättet.

Mot bakgrund av det sagda är det alltså enligt svensk rätt möjligt att på motsvarande sätt som regleras i EU-förordningen i ett inhemskt ärende inhämta abonnentuppgifter och andra användaruppgifter från de aktuella leverantörerna i fråga om alla typer av brott.

Några kompletterande nationella bestämmelser behövs därför inte för att det ska vara möjligt för en svensk behörig myndighet att utfärda en europeisk utlämnandeorder för att inhämta abonnentuppgifter eller andra användaruppgifter vid misstanke om brott från motsvarande utländska tjänsteleverantörer.

Särskilt om tillhandahållare av Noik och övriga leverantörer

När det gäller leverantörer av Noik samt de tjänsteleverantörer som omfattas av artikel 3.3 b och 3.3 c, kan lagen om elektronisk kommunikation inte tillämpas för att inhämta abonnentuppgifter eller andra användaruppgifter. Som angetts i avsnitt 6.7 bör svenska brottsbekämpande myndigheter emellertid kunna använda andra tvångsmedel för att inhämta motsvarande uppgifter från sådana leverantörer, främst husrannsakan och beslag. Enligt vår bedömning förutsätter inte EU-förordningen att inhämtande av abon-

nentuppgifter eller andra användaruppgifter från de tjänsteleverantörer som avses i artikel 3.3 måste ske genom det regelverk som genomför direktiv 2018/1972, dvs. lagen om elektronisk kommunikation. Andra möjligheter att inhämta motsvarande uppgifter bör enligt vår mening omfattas.

Under förutsättning att de förslag som lämnats av 2021 års data-lagringsutredning blir verklighet kommer emellertid även tjänsteleverantörer av Noik omfattas av bl.a. skyldigheten att lämna ut uppgifter om abonnemang i 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation (se avsnitt 4.2.6). Svenska myndigheters möjligheter att inhämta abonnentuppgifter och andra användaruppgifter från en leverantör av en Noik kommer då att grunda sig på bestämmelserna i lagen om elektronisk kommunikation.

Inhämtande av uppgifter i verkställighetssyfte

Enligt 9 kap. 33 § första stycket 1 lagen om elektronisk kommunikation ska den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, som inte är en Noik, på begäran lämna uppgift om abonnemang till Polismyndigheten, om myndigheten bedömer att uppgiften behövs i ett särskilt fall för att lokalisera en person som är dömd till fängelse, rättspsykiatrisk vård eller sluten ungdomsvård i syfte att möjliggöra verkställighet av påföljden (se även avsnitt 4.4.2).

Eftersom motsvarande möjlighet finns i nationell rätt kan svensk behörig myndighet utfärda en europeisk utlämnandeorder för inhämtning av abonnentuppgifter och andra användaruppgifter i syfte att möjliggöra verkställighet av frihetsberövande påföljder om minst fyra månader i enlighet med artikel 5.3 i EU-förordningen. Sluten ungdomsvård utgör en sådan annan frihetsberövande åtgärd som faller under EU-förordningens tillämpningsområde. Rättspsykiatrisk vård med särskild utskrivningsprövning är visserligen inte en tidsbestämd påföljd, men påföljdens faktiska längd uppgår teoretiskt sett till minst fyra månader och torde därför uppfylla EU-förordningens krav om ett frihetsberövande i minst fyra månader. Rättspsykiatrisk vård utan sådan prövning får dock anses falla utanför tillämpningsområdet.

Leverantörer av Noik omfattas i dag inte av bestämmelsen. Inte heller de tjänsteleverantörer som avses i artikel 3.3 b och 3.3 c omfattas av regleringen i nämnda lag. Några tvångsmedel som beslag är inte heller möjliga att tillämpa i syfte att verkställa en påföljd (se dock avsnitt 6.11 nedan angående bestämmelserna i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder). Det är således inte möjligt att gentemot dessa tjänsteleverantör utfärda en europeisk utlämnandeorder för att hämta in abonnentuppgifter eller andra användaruppgifter. Det torde dock vara möjligt att inhämta sådana uppgifter från Internetstiftelsen på den grunden att inhämtandet av uppgifterna är ett berättigat intresse enligt dataskyddsförordningens reglering.

De leverantörer som faller under artikel 3.3 b och 3.3 c torde emellertid endast i begränsad omfattning besitta sådana uppgifter som är av intresse. Det finns därför inte skäl att utöka kretsen av tjänsteleverantörer som omfattas av 9 kap. 33 § första stycket lagen om elektronisk kommunikation till att även avse dessa aktörer. Något sådant behov fanns inte heller när lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder infördes.

2021 års datalagringsutredning har, som angetts ovan, föreslagit att leverantörer av Noik ska omfattas av skyldigheten att lämna ut uppgifter enligt 9 kap. 33 § första stycket lagen om elektronisk kommunikation (se avsnitt 4.2.6). Om förslaget blir verklighet kommer det vara möjligt för brottsbekämpande myndigheter att inhämta uppgifter från en sådan leverantör för det syfte som nu avses.

6.9 Begreppen trafikuppgifter och innehållsdata och tillämpliga tvångsmedel enligt nationell rätt

Bedömning: Begreppen trafikuppgifter och innehållsdata såsom de definieras i EU-förordningen medför inte något behov av ändring i lag. Tillgängliga tvångsmedel i svensk rätt är också tillräckliga för att inhämta sådana uppgifter oavsett vilken tjänsteleverantör som avses.

Skälen för bedömningen

Innebörden av begreppen trafikuppgifter och innehållsdata i EU-förordningen och svensk rätt

Som utvecklats i avsnitt 6.3.1 avses med begreppet trafikuppgifter i artikel 3.11 i EU-förordningen uppgifter som rör tillhandahållandet av en tjänst som erbjuds av en tjänsteleverantör och vilka tjänar till att ge kontext eller ytterligare information om tjänsten, t.ex. källan till eller destinationen för ett meddelande eller en annan typ av interaktion, var utrustningen är belägen samt datum, tid, varaktighet, storlek, rutt, format och vilket protokoll som använts vid kommunikationen. Innehållsdata definieras i artikel 3.12 som alla uppgifter i digital form, t.ex. text, röst, video, bilder och ljud, med undantag för abonnentuppgifter och trafikuppgifter.

Trafikuppgifter definieras i svensk rätt som en uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande (se avsnitt 4.2.2). Definitionen får anses i sak innefatta de moment som definitionen av begreppet i EU-förordningen eftersom båda definitionerna omfattar sådana moment som krävs för att kunna följa vilken och hur en viss kommunikation har skett utan att avslöja själva innehållet i meddelandet. Det svenska begreppet lokaliseringsuppgift har dock inte någon direkt motsvarighet i EU-förordningen. Lokutionen ”var utrustningen är belägen” i definitionen av trafikuppgift i artikel 3.11 indikerar dock att begreppet även omfattar lokaliseringsuppgifter. Lokaliseringsuppgifter torde därför enligt vår uppfattning falla inom EU-förordningens tillämpningsområde, som en del av begreppet trafikuppgifter. Det bör således vara möjligt att utfärda en utlämnandeorder för sådan information.

Begreppet innehållsdata enligt EU-förordningen får anses i svensk rätt anses motsvaras av termen innehållet i ett meddelande (se t.ex. 9 kap. 31 § lagen om elektronisk kommunikation som reglerar leverantörers tystnadsplikt).

Några kompletterande bestämmelser i svensk lag behövs därför inte när det gäller begreppen trafikuppgifter och innehållsdata.

Inhämtning av trafikuppgifter och innehållsdata enligt nationell rätt

Svensk rätt ger möjlighet till inhämtning av elektronisk bevisning som avser trafikuppgifter och innehållsdata på sätt begreppen definieras i EU-förordningen genom tillstånd till olika typer av tvångsmedel (se avsnitt 4.4.3).

Hemlig avlyssning av elektronisk kommunikation kan tillämpas på alla former av kommunikation genom elektroniska kommunikationsnät, som telefontrafik, e-posttrafik och överföring av datafiler för att hämta in innehållsdata, dvs. olika uppgifter i digital form, som har överförts.

Med stöd av hemlig övervakning av elektronisk kommunikation kan uppgifter om meddelanden som i ett elektroniskt kommunikationsnät har överförts till eller från ett telefonnummer eller annan adress eller om elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område (s.k. basstationstömning) hämtas in. Genom tvångsmedlet kan sådana uppgifter som enligt EU-förordningen anses vara trafik inhämtas. Hemlig övervakning av elektronisk kommunikation är typiskt sett det mindre ingripande av de två tvångsmedlen och ett tillstånd till hemlig avlyssning ger rätt att använda även hemlig övervakning (27 kap. 18 § andra stycket rättegångsbalken).

Tvångsmedlen hemlig dataavläsning och genomsökning på distans, avser även dem inhämtning av elektronisk bevisning på sätt som beskrivs i avsnitt 4.4.3. Till skillnad från hemlig avlyssning respektive hemlig övervakning av elektronisk kommunikation innebär hemlig dataavläsning att brottsbekämpande myndigheter i hemlighet bereder sig tillgång till en dator, mobiltelefon eller annan teknisk kommunikationsutrustning och därigenom får besked om hur utrustningen används eller har använts och vilken information som finns i den.

Syftet med genomsökning på distans är att få tillgång till viss information i beslagtagna kommunikationsutrustning, såsom en dator eller mobiltelefon, som inte kan nå genom en traditionell och mer begränsad undersökning av ett beslag.

Hemlig dataavläsning respektive genomsökning på distans avser därmed inte inhämtning av lagrade uppgifter hos en tjänsteleverantör på det sätt som begreppet elektronisk bevisning definieras i EU-förordningen. Detta eftersom nämnda tvångsmedel – till skill-

nad från hemlig avlyssning av elektronisk kommunikation respektive hemlig övervakning av elektronisk kommunikation – inte förutsätter att uppgifterna begärs ut från tjänsteleverantören i fråga. De torde därför inte motsvara en sådan order som omfattas av EU-förordningens bestämmelser.

Sammanfattningsvis är det alltså genom tvångsmedlen hemlig avlyssning respektive hemlig övervakning av elektronisk kommunikation som trafikuppgifter och innehållsdata, såsom begreppen definieras i EU-förordningen, kan inhämtas i ett nationellt ärende. I sammanhanget bör framhållas att det inte möjligt att använda husrannsakan och beslag eller editionsföreläggande som substitut för hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation för inhämtning av uppgifter som finns hos en operatör som omfattas av anmälningsskyldigheten i lagen om elektronisk kommunikation (se avsnitt 4.4.3). För aktörer som inte omfattas av anmälningsskyldigheten enligt lagen om elektronisk kommunikation kan dock sådana tvångsmedel användas i stället för hemlig övervakning respektive hemlig avlyssning av elektronisk kommunikation, se avsnitt 6.7.

Beslut om beslag enligt 27 kap. 1 § rättegångsbalken kräver dock inte – till skillnad från hemlig avlyssning och hemlig övervakning av elektronisk kommunikation – domstols tillstånd för åtgärden. Användning av det tvångsmedlet är således inte att jämföras med en utfärdande av en europeisk utlämnandeorder för inhämtning av trafikuppgifter eller innehållsdata, eftersom en sådan order kräver att ordern utfärdas av eller godkänns av domstol. Beslag under förundersökning är en mycket vanlig utredningsåtgärd som kan beslutas av åklagare, förundersökningsledare eller enskild polisman. Att införa ett krav på godkännande av domstol för åtgärden i syfte att anpassa regelverket till EU-förordningens krav på obligatorisk domstolsprövning framstår därför inte som ändamålsenligt. De hemliga tvångsmedlen hemlig avlyssning och hemlig övervakning av elektronisk kommunikation är således de tvångsmedel som i svensk rätt är jämförbara med en europeisk utlämnandeorder för inhämtning av trafikuppgifter eller innehållsdata. Det bör framhållas att regleringen av dessa tvångsmedel är teknikneutral och att de därför kan riktas mot samtliga tjänsteleverantörer som omfattas av EU-förordningen. Som följer av avsnitt 6.7 är det dock förenat med praktiska svårigheter att använda sig av sådana tvångsmedel

mot de leverantörer som inte omfattas på lagrings- och anpassnings-skyldigheten i lagen om elektronisk kommunikation.

I avsnitt 6.10 redogörs för förutsättningar för svenska behöriga myndigheter att utfärda en europeisk utlämnandeorder avseende inhämtning av trafikuppgifter respektive innehållsdata från de tjänsteleverantörer som omfattas av EU-förordningen genom en jämförelse av de villkor som gäller för att utfärda en europeisk utlämnandeorder med de villkor som gäller enligt svensk rätt för tillstånd till hemlig avlyssning av elektronisk kommunikation respektive hemlig övervakning av elektronisk kommunikation.

6.10 Utfärdande av en europeisk utlämnandeorder för att inhämta trafikuppgifter och innehållsdata

6.10.1 Inledning

Som tidigare har konstaterats krävs det för att utfärda en europeisk utlämnandeorder att en motsvarande order ska kunna utfärdas i ett nationellt ärende. I detta avsnitt redogörs närmare för förutsättningarna för svenska behöriga myndigheter att inhämta trafikuppgifter och innehållsdata genom en europeisk utlämnandeorder. Detta görs genom att jämföra villkoren för en utlämnandeorder med de villkor som gäller enligt svensk rätt för att få tillstånd till hemlig avlyssning av elektronisk kommunikation respektive hemlig övervakning av elektronisk kommunikation.

Jämförelsen utgör en bakgrund till våra överväganden i avsnitt 6.10.6 om det finns skäl att ändra förutsättningarna i svensk rätt för att få tillstånd till de nämnda tvångsmedlen och på så sätt möjliggöra för svenska behöriga myndigheter att utfärda en europeisk utlämnandeorder avseende inhämtning av trafikuppgifter och innehållsdata i fler fall än vad svensk rätt i dag tillåter.

6.10.2 Förutsättningar enligt 27 kap. 18 a § rättegångsbalken för inhämtande av innehållsdata

I svensk rätt får hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 18 a § rättegångsbalken användas om *någon är skäligen misstänkt* för brott med ett minimistraff om två års fängelse samt

för vissa i paragrafen angivna brott om åtgärden är av synnerlig vikt för utredningen. Ett tillstånd till hemlig avlyssning omfattar även tillstånd till hemlig övervakning av elektronisk kommunikation, varför både trafikuppgifter och innehållsdata kan inhämtas med hjälp av tvångsmedlet (27 kap. 18 § andra stycket rättegångsbalken).

Som behandlats i avsnitt 6.3.2 krävs det att det är fråga om brott av viss svårhetsgrad eller ett visst i EU-förordningen angivet brott för att en europeisk utlämnandeorder beträffande trafikuppgifter eller innehållsdata ska kunna utfärdas enligt förordningens bestämmelser. Vilka brott dessa är anges i artikel 5.4 i EU-förordningen.

I det följande redovisas vilka brott som omfattas av såväl artikel 5.4 och den brottskatalog som finns i 27 kap. 18 a § rättegångsbalken.

Brott som uppfyller kraven i såväl artikel 5.4 a som 27 kap. 18 a § andra stycket rättegångsbalken

En europeisk utlämnandeorder kan enligt artikel 5.4 a utfärdas för brott för vilka maximistraftet är fängelse eller en annan frihetsberövande åtgärd i minst tre år. Det är således inte fråga om ett krav på ett minimistraff. Flertalet av de brott som anges i 27 kap. 18 a § andra stycket rättegångsbalken, för vilka hemlig avlyssning av elektronisk kommunikation får användas, har ett maximistraff om tre år eller mer.

Det rör sig om dels brotten i punkt 1, dvs. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år, dels flertal av de brott som räknas upp punkterna 2–20. Brott som faller in under den första kategorin är t.ex. mord, dråp, synnerligen grov misshandel, våldtäkt, grov våldtäkt, grovt rån, grov utpressning, grov mordbrand och grov allmänfarlig ödeläggelse.³⁸ I den andra kategorin kan nämnas grovt dataintrång, grovt sexuellt övergrepp mot barn, sexuellt utnyttjande av barn, grovt bedrägeri, mordbrand, sabotage och mened vilka alla har ett straff om minst tre års fängelse.³⁹

³⁸ Andra brott som faller inom denna kategori är t.ex. grovt sabotage, grovt sabotage mot blåljusverksamhet, penningförfalskning, grovt brott, grov mened, grovt övergrepp i rättsak, uppror, grovt spioneri och grovt utlandspioneri, grovt och synnerligen grovt vapenbrott, grovt och synnerligen grovt brott mot lagen om brandfarliga och explosiva varor, grovt och synnerligen grovt narkotikabrott, grovt och synnerligen grovt narkotikasmuggling samt grovt terroristbrott.

³⁹ Andra brott som faller inom denna kategori är t.ex. eller barnpornografibrott som inte är ringa, övergrepp i rättsak eller skyddande av brottsling, grovt skyddande av brottsling, brott

För dessa brott kan således en europeisk utlämnandeorder för innehållsdata (och trafikuppgifter) utfärdas i enlighet med artikel 5.4 a i EU-förordningen. Förutsättningen är dock enligt 27 kap. 18 a § första stycket rättegångsbalken att det finns någon som är skäligen misstänkt för brottet.

Brott som uppfyller kraven i såväl artikel 5.4 b som 27 kap. 18 a § andra stycket rättegångsbalken

En europeisk utlämnandeorder kan vidare enligt artikel 5.4 b utfärdas för brott som preciseras närmare i tre olika direktiv under förutsättning att brotten helt eller delvis begås med hjälp av ett informationssystem. Vilka brott som avses i den artikeln redogörs för i avsnitt 6.3.2. För dessa brott ställs således inget krav på något minsta straff eller ett maximistraff.

De brott som faller under *punkten b i* och vilka motsvarar brott enligt svensk rätt är främst olovlig befattning med betalningsverktyg, men även av egenmäktigt förfarande, bedrägeri, förberedelse till bedrägeri, häleri samt urkundsförfalskning.

Brottet olovlig befattning med betalningsverktyg har ett minimistraff som är lägre än två års fängelse och är inte heller upptaget i listan över brott i 27 kap. 18 a § andra stycket rättegångsbalken. Detsamma gäller för det grova brottet. Inte heller de övriga brotten i brottbalken som genomför de kriminaliseringsåtaganden som omfattas av denna punkt i EU-förordningen har ett minimistraff om två års fängelse. Endast brottet grovt bedrägeri återfinns i 27 kap. 18 § andra stycket 5 rättegångsbalken. För majoriteten av brotten under *punkten b i* kan alltså en svensk behörig myndighet inte utfärda en europeisk utlämnandeorder beträffande innehållsdata eftersom det inte är möjligt att besluta om hemlig avlyssning.

När det gäller de brott som faller under *punkten b ii* i artikel 5.4 motsvarar de i svensk rätt av de brott mot frihet och frid samt sexualbrott som anges i avsnitt 6.3.2.

mot medborgerlig frihet, spioneri, utlandsspioneri, grov obehörig befattning med hemlig uppgift eller olovlig underättelseverksamhet mot Sverige, mot främmande makt eller mot person, om brottet är att bedöma som grovt, grovt penningtvåtsbrott, näringspenningtvätt, grovt brott, grovt insiderbrott, företagsspioneri, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning, deltagande i en terroristorganisation samt samröre med en terroristorganisation.

Flera av dessa brott omfattas redan av artikel 5.4 a, dvs. de har ett maximistraff om minst tre års fängelse samt ett minimistraff om minst två års fängelse enligt 27 kap. 18 a § andra stycket 1 rättegångsbalken, vilket innebär att det på redan den grunden finns förutsättningar att utfärda en europeisk utlämnandeorder beträffande innehållsdata.

Vissa av de övriga svenska brott som omfattas av *punkten b ii* återfinns under de övriga punkterna i 27 kap. 18 a § andra stycket rättegångsbalken. För dessa brott kan således en europeisk utlämnandeorder utfärdas för innehållsdata trots att minimistraffet är lägre än två år och maximistraffet lägre än tre års fängelse. De brott det rör sig om är sexuellt övergrepp mot barn, utnyttjande av barn för sexuell posering, sexuellt ofredande mot barn och grovt sexuellt ofredande mot barn samt kontakt för att träffa barn i sexuellt syfte.

Vissa svenska brott som omfattas av *punkten b ii* har däremot ett lägre minimistraff än två års fängelse och återfinns inte heller bland de övriga brotten som listas i 27 kap. 18 a § andra stycket rättegångsbalken. Dessa är ofredande, olaga tvång, grovt olaga tvång, sexuellt övergrepp, sexuellt ofredande, grovt sexuellt ofredande och koppleri. För dessa brott kan en svensk behörig myndighet alltså inte utfärda en europeisk utlämnandeorder beträffande innehållsdata även om de omfattas av nämnda punkt i artikel 5.4.

Slutligen när det gäller de brott som avses i *punkten b iii* i artikel 5.4 i EU-förordningen motsvarar de i svensk rätt av dataintrång och grovt dataintrång, men även brytande av post- eller telehemlighet, skadegörelse och grov skadegörelse, sabotage och grovt sabotage samt genom bestämmelserna om försök och förberedelse till dessa brott. Hemlig avlyssning av elektronisk kommunikation kan användas vid grovt dataintrång, sabotage och grovt sabotage (27 kap. 18 a § andra stycket 1, 2 och 7 rättegångsbalken). De övriga brotten har ett lägre minimistraff än två års fängelse och finns inte heller listade bland övriga punkter i 27 kap. 18 a § andra stycket rättegångsbalken. För dessa brott kan således en europeisk utlämnandeorder inte utfärdas.

Brott som uppfyller kraven i såväl artikel 5.4 c som 27 kap. 18 a andra stycket § rättegångsbalken

En europeisk utlämnandeorder kan slutligen enligt *punkten c* i artikel 5.4 utfärdas för brott som anges direktiv 2017/541. Vilka brott som avses redogörs också för i avsnitt 6.3.2. Inte heller för dessa brott ställs i EU-förordningen något krav på något minsta straff eller ett maximistraff.

De brott som avses i nämnda direktiv finns upptagna i terroristbrottslagen, förutom deltagande i en terroristorganisation eftersom detta brott inte är föranlett av terrorismdirektivets kriminaliseringskrav. För sistnämnda brott kan dock en europeisk utlämnandeorder utfärdas eftersom brottet anges i 27 kap. 18 a § andra stycket 18 rättegångsbalken samt har ett maximistraff som överstiger fängelse tre år. Terroristbrott enligt terroristbrottslagen har ett minimistraff om fyra år och faller således in under artikel 5.4 a. Med stöd av *punkten c* i nämnda artikel är det vidare möjligt att utfärda en europeisk utlämnandeorder för innehållsdata för samröre med en terroristorganisation samt finansiering av, offentlig uppmaning till, rekrytering till, utbildning för eller resa för terrorism eller särskilt allvarlig brottslighet. Detta eftersom de finns upptagna i listan i 27 kap. 18 a § andra stycket 18 rättegångsbalken.

Brott som omfattas av i 27 kap. 18 a § andra stycket rättegångsbalken men inte artikel 5.4

För några av de brott som är upptagna i listan i 27 kap. 18 a § andra stycket rättegångsbalken är dels maximistraffet lägre än tre års fängelse, dels omfattas de inte av *punkterna b* eller *c* i artikel 5.4. Det rör sig om obehörig befattning med hemlig uppgift samt olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person, om brotten är av normalgraden. För dessa brott går det alltså att besluta om hemlig avlyssning av elektronisk kommunikation, men däremot inte utfärda en europeisk utlämnandeorder för innehållsdata.

Osjälvständiga brottsformer som omfattas av 27 kap. 18 a § andra stycket rättegångsbalken och artikel 5.4

Enligt 27 kap. 18 a § andra stycket rättegångsbalken kan hemlig avlyssning av elektronisk kommunikation användas vid försök, förberedelse och stämpling till vissa i paragrafen angivna brott.

När det gäller försöksbrott är de straffskalor som gäller det fullbordade brottet teoretiskt tillämpliga även om straffvärdet för en osjälvständig brottsform som huvudregel är lägre än det fullbordade brottet (jfr 23 kap. 1 § andra stycket brottsbalken).

Straffet för förberedelse eller stämpling ska bestämmas under maximistraffet och får sättas under den lägsta gräns som gäller för fullbordat brott. Högre straff än fängelse i två år får bestämmas endast om fängelse i sex år eller mer kan följa på det fullbordade brottet. (23 kap. 2 § tredje stycket brottsbalken). Straffskalan sträcker sig alltså från böter eller, om det fullbordade brottet har minimistraff på sex år eller mer, från allmänt fängelseminimum (14 dagar) till strax under straffmaximum för det fullbordade brottet som förberedelsen eller stämplingen avser.⁴⁰

En osjälvständig brottsform av ett fullbordat brott som uppfyller EU-förordningens krav i artikel 5.4 a på ett lägsta maximistraff om tre års fängelse kan således ha ett straffvärde som understiger maximistraffet. Straffvärdet som sådant bör dock inte vara styrande utan maximistraffet bör vara utgångspunkten, även om det gäller för den fullbordade gärningen.

Vidare kan konstateras att flertalet av de brott som anges i artikel 5.4 b och 5.4 c förutsätter att försök, förberedelse och stämpling till dessa brott också kriminaliseras. Vår utgångspunkt är således att i de fall det enligt nationell rätt går att besluta om hemlig avlyssning av elektronisk kommunikation för dessa brott är det också möjligt att utfärda en europeisk utlämnandeorder för innehållsdata under förutsättning att detta även är möjligt avseende det fullbordade brottet. Detta oaktat att fängelse i två år för stämpling eller förberedelse enligt 23 kap. 2 § tredje stycket brottsbalken endast får bestämmas om fängelse i sex år eller mer kan följa på det fullbordade brottet.

⁴⁰ SOU 2024:55 s. 68.

Brott som har ett straffvärde överstigande två års fängelse

Hemlig avlyssning av elektronisk kommunikation kan också tillämpas vid annat brott om det har ett straffvärde överstigande två års fängelse eller vid flera brott om bl.a. det samlade straffvärdet överstiger fängelse i två år (27 kap. 18 a § andra stycket 21 och 22 rättegångsbalken). EU-förordningen i artikel 5.4 a ställer som krav att maximistraffet ska uppgå till tre års fängelse, varför brottets straffvärde i det enskilda fallet är av mindre betydelse i sammanhanget. Det torde dock sällan vara fallet att ett brott som bedöms ha ett straffvärde överstigande två års fängelse inte har ett maximistraff som överstiger tre års fängelse, varför det i praktiken bör vara möjligt att för de allra flesta brott inom denna kategori utfärda en utlämnandeorder av aktuellt slag.

Flerfaldig brottslighet

Hemlig avlyssning kan även enligt 27 kap. 18 a § rättegångsbalken ske om det rör sig om flera brott och det sammanlagda straffvärdet överstiger fängelse i två år samt att vissa andra förutsättningar är uppfyllda. Här bör kravet om maximistraff om tre års fängelse enligt artikel 5.4 a eller om brotten förekommer under artikel 5.4 b eller c vara styrande för bedömningen om det är möjligt att utfärda en europeisk utlämnandeorder. Brotten sammanlagda straffvärde är således inte av relevans i sammanhanget.

Brott som omfattas av artikel 5.4 men inte av förutsättningarna i 27 kap. 18 a § andra stycket rättegångsbalken

Ett flertal brott i svensk rätt uppfyller de villkor som ställs i artikel 5.4 i EU-förordningen men eftersom hemlig avlyssning av elektronisk kommunikation inte kan användas för dessa brott finns alltså inte förutsättningar för en svensk behörig myndighet att utfärda en utlämnandeorder för utredning av ett sådant brott.

Förutom de ovan angivna brotten som faller under *punkten b* i artikel 5.4, för vilka det inte finns möjlighet att använda det aktuella tvångsmedlet, är det här fråga om brott som har ett maximistraff som överstiger tre års fängelse, men vars minimistraff är lägre än

två års fängelse och som inte heller finns upptagna i brottskatalogen i 27 kap. 18 a § andra stycket rättegångsbalken. Det rör t.ex. grov misshandel, olaga frihetsberövande, grovt olaga hot, grovt olaga identitetsintrång, grov stöld, rån, grov förskingring, grovt olovligt förfogande, och grov trolöshet mot huvudman.⁴¹

6.10.3 Förutsättningar enligt 27 kap. 18 b § rättegångsbalken för inhämtande av innehållsdata

Hemlig avlyssning av elektronisk kommunikation kan enligt 27 kap. 18 b § rättegångsbalken även användas under förundersökning för att utreda *vem som skäligen kan misstänkas för brott* om åtgärden är av synnerligen vikt för utredningen.

Som huvudregel krävs att brottet har ett minimistraff om fyra års fängelse. Vidare finns det i det andra stycket i bestämmelsen en brottskatalog över andra brott för vilka tvångsmedlet kan användas enligt de förutsättningar som anges i paragrafen.

Brott som har ett minimistraff om fyra års fängelse, har av naturliga skäl ett maximistraff om minst tre års fängelse. Brott med detta minimistraff är t.ex. mord, dråp, synnerligen grov misshandel, mäniskorov, grov våldtäkt, grovt rån, grov mordbrand, grov allmänfarlig ödeläggelse och spridande av gift eller smitta, grovt brott. För utredning av sådana brott kan således en europeisk utlämnandeorder utfärdas under de förutsättningar som följer av 27 kap. 18 b § rättegångsbalken. Av brott som anges i 27 kap. 18 b § andra stycket rättegångsbalken har vidare majoriteten ett maximistraff om minst tre års fängelse, varför det även för de brotten är möjligt att utfärda en europeisk lämnandeorder av aktuellt slag med stöd av artikel 5.4 a i EU-förordningen.

Brotten obehörig befattning med hemlig uppgift och olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller

⁴¹ Exempel på ytterligare brott är grovt vållande till annans död, grovt barnfridsbrott, olaga förföljelse, äktenskaps tvång, barnäktenskapsbrott, grovt hemfridsbrott, inbrottsstöld, grovt tillgrepp av fortskaffningsmedel, grovt egenmäktigt förfarande, grovt fordringsbedrägeri, grovt ocker, grovt häleri, grovt svindleri, grovt olovligt brukande, grov oredlighet mot borgenär, grovt bokföringsbrott, grov skadegörelse, sabotage mot blåljusverksamhet, grov urkunds förfalskning, hindrande av urkunds bevisfunktion, grovt brott, signaturförfalskning, grovt brott, penningförfalskning, bevisförfalskning, grovt brott, våldsamt upplopp, uppvigling, grovt brott, involverande av en underårig i brottslighet, myteri, grov hets mot folkgrupp, grovt gravfridsbrott, grovt djurplågeri, falskt larm, grovt brott, grovt våld eller hot mot tjänsteman, grov förgripelse mot tjänsteman, främjande av flykt, grovt brott, grovt tjänstefel och grovt brott mot tystnadsplikt.

mot person har dock ett för lågt straffmaximum för att en utlämnandeorder skulle kunna utfärdas, av samma skäl som angetts ovan beträffande förutsättningar för användning av tvångsmedlet enligt 27 kap. 18 a § rättegångsbalken.

När det gäller brotten i *punkten b i* i artikel 5.4 kan hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 18 b § andra stycket rättegångsbalken endast användas beträffande grovt bedrägeri, då det brottet är upptaget i paragrafens brottskatalog (punkt 4). För övriga brott i svensk rätt som faller under *punkten b i* kan alltså en svensk behörig myndighet inte utfärda en europeisk utlämnandeorder beträffande innehållsdata – likhet med vad som gäller för hemlig avlyssningen enligt 28 kap. 18 a § rättegångsbalken.

I fråga om brott som faller under *punkten b ii* gör sig samma resonemang gällande som beträffande hemlig avlyssning enligt 27 kap. 18 a § rättegångsbalken, se ovan. Detta då samma sexualbrott mot barn finns upptagna i brottskatalogen i 27 kap. 18 b § andra stycket 15 rättegångsbalken. Även beträffande *punkten b iii* i artikel 5.4 i EU-förordningen gäller samma systematik. De brott för vilka hemlig avlyssning enligt 27 kap. 18 a § rättegångsbalken kan användas gäller även hemlig avlyssning enligt 27 kap. 18 b § rättegångsbalken, eftersom brotten grovt dataintrång och sabotage samt grovt sabotage finns upptagna i den senare paragrafens brottskatalog.

Vad gäller brotten som faller under *punkten c* i artikel 5.4 i EU-förordningen, kan en utlämnandeorder utfärdas enligt motsvarande förutsättningar i 27 kap. 18 b § rättegångsbalken eftersom samtliga brott i svensk rätt som faller under punkten finns upptagna i paragrafens brottskatalog.

Ovan har vidare listats flera brott i svensk rätt som uppfyller de villkor som ställs i artikel 5.4 a i EU-förordningen men för vilka det inte är möjligt att utfärda en utlämnandeorder enligt förutsättningarna i 27 kap. 18 a § rättegångsbalken. Inte heller för dessa brott går det av naturliga skäl att utfärda en utlämnandeorder enligt 27 kap. 18 b § rättegångsbalken.

Hemlig avlyssning enligt 27 kap. 18 b § rättegångsbalken kan även användas i fråga om försök, förberedelse eller stämpling till vissa av de brott som anges i paragrafen, om en sådan gärning är belagd med straff och det kan antas att gärningens straffvärde överstiger fängelse i ett år. Vi har i avsnitt 6.10.2 beträffande motsvar-

ande reglering i 27 kap. 18 a § rättegångsbalken kommit fram till att om det möjligt att utfärda en europeisk utlämnandeorder för innehållsdata för det fullbordade brottet, är det också möjligt att utfärda en sådan order för en osjälvständig brottsform. Vi gör ingen annan bedömning beträffande regleringen i 27 kap. 18 b §, oaktat att det i bestämmelsen – till skillnad vad som är fallet beträffande 27 kap. 18 a § – anges ett krav på visst straffvärde.

Vidare kan det aktuella tvångsmedlet enligt 27 kap. 18 b § rättegångsbalken användas i fråga om ett annat brott, än de som specifikt anges i bestämmelsens brottskatalog, under förutsättning att det kan antas att brottets straffvärde överstiger fängelse i fyra år. EU-förordningen ställer som krav för de brott som inte särskilt specificeras i artikel 5 att maximistraffet ska uppgå till minst tre års fängelse. Detta krav är uppfyllt om straffvärdet för den enskilda gärningen överstiger fängelse fyra år varför det är möjligt att utfärda en order även i dessa fall. Slutligen kan tvångsmedlet enligt paragrafen användas vid förundersökning om flerfaldig brottslighet om det samlade straffvärdet överstiger fyra års fängelse och vissa andra förutsättningar är uppfyllda. Som konstaterats ovan bör dock det samlade straffvärdet inte vara av relevans i sammanhanget utan bedömningen om det är möjligt att utfärda en order bör utgå från om vart och ett av brotten faller under någon av punkterna i artikel 5.4 i EU-förordningen.

6.10.4 Förutsättningar enligt 27 kap. 19 a § rättegångsbalken för inhämtande av trafikuppgifter

Genom hemlig övervakning av elektronisk kommunikation kan, som angetts ovan, sådan information som faller inom EU-förordningens definition av trafikuppgifter inhämtas.

Enligt 27 kap. 19 a § rättegångsbalken får hemlig övervakning av elektronisk kommunikation användas vid förundersökning om *någon är skäligen misstänkt* för brott med ett minimistraff om sex månaders fängelse samt för vissa i paragrafen angivna brott om åtgärden är av synnerlig vikt för utredningen.

Som nämnts ovan kan hemlig övervakning av elektronisk kommunikation ske för alla de brott som omfattas av ett tillstånd av hemlig avlyssning av elektronisk kommunikation (27 kap. 18 § andra stycket rättegångsbalken).

Brott som uppfyller kraven i såväl artikel 5.4 a som 27 kap. 19 a § andra stycket rättegångsbalken

Flertalet grova brott i svensk rätt som har ett minimistraff om sex månaders fängelse eller mer har också ett maximistraff om minst tre års fängelse enligt EU-förordningens krav i artikel 5.4 a.

De brott som omfattas av 27 kap. 19 a § andra stycket 1 rättegångsbalken, utöver de brott för vilka hemlig avlyssning av elektronisk kommunikation kan användas, kan nämnas grov misshandel, rån, grovt tillgrepp av fortskaffningsmedel, grovt egenmäktigt förfarande, grov olovlig grovt bedrägeri, grov olovlig befattning med betalningsverktyg, grovt häleri, grov förskingring och grov tro-loshet mot huvudman.⁴²

I brottskatalogen i 27 kap. 19 a § andra stycket 4 och 5 rättegångsbalken finns brotten narkotikabrott och narkotikasmuggling upptagna, för vilka det också är möjligt att utfärda en europeisk utlämnandeorder för trafikuppgifter eftersom maximistraffet uppgår till tre års fängelse för brotten.

Brott som uppfyller kraven i såväl artikel 5.4 b och artikel 5.4 c som 27 kap. 19 a § andra stycket rättegångsbalken

Hemlig övervakning av elektronisk kommunikation får användas för de brott som anges i 27 kap. 18 a § andra stycket rättegångsbalken. De brott som omfattas av *punkterna b och c* i artikel 5.4 EU-förordningen och för vilka hemlig avlyssning av elektronisk kommunikation kan användas enligt nämnda lagrum kan därför även bli föremål en europeisk utlämnandeorder avseende trafikuppgifter (se avsnitt 6.10.2 ovan).

Utöver dessa brott kan hemlig övervakning (men inte hemlig avlyssning) även användas beträffande grov olovlig befattning med betalningsverktyg, grovt egenmäktigt förfarande, grovt häleri och

⁴² Exempel på fler brott är grovt barnfridsbrott, grov fridskränkning respektive grov kvinno-fridskränkning, hedersförtryck, grovt olaga hot, grovt hemfridsbrott, grovt olaga integritetsintrång, grovt dataintrång, våldtäkt, mindre grovt brott, egenmäktighet med barn, grovt brott, grovt stöld, inbrottsstöld, grovt ocker, , grovt svindleri, grovt olovligt förfogande, grovt tagande eller grovt givande av muta, grovt olovligt förfogande, grov oredlighet mot borgenärer, , grovt bokföringsbrott, grov skadegörelse, grov urkundsförfalskning, grov urkundsförfalskning, grov hets mot folkgrupp, grovt gravfridsbrott, grovt barnpornografi-brott, grovt djurplågeri, falskt larm, grovt brott, grovt våld eller hot mot tjänsteman, grovt skyddande av brottsling, främjande av flykt, grovt brott, olovlig underrättelseverksamhet, grovt brott, grovt tjänstefel och grovt brott mot tystnadsplikt.

grov urkundsförfalskning (*punkten b i*), grovt olaga tvång, sexuellt övergrepp och grovt sexuellt ofredande (*punkten b ii*) och grov skadegörelse (*punkten b iii*) eftersom det för nu nämnda brott är föreskrivet ett minimistraff om sex månaders fängelse. Hemlig övervakning kan även ske beträffande dataintrång, som faller under *punkten b iii*, eftersom det finns särskilt upptaget i 27 kap. 19 a § andra stycket 2 rättegångsbalken.

Även för brotten som faller under *punkten c* i artikel 5.4 kan hemlig övervakning användas.

Övriga brott som faller under de aktuella punkterna i artikel 5.4 har ett lägre straffminimum än sex månaders fängelse, t.ex. olovlig befattning med betalningsverktyg, bedrägeri, häleri, ofredande, olaga tvång, sexuellt ofredande, koppleri, brytande av post- och telehemlighet, skadegörelse samt sabotage. Det är därför inte möjligt att – i likhet med vad som gäller beträffande hemlig avlyssning av elektronisk kommunikation – att besluta om hemlig övervakning, varför det inte heller är möjligt att utfärda en europeisk utlämnandeorder avseende trafikavgifter för dessa brott.

Brott som uppfyller kraven i artikel 5.4 men inte 27 kap. 19 a § andra stycket rättegångsbalken

Vissa brottsbalksbrott har ett högre maximistraff än tre års fängelse, men ett minimistraff lägre än sex månader, varför en europeisk utlämnandeorder inte kan utfärdas för dessa brott. Sådana brott är t.ex. människoexploatering, olaga förföljelse, barnåktenskapsbrott, koppleri och involverande av en underårig i brottslighet.⁴³

⁴³ Fler exempel på brott inom denna kategori är vållande till kroppsskada eller sjukdom, grovt brott, äktenskapstvång, kapning, sjö- eller luftfartssabotage, flytplatsabotage, sabotage mot blåljusverksamhet, penningförfalskning, förfalskning av fast märke, uppvigling, grovt brott, myteri, grov förgripelse mot tjänsteman och otillbörligt verkande vid röstning, grovt brott.

6.10.5 Förutsättningar enligt 27 kap. 19 b § rättegångsbalken för inhämtande av trafikuppgifter

Hemlig övervakning av elektronisk kommunikation kan enligt 27 kap. 19 b § rättegångsbalken användas för att utreda *vem som skäligen kan misstänkas för brott* om åtgärden är av synnerligen vikt för utredningen.

Hemlig övervakning i dessa fall får enligt andra stycket användas vid förundersökning om brott som avses i 27 kap. 18 a § rättegångsbalken 1–21 eller om flera brott om bl.a. straffvärdet kan antas överstiga två års fängelse. Eftersom förutsättningarna för användning av tvångsmedlet enligt denna bestämmelse är densamma som beträffande 27 kap. 18 a § rättegångsbalken hänvisas till redogörelserna ovan om brott som uppfyller kraven enligt såväl artikel 5.4 i EU-förordningen och nämnda bestämmelse i rättegångsbalken.

6.10.6 Nationella bestämmelser bör inte ändras för att kunna utfärda en europeisk utlämnandeorder i fler fall

Bedömning: Brottskatalogerna i 27 kap. 18 a, 18 b, 19 a och 19 b §§ rättegångsbalken bör inte utvidgas till att omfatta ytterligare brott som har ett maximistraff om fängelse i minst tre år, men som inte har ett minimistraff som anges i nämnda bestämmelser.

En höjning av maximistraffen bör inte heller ske för de brott för vilka hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation kan användas, men som inte har ett maximistraff om fängelse i minst tre år.

Skälen för bedömningen: Som följer av genomgången ovan kommer flertalet av de brott för vilka hemlig avlyssning och hemlig övervakning av elektronisk kommunikation kan användas i en svensk förundersökning även kunna bli föremål för en europeisk utlämnandeorder för inhämtande av innehållsdata och trafikuppgifter.

De brott för vilka de hemliga tvångsmedlen kan användas, men där maximistraffet är för lågt i förhållande till det krav som följer av artikel 5.4 i EU-förordningen, är enligt vad som konstaterats ovan obehörig befattningsmedel med hemlig uppgift samt olovlig underrättelse-

verksamhet mot Sverige, mot främmande makt eller mot person, om brottet är av normalgraden. För att dessa brott ska kunna omfattas av en möjlighet att utfärda en europeisk utlämnandeorder om inhämtning av trafikuppgifter och innehållsdata krävs att brottsens maximistraff höjs.

Principerna om proportionalitet och ekvivalens är grundläggande för straffskalornas utformning. Principerna kan beskrivas på så sätt att straffet ska stå i proportion till brottets allvar, så att svårare brott bestraffas strängare än mindre allvarliga brott (proportionalitet) och att lika allvarliga brott bestraffas lika strängt (ekvivalens). Straffet ska alltså spegla hur allvarligt samhället ser på den brottsliga gärningen.⁴⁴

En utgångspunkt för bedömningen av ett brotts straffvärde är straffskalan för brottet. Straffskalan kan sägas ange brottets abstrakta straffvärde, dvs. hur lagstiftaren värderar brottstypens svårhet i relation till andra brott. Det abstrakta straffvärdet utgör alltså ett mått på hur allvarligt lagstiftaren ser på den aktuella brottstypen i förhållande till andra brott. Det innebär att även lagstiftaren måste göra en bedömning av vilken fara, kränkning eller skada en brottstyp rent generellt innebär. Vilken straffskala som ska gälla för ett visst brott avgörs av lagstiftaren utifrån värdet av det intresse som straffbudet avser att skydda. I princip bör straffskalan vara strängare ju viktigare intresse som berörs.⁴⁵

Straffet för ett brott indikerar därmed hur allvarlig gärningen är i förhållande till andra brott och ger uttryck för samhällets klander av brottet. En höjning av ett straff endast för att det skulle innebära att hemliga tvångsmedel kan användas i en utredning om brottet – dessutom endast i en EU-kontext – utgör i sig inte ett relevant skäl för att utforma en straffskala på ett visst sätt. Vår bedömning är således att det inte finns tillräckliga skäl att höja straffskalorna för de nu aktuella brotten för att möjliggöra en användning av en europeisk utlämnandeorder vid en utredning av dessa brott.

Vidare följer av genomgången ovan att flera brott både i brottsbalken och specialstraffrätten har ett sådant straffmaximum att det enligt EU-förordningen skulle vara möjligt att utfärda en utlämnandeorder. Brotten har dock ett för lågt minimistraff för att användning av de aktuella tvångsmedlen skulle komma i fråga och

⁴⁴ Prop. 1987/88:120 s. 77 f. och SOU 1986:14 s. 143.

⁴⁵ SOU 2021:68 s. 130 och SOU 1986:14 s. 145.

finns inte heller upptagna i brottskatalogerna i de aktuella bestämmelserna om hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation. Det är därför inte möjligt att utfärda en sådan utlämnandeorder eftersom nationell rätt inte ger möjlighet därtill i ett liknande inhemskt ärende, vilket är ett grundläggande krav enligt artikel 5.2 i EU-förordningen. Frågan är därför om något eller några av dessa brott bör läggas till i de brottskataloger som finns i 27 kap. 18 a, 18 b, 19 a eller 19 b §§ rättegångsbalken.

När det gäller förutsättningarna för att höja minimistraffen hänvisas till vad som sägs inledningsvis om att skärpa straffskalorna.

Vid bedömningen av om ett brott bör läggas till i brottskatalogerna är regeringsformens, Europakonventionens och EU:s rättighetsstadgas reglering om grundläggande fri- och rättigheter en väsentlig utgångspunkt (se avsnitt 4.3.3). Utvidgade brottskataloger kommer att medföra begränsningar av rätten till förtroliga meddelanden, rätten till privatliv och rätten till skydd mot intrång i den personliga integriteten. En sådan begränsning får göras endast 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. Det aktuella brottets allvar är av grundläggande betydelse vid bedömningen av om det är proportionerligt att utöka möjligheterna att använda hemliga tvångsmedel. Det ska således finnas ett tydligt behov av att hemliga tvångsmedel ska kunna användas för ett visst brott. Vi har svårt att se ett sådant behov.

Vidare har EU-domstolen i praxis om offentliga myndigheters tillgång till uppgifter som lagrats av leverantörer av elektroniska kommunikationstjänster framhållit att endast bekämpning av grov brottslighet och förebyggande av allvarliga hot mot allmän säkerhet kan motivera allvarliga ingrepp i de grundläggande rättigheter som anges i artiklarna 7 och 8 i EU:s rättighetsstadga (se EU-domstolens dom i mål C-746/18, H.K. p. 31–35).

De aktuella brottskatalogerna har också nyligen varit föremål för översyn och har kompletterats med flera olika brott som har bedömts vara av sådant allvar att det finns skäl att hemliga tvångsmedel ska kunna användas för brotten. Att göra en annan bedömning av allvaret av de brott för vilka det i dag inte kan användas hemliga tvångsmedel framstår därför inte som ändamålsenligt. Vår

bedömning är därför att det i nuläget inte finns skäl att utvidga de aktuella brottskatalogerna till att omfatta fler brott än i dag.

I sammanhanget bör det framhållas att det är också möjligt att utfärda en europeisk utredningsorder för inhämtning av sådan elektronisk bevisning som omfattas av EU-förordningen (se avsnitt 4.5.2). Om det inte går att utfärda en europeisk utlämnandeorder för inhämtning av trafikuppgifter eller innehållsdata på grund av den gärning som avses i den svenska förundersökningen inte omfattas av de krav som ställs i artikel 5.4, men däremot omfattas av 27 kap. 18 a, 18 b, 19 a eller 19 b §§ rättegångsbalken, kan bevisningen alltså inhämtas genom en europeisk utredningsorder som ställs till en behörig myndighet i annan medlemsstat. Genom att först utfärda en europeisk bevarandeorder av de uppgifter som efterfrågas, kan uppgifterna också säkras i väntan på att den europeiska utredningsordern verkställs.

6.11 Inhämtande av trafikuppgifter och innehållsdata för verkställighet av fängelsestraff

Bedömning: Några ändringar behövs inte i lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder för att det ska vara möjligt att utfärda en europeisk utlämnandeorder beträffande trafikuppgifter för att lokalisera en person som är dömd till fängelse, sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning.

Nämnda lag bör inte heller utvidgas till att även avse hemlig avlyssning av elektronisk kommunikation för att möjliggöra en europeisk utlämnandeorder avseende innehållsdata.

Skälen för bedömningen: Enligt artikel 5.4 d kan en europeisk utlämnandeorder för att inhämta trafikuppgifter eller innehållsdata även utfärdas för verkställighet av en frihetsberövande påföljd om minst fyra månader om verkställigheten avser ett straff som utdömts för brott som avses i artikel 5.4 a–5.4 c.

Hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning av vad avser kommunikationsövervaknings- och platsuppgifter får enligt 3 och 4 §§ lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder användas om åtgär-

den är av synnerlig vikt för att lokalisera en person som är dömd till fängelse, sluten ungdomsvård eller rättspsykiatrisk vård för att möjliggöra verkställighet av påföljden. En sådan åtgärd får endast användas om domen omfattar ett brott enligt 27 kap. 19 a § andra stycket rättegångsbalken och 4 § lagen om hemlig dataavläsning eller avser rättspsykiatrisk vård med särskild utskrivningsprövning.

I den omfattning det är möjligt att i en pågående förundersökning utfärda en europeisk utlämnandeorder avseende trafikuppgifter (se avsnitt 6.10.4) kommer det således att vara möjligt att utfärda en motsvarande order med syftet att lokalisera en person som är dömd till en frihetsberövande påföljd i Sverige.

Enligt 2024 års lag är det inte möjligt att besluta om hemlig avlyssning av elektronisk kommunikation i syfte att lokalisera dömda personer. Det innebär att svensk rätt inte uppfyller det grundläggande kravet i artikel 5.2 i EU-förordningen (vad avser innehållsdata) att en europeisk utlämnandeorder kan endast utfärdas om en liknande order hade kunnat utfärdas i ett inhemskt fall.

I propositionen till nuvarande reglering ansåg regeringen att mer ingripande åtgärder, såsom hemlig avlyssning av elektronisk kommunikation, inte tillför den mest användbara informationen för att uppnå syftet med tvångsmedelsanvändningen, dvs. att lokalisera dömda personer.⁴⁶ Av det skälet inkluderades inte hemlig avlyssning i bestämmelserna i 2024 års lag.

Vi ser ingen anledning att frångå denna bedömning och föreslå ändringar i 2024 års lag. En europeisk utlämnandeorder kommer således inte kunna utfärdas för att hämta in innehållsdata i syfte att lokalisera en dömd person.

6.12 Utfärdande av en europeisk bevarandeorder

6.12.1 Bevarande av uppgifter vid misstanke om brott

Bedömning: Det krävs inte några ändringar eller kompletteringar av svensk rätt för att en europeisk bevarandeorder ska kunna utfärdas vid misstanke om brott.

⁴⁶ Prop. 2023/24:108 s. 34.

Skälen för bedömningen: En europeisk bevarandeorder får enligt artikel 6.3 utfärdas för alla brott, om den skulle kunna ha utfärdats på samma villkor i ett liknande inhemskt ärende.

En europeisk bevarandeorder innebär att mottagaren föreläggs att bevara elektroniska bevis i avvaktan på en efterföljande framställan om utlämnande. Ett motsvarande instrument i svensk rätt är ett föreläggande om bevarande som regleras i 27 kap. 16 § rättegångsbalken. Den som i elektronisk form innehar en viss lagrad uppgift, som skäligen kan antas ha betydelse för utredningen om ett brott, får föreläggas att bevara uppgiften. I likhet med vad som är fallet beträffande en europeisk bevarandeorder får ett föreläggande enligt nämnda bestämmelse avse alla typer av brott. Vidare kan de uppgifter som avses vara av vilket slag som helst, som exempelvis innehållet i ett meddelande eller uppgifter om ett meddelandes ursprung och adressat, under förutsättning att uppgiften finns bevarad elektroniskt. Bestämmelsen i 27 kap. 16 § rättegångsbalken behandlas närmare i avsnitt 4.4.1 (se även avsnitt 11.3.1).

Ett föreläggande enligt bestämmelsen kan rikta sig mot vem som helst som innehar en lagrad uppgift, dvs. samtliga typer av tjänsteleverantörer som faller inom EU-förordningens tillämpningsområde omfattas av bestämmelsen, vilket inkluderar leverantörer av en Noik.

Mot bakgrund av det sagda är det således möjligt att i ett nationellt ärende utfärda ett föreläggande som motsvarar en europeisk bevarandeorder vid misstanke om brott. Det krävs därmed inte några ändringar eller kompletteringar av svensk rätt för att en europeisk bevarandeorder ska kunna utfärdas av svensk behörig myndighet i ett sådant fall.

6.12.2 En möjlighet att förelägga om bevarande av uppgifter i verkställighetssyfte bör införas i svensk rätt

Förslag: Den som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för att lokalisera en person för verkställighet av en frihetsberövande påföljd och som kan inhämtas med stöd av 3 § lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder eller 9 kap. 33 § första stycket 1 lagen om elektronisk kommunikation ska kunna föreläggas att bevara uppgiften. För ett sådant föreläggande ska 27 kap. 16 § andra och tredje styckena och 16 a § rättegångsbalken tillämpas.

Skälen för förslaget

Det bör införas en möjlighet till bevarande av uppgifter i verkställighetssyfte

En europeisk bevarandeorder får enligt artikel 6.3 utfärdas för verkställighet av frihetsberövande påföljd om minst fyra månader. En viss oklarhet råder dock om det enligt nämnda artikel också är ett krav på att motsvarande order ska kunna utfärdas i ett motsvarande inhemskt ärende, vilket mer tydligt framgår om en sådan order avser misstanke om brott. Lydelsen av texten skulle kunna tolkas som om ett sådant krav inte gäller.

Vi är emellertid av den uppfattning att detta är ett förbiseende av EU-lagstiftaren. Samarbetet mellan EU:s medlemsstater som bygger på en princip att medlemsstaterna ska ömsesidigt erkänna varandras beslut i straffrättsliga förfaranden har alltid som utgångspunkt att om en stat kräver att en åtgärd ska vidtas på en annan medlemsstats territorium ska en motsvarande åtgärd ha kunnat vidtas i ett inhemskt ärende under liknande förhållanden. Detta är således vår utgångspunkt i de fortsatta övervägandena.

Enligt svensk rätt kan en myndighet inte besluta om föreläggande om bevarande av uppgifter som syftar till att lokalisera en person för verkställighet av en frihetsberövande påföljd.

Enligt lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder är det möjligt att besluta om hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning

avseende kommunikationsövervaknings- och platsuppgifter för att lokalisera personer som håller sig undan eller har avvikit från verkställighet av en dom på fängelse, sluten ungdomsvård och rättspsykiatrisk vård med särskild utskrivningsprövning.

I 9 kap. 33 § första stycket 1 i lagen om elektronisk kommunikation har det också införts en skyldighet för den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, som inte är en Noik, att på begäran lämna ut uppgifter om abonnemang till Polismyndigheten om uppgiften behövs för att lokalisera en person i syfte att möjliggöra verkställighet av frihetsberövande påföljd.

Det är angeläget att person som eftersöks för verkställighet av en frihetsberövande påföljd hittas snabbt om personen som eftersöks är farlig, tex. allvarligt psykiskt sjuk, våldsbenägen eller riskerar att fortsätta att begå brott.⁴⁷ Det kan därför många gånger finnas ett behov av att snabbt kunna säkra och bevara vissa lagrade elektroniska uppgifter även i verkställighetssyfte, varför en sådan möjlighet bör införas.

Mot bakgrund av att det numera är möjligt att använda vissa hemliga tvångsmedel i syfte att lokalisera dömda framstår det vidare som lämpligt att det i svensk rätt finns en möjlighet att förelägga om bevarande av uppgifter för ett sådant syfte på motsvarande sätt som gäller för bevarande vid misstanke om brott enligt 27 kap. 16 § rättegångsbalken. En möjlighet att förelägga om bevarande av uppgifter i verkställighetssyfte bör därför införas i svensk rätt.

Ett föreläggande om bevarande vid misstanke om brott enligt 27 kap. 16 § rättegångsbalken ska avse en viss elektronisk uppgift. Det innebär att det i föreläggandet måste anges vilken specifik elektronisk uppgift som ska bevaras, t.ex. en viss datafil eller trafikuppgifter hänförliga till ett visst meddelande. Ett föreläggande kan alltså inte vara generellt och t.ex. utan närmare specificering endast ange att alla uppgifter som mottagits under en tid ska bevaras. Det samma bör gälla för ett bevarandeföreläggande i verkställighetssyfte. Ett sådant föreläggande bör i likhet med vad som är fallet gällande ett bevarandeföreläggande enligt 27 kap. 16 § rättegångsbalken avse specifika uppgifter som redan finns lagrade och medför endast en skyldighet att bevara en uppgift under en viss tid, inte att lämna ut den. Mot den bakgrunden får det integritetsintrång ett

⁴⁷ Prop. 2023/24:108 s. 32–33.

bevarandeföreläggande i verkställighetssyfte innebär anses vara förhållandevis begränsat.⁴⁸

Hur bör bestämmelsen om bevarande av uppgifter utformas?

Bestämmelsen i 27 kap. 16 § rättegångsbalken infördes till följd av Sveriges tillträde till Europarådets konvention om it-relaterad brottslighet för att i ett brottsbekämpande syfte säkerställa att uppgifter som är lagrade i elektronisk form inte försvinner. Ett föreläggande enligt 27 kap. 16 § rättegångsbalken kan avse alla typer av uppgifter, till skillnad från en europeisk bevarandeorder som endast får avse abonnentuppgifter, trafikuppgifter eller innehållsdata. Att utsträcka ett föreläggande enligt nämnda paragraf i rättegångsbalken till att även avse alla slags uppgifter som syftar till att lokalisera en person för verkställighet av en frihetsberövande påföljd är alltså att gå längre än EU-förordningens bestämmelser om en motsvarande bevarandeorder. En sådan utvidgning skulle också innebära att fler typer av uppgifter bevaras än vad som i ett senare led kan lämnas ut med stöd av t.ex. hemlig övervakning av elektronisk kommunikation enligt 2024 års lag.

Användningen av hemliga tvångsmedel för att lokalisera en dömd person är en mer ingripande åtgärd gentemot den enskilde än ett föreläggande att bevara uppgifter för ett sådant ändamål. I det senare fallet är det inte fråga om utlämnande av uppgifter, utan endast om bevarande av uppgifterna inför en eventuell framtida prövning om utlämnande av dem ska ske. Samtidigt framstår det som överflödigt att möjliggöra ett föreläggande om bevarande av uppgifter, om inte dessa uppgifter senare kan lämnas ut för att lokalisera en person som har undandragit sig verkställighet av en frihetsberövande påföljd enligt den lagstiftning som nyligen trätt i kraft.

Ett föreläggande om bevarande av uppgifter som syftar till att lokalisera en person som undanhåller sig verkställighet av en frihetsberövande påföljd bör mot bakgrund av vad som sagts ovan begränsas till att avse de uppgifter som enligt lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder i ett

⁴⁸ Se motsvarande resonemang beträffande ett föreläggande enligt 27 kap. 16 § rättegångsbalken i prop. 2020/21:72 s. 23–24.

senare led kan inhämtas för att lokalisera en person, dvs. sådana uppgifter som kan inhämtas genom användning av de aktuella tvångsmedlen enligt den lagen samt uppgifter om abonnemang enligt 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation. Eftersom lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder inte ger möjlighet till inhämtning av innehåll i meddelanden bör det inte heller vara möjligt att förelägga om bevarande av sådana uppgifter. Det innebär att en europeisk bevarandeorder kommer att kunna utfärdas av en svensk behörig myndighet för abonnentuppgifter och för trafikuppgifter men inte för innehållsdata.

Mot bakgrund av det sagda bör det i 2024 års lag införas en bestämmelse om en möjlighet att utfärda ett föreläggande om bevarande av uppgifter om abonnemang och trafikuppgifter som kan ha betydelse för lokalisering av en person för verkställighet av en frihetsberövande påföljd. De påföljder som bör komma i fråga är fängelse, sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning.

För ett föreläggande i verkställighetssyfte bör bestämmelserna i 27 kap. 16 § andra och tredje styckena rättegångsbalken ha motsvarande tillämpning. Detta innebär att samma tider för bevarande ska gälla för ett föreläggande om bevarande i verkställighetssyfte som för ett föreläggande i bevissäkringssyfte, dvs. tiden för bevarande får inte bestämmas till längre än nödvändigt och får inte överstiga 90 dagar från dagen för beslutet, om det inte finns särskilda skäl för förlängning. Även bestämmelserna i 27 kap. 16 a § rättegångsbalken bör tillämpas för ett sådant föreläggande. Bestämmelsen reglerar vem som får besluta om ett bevarandeföreläggande samt tystnadsplikt för den som mottagit ett föreläggande. Eftersom det är fråga om en lagakraftvunnen dom som ska verkställas i påföljdsdelen pågår det av förklarliga skäl ingen förundersökning vid utfärdande av ett föreläggande i verkställighetssyfte. Ett beslut om utfärdande av ett föreläggande i verkställighetssyfte bör därför fattas av åklagare.

Slutligen följer av 27 kap. 16 a § rättegångsbalken att den som förelagts att bevara en viss uppgift får begära rättens prövning av föreläggandet.

Den föreslagna bestämmelsen ger svensk behörig myndighet att utfärda en europeisk bevarandeorder under de förutsättningar som

följer av EU-förordningen, dvs. att straffet uppgår till minst fyra månaders frihetsberövande påföljd och att domen inte meddelats i den dömdes utvevaro.

Ett tillstånd för användning av tvångsmedel enligt lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder får meddelas om åtgärden är av synnerlig vikt för att kunna lokalisera en dömd person och förutsätter, som behandlats ovan, att den dom som ska verkställas avser ett sådant brott som kan motivera att åtgärden vidtas under en förundersökning eller att domen avser rättspsykiatrisk vård med särskild utskrivningsprövning. Samma förutsättningar bör gälla vid ett föreläggande om bevarande av uppgifter.

För uppgifter som bevarats med stöd den föreslagna bestämmelsen ska prövning om ett efterföljande utlämnande ske genom tillämpliga bestämmelser i lagen om elektronisk kommunikation eller bestämmelserna om hemliga tvångsmedel. En prövning om utlämning av uppgifter som bevarats i syfte att lokalisera en dömd person för verkställighet bör däremot ske enligt lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder.

7 Utfärdande och verkställande myndigheter och dess uppgifter

7.1 Inledning

Enligt EU-förordningen ska medlemsstaterna utse en eller flera myndigheter som ska vara behöriga och skyldiga att vidta olika åtgärder enligt EU-förordningen.

Medlemsstaterna ska till att börja med utse behöriga utfärdande myndigheter. Deras främsta uppgift är att utfärda och sända över en europeisk utlämnande- eller bevarandeorder. I EU-förordningen ställs olika krav på vilken myndighet som har rätt att utfärda dessa order. Den utfärdande myndigheten ska även vara skyldig att informera och samråda med myndigheter i den verkställande staten, bl.a. innan en order utfärdas.

Vidare ska medlemsstaterna utse en eller flera myndigheter som ska vara behöriga att dels ta ställning till om en utfärdad order ska erkännas eller vägras, dels informera och samråda med såväl den utfärdande myndigheten som det utsedda verksamhetsstället eller det rättsliga ombudet.

Enligt EU-förordningen finns även en möjlighet för medlemsstaterna att utse en eller flera centrala myndigheter med administrativa uppgifter som rör en europeisk utlämnande- eller bevarandeorder.

Utöver detta ska medlemsstaterna utse domstolar som ska pröva invändningar från en tjänsteleverantör om att ett tredjelands lag förhindrar ett utlämnande av de begärda uppgifterna.

Mot denna bakgrund ska vi enligt våra direktiv ta ställning till vilken eller vilka svenska myndigheter som bör utses till behöriga myndigheter enligt EU-förordningen samt analysera vilken eller vilka domstolar som bör kunna pröva invändningar om att ett tredjelands lag förhindrar ett utlämnande enligt EU-förordningen. Vi ska

också analysera om det finns behov av att utse en central myndighet enligt EU-förordningen. Slutligen ska vi analysera behovet av författningsändringar eller andra åtgärder som krävs för att de föreslagna myndigheterna och domstolarna ska kunna utföra sina skyldigheter enligt EU-förordningen på ett effektivt och rättssäkert sätt och lämna nödvändiga författningsförslag.

Avsnittet inleds med en redogörelse för EU-förordningens bestämmelser om behöriga utfärdande och verkställande myndigheter och deras uppgifter (avsnitt 7.2 och 7.3). Vidare behandlas bestämmelserna om behörig domstol (avsnitt 7.4). Därefter följer våra överväganden och förslag (avsnitt 7.5).

7.2 Utfärdande myndigheter

Enligt EU-förordningen ska medlemsstaterna utse en eller flera myndigheter som bland annat ska vara behöriga att utfärda och sända över en europeisk utlämnande- eller bevarandeorder. I förordningen ställs olika krav på den myndighet som ska ha rätt att utfärda en europeisk utlämnande- eller bevarandeorder. Vidare följer det av bestämmelserna i EU-förordningen olika skyldigheter som åligger den utfärdande myndigheten.

Av artikel 31.1 a följer att medlemsstaterna ska underrätta kommissionen om vilka myndigheter som i enlighet med landets nationella rätt är behöriga myndigheter att utfärda, godkänna eller över-sända en europeisk utlämnande- eller bevarandeorder enligt artikel 4.

7.2.1 Myndigheter som är behöriga att utfärda en europeisk utlämnande- eller bevarandeorder

I artiklarna 4.1–4.3 i EU-förordningen anges vilka myndigheter som kan vara behöriga att utfärda en europeisk utlämnande- eller bevarandeorder. Utgångspunkten är att det ska vara en rättslig myndighet (se skäl 36). En europeisk utlämnandeorder för att inhämta abonnentuppgifter eller andra användaruppgifter eller en europeisk bevarandeorder får enligt artiklarna 4.1 och 4.3 utfärdas av

- a) en domare, en domstol, en undersökningsdomare eller en allmän åklagare som är behörig i det berörda ärendet, eller

- b) en annan behörig myndighet, enligt den utfärdande statens definition, som i det berörda ärendet agerar i egenskap av utredande myndighet i straffrättsliga förfaranden, med behörighet att besluta om bevisinhämtning i enlighet med nationell rätt; i ett sådant ärende ska den europeiska utlämnandeordern eller bevarandeordern godkännas av en domare, domstol, undersökningsdomare eller allmän åklagare i den utfärdande staten.

Av artikel 4.2 a följer att en europeisk utlämnandeorder för att inhämta trafikuppgifter och innehållsdata får endast utfärdas av en domare, en domstol eller en undersökningsdomare som är behörig i det berörda ärendet (dvs. inte av en allmän åklagare). En annan behörig myndighet (t.ex. en åklagare) kan enligt punkten b också utfärda en sådan order, men den måste då godkännas av en domare, en domstol eller en undersökningsdomare.

Om en europeisk utlämnande- eller bevarandeorder har godkänts av en rättslig myndighet enligt punkten b i artikel 4.1–4.3 får den myndigheten också betraktas som en utfärdande myndighet för översändandet av intyget om en europeisk utlämnande- eller bevarandeorder (artikel 4.4).

I en nödsituation får de behöriga myndigheter som avses i punkten b i artiklarna 4.1 och 4.3 (men inte i artikel 4.2) undantagsvis enligt artikel 4.5 utfärda en europeisk utlämnandeorder för abonnentuppgifter eller andra användaruppgifter eller en europeisk bevarandeorder, utan förhandsgodkännande av den berörda ordern, om godkännandet inte kan erhållas i tid och om dessa myndigheter skulle kunna utfärda en order i ett liknande inhemskt ärende utan ett förhandsgodkännande (se även skäl 37). Den utfärdande myndigheten ska i dessa fall utan onödigt dröjsmål och senast inom 48 timmar inhämta ett godkännande av ordern. Om ett sådant godkännande inte lämnas ska den utfärdande myndigheten omedelbart återkalla ordern och radera eller på annat sätt begränsa användningen av alla uppgifter som inhämtats. En nödsituation definieras i artikel 3.18 som en situation där det råder ett överhängande hot mot en persons liv, fysiska integritet eller säkerhet. Vidare avses med en nödsituation ett överhängande hot mot en kritisk infrastruktur enligt definitionen i artikel 2 a i direktiv 2008/114, om en driftsstörning vid eller en förstörelse av kritisk infrastruktur skulle leda till en omedelbar fara för en persons liv, fysiska integritet eller

säkerhet, genom t.ex. allvarlig skada på tillhandahållandet av basförnödenheter till befolkningen eller på utövdandet av statens kärnfunktioner (se även skäl 35).

7.2.2 Den utfärdande myndighetens uppgifter

Den utfärdande myndighetens huvudsakliga uppgift är att utfärda europeiska utlämnande- eller bevarandeorder. Myndigheten har emellertid även andra uppgifter som regleras i flera olika bestämmelser i EU-förordningen.

Av artikel 7.1 följer att den utfärdande myndigheten ska ställa en europeisk utlämnande- respektive bevarandeorder direkt till ett utsett verksamhetsställe eller till ett rättsligt ombud för den berörda tjänsteleverantören. I en nödsituation kan en order ställas till något annat av tjänsteleverantörens utsedda verksamhetsställen eller rättsliga ombud i unionen om det verksamhetsstället eller rättsliga ombudet som ordern först ställts till inte reagerar på ordern (artikel 7.2). Se även skäl 50.

Om en europeisk utlämnandeorder utfärdas för att inhämta trafikuppgifter eller innehållsdata, ska den utfärdande myndigheten enligt artikel 8.1 anmäla detta till den verkställande myndigheten genom att översända ordern till den myndigheten samtidigt som den översänder intyget om ordern till mottagaren enligt artikel 9.1. Någon anmälan krävs dock inte enligt artikel 8.2 om den utfärdande myndigheten vid tidpunkten för utfärdandet av ordern har rimliga skäl att anta att brottet har begåtts, är på väg att begås eller sannolikt kommer att begås i den utfärdande staten, och den person vars uppgifter begärs är bosatt i den utfärdande staten (se även skäl 51 och 54). När den utfärdande myndigheten anmäler en order till den verkställande myndigheten i den andra staten ska den, när så är lämpligt, inkludera all ytterligare information som kan behövas för att bedöma möjligheten att åberopa en vägransgrund i enlighet med artikel 12 (artikel 8.3). En anmälan har enligt artikel 8.4 en suspensiv verkan på mottagaren skyldigheter utom i nödsituationer. I skäl 52 och 53 utvecklas närmare vad som avses med var ett brott är begånget och var en person är bosatt.

Om mottagaren har informerat den utfärdande myndigheten enligt artikel 10.5 eller artikel 11.4 ska myndigheten ta ställning till

om ordern ska återkallas, anpassas eller upprätthållas. Nämda artiklar rör det förhållandet att mottagaren anser att en verkställighet av en europeisk utlämnande- eller bevarandeorder skulle inkräkta på immunitet och privilegier eller på regler om fastställande eller begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet eller yttrandefrihet i andra medier enligt den verkställande statens rätt.

Av artikel 12.5 följer vidare att om en myndighet i en annan medlemsstat eller ett tredjeland eller en internationell organisation har behörighet att upphäva en immunitet eller privilegier, som den verkställande myndigheten har åberopat som vägransgrund enligt artikel 12.1 a (efter en anmälan enligt artikel 8.1) får den utfärdande myndigheten begära att den berörda myndigheten utövar den behörigheten.

Av artikel 13.1 följer att den utfärdande myndigheten utan onödigt dröjsmål ska informera den person vars uppgifter begärs genom en europeisk utlämnandeorder om utlämnandet av uppgifter, dock under förutsättning att det inte föreligger en sådan situation som anges i artikel 13.2 då en sådan underrättelseskyldighet kan begränsas (se även avsnitt 10.4.1).

Vidare följer av artikel 16.1 att den utfärdande myndigheten har rätt att begära att den verkställande myndigheten verkställer den europeiska utlämnande- respektive bevarandeordern i de fall mottagaren inte efterlever ordern, utan att ange orsaker som godtas av den utfärdande myndigheten.

Den utfärdande myndigheten ska vid tillämpningen av såväl artikel 12 som artikel 16 samråda med och lämna kompletterande information till den verkställande myndigheten i fråga om de vägransgrunder som kan bli aktuella att tillämpa för den sistnämnda myndigheten.

Om mottagaren av en europeisk utlämnandeorder har invänt mot den enligt artikel 17.1–17.2 ska den utfärdande myndigheten ompröva ordern. Om den utfärdande myndigheten avser att upprätthålla ordern ska den begära en prövning av domstol i den utfärdande staten, samtidigt som fullföljandet av den ordern ska avbrytas (artikel 17.3, se även avsnitt 7.4).

7.3 Verkställande myndighet och dess uppgifter

7.3.1 Myndigheter som kan vara verkställande myndighet

En verkställande myndighet definieras i artikel 3.17 som den myndighet i den verkställande staten som i enlighet med den statens nationella rätt är behörig att ta emot en europeisk utlämnande- eller bevarandeorder som översänds av den utfärdande myndigheten för anmälan eller verkställighet. Några krav på vilken myndighet som får utses ställs inte i EU-förordningen. Det är således upp till varje medlemsstat att själv avgöra vilken eller vilka myndigheter som ska agera som en verkställande myndighet.

Av artikel 31.1 b följer att medlemsstaterna ska underrätta kommissionen om vilka myndigheter som i enlighet med landets nationella rätt är behöriga myndigheter att ta emot anmälningar enligt artikel 8 och besluta om att erkänna och verkställa en europeisk utlämnande- eller bevarandeorder enligt artikel 16.

7.3.2 Den verkställande myndighetens uppgifter

Den verkställande myndigheten kommer i samarbetet enligt EU-förordningen att involveras dels efter det att en anmälan gjorts enligt artikel 8.1, dels när den utfärdande myndigheten enligt artikel 16.1 begär att den europeiska utlämnande- eller bevarandeordern ska verkställas för att det utsedda verksamhetsstället eller det rättsliga ombudet inte efterlever en utfärdad order.

Artiklarna 8 och 12

I de fall den utfärdande myndigheten har gjort en anmälan enligt artikel 8.1 tillämpas artikel 12. Den verkställande myndigheten främsta uppgift är att den enligt artikel 12.1 så snart som möjligt och senast tio dagar efter mottagandet av anmälan eller, i nödsituationer, senast 96 timmar efter mottagandet, ska ta ställning till om det kan finnas skäl att åberopa en av de vägransgrunder som anges i artikel 12.1. En vägran får enligt den bestämmelsen ske i följande fall:

- a) De begärda uppgifterna skyddas av immunitet eller privilegier som beviljas enligt den verkställande statens rätt eller omfattas av regler om fastställande eller begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet eller yttrandefrihet i andra medier och som hindrar ordern från att fullföljas eller verkställas (se även skäl 47 beträffande immunitet och privilegier).
- b) Ett fullföljande av ordern skulle innebära ett uppenbart åsidosättande av en relevant grundläggande rättighet enligt artikel 6 i EU-fördraget och EU:s rättighetsstadga.
- c) Fullföljandet av ordern skulle strida mot principen *ne bis in idem* (förbud mot dubbelbestraffning).
- d) Den gärning som ordern avser utgör inte ett brott enligt den verkställande statens rätt, såvida det inte gäller ett brott som förtecknas i de brottskategorier som anges i bilaga IV till EU-förordningen, under förutsättning att maximistraffet för brottet i fråga i den utfärdande staten är fängelsestraff eller annan frihetsberövande åtgärd i minst tre år.

I skäl 61–66 beskrivs vägransgrunderna i 12.1 närmare, särskilt den vägransgrund som återfinns i artikel 12.1 b (skäl 64). Det ska också noteras att vägransgrunderna ska tillämpas fakultativt, dvs ett visst utrymme för en skönsmässig bedömning ska finnas (skäl 62).

Om den verkställande myndigheten åberopar en vägransgrund ska myndigheten enligt artikel 12.2 underrätta det utsedda verksamhetsstället eller det rättsliga ombudet och den utfärdande myndigheten.

Innan beslut fattas om att åberopa en vägransgrund ska den verkställande myndigheten enligt artikel 12.3 på lämpligt sätt kontakta den utfärdande myndigheten för att diskutera lämpliga åtgärder. Om ingen lösning nås efter sådana diskussioner får den verkställande myndigheten besluta om att vägra verkställighet. I dessa fall ska den verkställande myndigheten ta ställning till om vissa uppgifter får överföras eller användas på villkor som anges av den myndigheten (artikel 12.4).

Om immuniteten eller privilegierna (se vägransgrunden i artikel 12.1 a) kan upphävas får den utfärdande myndigheten begära att den verkställande myndigheten vidtar de åtgärder som krävs för att upphäva immuniteten eller privilegierna (artikel 12.5).

Artikel 16

Om det utsedda verksamhetsstället eller det rättsliga ombudet inte efterlever en utfärdad europeisk utlämnande- eller bevarandeorder utan godtagbara skäl får den utfärdande myndigheten enligt artikel 16.1 begära att den verkställande myndigheten verkställer ordern – om den i tillämpliga fall inte redan har vägrat att verkställa ordern enligt artikel 12 (se även skäl 72).

Den verkställande myndigheten ska som huvudregel utan vidare formaliteter erkänna och vidta de åtgärder som krävs för att verkställa ordern (artikel 16.2), vilket ska ske utan onödigt dröjsmål och senast fem arbetsdagar efter mottagandet av ordern. Tidsfristerna gäller inte om den verkställande myndigheten anser att det finns skäl att vägra med stöd av artikel 16.4 eller 16.5.

Om den verkställande myndigheten beslutar att erkänna ordern ska den enligt artikel 16.3 kräva att det utsedda verksamhetsstället eller det rättsliga ombudet fullgör sina skyldigheter och informera dem om möjligheten att invända mot fullföljandet av den berörda ordern med stöd av artikel 16.4 eller 16.5. Vidare ska den verkställande myndigheten informera mottagaren om vilka tidsfrister som gäller samt att sanktioner kan åläggas vid bristande efterlevnad. Se även skäl 73.

En europeisk utlämnandeorder som avser trafikuppgifter och innehållsdata kan således vägras av den verkställande myndigheten dels i det inledande skede efter en anmälan enligt artikel 8.1, dels efter det att det utsedda verksamhetsstället eller det rättsliga ombudet har invänt eller på annat sätt inte velat fullfölja ordern. En europeisk utlämnandeorder beträffande abonnentuppgifter eller andra användaruppgifter eller en europeisk bevarandeorder kan emellertid endast vägras enligt det förfarande som anges i artikel 16.

Enligt artikel 16.4–16.5 kan en europeisk utlämnandeorder respektive europeisk bevarandeorder vägras i följande fall:

- Ordern har inte utfärdats eller godkänts av en utfärdande myndighet som anges i artikel 4.
- Ordern har inte utfärdats för ett brott som anges i artikel 5.4 (endast tillämplig i förhållande till en europeisk utlämnandeorder).

- Ordern kan inte efterlevas på grund av en faktisk omöjlighet med hänsyn till omständigheter som inte beror på mottagaren, eller på grund av att intyget innehåller uppenbara fel (se även skäl 59).
- Ordern avser inte uppgifter som lagras av eller på uppdrag av tjänsteleverantören vid den tidpunkt då intyget om ordern mottas.
- Tjänsten omfattas inte av EU-förordningen.
- De begärda uppgifterna skyddas av immunitet eller privilegier eller uppgifterna omfattas av reglerna för fastställande eller begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet eller yttrandefrihet.
- Det finns grundad anledning att anta att verkställigheten skulle innebära ett uppenbart åsidosättande av en relevant grundläggande rättighet enligt artikel 6 i EU-fördraget och EU:s rättighetsstadga.

Den sist nämnda vägransgrunden kan det utsedda verksamhetsstället eller det rättsliga ombudet inte åberopa som skäl för att inte fullfölja ordern utan endast den verkställande myndigheten kan beakta denna vägransgrund (se artikel 16.3 a).

Om det utsedda verksamhetsstället eller det rättsliga ombudet invänder mot ordern enligt någon av de vägransgrunder som föreskrivs i artiklarna 16.4 eller 16.5 ska den verkställande myndigheten på nytt ta ställning till om ordern ska verkställas eller inte på grundval av information som lämnats av mottagaren och, vid behov, kompletterande information från den utfärdande myndigheten (artikel 16.6).

Innan den verkställande myndigheten beslutar att inte erkänna och verkställa ordern enligt artiklarna 16.2 eller 16.6 ska den samråda med den utfärdande myndigheten, bl.a. kan ytterligare information inhämtas från den utfärdande myndigheten. Den utfärdande myndigheten ska svara på en sådan begäran inom fem arbetsdagar (artikel 16.7).

Den verkställande myndigheten ska omedelbart meddela den utfärdande myndigheten och det utsedda verksamhetsstället eller det rättsliga ombudet om alla sina beslut (artikel 16.8).

Om den verkställande myndigheten inhämtar de uppgifter som begärs genom en europeisk utlämnandeorder från det utsedda verksamhetsstället eller det rättsliga ombudet ska den enligt artikel 16.9

översända dessa uppgifter till den utfärdande myndigheten utan onödigt dröjsmål.

Om det utsedda verksamhetsstället eller det rättsliga ombudet inte fullgör sina skyldigheter trots den verkställande myndighetens beslut om verkställighet ska verksamhetsstället eller det rättsliga ombudet åläggas en sanktionsavgift (artikel 16.10). Ett effektivt rättsmedel ska finnas tillgängligt mot ett beslut att ålägga en sanktionsavgift.

7.4 Behörig domstol

Artikel 17 innehåller bestämmelser om domstolsprövning av en tjänsteleverantörs motstridiga skyldigheter (se även skäl 74).

Om en mottagare anser att efterlevnaden av en europeisk utlämnandeorder skulle strida mot en skyldighet enligt ett tredjelands tillämpliga rätt, ska den informera den utfärdande myndigheten och den verkställande myndigheten om sina skäl till att inte följa den europeiska utlämnandeordern, i enlighet med det förfarande som följer av artikel 10.8–10.9. Formuläret i bilaga III till förordningen ska användas (artikel 17.1). En sådan anmälan kallas i EU-förordningen *en motiverad invändning*.

En motiverad invändning ska enligt artikel 17.2 innehålla alla relevanta uppgifter om tredjelandets rätt, dess tillämpning i det aktuella fallet och arten av den motstridiga skyldigheten. Invändningen ska ges in senast tio dagar efter den dag då mottagaren mottog intyget om utlämnandeordern. En motiverad invändning får enligt artikeln inte grundas på

- a) att liknande bestämmelser om villkor, formaliteter och förfaranden för utfärdande av en order om utlämnade inte existerar i tredjelandets tillämpliga rätt, eller
- b) endast det faktum att uppgifterna lagras i ett tredjeland.

Den utfärdande myndigheten ska, som angetts i avsnitt 7.2.2, ompröva den europeiska utlämnandeordern utifrån den motiverade invändningen och eventuella synpunkter från den verkställande staten (se även skäl 75). Avser den utfärdande myndigheten att stå fast vid ordern, ska den begära en prövning av domstol i den utfärd-

ande staten. Fullföljandet av den europeiska utlämnandeordern ska avbrytas i avvaktan på att prövningsförfarandet avslutas (artikel 17.3).

Domstolen ska enligt artikel 17.4 först bedöma om en motstridig skyldighet föreligger, genom en granskning av om

- a) tredjelandets rätt är tillämplig utifrån de särskilda omständigheterna i ärendet i fråga, och
- b) tredjelandets rätt, om den är tillämplig, förbjuder röjande av de berörda uppgifterna när den tillämpas på de särskilda omständigheterna i ärendet.

Om domstolen anser att det inte föreligger några motstridiga skyldigheter ska den upprätthålla den europeiska utlämnandeordern (artikel 17.5). Har domstolen fastställt att tredjelandets rätt förbjuder röjande av de berörda uppgifterna, ska den enligt artikel 17.6 avgöra huruvida den europeiska utlämnandeordern ändå ska upprätthållas eller upphävas. Denna bedömning ska i synnerhet baseras på följande faktorer, där särskild vikt ska ges till de omständigheter som anges i punkterna a och b (se även skäl 78):

- a) Det intresse som skyddas genom tredjelandets relevanta rätt, inklusive grundläggande rättigheter samt andra grundläggande intressen som förhindrar röjande av uppgifterna, framför allt tredjelandets nationella säkerhetsintressen.
- b) Graden av anknytning mellan det brottmål för vilket den europeiska utlämnandeordern utfärdades och endera av de två jurisdiktionerna, vilken bland annat kan framgå av
 - i. plats, medborgarskap och bosättningsort för den person vars uppgifter begärs eller för offret eller offren för brottet i fråga,
 - ii. platsen där brottet i fråga begicks,
- c) Graden av anknytning mellan tjänsteleverantören och tredjelandet i fråga; i detta sammanhang ska inte enbart platsen för lagring av uppgifterna räcka för att fastställa en betydande grad av anknytning,
- d) Den utredande statens intresse av att inhämta de aktuella bevisen, utifrån en bedömning av brottets svårhetsgrad och vikten av att inhämta bevis på ett snabbt sätt,

- e) Möjliga konsekvenser för mottagaren eller för tjänsteleverantören av att efterleva den europeiska utlämnandeordern, inklusive eventuella sanktioner.

Domstolen får begära information från tredjelandets behöriga myndighet med beaktande av direktiv 2016/680¹, särskilt kapitel V, och i den mån en sådan begäran inte hindrar det berörda straffrättsliga förfarandet (se även skäl 76 och 77). Den ska framför allt begära information från den behöriga myndigheten i tredjelandet om den motstridiga skyldigheten rör grundläggande rättigheter eller andra grundläggande intressen i tredjelandet avseende nationell säkerhet och försvar (artikel 17.7).

Om domstolen beslutar att upphäva eller upprätthålla den europeiska utlämnandeordern ska den informera den utfärdande myndigheten och mottagaren.² I de fall ordern ska upprätthållas ska mottagaren fullfölja ordern (artikel 17.8). Den utfärdande myndigheten ska även informera den verkställande myndigheten om resultatet av prövningsförfarandet (artikel 17.10). Av skäl 79 framgår att om den behöriga domstolen beslutar att upphäva den utfärdade europeiska utlämnandeordern bör det vara möjligt att utfärda europeisk bevarandeorder för att därefter ansöka om att få ut uppgifterna på annat sätt, t.ex. genom rättslig hjälp i brottmål.

Vid tillämpning av förfarandena enligt artikeln ska tidsfristerna enligt artikel 17.9 beräknas i enlighet med den utfärdande myndighetens nationella rätt.

Av artikel 31.1 c följer att Sverige ska underrätta kommissionen om vilka myndigheter som är behöriga att pröva en motiverad invändning enligt artikel 17.

¹ 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.

² Orden ”behörig myndighet” i den andra meningen i artikel 17.8 torde vara felöversatt och ska rätteligen lyda ”behörig domstol” (jfr t.ex. den engelska, franska och den danska språkversionen).

7.5 Överväganden och förslag

7.5.1 Behörig utfärdande myndighet

Förslag: Åklagare ska vara behöriga att utfärda en europeisk utlämnandeorder respektive europeisk bevarandeorder i Sverige.

Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som ska ingripa mot brott eller brottslig verksamhet ska vara behöriga att besluta om utfärdande av en europeisk utlämnandeorder avseende inhämtning av abonnentuppgifter och andra användaruppgifter samt av en europeisk bevarandeorder. En sådan order ska godkännas av åklagare.

Skälen för förslaget

Allmänna utgångspunkter

Det straffrättsliga samarbetet mellan unionens medlemsstater baserar sig på principen om ömsesidigt erkännande och bygger på ett samarbete mellan medlemsstaternas behöriga myndigheter. Detta gäller i huvudsak även för samarbetet enligt EU-förordningen. En europeisk utlämnande- eller bevarandeorder som sänds över till en mottagare ska verkställas utan, med vissa undantag, något ifrågasättande. Den behöriga myndigheten i den utfärdande staten ska vidare i vissa fall ha direktkontakt med den verkställande myndigheten i den stat där tjänsteleverantörens utsedda verksamhetsställe eller rättsliga ombud finns. EU-förordningen reglerar ett samarbete som i huvudsak kommer att ske under pågående brottsutredningar.

I Sverige finns framför allt två regelverk med närmare bestämmelser om samarbetet under pågående brottsutredningar. Det rör sig om lagen (2000:562) om internationell rättslig hjälp i brottmål och lagen (2017:1000) om en europeisk utredningsorder. Den sistnämnda lagen baserar sig på principen om ömsesidigt erkännande. Enligt dessa två regelverk är det åklagare och allmän domstol som har getts behörighet att ansöka om rättslig hjälp utomlands respektive utfärda en europeisk utredningsorder.

EU-förordningen hindrar emellertid inte att även andra myndigheter än åklagare och domstol under vissa förutsättningar utses till behöriga myndigheter med rätt att utfärda en europeisk utlämnande-

eller bevarandeorder. Vid bedömningen av vilka myndigheter som utses bör utgångspunkten vara att ordningen så nära som möjligt ansluter till vad som gäller för bevisinhämtning i ett motsvarande svenskt straffrättsligt förfarande och till reglerna om det internationella straffrättsliga samarbetet.

Behörig myndighet vid utfärdande av en europeisk utredningsorder för inhämtning av trafikuppgifter och innehållsdata

Av artikel 4.2 följer att en europeisk utlämnandeorder för inhämtning av trafikuppgifter respektive innehållsdata endast får utfärdas av en domare, en domstol eller en undersökningsdomare som är behörig i det berörda ärendet (dvs. inte av en åklagare). En annan behörig myndighet kan dock under vissa förutsättningar också utfärda en sådan order, men den måste då godkännas av en domare, en domstol eller en undersökningsdomare.

Inhämtning av elektronisk bevisning enligt EU-förordningen är typiskt sett en sådan åtgärd som i svensk rätt vidtas under förundersökningen om ett brott. Det är i detta skede i en brottsutredning som beslut tas om hemlig avlysning och hemlig övervakning av elektronisk kommunikation som motsvaras av en europeisk utlämnandeorder i fråga om inhämtning av innehållsdata och trafikuppgifter (om dessa tvångsmedel, se avsnitt 4.4.3 och 6.10). För användning av de nämnda tvångsmedlen krävs rättens tillstånd (27 kap. 21 § rättegångsbalken). Föreligger det fara i dröjsmål får dock åklagaren besluta om en sådan åtgärd i väntan på rättens tillstånd (27 kap. 21 a § rättegångsbalken).

Beslut om de aktuella tvångsmedlen sker normalt inte efter att åtal har väckts och brottmålet handläggs av domstol. Den utfärdande myndighetens uppgifter enligt EU-förordningen har stora likheter med åklagarens uppgifter i ett inhemskt ärende avseende de nämnda tvångsmedlen. En åklagares kontakt och samarbete med utländska myndigheter i ärenden enligt EU-förordningen ligger också väl i linje med den funktion som åklagaren har i den svenska brottmålsprocessen.

Vid en sammantagen bedömning framstår det som mest ändamålsenligt att Åklagarmyndigheten och Ekobrottsmyndigheten är behöriga myndigheter avseende beslut om utfärdande av en europeisk utlämnandeorder avseende inhämtning av innehållsdata och

trafikuppgifter som översänds från Sverige med stöd av EU-förordningen. Detta bör framgå av lag.

En åklagare kan enligt artikel 4.2 a i EU-förordningen inte utfärda en europeisk utlämnandeorder som avser inhämtande av trafikuppgifter eller innehållsdata, men däremot enligt artikel 4.2 b. Som utvecklas i avsnitt 7.5.3 ska en domstol enligt artikel 4.2 b dock godkänna en sådan order innan den sänds över till det utsedda verksamhetsställe eller rättsliga ombud som ska verkställa ordern. Även om åklagaren självständigt enligt svensk rätt inte beslutar om sådana tvångsmedel kan konstateras att åklagaren kommer i det aktuella ärendet agera som utredande myndighet i egenskap av undersökningsledare och har enligt svensk rätt i allmänhet behörighet att besluta om bevisinhämtning. Förfarandet enligt svensk rätt får anses motsvara det som beskrivs i artikel 4.2 b i EU-förordningen, varav det viktigaste är att frågan blir föremål för en domstolsprövning innan en europeisk utlämnandeorder skickas över till mottagaren. Det svenska förfarandet får således anses motsvara de krav som ställs upp av EU-förordningen.

Behöriga myndigheter vid utfärdande av en europeisk utlämnandeorder för övriga uppgifter och en europeisk bevarandeorder

En europeisk utlämnandeorder för att inhämta abonnentuppgifter eller andra användaruppgifter eller en europeisk bevarandeorder avseende bevarande av alla typer av elektronisk bevisning som omfattas av förordningen får enligt artiklarna 4.1 och 4.3 utfärdas av en domare, en domstol, en undersökningsdomare eller en allmän åklagare. En sådan order får också utfärdas av en annan behörig myndighet, som har till uppgift att utreda brott, med behörighet i nationell rätt att besluta om bevisinhämtning. Det krävs dock i ett sådant fall att ordern godkänns av en domare, domstol, undersökningsdomare eller allmän åklagare i den utfärdande staten.

Uppgift om abonnemang som gäller brottslig verksamhet eller misstanke om brott kan – utöver åklagare – Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som ska ingripa mot brottet eller den brottsliga verksamheten, såsom Kustbevakningen, begära in från de tjänsteleverantörer som omfattas av 9 kap. 33 § lagen (2022:482) om elektronisk kommunikation (se avsnitt 4.4.2).

Ett föreläggande om att bevara en elektronisk uppgift enligt 27 kap. 16 § rättegångsbalken får beslutas av åklagare eller undersökningsledare (27 kap. 16 a § rättegångsbalken). Polismyndigheten och andra brottsbekämpande myndigheter kan därmed besluta om ett sådant föreläggande om företrädare för myndigheten är förundersökningsledare.

De nu nämnda åtgärderna i nationell rätt får anses motsvara en europeisk utlämnandeorder för inhämtning av abonnentuppgifter och andra användaruppgifter respektive en europeisk bevarandeorder för samtliga typer av uppgifter som omfattas av EU-förordningen (se avsnitt 6.8 och 6.12). Det kan dock konstateras att flera av de myndigheter som enligt svensk rätt kan inhämta eller besluta om bevarande av nu aktuella uppgifter inte enligt huvudregeln i artikel 4.1 a respektive artikel 4.3 a kan utfärda en motsvarande order. Frågan är således som dessa myndigheter ska ges behörighet att i dessa fall utfärda en order med stöd av artikel 4.1 b och 4.3 b.

Polismyndighetens kontaktpunkt för internationella operativa ärenden, SPOC (Single Point of Operational Contact), hanterar bl.a. förfrågningar om aktuell information i relation till ett antal utländska tjänsteleverantörer. SPOC-samarbetet bygger på Polismyndighetens informella överenskommelser med respektive tjänsteleverantör. SPOC representerar inte endast den svenska Polismyndigheten i förhållande till de aktuella tjänsteleverantörerna, utan även Åklagarmyndigheten, Ekobrottsmyndigheten och Tullverket vid deras förfrågningar avseende frysningar och uppgifter om abonnemang och annan användarinformation. Under 2023 hanterade SPOC enligt uppgift drygt 7 000 förfrågningar.

I EU-förordningen ställs krav på att en åklagare eller domstol ska godkänna en europeisk utlämnandeorder respektive bevarandeorder, om den har utfärdats av en annan behörig myndighet (se ovan angående artikel 4.1 b och 4.3 b). Det kan därför framstå som en onödig omgång att ge Polismyndigheten eller andra brottsutredande myndigheter behörighet att utfärda en utlämnande- eller bevarandeorder om åklagare eller domstol likväl måste godkänna beslutet innan ordern kan översändas.³

Skäl som talar för att ändå utse även Polismyndigheten och andra brottsbekämpande myndigheter till behöriga myndigheter än

³ Jfr prop. 2016/17:218 s. 88 och den bedömning som gjordes beträffande hanteringen av en europeisk utredningsorder.

åklagare är att en sådan ordning skulle medge större utrymme till samarbete och bidra till en större effektivitet, vilket det beskrivna SPOC-samarbetet är ett tydligt exempel på. Polismyndigheten har genom SPOC-verksamheten etablerat ett arbetssätt som innebär att uppgifterna kan erhållas skyndsamt, vilket minskar risken för att de förändras eller raderas.

Skulle en europeisk utlämnandeorder i fråga om abonnentuppgifter och andra användaruppgifter eller en bevarandeorder endast få utfärdas av åklagare, riskeras effektiviteten i hanteringen av förfrågningar avseende de aktuella uppgifterna att gå förlorad. Polismyndigheten och övriga brottsbekämpande myndigheter har även möjlighet att i inhemska ärenden inhämta de aktuella uppgifterna med stöd av bestämmelserna i lagen om elektronisk kommunikation samt i vissa fall besluta om ett föreläggande om bevarande, vilket också talar för att samma myndigheter bör kunna hämta in och besluta om bevarande för motsvarande uppgifter från tjänstleverantörer i andra medlemsstater.

Det är mest ändamålsenligt att en order av aktuellt slag godkänns av åklagare, och inte av domstol, eftersom det är fråga om åtgärder som typiskt sett sker under förundersökningsstadiet. Det godkännande som krävs av åklagare bör kunna hanteras genom de it-system som myndigheterna använder i sin kommunikation med varandra, och bör kunna erhållas förhållandevis skyndsamt.

Mot bakgrund av det sagda bör Polismyndigheten, Säkerhetspolisen, Tullverket samt annan brottsbekämpande myndighet – utöver åklagare – vara behöriga att besluta om utfärdande av en europeisk utlämnandeorder avseende inhämtning av abonnentuppgifter och annan användarinformation samt om en europeisk bevarandeorder. Det bör följa av lag vilka myndigheter som är behöriga att utfärda en order av aktuellt slag samt att en order ska godkännas av åklagare. Det sistnämnda torde visserligen framgå direkt av artikel 4.1 b och 4.3 b men för att det ska vara tydligt att det är endast åklagare, och inte domstol, som ska godkänna en order i dessa fall bör det framgå av lag att det är åklagare som avses.

Vad som nu sagts ska även gälla i fråga om en sådan nödsituation som avses i artikel 4.5. De nu nämnda myndigheterna ska således också vara behöriga att i en sådan situation besluta om utfärdande av en europeisk utlämnandeorder avseende inhämtning av abonnentuppgifter och andra användaruppgifter samt om en euro-

peisk bevarandeorder. Ordern ska dock enligt EU-förordningen godkännas av åklagare innan den i artikeln angivna tidsfristen löper ut.

7.5.2 Skyldigheten att följa de regler som följer direkt av EU-förordningen behöver inte regleras i lag

Bedömning: Den behöriga utfärdande myndigheten är skyldig att följa de bestämmelser som reglerar de uppgifter som faller på myndigheten och som följer direkt EU-förordningen, utan att detta regleras i nationell rätt.

Skälen för bedömningen: EU-förordningen innehåller, som redogjorts för i avsnitt 7.2.2, flera bestämmelser som reglerar olika skyldigheter som tillkommer den myndighet som har utfärdat en europeisk utlämnande- eller bevarandeorder. Detta gäller t.ex. skyldigheten enligt artikel 8 att anmäla en utlämnandeorder som avser inhämtning av trafikuppgifter eller innehållsdata till den verkställande myndigheten i den andra medlemsstaten och skyldigheten enligt artikel 13.1 att som huvudregel underrätta den person vars uppgifter begärs genom en europeisk utlämnandeorder om att uppgifter har lämnats ut. De nämnda skyldigheterna följer alltså direkt av EU-förordningen. Eftersom EU-förordningen är direkt tillämplig ska den inte, som utvecklats i avsnitt 5.2, införlivas eller kompletteras i nationell rätt. Någon nationell reglering vad gäller de skyldigheter som följer av förordningen behövs därför inte.

7.5.3 Förfaranderegler för domstols godkännande av en europeisk utlämnandeorder

Förslag: För domstolens handläggning av ett ärende om godkännande av en europeisk utlämnandeorder för inhämtning av trafikuppgifter eller innehållsdata enligt artikel 4.2 b ska i tillämpliga delar gälla vad som är föreskrivet i rättegångsbalken om rättens tillstånd till hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation. Vid utfärdande av en sådan order ska även 27 kap. 22, 23–24, 31–33 samt 35 §§ rättegångsbalken gälla.

Skälen för förslaget

Rättegångsbalkens regler ska i tillämpliga delar gälla i ett ärende om domstolens godkännande av en order

EU-förordningen innehåller detaljerade regler om villkoren för utfärdande av en europeisk utlämnandeorder för trafikuppgifter och innehållsdata. Vidare finns bestämmelser om att en domstolsprövning krävs innan en utlämnandeorder översänds till mottagaren och om formerna för översändandet av en order till mottagaren.

Det ska alltså inte följa av nationell rätt att domstol ska godkänna en europeisk utlämnandeorder som avser trafikuppgifter och innehållsdata eftersom detta följer av artikel 4.2 b i EU-förordningen. Däremot krävs det nationella regler avseende vilket förfarande som ska gälla för domstolens godkännande. En europeisk utlämnandeorder av aktuellt slag motsvaras i nationell rätt av ett beslut om hemlig avlyssning respektive hemlig övervakning av elektronisk kommunikation (se avsnitt 6.9). Det bör därför följa av lag att det för domstolens handläggning gäller vad som föreskrivs i rättegångsbalken i tillämpliga delar. Detta innebär att de regler som anges i 27 kap. 21 § rättegångsbalken andra, tredje och sjätte stycket är tillämpliga. Dessa regler avser att det i tillståndet ska anges vilken tid tillståndet gäller, vilket telefonnummer, adress, kommunikationsutrustning eller geografiskt område tillståndet avser samt att tillståndet ska innehålla uppgift om villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Vidare är bestämmelserna om offentligt ombud i 27 kap. 26–30 §§ rättegångs-

balken tillämpliga, vilka behandlas närmare i avsnitt 10.4. Av hänvisningen till rättegångsbalken följer även att tingsrättens beslut får överklagas särskilt enligt 49 kap. 5 §, se även avsnitt 10.4. Även 27 kap. 34 § rättegångsbalken, som innehåller en alternativ forumregel för prövning av vissa frågor om hemliga tvångsmedel, är tillämplig.

Bestämmelserna i 27 kap. 22 och 23–24 §§ rättegångsbalken

Bestämmelserna i 27 kap. 22 och 23–24 §§ rättegångsbalken bör också ha motsvarande tillämplighet vid utfärdande av en europeisk utlämnandeorder. Dessa paragrafer uppställer bl.a. vissa begränsningar när det gäller vem eller vilka hemlig avlyssning av elektronisk kommunikation kan riktas mot. Detta innebär bl.a. att det inte är tillåtet att genomföra hemlig avlyssning av elektronisk kommunikation av telefonsamtal eller andra meddelanden där någon som yttrar sig inte skulle ha kunnat höras som vittne om det som sagts eller på annat sätt kommit fram (se 27 kap. 22 § första stycket och 36 kap. 5 § andra–sjätte styckena). Vidare regleras under vilka förutsättningar uppgifter som framkommit om ett annat brott än det som legat till grund för beslutet om avlyssning eller övervakning får användas (27 kap. 23 a §). Därutöver finns bestämmelser om granskning och bevarande av upptagning eller uppteckning som har gjorts (27 kap. 24 §).

Bestämmelserna i 27 kap. 31–33 och 35 §§ rättegångsbalken

Vid en begäran om rättslig hjälp enligt lagen om internationell rättslig hjälp i brottmål respektive vid utfärdande av en europeisk utredningsorder enligt lagen om en europeisk utredningsorder i fråga om hemlig avlyssning respektive hemlig övervakning av elektronisk kommunikation är bestämmelserna om underrättelse till enskild i 27 kap. 31–33 §§ rättegångsbalken endast tillämpliga när upptagning eller uppteckning av avlyssningen eller övervakningen sker i Sverige (se 4 kap. 26 § fjärde stycket lagen om internationell rättslig hjälp i brottmål respektive 2 kap. 18 § lagen om en europeisk utredningsorder).

Som princip i det internationella rättsliga samarbetet gäller att de åtgärder som vidtas i en annan stat med anledning av en svensk

ansökan om rättslig hjälp ska ske i enlighet med de villkor och förfaranden som gäller i den andra staten. Att införa svenska regler om sådana underrättelser i de aktuella fallen har inte bedömts vara förenligt med den grundläggande systematik som staterna har kommit överens om och förväntar sig gälla för det internationella straffrättsliga samarbetet.⁴ I fråga om utfärdande av en europeisk utlämnandeorder för inhämtning av trafikuppgifter eller innehållsdata ska uppgifterna inhämtas direkt från den tjänsteleverantör som en order riktats mot, utan bistånd av den andra staten (under förutsättning att det inte krävs verkställighetsåtgärder i de fall tjänsteleverantören inte följer ordern). Det finns alltså inte någon mottagande myndighet av ordern i den andra staten, till skillnad från vad som gäller vid en begäran om rättslig hjälp respektive vid utfärdande av en europeisk utredningsorder som ska ta ställning till orderns innehåll och vidta åtgärder för dess verkställighet. Eftersom en sådan motpart saknas, kan det inte ske någon underrättelse till enskild enligt den andra statens regelverk. Därför bör de nationella reglerna om underrättelseskyldighet äga motsvarande tillämpning vid utfärdande av en europeisk utlämnandeorder för inhämtning av trafikuppgifter respektive innehållsdata även om upptagning eller uppteckning sker utanför Sverige. Av samma skäl bör bestämmelserna i 27 kap. 35 § om dokumentation av beslut om hemliga tvångsmedel äga motsvarande tillämpning för en sådan order. Något ytterligare behov av särskilda förfaranderegler för den behöriga myndigheten eller domstolen bedöms inte föreligga. I avsnitt 10.4.6 återkommer vi till bestämmelserna om underrättelse till enskild.

7.5.4 Behörig verkställande myndighet

Förslag: Åklagarmyndigheten ska vara behörig verkställande myndighet enligt EU-förordningen.

Skälen för förslaget: Den verkställande myndigheten har, som redovisas i avsnitt 7.3.2, vissa uppgifter. En sådan är att, efter en anmälan enligt artikel 8.1, ta ställning till om en europeisk utlämnandeorder som avser trafikuppgifter eller innehållsdata ska vägras.

⁴ Prop. 2006/07:133 s. 57 och prop. 2016/17:218 s. 116.

En annan är att enligt artikel 16 besluta om verkställighet av en europeisk utlämnande- eller bevarandeorder för det fall mottagaren, dvs. det utsedda verksamhetsstället eller det rättsliga ombudet, inte följer ordern. Den verkställande myndigheten har vidare till uppgift att enligt artikel 15.1 ålägga tjänsteleverantören en sanktionsavgift för det fall denne inte fullgör sina skyldigheter. Slutligen ska den verkställande myndigheten ta del av information som rör en prövning enligt artikel 17.

Enligt lagen om internationell rättslig hjälp i brottmål får rättslig hjälp i brottmål i Sverige lämnas av åklagare eller domstol. Rollfördelningen motsvarar den som gäller i ett inhemskt straffrättsligt förfarande. Detsamma gäller enligt lagen om en europeisk utredningsorder, där huvudregeln är att åklagare är behörig att besluta om den begärda utredningsåtgärden ska erkännas och verkställas, om det inte är fråga om åtgärd som i ett motsvarande inhemskt ärende ska vidtas av domstol, dvs. åtgärder i samband med rättegång. Det sagda innebär att i det straffrättsliga samarbetet är det alltid en åklagare som tar ställning till om abonnentuppgifter eller andra användaruppgifter ska lämnas över till en annan stats myndigheter samt om lagrade uppgifter ska bli föremål för ett bevarandeföreläggande enligt 27 kap. 16 § rättegångsbalken. När det däremot gäller inhämtande av trafikuppgifter och innehållsdata är det alltid en domstol som beslutar om åtgärden kan vidtas. Denna ordning motsvarar som sagts den ordning som gäller i ett inhemskt ärende.

Mot denna bakgrund bör till att börja med Åklagarmyndigheten utses att vara verkställande myndighet enligt EU-förordningen när det rör sig om en europeisk utlämnandeorder som avser inhämtning av abonnentuppgifter och andra användaruppgifter samt en europeisk bevarandeorder.

Beslut om hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation fattas, efter en ansökan från åklagaren, under en förundersökning i svensk rätt av allmän domstol. Motsvarande gäller då en europeisk utredningsorder avseende samma typ av åtgärd ska verkställas i Sverige eller i en annan medlemsstat. Dessa omständigheter talar för att allmän domstol i dessa fall bör utses att vara behörig verkställande myndighet enligt EU-förordningen. En sådan order ska dock godkännas av domstol i den utfärdande staten enligt förordningen. Domstolen i den staten har alltså redan provat en utlämnandeorder som är föremål för verkställighet i Sverige,

varför det av detta skäl inte bör krävas att en domstol är verkställande myndighet i dessa fall. Därutöver ska den verkställande myndigheten endast pröva ett antal vägransgrunder, vilka anges i artikel 12 och 16 och inte, såsom vid verkställighet av en europeisk utredningsorder i Sverige, om det enligt nationell rätt är möjligt att vidta en åtgärd motsvarande hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation.

Vidare ska en verkställande myndighet – efter en anmälan enligt artikel 8.1 – ha möjlighet att med kort varsel hantera verkställighetsfrågan om en sådan nödsituation som avses i artikel 3.18 föreligger. Är en sådan situation för handen ska den verkställande myndigheten senast 96 timmar efter mottagandet, bedöma informationen i ordern och vid behov åberopa en eller flera vägransgrunder (artikel 12.1). Den verkställande myndigheten bör alltså ha beredskap för att med kort varsel kunna hantera en europeisk utlämnandeorder av nu aktuellt slag. De allmänna domstolarna i Sverige har förvisso jourberedskap på helger för prövning av bland annat häktningsfrågor och tillstånd till hemliga tvångsmedel, men åklagarna har, utöver häktningsberedskap under helgtid, jourberedskap dygnet om alla dagar i veckan. Åklagarmyndigheten ansvarar för åklagarväsendets jour- och beredskapssystem och indelar även Ekobrottsmyndighetens åklagare till jour och beredskap, se 13 § åklagarförordningen (2004:1265). Utgångspunkten är enligt Åklagarmyndighetens föreskrifter (ÅFS 2005:17) om åklagares jour- och beredskaps-tjänstgöring att samtliga allmänna åklagare kan indelas till jour. Både de allmänna domstolarna och åklagare har således beredskap för att kunna hantera en europeisk utlämnandeorder i brådskande fall, men åklagarna får anses ha bättre förutsättningar att hantera sådana frågor.

Den verkställande myndighetens uppgifter enligt artikel 12, som ska tillämpas för en europeisk utlämnandeorder som avser inhämtande av de nämnda uppgifterna, samt uppgifterna i artikel 16, inklusive uppgiften att besluta om sanktionsavgifter, är vidare inte sådana att de kräver att en domstol är involverad.

Vid en sammantagen bedömning av nu nämnda omständigheter framstår det enligt vår mening som mest ändamålsenligt att Åklagarmyndigheten även utses till att vara verkställande myndighet när det rör sig om en europeisk utlämnandeorder som avser inhämt-

ande av trafikuppgifter och innehållsdata. Åklagarmyndigheten föreslås således att vara verkställande myndighet i samtliga fall.

Uppgiften som verkställande myndighet innebär, som utvecklats i avsnitt 7.3.2 mottagande av anmälan samt verkställighet av en order. I fråga om bristande verkställighet kan det bli aktuellt att besluta om sanktionsavgift. För att det ska vara tydligt för den utfärdande myndigheten och för den enskilde tjänsteleverantören vem som kan besluta om sanktionsavgift framstår det som mest ändamålsenligt att uppgiften som verkställande myndighet tillkommer Åklagarmyndigheten ensam. Uppgiften bör således inte delas med Ekobrottsmyndigheten. Åklagarmyndighetens uppgift som verkställande myndighet bör följa av lag. Myndigheten bör på sedvanligt sätt ange vem inom organisationen som ansvarar för uppgiften. Kommissionen ska enligt artikel 31.1 b underrättas om vilken myndighet som är behörig verkställande myndighet enligt EU-förordningen.

Den enskildes rätt till effektiva rättsmedel enligt artikel 18 mot en europeisk utlämnandeorder behandlas i avsnitt 10.4. Utformningen av ett system med sanktionsavgifter redogörs för i avsnitt 9.

7.5.5 Den verkställande myndighetens prövning

Förslag: Åklagarens beslut i fråga om återopande av vägransgrunder enligt artikel 12.1 och verkställighet enligt artikel 16.6 ska innehålla skälen för beslutet.

Skälen för förslaget: I EU-förordningen finns regler om den verkställande myndighetens prövning enligt artikel 12 och 16 (se avsnitt 7.3.2). Förutom en prövning om någon vägransgrund ska tillämpas, gäller tidsfrister för att fatta beslut i frågan (se t.ex. artiklarna 12.1 och 16.2) och krav på att den verkställande myndigheten i vissa situationer ska informera och samråda med den utfärdande myndigheten (se t.ex. artiklarna 12.3, 16.6 och 16.7). I övrigt innehåller EU-förordningen i princip inte några regler om den verkställande myndighetens handläggning vid sin prövning om en order ska vägras eller fullföljas.

För åklagarens handläggning av brottmålsärenden finns ett omfattande regelverk (främst rättegångsbalken och förundersök-

ningskungörelsen). Vid annan handläggning hos åklagaren gäller förvaltningslagen (2017:900). Merparten av bestämmelserna i förvaltningslagen gäller dock inte för åklagarmyndigheternas brottsbekämpande verksamhet (3 §). Den verksamhet som regleras i EU-förordningen får anses vara brottsbekämpande. Om det bedöms finnas behov av särskilda förfaranderegler bör dessa således införas i lag, antingen direkt eller genom hänvisningar till andra bestämmelser. Vid bedömningen av behovet av särskilda förfaranderegler bör genomföranden av andra rättsakter beaktas.

Regeringen har i fråga om andra EU-rättsakter på området bedömt att behovet av förfaranderegler för åklagarens handläggning är begränsat.⁵ Skälet till det har framför allt varit att åklagaren inte ska göra någon materiell prövning av de omständigheter eller överväganden som ligger bakom det utländska beslutet och att prövningen således är av formellt slag och endast innefattar en kontroll av att det föreligger förutsättningar för erkännande och verkställighet. Samma skäl gör sig gällande nu. Utgångspunkten bör därmed vara densamma som de nämnda rättsakterna, dvs. att behovet av förfaranderegler för åklagarens handläggning är begränsat. Det finns dock skäl att överväga behovet av att komplettera EU-förordningen med vissa förfaranderegler.

Förutsättningarna för den materiella prövningen, dvs. om det finns skäl att återopa en vägransgrund följer direkt av EU-förordningen och är direkt tillämpliga. Tidsfrister för åklagarens beslut och åklagarens samråds- och underrättelseskyldighet gentemot den utfärdande myndigheten regleras i förordningen och behöver inte heller regleras ytterligare. I EU-förordningen finns bestämmelser om olika beslut som åklagaren ska fatta under handläggningen av ett ärende om en sådan order som omfattas av EU-förordningen. Av artiklarna 12.3 och 16.8 i EU-förordningen följer att den verkställande myndigheten är skyldig att informera den utfärdande myndigheten och mottagaren om sina beslut. Det är mot den bakgrunden lämpligt att ställa upp ett krav på att åklagarens beslut ska motiveras, vilket bör framgå av lag (jfr 4 kap. 4 § lagen [2020:968])

⁵ Se t.ex. prop. 2014/15:116 s. 70 angående rådets rambeslut 2009/829/RIF om tillämpning mellan Europeiska unionens medlemsstater av principen om ömsesidigt erkännande på beslut om övervakningsåtgärder som ett alternativ till tillfälligt frihetsberövande och prop. 2019/20:198 s. 69–70 angående kompletterande bestämmelser till EU:s förordning om ömsesidigt erkännande av beslut om frysning och beslut om förverkande.

med kompletterande bestämmelser till EU:s förordning om ömsesidigt erkännande av beslut om frysning och beslut om förverkande).

När en anmälan om en europeisk utlämnandeorder översänds till Sverige enligt artikel 8.1 ska åklagaren enligt artikel 12.1 överväga om det finns skäl åberopa någon eller några av de vägransgrunder som anges i artikeln. En av vägransgrunderna är fullföljandet av ordern skulle strida mot principen *ne bis in idem*. En bedömning ska alltså göras om den person som ordern avser tidigare har blivit dömd för samma gärning som den som orden grundar sig på. För att åklagaren ska kunna ta ställning till den frågan behöver åklagaren tillgång till uppgifter i belastningsregistret.

Regeringen har vid genomförandet av andra EU-rättsakter på området bedömt att den verkställande myndighetens tillgång till belastningsregistret inte behöver regleras i lag.⁶ Åklagarens behov av tillgång till uppgifter i belastningsregistret i de aktuella ärendena bedöms kunna tillgodoses genom 6 § första stycket 4 lagen (1998:620) om belastningsregister och 10 § första stycket 3 förordningen (1999:1134) om belastningsregister i fråga om uppgifter i belastningsregistret. Några ytterligare lagstiftningsåtgärder i detta avseende behövs alltså inte.

7.5.6 Centralmyndighet

Bedömning: Det finns inte skäl att utse en centralmyndighet för den administrativa hanteringen av en europeisk utlämnandeorder eller europeisk bevarandeorder.

Skälen för bedömningen: En medlemsstat kan enligt artikel 4.6 utse en eller flera centralmyndigheter för att ansvara för det administrativa översändandet och mottagandet av en utlämnandeorder respektive bevarandeorder samt för annan relevant korrespondens.

Redan i dag har medlemsstaternas myndigheter direktkontakt med varandra vid ansökningar om rättslig hjälp i brottmål och vid utfärdande av en europeisk utredningsorder. Vid genomförandet av direktivet om en europeisk utredningsorder ansåg regeringen att det inte fanns behov av att utse en centralmyndighet. Regeringen

⁶Se t.ex. prop. 2014/15:116 s. 71 och 2016/17:218 s. 173.

konstaterade då att ytterst få av ärendena enligt lagen om internationell rättslig hjälp i brottmål och som avsåg en medlemsstat i EU skickades via eller hanterades av centralmyndigheten på Justitiedepartementet. Vidare var erfarenheterna av direktkontakter mellan medlemsstaternas myndigheter goda. Regeringen hade inte heller några farhågor om att direktkontakter inte skulle fungera väl enligt det samarbete som regleras i direktivet.⁷

Det finns inte skäl att göra någon annan bedömning vad gäller kommunikationen mellan medlemsstaternas myndigheter i fråga om EU-förordningen. Uppgiften att översända en europeisk utlämnande- eller bevarandeorder samt att sköta all kommunikation i anledning av ordern med den andra statens behöriga och verkställande myndigheter bör således anförtros den behöriga utfärdande myndigheten, dvs. åklagaren eller någon annan myndighet som är behörig att utfärda en order. Den åklagare eller myndighet som har utfärdat en europeisk utlämnande- eller bevarandeorder ska således – i förekommande fall – svara för översändande av ordern till mottagaren eller den verkställande myndigheten och all annan kommunikation som följer av att en order utfärdats.

7.5.7 Behörig domstol

Förslag: Stockholms tingsrätt ska vara behörig domstol enligt artikel 17 i EU-förordningen.

Reglerna om domstols handläggning i brottmål och överklagande av domstols beslut ska vara tillämpliga vid handläggningen. Handläggningen ska som huvudregel ske skriftligen. Sammanträde ska hållas endast om mottagaren begär det, om det inte är uppenbart att den europeiska utlämnandeordern ska upphävas. Domstolen ska avgöra ett ärende enligt artikel 17 inom 30 dagar efter att den utfärdande myndigheten har begärt domstolens prövning. Endast om det finns särskilda skäl får denna tidsfrist överskridas.

Domstolens beslut ska kunna överklagas till hovrätt.

⁷ Prop. 2016/17:218 s. 88.

Skälen för förslaget

Behörig domstol

Som följer av avsnitt 7.4 ska den behöriga domstolen i den utfärdande staten enligt artikel 17 i EU-förordningen – på begäran av den myndighet som utfärdat en europeisk utlämnandeorder – pröva om efterlevnaden av en europeisk utlämnandeorder skulle strida mot en skyldighet enligt ett tredjelands tillämpliga rätt.

Huvudregeln i svensk rätt är att alla allmänna domstolar eller alla allmänna förvaltningsdomstolar har behörighet att handlägga alla typer av mål som hör till respektive domstolsslag. Vilken domstol som är behörig att ta upp ett visst enskilt mål till prövning följer av ett stort antal forumregler.

Forumreglerna för allmän domstol och allmän förvaltningsdomstol är generella i det avseendet att i princip vilken tingsrätt respektive förvaltningsrätt som helst kan bli behörig. Det stora flertalet typer av mål faller också under tillämpningsområdet för dessa bestämmelser. Flertalet måltyper kan således förekomma vid alla allmänna domstolar respektive alla allmänna förvaltningsdomstolar.

Med undantag från de generella forumreglerna är för vissa typer av mål föreskrivet att de ska handläggas av specialdomstolar eller särskilda domstolar (jfr 10 kap. 17 § första stycket 1 rättegångsbalken). För vissa speciella typer av mål och ärenden finns vidare särskilda forumregler som innebär att dessa mål eller ärenden koncentreras till en eller vissa domstolar (jfr 10 kap. 17 § första stycket 2 och 3 rättegångsbalken).

Specialdestinering av måltyper till viss domstol bör som utgångspunkt undvikas. En sådan lösning kan emellertid användas om behovet av särskild kompetens inte kan tillgodoses genom domstolsintern specialisering på grund av att målunderlaget är för litet, ett krav på koncentration följer av Sveriges internationella åtaganden, eller det behövs till följd av att särskilda ledamöter deltar i handläggningen. När det gäller målunderlag kan koncentration av mål till en eller ett fåtal domstolar vara mer ändamålsenligt om detta är så begränsat att inte ens ett par domare på varje domstol kan få någon egentlig erfarenhet av att handlägga den aktuella måltypen.⁸

⁸ SOU 2010 :44 s. 377–381. Regeringen har uttalat att de principiella överväganden som görs i betänkandet ska gälla som inriktning för det fortsatta arbetet med att säkerställa att mål och

Det kan konstateras att specialdestinering av mål som är hänförliga till artikel 17 i EU-förordningen inte kan motiveras på grund av internationella åtaganden eller att måltypen kräver att särskilda ledamöter deltar i avgörandet.

Det är vidare svårt att med någon mån av säkerhet uttala sig om hur många mål som med stöd av artikel 17 kommer att kräva hantering av svensk domstol. Det beror dels på antalet utlämnandeorder som svenska behöriga myndigheter utfärdar med stöd av EU-förordningen, dels på hur många av dessa där mottagaren, dvs. den enskilde tjänsteleverantören, invänder att en order strider mot en skyldighet enligt ett tredjelands tillämpliga rätt. Det kan dock antas att ett begränsat antal ärenden kommer att bli föremål för en domstolsprövning enligt artikel 17. Antalet mål kan emellertid inte ensamt vara avgörande för om en specialdestinering bör ske eller inte. Av betydelse är också om den juridiska komplexiteten i ärendena är stor, förfarandereglerna i hög grad avviker från de allmänna processrättsliga reglerna eller när det för en korrekt prövning av saken krävs särskild fackkunskap.⁹

Som utvecklats i avsnitt 7.3 ska den behöriga domstolen bl.a. granska om tredjelands rätt förbjuder rövande av de berörda uppgifterna och om så är fallet avgöra om den europeiska utlämnandeordern ska upprätthållas eller upphävas. Denna bedömning ska i sin tur enligt artikel 17.6 baseras på flera olika omständigheter hänförliga till tredjelands rätt, bl.a. vad gäller möjliga konsekvenser för mottagaren eller för tjänsteleverantören av att efterleva den europeiska utlämnandeordern, vilket inkluderar eventuella sanktioner. Det kan alltså konstateras att mål som är föremål för domstolsprövning enligt artikel 17 i många fall kan kräva komplexa juridiska bedömningar och särskild kunskap om tredjelands rätt. Mot denna bakgrund och eftersom antalet ärenden som kan bli föremål för domstolsprövning enligt artikel 17 kan antas vara begränsat bedömer vi att en specialdestinering bör ske.

Stockholms tingsrätt är laga domstol i mål och ärenden enligt flera författningar av internationell karaktär inom olika områden, t.ex. lagen (1972:260) om internationellt samarbete rörande verkställighet av brottmålsdom, ifråga om ansökan om överflyttning av

ärenden i domstol avgörs effektivt och med hög kvalitet (prop. 2011/12:1 utg. omr.4 s. 27).

Se även t.ex. prop. 2014/15 :29 s. 158.

⁹ Prop. 2014/15 :29 s. 158.

barn enligt lagen (1989:14) om erkännande och verkställighet av utländska vårdnadsavgöranden m.m. samt är exklusivt forum för de flesta patentmål och konkurrens mål. Domstolen har alltså stor erfarenhet av att hantera mål med internationell karaktär eller som av annat skäl kräver specialkompetens. Stockholms tingsrätt bör mot denna bakgrund även vara behörig domstol att pröva mål enligt artikel 17 i EU-förordningen.

Närmare om förfarandet vid domstolens prövning

Den behöriga domstolens prövning enligt artikel 17 avser inte de materiella förutsättningarna för utfärdande av en europeisk utlämnandeorder, utan prövningen är koncentrerad till frågan om fullföljande av en sådan order skulle stå i strid med en skyldighet enligt tredjelands rätt. I artikeln finns vissa regler om tidsfrister för mottagaren av en order att göra en s.k. motiverad invändning (se artikel 17.2). Vid tillämpning av förfarandena enligt artikel 17 ska tidsfristerna beräknas enligt nationell rätt (se artikel 17.9). Därutöver saknas regler om den behöriga domstolens handläggning av frågan. Med hänsyn till den EU-rättsliga principen om processuell autonomi får det i stället vara upp till varje medlemsstat att besluta om.

När det gäller hanteringen av tidsfristerna i ett svenskt domstolsförfarande kan följande framhållas.

Som framhålls i skäl 2 till EU-förordningen är effektiva förfaranden för att inhämta elektroniska bevis av yttersta vikt för att bekämpa brottslighet. Detta kännetecknas av de förhållandevis korta tidsfrister som gäller enligt EU-förordningen avseende t.ex. åberopande av vägransgrunder (tio dagar som huvudregel) och verkställighet (fem arbetsdagar). En order som omfattas av EU-förordningen utfärdas dessutom under en pågående brottmålsprocess i den utfärdande medlemsstaten, låt vara att domstolsprocessen ska ske i samma stat. För att inte äventyra syftet med EU-förordningen bör domstolens handläggning av en fråga om lagkonflikt enligt artikel 17 därför ske med viss skyndsamhet. För

att Sverige ska uppfylla sina internationella förpliktelser finns det alltså behov av ett särskilt skyndsamhetskrav.¹⁰

Ett krav på skyndsamt handläggning kan utformas på olika sätt, antingen som ett allmänt utformat krav eller i form av en särskild angiven tidsfrist. När det konstateras att en måltyp har behov av extra skyndsamt bör alltid den minst ingripande åtgärd som kan möta behovet användas. Bestämmelser om att en måltyp ska handläggas skyndsamt, dvs. med förtur, bör användas när det finns behov av att avgöra målen inom en tid av några få månader från det att förfarandet inleds i domstolen eller överklagandefristen går ut, medan tidsfrister bör användas när det finns behov av att ta upp målen till prövning inom en kortare tid, normalt högst en månad, från det att förfarandet inleds i domstolen eller överklagandefristen går ut och i de fall där det krävs enligt Sveriges internationella åtaganden. Det kan noteras att ett krav på skyndsamt handläggning med närmare bestämda tidsfrister är förbehållen lagstiftning där skyndsamhetskravet korresponderar med ett särskilt starkt skyddsintresse.¹¹

Syftet med EU-förordningens bestämmelser om en effektiv hantering av bevarande respektive utlämnande av elektroniska bevis får anses utgöra ett sådant starkt skyddsintresse att det är motiverat att införa en bestämd tidsfrist för domstolens prövning enligt artikel 17. Med hänsyn till de ovan nämnda tidsfristerna som gäller enligt EU-förordningen bör fristen vara förhållandevis kort, men ändå ge domstolen en rimlig tid att avgöra frågan efter att den utfärdande myndigheten har begärt domstolens prövning. En tidsfrist om 30 dagar är enligt vår mening en lämplig avvägning. En sådan tidsfrist bör dock kunna överskridas om det finns särskilda skäl. Sådana skäl kan t.ex. vara att domstolen inte fått svar på en begäran enligt artikel 17.7 om innehållet i tredjelandets rätt inom tidsfristen eller fått svar först kort innan tidsfristen löper ut. Tidsfristen bör följa av lag.

En annan fråga gäller om en fråga om lagkonflikt enligt artikel 17 ska prövas i ett muntligt förfarande eller skriftligt förfarande i tingsrätten. Det kan konstateras att en motiverad invändning enligt

¹⁰ Fyra principer gäller för när det finns ett behov av särskilda åtgärder för att uppnå särskild skyndsamt. Dessa är om prövningen har betydelse för om en person ska vara fortsatt frihetsberövad, om särskilt skyddsvärda eller utsatta personer är parter och utgången i målet har betydelse för deras grundläggande levnadsbetingelser, om avgörandet blir meningslöst om det inte fattas inom viss kortare tid eller om särskilda skyndsamhetskrav följer av Sveriges internationella åtaganden., se SOU 2010:44 s. 335–338.

¹¹ SOU 2010:44 s. 351–352.

artikel 17.1 redan från början ska innehålla alla de uppgifter som krävs för att frågan ska kunna prövas. Utrymmet är vidare begränsat för bedömningar som kräver muntlig handläggning. Det torde därför endast vara sällan vara nödvändigt med en muntlig förhandling i ärendet. Huvudregeln bör därför vara att ett ärende ska kunna avgöras på handlingarna. Av rättssäkerhetsskäl bör dock sammanträde hållas, om det begärs av mottagaren, dvs. tjänsteleverantörens utsedda verksamhetsställe eller rättsliga ombud. Sammanträde behöver dock inte hållas om det är uppenbart att den europeiska utlämnandeordern ska upphävas. Till sammanträdet ska mottagaren och den utfärdande myndigheten kallas.

För rättens prövning bör de allmänna reglerna i brottmål gälla, dvs. i första hand de bestämmelser som finns i rättegångsbalken. Eftersom det inte ska hållas någon huvudförhandling kommer tingsrätten enligt 1 kap. 3 § rättegångsbalken att vara domför med en lagfaren domare. Övriga regler som kan bli tillämpliga, är t.ex. reglerna om jäv, anteckningar vid sammanträde, bevisupptagning och offentlighet och ordning. Rättegångsbalkens regler om domstols handläggning i brottmål innebär vidare bl.a. att reglerna i 30 kap. rättegångsbalken om motivering av beslut gäller för domstolen.

Slutligen bör den behöriga domstolens slutliga beslut avseende en prövning enligt artikel 17 i EU-förordningen kunna överklagas. Här bör rättegångsbalkens regler om överklagande av tingsrätts slutliga beslut i ett brottmål ha motsvarande tillämpning. Av 49 kap. 13 § femte stycket rättegångsbalken följer att prövningstillstånd inte krävs för prövning i hovrätten.

Det bör således uttryckligen anges att reglerna om domstols handläggning i brottmål och överklagande av domstols beslut ska vara tillämpliga vid handläggningen av en fråga enligt artikel 17.

8 Direktivet (EU) 2023/1544

8.1 Inledning

Direktiv (EU) 2023/1544 utgör ett komplement till EU-förordningen och vissa andra rättsliga instrument som rör inhämtande av elektroniska bevis i straffrättsliga förfaranden. I EU-direktivet finns bestämmelser om att tjänsteleverantörer som omfattas av regleringen ska vara skyldiga att utse minst ett utsett verksamhetsställe eller ett rättsligt ombud i unionen, som medlemsstaterna ska kunna vända sig till med framställningar om insamling av bevis i straffrättsliga förfaranden. Ett av syftena med EU-direktivet är att undvika olika lösningar i medlemsstaterna och i stället skapa en enhetlig unionslösning (se skäl 1–4).

Uppdraget för de utsedda verksamhetsställena och rättsliga ombuden är att ta emot, följa och fullfölja förelägganden och beslut om insamling av bevis i straffrättsliga förfaranden från medlemsstater. Av EU-direktivet följer också att var och en av medlemsstaterna ska utse en eller flera centrala myndigheter med uppgift att samarbeta och samordna åtgärder med andra centrala myndigheter och kommissionen samt säkerställa tillämpningen av direktivet.

Vi ska enligt våra direktiv analysera hur EU-direktivet bör genomföras i svensk rätt samt föreslå vilken eller vilka myndigheter som bör utses till centrala myndigheter enligt EU-direktivet. Vidare ska vi analysera behovet av författningsändringar eller andra åtgärder som krävs för att den eller de föreslagna myndigheterna ska kunna utföra sina uppdrag enligt EU-direktivet på ett effektivt och rättssäkert sätt, och lämna nödvändiga författningsförslag. Kapitlet inleds med en redogörelse för EU-direktivets innehåll (avsnitt 8.2). Därefter följer våra överväganden och förslag (avsnitt 8.3–8.6).

8.2 EU-direktivets innehåll

8.2.1 Tillämpningsområde och definitioner

EU-direktivet innehåller regler om skyldigheten för vissa tjänsteleverantörer som erbjuder tjänster inom unionen att utse verksamhetsställen och rättsliga ombud. Direktivet syftar till att fastställa harmoniserade regler för inhämtande av elektroniska bevis i straffrättsliga förfaranden för att på så sätt underlätta en effektivare brottsbekämpning (artikel 1 och skäl 5 i direktivet).

De utsedda verksamhetsställen och rättsliga ombuden är enligt artikel 1.2 i EU-direktivet mottagare av beslut och förelägganden för insamling av elektroniska bevis som utfärdats med stöd av EU-förordningen, direktivet om en europeisk utredningsorder och den konvention som upprättats av rådet i enlighet med artikel 34 i fördraget om Europeiska unionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater (EU-konventionen). EU-direktivet är enligt nämnda artikel även tillämpligt på beslut och förelägganden för insamling av elektroniska bevis som utfärdats med stöd av nationell rätt och som en medlemsstat riktar till en fysisk eller juridisk person som agerar som rättsligt ombud eller som utsett verksamhetsställe åt en tjänsteleverantör på den medlemsstatens territorium, dvs. inhemska förfaranden (se skäl 6). EU-direktivet har således ett vidare tillämpningsområde än att endast se till att samarbetet fungerar enligt EU-förordningen och omfattar även inhämtning av motsvarande elektroniska bevis med stöd av direktivet om en europeisk utredningsorder och EU-konvention. Därutöver ska behöriga myndigheter kunna vända sig till det utsedda verksamhetsstället eller det rättsliga ombudet i inhemska ärenden för att få ut eller bevara elektronisk bevisning. Oaktat artikel 1.2 följer av artikel 1.3 att direktivet inte påverkar de nationella myndigheternas befogenheter att i enlighet med unionsrätten och nationell rätt rikta framställningar direkt till tjänsteleverantörer som är etablerade på deras territorium i syfte att samla in elektroniska bevis i straffrättsliga förfaranden (se även skäl 9). Sistnämnda bestämmelse ger således de behöriga myndigheterna en möjlighet att använda sig av andra regelverk för att inhämta motsvarande uppgifter, dvs. EU-direktivet är inte avsett att ersätta dessa.

Medlemsstaterna får enligt artikel 1.4 inte ålägga tjänsteleverantörer ytterligare skyldigheter utöver dem som följer av direktivet.

Detta gäller i synnerhet i fråga om att utse verksamhetsställen eller rättsliga ombud, för de ändamål som anges i artikel 1.2.

EU-direktivet är tillämpligt på tjänsteleverantörer enligt definitionen i artikel 2.1 som erbjuder sina tjänster i unionen. Det är inte tillämpligt på tjänsteleverantörer som är etablerade på en enda medlemsstats territorium och som erbjuder tjänster uteslutande på den medlemsstatens territorium (artikel 1.5, se även skäl 8).

Artikel 2 innehåller definitioner av de begrepp som används i EU-direktivet. Begreppet tjänsteleverantör i artikel 2.1 har samma innebörd som motsvarande begrepp i EU-förordningen (se även skäl 14 och 15 samt avsnitt 6.2). Detsamma gäller begreppet ”erbjuda tjänster i unionen” i artikel 2.3. För att fastställa huruvida en tjänsteleverantör erbjuder tjänster i unionen krävs enligt definitionen, utöver en bedömning av huruvida tjänsteleverantören gör det möjligt för fysiska eller juridiska personer i en eller flera medlemsstater att använda dess tjänster, att det finns en betydande anknytning till unionen. En sådan betydande anknytning till unionen ska enligt definitionen anses föreligga om tjänsteleverantören har ett verksamhetsställe i en medlemsstat, eller i avsaknad av verksamhetsställe, att det finns ett betydande antal användare i en eller flera medlemsstater eller om verksamheten är inriktad på en eller flera medlemsstater. I skäl 10 och 11 utvecklas innebörden av begreppet ”erbjuda tjänster i unionen”.

Artikeln innehåller även en definition av begreppet erbjudande av tjänster på en medlemsstats territorium (artikel 2.2). Begreppet har i huvudsak samma innebörd som termen erbjuda tjänster i unionen, med den skillnaden att begreppet avser tjänsteleverantörens anknytning till den enskilda medlemsstaten.

Även begreppen verksamhetsställe, utsett verksamhetsställe samt rättsligt ombud har samma definition som i EU-förordningen. Begreppen definieras enligt artikel 2.4–2.6 på följande sätt.

verksamhetsställe: en enhet som de facto utövar ekonomisk verksamhet under en obegränsad tid genom en stabil infrastruktur varifrån tillhandahållandet av tjänster genomförs eller verksamheten förvaltas.

utsett verksamhetsställe: ett verksamhetsställe med ställning som juridisk person vilket skriftligen utsetts av en tjänsteleverantör som är etablerad i en medlemsstat, och vilket deltar i ett rättsligt instrument som avses i artikel 1.2, för de ändamål som avses i artiklarna 1.1 och 3.1.

rättsligt ombud: en fysisk eller juridisk person som skriftligen utsetts av en tjänsteleverantör som inte är etablerad i en medlemsstat, och som

deltar i ett rättsligt instrument som avses i artikel 1.2, för de ändamål som avses i artiklarna 1.1 och 3.1.

Det kan särskilt påpekas att det görs en skillnad mellan begreppen ”verksamhetsställe” och ”utsett verksamhetsställe”.

8.2.2 Skyldigheten att utse verksamhetsställen och rättsliga ombud

Artikel 3 reglerar tjänsteleverantörernas skyldighet att utse verksamhetsställen eller rättsliga ombud.

Medlemsstaterna ska enligt artikel 3.1 säkerställa att tjänsteleverantörer som erbjuder tjänster i unionen utser minst en mottagare för mottagande, efterlevnad och verkställighet av beslut och förelägganden som omfattas av direktivets tillämpningsområde enligt artikel 1.2 som utfärdats av medlemsstaternas behöriga myndigheter för insamling av bevis i straffrättsliga förfaranden, enligt följande:

- a) För tjänsteleverantörer som är etablerade i unionen och som är juridiska personer ska de medlemsstater där tjänsteleverantörerna är etablerade säkerställa att dessa tjänsteleverantörer utser det eller de utsedda verksamhetsställen som ansvarar för mottagande, efterlevnad och verkställighet av de beslut och förelägganden som anges ovan.
- b) För tjänsteleverantörer som inte är etablerade i unionen och som är juridiska personer ska medlemsstaterna säkerställa att sådana tjänsteleverantörer som erbjuder tjänster på deras territorium utser det eller de rättsliga ombud som ansvarar för mottagande, efterlevnad och verkställighet av de beslut och förelägganden som anges ovan, i de medlemsstater som deltar i de instrument som avses i artikel 1.2.
- c) För tjänsteleverantörer som är etablerade i medlemsstater som inte deltar i de instrument som avses i artikel 1.2 ska medlemsstaterna säkerställa att de tjänsteleverantörer som erbjuder tjänster på deras territorium utser det eller de rättsliga ombud som ansvarar för mottagande, efterlevnad och verkställighet av de beslut och förelägganden som anges ovan i de medlemsstater som deltar i de angivna instrumenten.

Danmark deltar inte i samarbetet enligt i EU-förordningen (se skäl 101 i EU-förordningen). När det gäller direktivet om en europeisk utredningsorder deltar Danmark och Irland inte i samarbetet enligt det direktivet. När det gäller EU-konvention har samtliga medlemsstater ratificerat EU-konventionen utom Grekland och Kroatien.

Syftet med artikel 3.1 är att se till att tjänsteleverantörer som är erbjuder tjänster inom unionen utser i vart fall ett verksamhetsställe eller ett rättsligt ombud i en medlemsstat som deltar i de nämnda instrumenten så att det blir möjligt att på ett smidigt sätt inhämta uppgifter från dessa tjänsteleverantörer (se skäl 12¹). Detta torde dock förutsätta att denna tjänsteleverantör erbjuder tjänster i mer än en medlemsstat (se artikel 1.5). Det ska noteras att även om vissa stater inte samarbetar enligt de instrument som anges i artikel 1.2 i direktivet är samtliga medlemsstater bundna av direktivet. Exempelvis kommer tjänsteleverantörer i Danmark att behöva utse ett rättsligt ombud i en annan medlemsstat enligt artikel 3.1 c. Det ska slutligen betonas att artikel 1.2 och 3.1 tillsammans inte bör kunna tolkas på annat sätt att de verksamhetsställen och rättsliga ombud som utses ska kunna ta emot beslut och förelägganden enligt samtliga tre rättsakter som anges i artikel 1.2 och i inhemska ärenden.

I sammanhanget ska det påpekas att det står tjänsteleverantörerna fritt att välja i vilken medlemsstat de utser sitt verksamhetsställe eller rättsliga ombud och en medlemsstat kan t.ex. inte tvinga en tjänsteleverantör att utse en sådan mottagare just i den staten (se skäl 13). Detta gäller dock med vissa begränsningar då medlemsstaterna ska enligt artikel 3.2 säkerställa att de mottagare som avses i artikel 3.1

- a) är etablerade eller har sin hemvist i en medlemsstat där tjänsteleverantörerna erbjuder sina tjänster, och
- b) kan bli föremål för verkställighetsförfaranden.

Enligt artikel 3.3. ska medlemsstaterna vidare säkerställa att beslut och förelägganden som omfattas av direktivets tillämpningsområde riktas till det utsedda verksamhetsställe eller rättsliga ombud som utsetts för det ändamålet i enlighet med artikel 3.1.

¹ Det kan noteras att den svenska översättningen av den andra meningen är felöversatt och att orden ”se till” torde föregås av en negation (jfr den engelska översättningen).

Medlemsstaterna ska därutöver enligt artikel 3.4 säkerställa att tjänsteleverantörer som är etablerade eller erbjuder tjänster på deras territorium ger sina utsedda verksamhetsställen och rättsliga ombud, oaktat var de utses, de befogenheter och resurser som krävs för att efterleva beslut och förelägganden som omfattas av direktivets tillämpningsområde och som mottas från en medlemsstat. En medlemsstat ska också enligt samma bestämmelse kontrollera att de utsedda verksamhetsställena eller rättsliga ombuden i den medlemsstaten av tjänsteleverantörerna har fått de befogenheter och resurser som krävs för att efterleva beslut och förelägganden som mottas från en medlemsstat och att de samarbetar med de behöriga myndigheterna vid mottagandet av dessa beslut och förelägganden. Se även skäl 16.

Medlemsstaterna ska enligt artikel 3.5 säkerställa att både det utsedda verksamhetsstället eller det rättsliga ombudet och tjänsteleverantören kan hållas solidariskt ansvariga för bristande efterlevnad av de skyldigheter som följer av den tillämpliga rättsliga ramen vid mottagande av beslut och förelägganden som omfattas av direktivets tillämpningsområde, så att var och en av dem kan bli föremål för sanktioner vid bristande efterlevnad. I synnerhet ska säkerställas att det inte är möjligt för tjänsteleverantören eller det utsedda verksamhetsstället, eller i förekommande fall det rättsliga ombudet, att använda avsaknaden av lämpliga interna rutiner mellan tjänsteleverantören och det utsedda verksamhetsstället eller det rättsliga ombudet för att rättfärdiga sin bristande efterlevnad av dessa skyldigheter. Solidariskt ansvar ska inte gälla för något som antingen tjänsteleverantören eller det utsedda verksamhetsstället, eller det rättsliga ombudet i förekommande fall, har gjort eller försummat att göra och som utgör ett brott i den medlemsstat som påför sanktionerna. Se även skäl 16.

Medlemsstaterna ska slutligen enligt artikel 3.6 säkerställa att tjänsteleverantörer som erbjuder tjänster i unionen den 18 februari 2026 är skyldiga att utse utsedda verksamhetsställen eller rättsliga ombud senast den 18 augusti 2026 och att tjänsteleverantörer som börjar erbjuda tjänster i unionen efter den 18 februari 2026 är skyldiga att utse utsedda verksamhetsställen eller rättsliga ombud inom sex månader efter den dag då de börjar erbjuda tjänster i unionen (se även skäl 7).

8.2.3 Övriga bestämmelser

Av artikel 4.1 följer att medlemsstaterna ska säkerställa att varje tjänsteleverantör som är etablerad eller erbjuder tjänster på deras territorium skriftligen underrättar den centralmyndighet som utsetts i enlighet med artikel 6 i den medlemsstat där dess utsedda verksamhetsställe är etablerat eller där dess rättsliga ombud har sin hemvist om kontaktuppgifterna för det verksamhetsstället eller rättsliga ombudet och om eventuella ändringar av dessa. I denna underrättelse ska det anges på vilket eller vilka av unionens officiella språk som framställningar kan riktas till det utsedda verksamhetsstället eller rättsliga ombudet. Dessa språk ska innefatta ett eller flera av de officiella språk i den medlemsstat där det utsedda verksamhetsstället är etablerat eller det rättsliga ombudet har sin hemvist (artikel 4.2).

Om en tjänsteleverantör utser flera utsedda verksamhetsställen eller flera rättsliga ombud ska medlemsstaterna säkerställa att en sådan tjänsteleverantör i den underrättelse som avses i artikel 4.1 anger det exakta territoriella tillämpningsområdet för utseendet av dessa utsedda verksamhetsställen eller rättsliga ombud. I underrättelsen ska det anges på vilket eller vilka av de officiella språken i unionen eller medlemsstaterna som framställningar kan riktas till vart och ett av de utsedda verksamhetsställena eller de rättsliga ombuden (artikel 4.3).

Medlemsstaterna ska enligt artikel 4.4 säkerställa att den information som avses i artikel 4 offentliggörs på en särskild webbsida hos det europeiska straffrättsliga nätverket och att informationen uppdateras regelbundet. Informationen får spridas vidare i syfte att underlätta de behöriga myndigheternas åtkomst till den.

Artikel 5 innehåller bestämmelser om sanktioner. Bestämmelserna om sanktioner behandlas i avsnitt 9.

Enligt artikel 6.1 ska medlemsstaterna utse en eller flera centralmyndigheter för att säkerställa att direktivet tillämpas på ett enhetligt och proportionellt sätt. Medlemsstaterna ska underrätta kommissionen om den eller de centralmyndigheter som de utser (artikel 6.2).

Medlemsstaterna ska enligt artikel 6.3 säkerställa att centralmyndigheterna samordnar och samarbetar med varandra och vid behov med kommissionen, och att centralmyndigheterna förser varandra med information och stöd. Samordning, samarbete och

tillhandahållande av information och stöd ska i synnerhet omfatta verkställighetsåtgärder.

Artikel 7 innehåller bestämmelser om införlivande av EU-direktivet. Artikel 7.1 stadgar att EU-direktivet ska vara införlivat senast den 18 februari 2026. Artikel 8 reglerar utvärdering av EU-direktivets bestämmelser och riktar sig till kommissionen. Av artikel 9 följer att direktivet trädde i kraft den 18 augusti 2023.

8.3 Utsedda verksamhetsställen och rättsliga ombud

8.3.1 Skyldigheten att utse verksamhetsställen och rättsliga ombud

Förslag: En tjänsteleverantör som är etablerad i Sverige ska utse ett verksamhetsställe i Sverige eller i en annan medlemsstat för mottagande, efterlevnad och verkställighet av beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet. Om tjänsteleverantören utser ett verksamhetsställe i en annan medlemsstat ska tjänsteleverantören inte även vara skyldig att utse ett verksamhetsställe i Sverige under förutsättning att verksamhetsstället är etablerat i en medlemsstat där tjänsteleverantören erbjuder sina tjänster och att den staten deltar i en av de rättsakter som anges i artikel 1.2.

Skyldigheten att utse ett verksamhetsställe gäller inte om tjänsteleverantören endast är etablerad i Sverige och enbart erbjuder tjänster inom Sveriges territorium.

En tjänsteleverantör som inte är etablerad i någon av unionens medlemsstater, men som erbjuder tjänster i Sverige ska utse ett rättsligt ombud med hemvist i Sverige för mottagande, efterlevnad och verkställighet av beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet. Denna skyldighet ska inte gälla om tjänsteleverantören har utsett ett rättsligt ombud med hemvist i en annan medlemsstat i vilken tjänsteleverantören erbjuder sina tjänster och vilken stat deltar i en av de rättsakter som anges i artikel 1.2.

Skälen för förslaget

Utgångspunkter i EU-direktivet

Som angetts i avsnitt 8.2 ska medlemsstaterna enligt artikel 3.1 säkerställa att tjänsteleverantörer som erbjuder tjänster i unionen utser minst en mottagare för mottagande, efterlevnad och verkställighet av beslut och förelägganden som omfattas av artikel 1.2 i EU-direktivet och som utfärdats av medlemsstaternas behöriga myndigheter för insamling av bevis i straffrättsliga förfaranden.

I skäl 13 till direktivet anges att det bör stå tjänsteleverantörerna fritt att välja i vilken medlemsstat de utser sitt verksamhetsställe eller rättsliga ombud. Medlemsstaterna bör inte kunna begränsa denna valfrihet, t.ex. genom att införa en skyldighet att tjänsteleverantören ska utse verksamhetsstället eller det rättsliga ombudet på deras territorium. Denna valfrihet har dock vissa begränsningar, vilka framgår av artikel 3.2 i EU-direktivet. Av den bestämmelsen framgår att det utsedda verksamhetsstället eller det rättsliga ombudet ska vara etablerat respektive ha sin hemvist i en medlemsstat där tjänsteleverantören tillhandahåller tjänster (se avsnitt 8.2.2). Vidare ska verksamhetsstället utses i en medlemsstat som deltar i en av de rättsakter som anges i artikel 1.2 i direktivet.

Artiklarna 3.1 a och 3.2 a samt skäl 13 innebär således att en tjänsteleverantör som är etablerad i en medlemsstat och som erbjuder tjänster inom unionen är skyldig att utse ett verksamhetsställe i den medlemsstaten eller i någon annan medlemsstat där tjänsteleverantören erbjuder sina tjänster. Tjänsteleverantören kan alltså välja i vilken av dessa medlemsstater verksamhetsstället ska utses. Verksamhetsstället ska dock vara etablerat i aktuell medlemsstat. Eftersom dessa tjänsteleverantörer är etablerade inom unionen är de inte också skyldiga att utse rättsliga ombud i övriga medlemsstater.

En tjänsteleverantör som däremot inte är etablerad inom unionen, men som erbjuder tjänster inom unionen, är i stället enligt artiklarna 3.1 b och 3.2 a skyldig att utse ett rättsligt ombud i någon av de medlemsstater i vilken leverantören erbjuder sina tjänster. Vidare krävs att det rättsliga ombudet har sin hemvist i aktuell medlemsstat och att den staten deltar i en av de rättsakter som anges i artikel 1.2 i EU-direktivet.

För att konstatera att tjänsteleverantören erbjuder sina tjänster i en enskild medlemsstat krävs, enligt definitionen i artikel 2.3, att leverantören ska göra det möjligt för fysiska eller juridiska personer i den enskilda medlemsstaten att använda de tjänster som anges i artikel 2.1 i direktivet samt att leverantören har en betydande anknytning till medlemsstaten. En sådan betydande anknytning ska anses föreligga om tjänsteleverantören har ett verksamhetsställe enligt definitionen i artikel 2.4 i medlemsstaten (inte att förväxla med definitionen i artikel 2.5 om utsett verksamhetsställe), eller annars har ett betydande antal användare i landet eller om dess verksamhet är inriktad på medlemsstaten.

Enligt artikel 3.1 c ska en tjänsteleverantör som är etablerad i en medlemsstat som inte deltar i de instrument som anges i artikel 1.2 utse ett rättsligt ombud i en medlemsstat som deltar i någon av de instrument som anges i artikel 1.2. Eftersom Sverige deltar i samtliga de rättsakter som avses, berörs Sverige inte av denna bestämmelse.

Frågan om de skyldigheter som åligger ett utsett verksamhetsställe eller rättsligt ombud enligt artikel 3.3 och 3.4 behandlas i avsnitten 8.4 och 8.6.

Närmare om innebörden av begreppet etablerad

I artikel 3.1 a–3.1 b används begreppen *etablerad*. Vad som avses med en tjänsteleverantör ska anses vara etablerad i unionen eller i en medlemsstat följer inte av direktivets (eller EU-förordningens) bestämmelser eller dess skäl. Begreppet etablerad används i flera EU-rättsakter, bl.a. i EU:s dataskyddsförordning och lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. Av förarbetena till den sistnämnda lagen följer att en aktör som omfattas av den lagen, dvs. en personuppgiftsansvarig, kan ha verksamhetsställen i flera länder och därmed vara etablerad i dataskyddsförordningens mening, i flera stater. Aktören är således etablerad i en medlemsstat genom förekomsten av ett verksamhetsställe.² Innebörden av begreppet etablerad får anses vara detsamma i EU-direktivet, dvs. förekomsten av ett verksamhetsställe i en eller flera medlemsstater, är avgörande för bedömningen om en tjänsteleverantör ska anses vara etablerad där eller inte. Detta följer också av

² Prop. 2017/18:105 s. 38.

definitionen av begreppet *erbjuda tjänster i unionen* enligt artikel 2.3 där en betydande anknytning till unionen ska anses föreligga om tjänsteleverantören har ett verksamhetsställe i en medlemsstat (se avsnitt 8.2.1). Det bör i sammanhanget framhållas att termen verksamhetsställe inte ska förväxlas med begreppet utsett verksamhetsställe (se avsnitt 8.2.1). Med verksamhetsställe avses enligt artikel 2.4 i direktivet, som behandlats i avsnitt 8.2.1, en enhet som de facto utövar ekonomisk verksamhet under en obegränsad tid genom en stabil infrastruktur varifrån tillhandahållandet av tjänster genomförs eller verksamheten förvaltas. Det kan t.ex. vara fråga om ett dotterbolag eller en filial, men den rättsliga formen för en sådan struktur bör inte vara en avgörande faktor. Kan en sådan etablering konstateras infaller skyldigheten för tjänsteleverantören att utse ett verksamhetsställe enligt definitionen i artikel 2.5 för mottagande av de beslut och förelägganden som avses i artikel 1.2 i direktivet.

Tjänsteleverantörer etablerade i Sverige

För att genomföra direktivets bestämmelser i artikel 3.1 a samt artikel 3.2 a bör det av nationell rätt följa att en tjänsteleverantör som är etablerad i Sverige, ska utse ett verksamhetsställe i Sverige eller annan medlemsstat.

Den föreslagna bestämmelsen innebär alltså att en tjänsteleverantör som är etablerad i Sverige, med den innebörd begreppet har enligt vad som angetts ovan, är skyldig att utse ett verksamhetsställe i Sverige eller i en annan medlemsstat, som i sin tur också ska vara etablerat i Sverige eller den andra medlemsstaten.

En tjänsteleverantör som är etablerad i Sverige eller i annan medlemsstat och som erbjuder tjänster i flera medlemsstater kan mot bakgrund av skäl 13 fritt välja i vilken av dessa ett verksamhetsställe enligt definitionen i artikel 2.5 ska utses. Har tjänsteleverantören utsett ett verksamhetsställe i en annan medlemsstat där denne erbjuder tjänster ska den således inte vara skyldig att även utse ett verksamhetsställe i Sverige. Det krävs dock att det utsedda verksamhetsstället är etablerat i den staten och att staten deltar i en av de rättsakter som anges i artikel 1.2.

Det ska också poängteras att det är den medlemsstat i vilken tjänsteleverantören är etablerad som enligt direktivet ska tillse att

tjänsteleverantören utser ett verksamhetsställe. En tjänsteleverantör som är etablerad i en annan medlemsstat, men som erbjuder tjänster i Sverige, omfattas alltså inte av skyldigheten i nationell rätt att utse ett verksamhetsställe. Däremot finns det inget hinder mot att den tjänsteleverantören utser ett verksamhetsställe i Sverige enligt de krav som följer av direktivet.

En bestämmelse med beskrivet innehåll motsvarar bestämmelsen i artikel 3.1 a och artikel 3.2 a samt skäl 13. Den föreslagna bestämmelsen bör också, för att beakta artikel 1.5, förses med ett undantag för den tjänsteleverantör som är etablerad i Sverige och som enbart erbjuder tjänster på Sveriges territorium.

Tjänsteleverantörer etablerade utanför EU men som erbjuder tjänster i Sverige

En tjänsteleverantör som inte är etablerad i någon av unionens medlemsstater, men som erbjuder tjänster i Sverige enligt definitionen av begreppet erbjudande av tjänster på en medlemsstats territorium i 2.2 artikel ska utse ett rättsligt ombud med hemvist i Sverige. Detta ska dock inte gälla om tjänsteleverantören utser ett rättsligt ombud med hemvist i en annan medlemsstat i vilken tjänsteleverantören erbjuder sina tjänster och vilken stat deltar i en av de rättsakter som anges i artikel 1.2.

En tjänsteleverantör ska alltså, för att omfattas av den föreslagna bestämmelsen, erbjuda tjänster i Sverige, se ovan om vilka parametrar som hänsyn ska tas till vid bedömningen om en tjänsteleverantör erbjuder tjänster i en enskild medlemsstat.

Med begreppet hemvist i fråga om en juridisk person avses vanligen dess stadgeenliga säte, dess huvudkontor eller där det bedriver sin huvudsakliga verksamhet (se t.ex. 10 kap. 1 § andra stycket rättegångsbalken och artikel 63 i den s.k. Bryssel I förordningen³). Det rättsliga ombudet ska alltså ha en sådan anknytning till Sverige för att kravet på hemvist ska vara uppfyllt.

³ Europaparlamentets och rådets förordning (EU) nr 1215/2012 av den 12 december 2012 om domstols behörighet och om erkännande och verkställighet av domar på privaträttens område.

Tidpunkt för utseende av verksamhetsställe eller rättsligt ombud

Bestämmelsen i artikel 3.6 innebär att skyldigheten att utse verksamhetsställen eller rättsliga ombud ska vara uppfylld redan vid den tidpunkt EU-förordningen ska börja tillämpas, dvs. den 18 augusti 2026. Skyldigheten avser de tjänsteleverantörer som erbjuder tjänster per den 18 februari 2026. Tjänsteleverantörer som efter den 18 februari 2026 börjat erbjuda tjänster inom unionen har sex månader på sig att utse ett verksamhetsställe eller rättsligt ombud från den dag då tjänsten började erbjudas. I avsnitt 14 behandlas dessa frågor.

8.3.2 Erbjudande av tjänster på en medlemsstats territorium

Bedömning: Några bestämmelser i lag om vad som avses med begreppet erbjuda tjänster på en medlemsstats territorium behövs inte.

Skälen för bedömningen: Innebörden av begreppen tjänsteleverantör samt erbjuda tjänster inom unionen definieras både i EU-förordningen och i direktivet. Definitionerna har behandlats i avsnitt 3.2.2. Eftersom definitionerna även anges i EU-förordningen, bör de inte föras in i svensk lag. Begreppet erbjuda tjänster på medlemsstats territorium är dock enbart definierat i direktivet. Det kan dock konstateras att begreppet är i stort sett identiskt med definitionen *erbjuda tjänster inom unionen* men med den skillnaden att det förra begreppet avgränsas till endast en medlemsstat. Några kompletterande bestämmelser i lag behövs därför inte.

8.4 Skyldigheten att motta förelägganden och beslut samt tillhandahålla resurser och befogenheter

Förslag: Det ska följa av lag att ett utsett verksamhetsställe och ett rättsligt ombud i Sverige ska ta emot sådana beslut och förelägganden som omfattas av tillämpningsområdet enligt artikel 1.2 i direktivet.

Vidare ska det framgå av lag att en tjänsteleverantör som utser ett verksamhetsställe i Sverige eller i en annan medlemsstat eller ett rättsligt ombud i Sverige ska ge verksamhetsstället eller det rättsliga ombudet de befogenheter och resurser som följer av direktivet.

Skälen för förslaget

Skyldigheten för i Sverige utsedda verksamhetsställen och rättsliga ombud att ta emot beslut och förelägganden

Enligt artikel 3.3 ska beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 riktas till det utsedda verksamhetsstället eller det rättsliga ombudet. Motsvarande framgår av inledningen i artikel 3.1. Förutom EU-förordningen omfattas direktivet om en europeisk utredningsorder och EU:s konvention om ömsesidig rättslig hjälp samt inhemska ärenden (se avsnitt 8.2.2).

En europeisk utlämnande- eller bevarandeorder som utfärdas med stöd av bestämmelserna i EU-förordningen ska således riktas direkt till det av tjänsteleverantören utsedda verksamhetsstället eller rättsliga ombudet.

När det gäller övriga rättsakter och de inhemska förfarandena kan följande sägas.

I lagen om internationell rättslig hjälp i brottmål finns bestämmelser om hur en ansökan om rättslig hjälp för att inhämta elektroniska bevis ska hanteras när Sverige är anmodad stat. En sådan begäran hanteras av åklagare och beslutas av domstol om det blir aktuellt med hemliga tvångsmedel. Inte i något fall skickas en begäran med stöd av denna lag eller EU-konventionen om ömsesidig rättslig hjälp om inhämtande av elektronisk bevisning från den

ansökande staten direkt till en tjänsteleverantör i Sverige. Motsvarande gäller vid en ansökan om rättslig hjälp utomlands. EU-direktivet ska dock inte tolkas som att denna ordning ska ändras, utan endast att i de fall en svensk åklagare t.ex. får en ansökan om att hämta ut abonnentuppgifter kan han eller hon vända sig till ett utsett verksamhetsställe eller rättsligt ombud i Sverige.

Motsvarande utgångspunkter får anses gälla vid tillämpningen av lagen och direktivet om en europeisk utredningsorder. En svensk åklagare som ska erkänna och verkställa en utfärdad europeisk utredningsorder om att inhämta abonnentuppgifter kan vända sig till ett utsett verksamhetsställe eller rättsligt ombud i Sverige. Samma får anses gälla i inhemska förfaranden.

Som påpekats i avsnitt 8.2.2 framgår av artikel 1.3 att EU-direktivet inte påverkar de nationella myndigheternas befogenheter att i enlighet med unionsrätten och nationell rätt rikta framställningar direkt till tjänsteleverantörer som är etablerade i landet i syfte att samla in elektroniska bevis i straffrättsliga förfaranden. Vill t.ex. den svenska åklagaren vända sig direkt till tjänsteleverantören så är det möjligt. Direktivet hindrar inte detta utan ger endast alternativ för de brottsbekämpande myndigheterna.

Sammantaget anser vi att de skyldigheter för utsedda verksamhetsställen och rättsliga ombud att motta beslut och förelägganden ska omfatta det tillämpningsområde som anges i artikel 1.2 samt inhemska förfaranden. Detta bör framgå av lag.

Tjänsteleverantören ska ge utsedda verksamhetsställen och rättsliga ombud tillräckliga resurser och befogenheter

Enligt artikel 3.4 har tjänsteleverantörer vissa skyldigheter gentemot utsedda verksamhetsställen och rättsliga ombud genom att de ska ha sådan de befogenheter och resurser som krävs för att efterleva ett sådant beslut eller föreläggande som omfattas av tillämpningsområdet i artikel 1.2 i EU-direktivet.

Det kan vid en första anblick te sig främmande att i författning reglera ramarna för ett internt förhållande mellan tjänsteleverantören och det utsedda verksamhetsstället eller rättsliga ombudet vad avser de befogenheter och resurser som tjänsteleverantören ska förse verksamhetsstället eller det rättsliga ombudet med. Har ett verksamhetsställe eller rättsligt ombud utsetts av en tjänsteleverantör

får det också förutsättas att verksamhetsstället eller det rättsliga ombudet ges de befogenheter och resurser som krävs. Å andra sidan anges i artikel 5 om sanktioner att sådana syftar till överträdelser av *nationella bestämmelser* som har antagits för att bl.a. genomföra artikel 3. Av det skälet bör det i lag regleras de krav som anges i artikel 3.4. I avsnitt 8.6 lämnar vi förslag om att centralmyndigheten ska utöva tillsyn över att bestämmelserna i artikel 3.4 följs. Detta innebär att centralmyndigheten ska ha tillsyn över att tjänsteleverantörer, som är etablerade i Sverige, har utsett verksamhetsställen och har gett de tillräckliga resurser och befogenheter för att motta sådana beslut och förelägganden som omfattas av tillämpningsområdet för artikel 1.2 i EU-direktivet. Centralmyndighetens tillsynsansvar gäller även de verksamhetsställen eller rättsliga ombud som utsetts i Sverige av tjänsteleverantörer som inte är etablerade i landet. Vilka befogenheter och sanktionsmöjligheter som bör tillkomma centralmyndigheten i sin tillsynsverksamhet behandlas i avsnitt 8.6.3 och avsnitt 9.

8.5 Underrättelser och språk

Bedömning: De utsedda verksamhetsställen och rättsliga ombudens skyldighet att underrätta centralmyndigheten om de uppgifter som följer av artikel 4.1–4.3 kan regleras i förordning.

Skälen för bedömningen: I artikel 4.1–4.3 regleras, som behandlats i avsnitt 8.2.3, vilka uppgifter som tjänsteleverantörerna ska underrätta centralmyndigheten om. Det avser kontaktuppgifter, vilket av unionens officiella språk som ska användas vid en framställning till det utsedda verksamhetsstället eller det rättsliga ombudet samt det exakta territoriella tillämpningsområdet för varje verksamhetsställe eller rättsliga ombud för det fall tjänsteleverantören har utsett flera sådana representanter. När det gäller språk regleras det även i artikel 9.4 i EU-förordningen. De aktuella uppgifterna är av administrativ natur och genomförandet av bestämmelserna i artikel 4.1–4.3 bör därför lämpligast ske genom reglering i förordning. Skyldigheten för medlemsstaterna enligt artikel 4.4 att publicera informationen på en särskild webbplats bör tillkomma centralmyndigheten. Någon särskild lagreglering i detta avseende krävs inte.

8.6 Centralmyndighet

8.6.1 Endast en myndighet ska utses till centralmyndighet

Bedömning: Endast en myndighet bör utses till centralmyndighet.

Skälen för bedömningen: Det är lämpligt att uppgiften att vara centralmyndighet tillkommer endast en myndighet, och inte flera. En nationell centralmyndighet med ensamt ansvar kan antas innebära att myndigheten får en mer heltäckande bild av de tjänsteleverantörer som omfattas av EU-direktivets bestämmelser. Det är också svårt att på ett överskådligt och effektivt sätt fördela de uppgifter som tillkommer centralmyndigheten mellan olika myndigheter, t.ex. vilka olika typer av kategorier av tjänsteleverantörer som kan kontrolleras av olika myndigheter. Vidare får omfattningen av uppgifterna antas vara begränsad, både var för sig och tillsammans.

Som följer av artikel 6 i EU-direktivet ska centralmyndigheterna inom EU samarbeta med varandra med och även med kommissionen och förse varandra med information och stöd. Denna uppgift är central vad gäller frågan att avgöra om en tjänsteleverantör som erbjuder tjänster i flera olika medlemsstater har uppfyllt sin skyldighet att utse ett verksamhetsställe eller rättsligt ombud i någon av de medlemsstater där denna skyldighet kan aktualiseras. Det framstår därför även i detta avseende som mer ändamålsenligt att uppgiften som centralmyndighet tillkommer en ensam myndighet i Sverige för att underlätta detta arbete. En uppdelning av ansvar mellan olika myndigheter skulle sannolikt skapa merarbete i form av samordning, särskilt i fråga om samarbetet med andra medlemsstaters centralmyndigheter, vilket i sig skulle kunna innebära mer arbete än vad myndighetsuppgiften som sådan innebär.

För tjänsteleverantörernas del innebär en ensam centralmyndighet att det blir tydligt vilken myndighet som har ansvar att kontrollera att direktivets bestämmelser efterlevs och i förlängningen kan meddela sanktioner mot den tjänsteleverantör som inte efterföljer direktivets bestämmelser (se vidare avsnitt 8.6.3 nedan).

8.6.2 Post- och telestyrelsen bör utses till centralmyndighet

Förslag: Post- och telestyrelsen bör utses till centralmyndighet.

Skälen för förslaget

Utgångspunkter

Det är mest effektivt att utse en myndighet som har så många befintliga kompetenser och strukturer på plats som möjligt till centralmyndighet. Skälet till detta är flera. Dels ska EU-direktiv börja tillämpas relativt snart, vilket ger kort om tid för att bygga upp helt nya rutiner, strukturer och kompetenser. Det kommer sannolikt inte heller att röra sig om stora ärendeflöden inledningsvis. Att inrätta nya myndigheter är kostsamt och komplext. Att dessutom göra det för att hantera små ärendeflöden är dyrt och ineffektivt. De kompetenser som krävs för uppgiften finns hos befintliga myndigheter. Uppgiften bör därför fördelas på en befintlig myndighet.

Den centralmyndighet som ska utses enligt artikel 6.1 bör ha kännedom inom de sakområden som är aktuella. För att centralmyndigheten på ett effektivt sätt ska kunna utföra sina uppgifter är branschkunskap och marknadsförståelse av vikt. Kraven på myndigheten enligt EU-direktivet innebär att det är en fördel om myndigheten har kunskap om de tjänsteleverantörer som omfattas av EU-direktivet och av EU-förordningen.

Bör den behöriga utfärdande respektive verkställande myndigheten enligt EU-förordningen också utses till centralmyndighet?

Vi har i avsnitt 7.5.1 föreslagit att samtliga brottsbekämpande myndigheter ska vara behöriga myndigheter att utfärda en europeisk utlämnande eller bevarandeorder, dock med godkännande av åklagare om ordern inte utfärdats av åklagare. I avsnitt 7.5.3 har vi föreslagit att Åklagarmyndigheten ska vara ensam verkställande myndighet enligt EU-förordningen.

Frågan är då om den verkställande myndigheten också bör utses till centralmyndighet enligt EU-direktivets bestämmelser. Efter-

som Åklagarmyndigheten har föreslagits som verkställande myndighet bör bedömningen omfatta frågan om den myndigheten också bör utses till centralmyndighet.

Det kan konstateras att de uppgifter som tillkommer den verkställande myndigheten inkluderar behörigheten att besluta om sanktionsavgift för det fall en mottagare av en order vägrar att följa den. Centralmyndigheten ska också å sin sida, enligt vår bedömning i avsnitt 8.6.3 nedan, kunna besluta om sanktioner vid bristande efterlevnad av de nationella bestämmelser som genomför artiklarna 3 och 4 i EU-direktivet, vilket kan inkludera sanktionsavgifter (se även avsnitt 9.4).

EU-förordningen och EU-direktivet omfattar samma grupp av tjänsteleverantörer. De båda regelverken är också tätt sammanflätade eftersom EU-direktivet kompletterar förordningens bestämmelser i fråga om hur en tjänsteleverantör ska organisera sin verksamhet för att svara på en europeisk utlämnande- eller bevarandeorder. Att då en och samma myndighet fattar beslut om sanktioner vid överträdelser av de båda regelverken kan därför vid en första anblick te sig naturligt. En sådan ordning skulle också vara fördelaktig ur de enskilda tjänsteleverantörernas perspektiv, eftersom det skulle bidra till tydlighet i fråga om vilken myndighet som kan besluta om sanktioner på området.

En vägran att följa en europeisk utlämnande- eller bevarandeorder, vilket alltså ska sanktioneras med avgift enligt EU-förordningen, är emellertid en specifik enskild händelse där mottagaren av ordern har brustit i sin skyldighet av ett eller annat skäl. En bristande efterlevnad av EU-direktivets bestämmelser kommer främst att bero på att tjänsteleverantören inte har organiserat sin verksamhet på det sätt som direktivet kräver. Tillsynen på området elektronisk kommunikation, under vilket flertalet tjänsteleverantörer som omfattas av EU-förordningen och EU-direktivet faller, inkluderar tillsyn över hur aktörer på området har organiserat sin verksamhet för att t.ex. uppfylla kraven i 9 kap. 29 § lagen (2022:482) om elektronisk kommunikation om anpassning av verksamheten. Det framstår mot den bakgrunden att den myndighet som utövar operativ tillsyn på området elektronisk kommunikation torde vara mer lämpad att också besluta om sanktioner vid bristande efterlevnad av direktivets bestämmelser eftersom dessa alltså rör tjänsteleverantörernas organisation. Det framstår också som främmande

att en brottsbekämpande myndighet, såsom Åklagarmyndigheten, även skulle utöva tillsyn över hur tjänsteleverantörerna har organiserat sin verksamhet.

Vidare är det aktuella EU-direktivet ett inre marknadsdirektiv och inte ett direktiv som avser det straffrättsliga samarbetet, varför det även i det avseendet ter sig mer naturligt att en förvaltningsmyndighet snarare än en brottsbekämpande myndighet utses till centralmyndighet.

Mot bakgrund av det sagda gör vi alltså bedömningen att Åklagarmyndigheten i egenskap av utfärdande respektive verkställande myndighet enligt EU-förordningen inte bör utses till centralmyndighet.

I sammanhanget kan det framhållas att en särskild situation uppstår om en vägran att följa en sådan order som omfattas av EU-förordningens bestämmelser beror på att tjänsteleverantören i fråga inte har utsett ett verksamhetsställe eller rättsligt ombud på föreskrivet sätt, vilket alltså innebär att det saknas en organisation att ta hand om ordern. En sådan situation skulle innebära att det finns förutsättningar att fatta beslut om sanktioner både utifrån EU-förordningens och EU-direktivets bestämmelser. För att undvika ett sådant fall som har karaktär av dubbelbestraffning bör därför den verkställande myndigheten och centralmyndigheten samråda med varandra innan beslut om sanktionsavgift fattas. Vi återkommer till denna fråga i avsnitt 9.

Post- och telestyrelsens kompetenser

Post- och telestyrelsen (PTS) är en förvaltningsmyndighet med ett samlat ansvar inom postområdet och området för elektronisk kommunikation. Myndigheten ska, inom ramen för sina uppgifter enligt lagen om elektronisk kommunikation verka för att de mål som anges i lagen uppnås. PTS hanterar flera olika anmälnings- och registreringsförfaranden, bl.a. anmälningar för elektroniska kommunikationsnät och kommunikationstjänster och tillstånd för paketförmedlingsverksamhet. Myndigheten utövar tillsyn över ett flertal författningar på olika områden. I sammanhanget är det av relevans att myndigheten utövar tillsyn över elektronisk kommunikation och att regleringen i lagen om elektronisk kommunikation följs. Detta innebär t.ex. att myndigheten utövar tillsyn över att

reglerna om datalagring i 9 kap. 18–22 §§ och anpassningskyldighet av verksamhet i 9 kap. 29 § lagen om elektronisk kommunikation efterlevs av de operatörer som omfattas av lagen. PTS beslutar också om vilka avgifter som fås tas ut av den som tillhandahåller en anmäld tjänst enligt lagen.

PTS är också samordnare för digitala tjänster enligt 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(DSA).⁴ PTS har genom sina tillsynsuppgifter en bred vana av att arbeta med EU-rätt. Av relevans är även PTS omfattande och mångåriga erfarenhet av internationella samarbeten och internationell samordning, inte minst inom ramen för Organet för europeiska regleringsmyndigheter för elektronisk kommunikation (Berec), där även kommissionen deltar.

Det kan också nämnas att PTS ska verka för att målen inom politiken för informationssamhället uppnås. Av PTS:s instruktion framgår även att myndigheten ska delta i nationellt och internationellt standardiseringsarbete. Andra uppgifter för PTS är att vara en marknadskontrollmyndighet, beredskapsmyndighet och sektorsansvarig myndighet enligt förordningen (2022:524) om statliga myndigheters beredskap. PTS är också en av de sju myndigheter som har uppgifter och förmågor inom cybersäkerhetsområdet och som samverkar med övriga inom Nationellt cybersäkerhetscenter.

Post- och telestyrelsen bör utses till centralmyndighet

PTS utövar tillsyn över ett flertal lagar och EU-förordningar, där flera av tillsynsobjekten är leverantörer av sådana tjänster som omfattas av EU-förordningen och EU-direktivet. PTS har med anledning av sina nuvarande uppgifter således särskilt god kännedom om leverantörer av elektroniska kommunikationstjänster. Här bör särskilt framhållas att myndigheten genom sin tillsyn enligt lagen om elektronisk kommunikation övervakar att tillhandahållare av elektroniska kommunikationstjänster anpassar sin verksamhet på så sätt att beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verk-

⁴ Se 4§ förordningen (2024:958) med kompletterande bestämmelser till EU:s förordning om digitala tjänster.

ställandet inte röjs enligt ovan nämnda bestämmelse i 9 kap. 29 § lagen om elektronisk kommunikation. Myndigheten har således en befintlig organisation för att övervaka verksamheten hos de tjänsteleverantörer som faller inom EU-förordningens respektive EU-direktivets tillämpningsområde. Det ter sig därför naturligt att samma myndighet även övervakar att tjänsteleverantörerna utser verksamhetsställen eller rättsliga ombud samt att dessa ges resurser och befogenheter att svara på en europeisk utlämnandeorder respektive bevarandeorder.

Vidare har PTS en väl utbyggd tillsynsorganisation över ett brett spektrum av den digitala infrastrukturen. PTS har befogenhet att besluta om sanktioner, däribland sanktionsavgifter, enligt lagen om elektronisk kommunikation, lagen (2018:1174) om informations-säkerhet för samhällsviktiga och digitala tjänster och säkerhets-skyddslagen (2018:585). Det finns därför en uppbyggd kompetens om bedömning av lämpliga sanktioner samt beräkning av sanktionsavgifter och beslut om sådana. PTS har vidare god vana av att arbeta mot EU-kommissionen och att vara representanter i olika EU-sammanhang, vilket krävs i fråga den uppgift enligt EU-direktivet som tillkommer centralmyndigheten vad gäller samarbete och samordning med andra centralmyndigheter inom EU

Någon annan befintlig förvaltningsmyndighet har inte heller samma heltäckande tillsynsansvar för området elektronisk kommunikation. PTS bör därför utses till centralmyndighet enligt EU-direktivet.

8.6.3 Centralmyndighetens befogenheter och rätt att besluta om sanktioner

Förslag: Centralmyndigheten ska utöva tillsyn över att tjänsteleverantörer som är etablerade i Sverige utser ett verksamhetsställe i enlighet med de krav som följer av direktivet och att dessa aktörer ges befogenheter och resurser att ta emot de beslut och förelägganden som avses i artikel 1.2 i EU-direktivet. Centralmyndigheten ska även utöva tillsyn över att i Sverige utsedda verksamhetsställen och rättsliga ombud, vilka har utsetts enligt direktivet, ges motsvarande befogenheter och resurser.

Centralmyndigheten ska vidare genom förelägganden ha rätt att få ta del av handlingar och upplysningar för att kunna utöva sin tillsyn samt ha tillträdesrätt till områden, lokaler och andra utrymmen där verksamheten bedrivs, med undantag för bostäder. För dessa ändamål ska centralmyndigheten kunna begära biträde från Kronofogdemyndigheten för att kontrollera efterlevnaden av de bestämmelser som genomför artikel 3 i EU-direktivet. Ett föreläggande att lämna ut handlingar och upplysningar ska kunna förenas med vite.

Bedömning: Förvaltningslagen gäller vid handläggningen hos centralmyndigheten i ett ärende om tillsyn enligt den kompletterande lagen, vilket inkluderar kravet på kommunikation i 25 § och möjligheten att överklaga ett beslut enligt 41 §.

Centralmyndighetens samrådsskyldighet med övriga centralmyndigheter inom unionen bör regleras i förordning.

Centralmyndigheten bör ha till uppgift att besluta om sanktioner.

Skälen för förslaget

Generellt om tillsyn i nationell rätt

I regeringens skrivelse till riksdagen, En tydlig, rättssäker och effektiv tillsyn⁵, redovisas generella bedömningar av hur en tillsynsreglering bör vara utformad. Skrivelsen är avsedd att vara ett stöd och en vägledning vid bl.a. översyn av materiella regelverk av olika slag. I skrivelsen framhålls betydelsen av enhetlighet i fråga om offentlig tillsyn. Det lämnas dock utrymme för att göra avsteg från de bedömningar som görs i skrivelsen. En utgångspunkt i skrivelsen är att begreppet tillsyn främst bör användas för verksamhet som avser självständig granskning för att kontrollera om tillsynsobjektet uppfyller krav som följer av lagar och andra bindande föreskrifter. Ett grundläggande moment i tillsynen är därför enligt skrivelsen att tillsynsorganet har författningsreglerade möjligheter att ingripa. Tillsynsorganen bör också ha rätt att av den objektsansvarige få del av de upplysningar eller handlingar som behövs för

⁵ Skr. 2009/10:79, bet. 2009/10:FiU12.

tillsynen. Likaså bör organet ha tillträdesrätt till utrymmen som används i den tillsynspliktiga verksamheten. Tillsynsorganen bör även enligt skrivelsen ha möjlighet att begära biträde från Polismyndigheten och Kronofogdemyndigheten, om t.ex. tillsynsmyndigheten vägras tillträde till en lokal eller liknande för undersökning. När det finns risk för hot eller handgripligheter i samband med tillsynens utövande bör enligt skrivelsen det finnas möjlighet att begära biträde av Polismyndigheten. Är det fråga om att undanröja fysiska hinder för tillsynens genomförande bör det finnas möjlighet att begära biträde av Kronofogdemyndigheten.

Utgångspunkterna för tillsynen

En centralmyndighet har enligt EU-direktivet till uppgift att tillse att direktivet tillämpas proportionerligt och enhetligt. Medlemsstaterna ska vidare enligt artikel 5 i EU-direktivet fastställa regler om sanktioner för överträdelse av nationella bestämmelser som antagits enligt artiklarna 3 och 4 och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Dessa uppgifter får anses nära besläktade. Det framstår därför som mest ändamålsenligt att centralmyndigheten även får till uppgift att besluta om sanktioner. För att så ska kunna ske måste centralmyndigheten kunna utöva en viss tillsyn.

Några särskilda befogenheter tillkommer inte centralmyndigheten enligt direktivet.

De skyldigheter som tillkommer tjänsteleverantörerna enligt artikel 3 är främst att utse ett verksamhetsställe eller rättsligt ombud i enlighet med vad vi föreslår i avsnitt 8.3.1.

Av artikel 3.4 följer vidare att tjänsteleverantörer som är etablerade eller erbjuder tjänster på deras territorium ska ge sina utsedda verksamhetsställen och rättsliga ombud de befogenheter och resurser som behövs att svara på ett sådant föreläggande eller beslut som omfattas av tillämpningsområdet enligt artikel 1.2 i EU-direktivet. Medlemsstaterna ska *säkerställa* att så sker.

Tjänsteleverantörer som är etablerade i en medlemsstat kan, som konstaterats i avsnitt 8.3.1, utse ett verksamhetsställe i en annan medlemsstat under förutsättning att leverantören erbjuder tjänster i den staten. En tjänsteleverantör som är etablerad i Sverige

kan således välja att utse ett verksamhetsställe i annan medlemsstat där denne erbjuder tjänster. Centralmyndigheten har alltså i uppgift att säkerställa att så har skett samt att detta verksamhetsställe är etablerat i den andra medlemsstaten. Om det kan konstateras att tjänsteleverantören i strid med de ovan föreslagna nationella bestämmelserna inte har utsett något verksamhetsställe som är etablerat i Sverige eller någon annan medlemsstat kan centralmyndigheten ingripa med olika åtgärder, som vi behandlar närmare nedan och avsnitt 9. För att fullgöra denna uppgift kan det bli aktuellt för den svenska centralmyndigheten att samråda med centralmyndigheten i den andra medlemsstaten.

Medlemsstaterna ska också enligt artikel 3.4 *kontrollera* att de utsedda verksamhetsställen som är etablerade på eller rättsliga ombud som har sin hemvist på deras territorium av tjänsteleverantörerna har fått de befogenheter och resurser som anges i artikeln. Centralmyndigheten har därför också till uppgift att kontrollera att de verksamhetsställen eller rättsliga ombud som har utsetts i Sverige är etablerade respektive har sin hemvist här. Om tjänsteleverantören är etablerad i en annan medlemsstat är det primärt den medlemsstatens centralmyndighet som ska vidta åtgärder mot tjänsteleverantören i enlighet med första meningen i artikel 3.4, t.ex. vad gäller beslut om sanktioner. Den svenska centralmyndigheten kan dock bistå i detta arbete genom att samråda med centralmyndigheten i den andra staten.

Centralmyndigheten ska sammanfattningsvis utöva tillsyn dels över att tjänsteleverantörer som är etablerade i Sverige utser ett verksamhetsställe och att dessa aktörer kan ta emot beslut och förelägganden som avses i artikel 1.2 i direktivet, dels över att utsedda verksamhetsställen och rättsliga ombud som är etablerade respektive har sin hemvist i Sverige ges de resurser och befogenheter som krävs för att efterleva sådana beslut och förelägganden.

Vad som nu sagts om centralmyndighetens uppgifter bör anges i lag. Frågan om samråd med centralmyndigheter i andra medlemsstater bör dock inte regleras i lag, utan det är tillräckligt att detta följer av förordning.

Det torde vara förhållandevis enkelt att konstatera om en tjänsteleverantör har uppfyllt sina skyldigheter enligt EU-direktivet. Det bör därför i normalfallet inte krävas några tillsynsbefogenheter, men det kan inte uteslutas att sådana krävs för att konstatera om en

tjänsteleverantör har utsett ett verksamhetsställe eller rättsligt ombud. Däremot kan närmare tillsyn behövas för att konstatera om en tjänsteleverantör har uppfyllt sina skyldigheter enligt artikel 3.4 i EU-direktivet, dvs. om en tjänsteleverantör har gett sina utsedda verksamhetsställen eller rättsliga ombud de befogenheter och resurser som krävs.

Artikel 4 stadgar om skyldigheter för tjänsteleverantören att ange kontaktuppgifter och språk avseende det utsedda verksamhetsstället eller rättsliga ombudet. Skyldigheterna som följer av den artikeln torde inte kräva några tillsynsåtgärder utan det framstår som tillräckligt att en underlåtenhet att följa dem sanktioneras på lämpligt sätt.

Centralmyndighetens befogenheter

Centralmyndigheten kan – för att kunna avgöra om en sanktion ska påföras eller inte – behöva ha tillgång till handlingar eller upplysningar från en enskild tjänsteleverantör. Detta bl.a. för att kunna avgöra om tjänsteleverantören är skyldig att utse ett verksamhetsställe eller rättsligt ombud, t.ex. vad avser bedömningen om en tjänsteleverantör ska anses vara etablerad inom unionen eller erbjuder tjänster på den enskilda medlemsstatens territorium eller om tjänsteleverantören har gett sitt utsedda verksamhetsställe eller rättsliga ombud tillräckliga resurser eller befogenheter. Vidare följer av artikel 3.2 b att medlemsstaterna ska säkerställa att tjänsteleverantörerna kan bli föremål för verkställighetsförfaranden. Denna term torde främst avse vidtagande av olika åtgärder för att bestämmelserna i EU-direktivet ska följas, vilket utgörs av sedvanliga tillsynsåtgärder.

Det krävs därför att centralmyndigheten ges tillsynsbefogenheter. Vi har ovan föreslagit att PTS ska utses till centralmyndighet. PTS har enligt 11 kap 1 § lagen om elektronisk kommunikation tillsyn över att lagen, de beslut om skyldigheter, åtaganden eller villkor som har meddelats med stöd av lagen och de föreskrifter som har meddelats i anslutning till lagen följs. Tillsynen inkluderar alltså t.ex. bristande efterlevnad av bestämmelserna om anpassnings-skyldighet, vilket alltså gäller sättet tjänsteleverantörerna bedriver sin verksamhet. I 11 kap. 2–4 §§ i lagen om elektronisk kommuni-

kation anges de befogenheter som tillkommer myndigheten i detta avseende. Motsvarande tillsynsbefogenheter bör komma i fråga om efterlevnaden av de bestämmelser som genomför artikel 3 i EU-direktivet. Det finns därför skäl att föreskriva att centralmyndigheten ska ha rätt att få ta del av handlingar och upplysningar samt ha tillträdesrätt till utrymmen och för dessa ändamål kunna begära biträde Kronofogdemyndigheten. Ett föreläggande att lämna ut handlingar och upplysningar ska kunna förenas med vite.

Förvaltningslagen (2017:900) är tillämplig vid handläggningen av ett ärende hos centralmyndigheten (se även avsnitt 9.4.2). Enligt 25 § första stycket ska en myndighet innan den fattar ett beslut i ett ärende, om det inte är uppenbart obehövt, underrätta den som är part om allt material av betydelse för beslutet och ge parten tillfälle att inom en bestämd tid yttra sig över materialet. Bestämmelsen i 11 kap. 5 § lagen om elektronisk kommunikation som föreskriver att den som är föremål för tillsyn ska underrättas om en misstanke om att aktören inte följer regelverket för att ge denne en möjlighet att bemöta misstanken och eventuellt vidta rättelse på frivillig väg genomför artikel 30.2 i direktiv 2018/1772. En bestämmelse med motsvarande innehåll bör därför inte införas i den kompletterande lagen, utan 25 § förvaltningslagen uppfyller kravet på kommunikation före beslut.

Vidare följer av 41 § förvaltningslagen att ett beslut får överklagas om beslutet kan antas påverka någons situation på ett inte obetydligt sätt. Enligt 42 § samma lag får ett beslut överklagas av den som beslutet angår, om det har gått honom eller henne emot. Någon särskild överklagandebestämmelse behövs därmed inte när det gäller de beslut som centralmyndigheten fattar i sin tillsynsverksamhet.

I avsnitt 9.4 behandlas i vilken utsträckning förelägganden i förening med vite ska kunna meddelas vid bristande efterlevnad av de nationella bestämmelser som genomför EU-direktivet samt vilka övriga sanktioner som bör aktualiseras vid överträdelser av det nationella regelverket som genomför direktivets bestämmelser.

9 Sanktioner

9.1 Inledning

EU-förordningen och EU-direktivet innehåller bestämmelser om att medlemsstaterna ska fastställa regler om sanktioner vid tjänsteverantörers överträdelser av skyldigheter enligt förordningen respektive de nationella bestämmelser som genomför vissa delar av EU-direktivet. Sanktionerna ska vara effektiva, proportionerliga och avskräckande.

Vi ska enligt våra direktiv kartlägga och analysera vilka sanktioner som bör aktualiseras vid överträdelser av EU-förordningen och relevanta nationella bestämmelser som genomför EU-direktivet. I avsnitt 9.2 finns en allmän beskrivning av sanktioner. Avsnitten 9.3 och 9.4 innehåller våra överväganden och förslag avseende utformningen av ett system med sanktioner. Slutligen behandlas i avsnitt 9.5 förslag till gemensamma förfaranderegler.

9.2 Allmänt om sanktioner och sanktionsavgifter

Det saknas en legaldefinition av begreppet sanktion i svensk rätt. En sanktion ska ha ett handlingsdirigerande eller bestraffande syfte. Sanktioner kan sägas omfatta alla former av påföljder som kan följa på ett rättsstridigt handlande.

Det finns flera olika sorters repressiva sanktioner. Den mest ingripande formen är straff och andra påföljder som följer av en kriminalisering. En annan typ av repressiv sanktion är administrativa avgifter, t.ex. sanktionsavgifter. Sanktionsavgift kan i vissa fall vara ett komplement till andra åtgärder och användas för att i enskilda fall nyansera ingripandet vid en överträdelse av något som är kriminaliserat. Sanktionsavgift ersätter i andra fall kriminalisering. Andra exempel på repressiva administrativa sanktioner är åtgärds-

föreläggande (i förening med vite), möjlighet för en tillsynsmyndighet att meddela förbud (i förening med vite) och återkallelse av tillstånd. Straff, sanktionsavgift, förbud och återkallelse av tillstånd är i huvudsak tillbakaverkande sanktioner. Förbud och återkallelse av tillstånd kan på sätt och vis även ses som en framåtriktad sanktion, i den mån återkallelsen syftar till att förhindra fortsatt bristande efterlevnad av ett regelverk. Vitesföreläggande är däremot alltid en framåtsyftande sanktion som syftar till att tvinga fram ett önskat agerande eller att få ett pågående oönskat agerande att upphöra.¹

En sanktionsavgift är, likt vitesförelägganden, en administrativ sanktion som kan påföras både fysiska och juridiska personer. En sanktionsavgift kan antingen beslutas av förvaltningsmyndighet eller av domstol och tillfaller normalt staten. Bestämmelser om sanktionsavgifter införs vanligtvis i syfte att verka avskräckande och bestraffande eftersom en sanktionsavgift kan bli aktuell först när en överträdelse har ägt rum. Sanktionsavgifter är därför inte, till skillnad från vitesföreläggande, handlingsdirigerande genom att verka framåtsyftande.

En sanktionsavgift är inte en straffrättslig påföljd i direkt mening (jfr 1 kap. 3 § brottsbalken). I flera förarbeten har lagstiftaren emellertid haft som utgångspunkt att sanktionsavgifter är att betrakta som ett straff i enlighet med Europakonventionen. Ett förfarande i vilket sanktionsavgifter beslutas ska därför uppfylla de rättigheter och skyldigheter som följer av den konventionen. Det innebär att mottagaren, dvs. den som påstås ha överträtt en bestämmelse, exempelvis har rätt att underrättas om vad som läggs denne till last, rätt att yttra sig över anklagelsen och rätt till domstolsprövning inom rimlig tid.²

Antalet författningar som innehåller bestämmelser om sanktionsavgifter har ökat över tid. Inledningsvis berodde ökningen på en växling från straff för lindrigare brottslighet till sanktionsavgifter. Under senare år har sanktionsavgifter ofta införts i svensk rätt vid överträdelser av unionslagstiftning, se t.ex. lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, lagen (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt och lagen (2023:319) med kompletterande bestäm-

¹ Se t.ex. SOU 2013:38 s. 537 och prop. 2017/18:205 s. 66.

² Se t.ex. prop. 2012/13:143 s. 71–72 och prop. 2017/18:165 s. 67.

meler till EU:s förordning om åtgärder mot spridning av terrorism-innehåll online. Ytterligare en anledning till ökningen av antalet bestämmelser om sanktionsavgifter har varit lagstiftarens önskan att införa sanktioner mot juridiska personer. Eftersom endast fysiska personer kan bli föremål för straffrättsliga påföljder anses sanktionsavgifter ofta vara ett effektivt redskap för att beivra överträdelser som begås i näringsverksamhet.

9.3 Sanktionsavgifter vid överträdelser av EU-förordningens bestämmelser

9.3.1 Utgångspunkterna i EU-förordningen

I artikel 16.10 anges att den verkställande myndigheten ska ålägga en sanktionsavgift enligt artikel 15 för det fall ett utsett verksamhetsställe eller rättsligt ombud inte fullgör sina skyldigheter enligt en erkänd europeisk utlämnandeorder eller europeisk bevarandeorder vars verkställbarhet har bekräftats av den verkställande myndigheten. Ett effektivt rättsmedel ska finnas tillgängligt mot ett beslut att ålägga en avgift.

De fall då en sanktionsavgift kan aktualiseras enligt artikel 15.1 är vid överträdelser av artiklarna 10, 11 och 13.4. Det rör sig om situationer då verksamhetsstället eller det rättsliga ombudet inte har efterlevt en europeisk utlämnande- eller bevarandeorder eller om konfidentialiteten, sekretessen och integriteten för intyget om en europeisk utlämnande- eller bevarandeorder och för de uppgifter som lämnas ut eller bevaras inte har säkerställts.

EU-förordningen överlåter till medlemsstaterna att fastställa nationella regler om sanktionsavgifter vid överträdelser av nämnda artiklar. Några andra sanktioner än sanktionsavgifter är inte aktuella att besluta om enligt EU-förordningen. Det åligger medlemsstaterna enligt artikel 15.1 att vidta alla åtgärder som krävs för att säkerställa att det nationella sanktionsavgiftssystemet tillämpas (se även skäl 69). Sanktionsavgifterna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska säkerställa att sanktionsavgifter på upp till två procent av tjänsteleverantörens totala globala årsomsättning föregående räkenskapsår kan åläggas i sanktionsavgift. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder utan dröjsmål samt eventuella ändringar som berör dem.

Av skäl 70 i EU-förordningen följer vilka särskilda omständigheter som ska beaktas när en sanktionsavgift ska tas ut i ett enskilt fall.

Det ska noteras att det av artikel 15.2 i EU-förordningen framgår att en tjänsteleverantör inte ska hållas ansvarig för de olägenheter som orsakas deras användare eller tredje parter till följd av att de i god tro rättar sig efter en utfärdad europeisk utlämnande- eller bevarandeorder (se även skäl 71 i EU-förordningen).

9.3.2 Utformningen av sanktionsavgiftssystemet

Förslag: Den verkställande myndigheten ska besluta att ta ut en sanktionsavgift av ett utsett verksamhetsställe eller rättsligt ombud i Sverige som åsidosätter någon av sina skyldigheter enligt artiklarna 10, 11 och 13.4 i EU-förordningen. Tjänsteleverantören ska svara solidariskt för betalningen av avgiften tillsammans med det i Sverige utsedda verksamhetsstället eller rättsliga ombudet.

Sanktionsavgiften ska bestämmas till lägst 10 000 kronor och högst till ett sådant högre belopp som följer av artikel 15.1 i EU-förordningen.

Vid bedömningen av om någon sanktionsavgift ska tas ut och av storleken på avgiften, ska särskild hänsyn tas till om överträdelsen varit uppsåtlig eller berott på oaktsamhet, den skada, fara eller kränkning som överträdelsen inneburit, överträdelsens karaktär, svårhetsgrad och varaktighet, samt om den tjänsteleverantör som har begått överträdelsen tidigare begått en liknande överträdelse samt den berörda tjänsteleverantörens finansiella ställning.

Sanktionsavgiften ska få sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

Skälen för förslaget

Det ska gälla strikt ansvar för överträdelser

I de flesta sanktionsavgiftssystem som i dag tillämpas krävs varken uppsåt eller oaktsamhet för att en avgift ska kunna påföras vid en regelöverträdelse. Huvudregeln kan således sägas vara att sanktions-

avgifter bygger på ett strikt ansvar.³ Det krävs alltså inte att överträdelser skett uppsåtligen eller av oaktsamhet för att avgift ska kunna tas ut.

Vår bedömning är att det inte finns skäl att avvika från denna princip när det gäller de sanktionsavgifter som ska införas för överträdelser av vissa av EU-förordningens bestämmelser. Det är framför allt den omständigheten att den beslutande myndigheten inte behöver bevisa att en regelöverträdelse har skett uppsåtligen eller av oaktsamhet som gör att ett system med sanktionsavgifter är effektivt. För att en överträdelse ska leda till en snabb reaktion krävs således att avgiften ska kunna påföras utan någon närmare utredning och en skyldighet som bygger på strikt ansvar bidrar därför till en förenkling och effektivisering av sanktionssystemet. Detta gäller särskilt när det är juridiska personer som ska påföras en sanktion. Myndigheten behöver i ett sådant fall endast kontrollera objektivt att en överträdelse har ägt rum och bestämma avgiften enligt en fastställd beräkningsgrund. Bedömningsinslaget blir betydligt mer begränsat och för att inte effektivitetsfördelen ska gå förlorad bör det föreslagna systemet med sanktionsavgifter därför bygga på ett strikt ansvar.

För att en konstruktion med strikt ansvar ska vara försvarbar utifrån rättssäkerhets- och rimlighetsskäl bör det dock finnas ett starkt stöd för en presumtion som innebär att överträdelser på området inte kan ske på annat sätt än som en följd av uppsåt eller oaktsamhet.⁴ Om en europeisk utlämnande- eller bevarandeorder inte efterlevs torde det i de allra flesta fallen kunna betraktas som i vart fall oaktsamt att inte följa en sådan order. De överträdelser som enligt EU-förordningen ska omfattas av ett sanktionsavgiftssystem får till sin karaktär anses vara sådana att det är svårt att se att sådana överträdelser i normalfallet kan bero på annat än uppsåt eller oaktsamhet.

Enligt artikel 6.2 Europakonventionen ska var och en som blivit anklagad för brott betraktas som oskyldig till dess hans eller hennes skuld lagligen fastställts (den s.k. oskuldspresumtionen). Presumtionen innebär att en sanktionsavgift inte får utkrävas automatiskt när de objektiva rekvisiten är uppfyllda, utan den som avgiften riktar sig mot ska ha en möjlighet till någon form av försvar som

³ Se t.ex. SOU 2013:38 s. 545 och prop. 2017/18:232 s. 324.

⁴ Se SOU 2013:38 s. 545.

grundas på subjektiva förhållanden. För att inte stå i strid med oskuldspresumtionen i Europakonventionen föreslår vi i det följande att systemet med sanktionsavgifter innehåller en möjlighet till eftergift eller jämkning av avgiften, bl.a. baserat på subjektiva omständigheter (se nedan). Ett system baserat på strikt ansvar med dessa utgångspunkter torde enligt vår bedömning inte strida mot konventionens bestämmelser.⁵

Mot bakgrund av det sagda ska det föreslagna systemet med sanktionsavgifter utgå från ett strikt ansvar vid prövning av avgiftsskyldighet. Därigenom blir det tillräckligt för den beslutande myndigheten att konstatera att en överträdelse har ägt rum för att en sanktionsavgift som utgångspunkt ska utgå. Det strikta ansvaret behöver inte följa uttryckligen av lag.⁶

Det ska vara obligatoriskt att ta ut sanktionsavgift

Strikt ansvar innebär inte att en sanktionsavgift måste tas ut vid varje överträdelse som sker. En viktig fråga är därför om det ska vara obligatoriskt att ta ut sanktionsavgift när en viss bestämmelse har överträtts. Bestämmelser om sanktionsavgift är ofta obligatoriska, dvs. utformade så att sanktionsavgift ska tas ut när de objektiva förutsättningarna för det är uppfyllda. Med hänsyn till behovet av likabehandling, objektivitet och proportionalitet bör möjligheter till mer skönmässiga bedömningar som utgångspunkt vara begränsade.⁷

Vi ser således inga skäl som talar för att de sanktionsavgifter som ska kunna beslutas vid överträdelser av vissa bestämmelser enligt EU-förordningen inte bör vara obligatoriska när förutsättningarna för detta är uppfyllda. Utrymmet för skönmässiga bedömningar minskar och ett obligatoriskt system framstår även som mest ändamålsenligt vid mer allvarliga överträdelser av regelverket. Bestämmelserna om sanktionsavgift bör därför formuleras på så sätt att sanktionsavgift ska tas ut om förutsättningarna för det är uppfyllda.

Det ska dock påpekas att sanktionsavgifter enligt EU-förordningen endast får tas ut i enlighet artikel 16.10 i förordningen.

⁵ Se t.ex. prop. 2017/18:232 s.336.

⁶ Se t.ex. prop. 2022/23:71 s. 31.

⁷ Se t.ex. prop. 2017/18:205 s. 69–70 och prop. 2021/22:18 s. 58.

I den bestämmelsen anges att om mottagaren, dvs. det utsedda verksamhetsstället eller det rättsliga ombudet, inte fullgör sina skyldigheter enligt en erkänd en europeisk utlämnande- eller bevarandeorder vars verkställbarhet har bekräftats av den verkställande myndigheten ska sanktionsavgifter åläggas enligt artikel 15 i EU-förordningen. Det innebär således att först efter det förfarande som föreskrivs i artikel 16 har resulterat i att den verkställande myndigheten beslutat om att en europeisk utlämnande- eller bevarandeorder ska verkställas, men verksamhetsstället eller det rättsliga ombudet ändå inte efterlever ett sådant beslut ska sanktionsavgifter beslutas. Vidare ska noteras att enligt artikel 15.1 är det överträdelse av artiklarna 10, 11 eller 13.4 som kan resultera i en sanktionsavgift.

Som tidigare nämnts bör det emellertid finnas möjlighet att i vissa fall helt eller delvis efterge sanktionsavgiften, bl.a. med beaktande av subjektiva omständigheter (se nedan). Vi föreslår även att det ska vara möjligt att överklaga ett beslut om sanktionsavgift (se avsnitt 9.5).

Den verkställande myndigheten ska besluta om sanktionsavgift

I de sanktionssystem som i dag tillämpas är det vanligaste att sanktionsavgiften beslutas av en myndighet. Endast i ett fåtal system beslutas avgiften av domstol efter ansökan av myndighet. I det senare fallet är det ofta fråga om system där uppsåt eller oaktsamhet måste kunna konstateras för att avgift ska aktualiseras över huvud taget. En förutsättning för att låta en sanktionsavgift beslutas av en myndighet och inte av domstol är att det finns någon lämplig myndighet som kan besluta om avgiften. Vidare bör den myndigheten ha någon form av tillsynsansvar över den verksamhet som omfattas av avgifterna eller på annat sätt ha god insyn i verksamheten samt vara väl förtrogen med det aktuella regelverket och ha goda förutsättningar att upptäcka regelöverträdelser.⁸

Enligt artikel 16.10 i EU-förordningen ska den verkställande myndigheten besluta om sanktionsavgifter. Den verkställande myndigheten har visserligen inte något allmänt tillsynsansvar över de tjänsteleverantörer som omfattas av EU-förordningen, men

⁸ SOU 2013:38 s. 546.

denna myndighet kommer – med hänsyn till den uppgift den har att se till att en europeisk utlämnande- eller bevarandeorder verkställs – ha goda möjligheter att uppmärksamma regelöverträdelser. Det bör därför vara den verkställande myndigheten som beslutar om sanktionsavgift, och således inte en domstol efter ansökan av den verkställande myndigheten.

Vi har i avsnitt 7.5.4 föreslagit att Åklagarmyndigheten ska utses till verkställande myndighet enligt EU-förordningens bestämmelser.

Sanktionsavgiftens storlek

I regelverk om sanktionsavgifter anges ibland fasta belopp som en sanktionsavgift ska tas ut för olika typer av överträdelser. I andra fall är reglerna utformade på så sätt att sanktionsavgifter ska fastställas till ett belopp inom ett bestämt beloppsintervall eller till en viss procent av årsomsättningen i näringsverksamhet.

Utgångspunkten för utformningen av ett sanktionsavgiftssystem måste vara att en sanktionsavgift, i enlighet med EU-förordningens krav, ska vara effektiv, proportionerlig och avskräckande för samtliga tjänsteleverantörer, dvs. oavsett om det rör sig om fysiska eller juridiska personer eller om de bedriver en mindre verksamhet med begränsade resurser eller en större verksamhet med mycket stora resurser. De tjänsteleverantörer som faller inom EU-förordningens tillämpningsområde torde med få undantag vara juridiska personer. Tjänsteleverantörer som är juridiska personer kan skilja sig markant från varandra både i fråga om storlek och ekonomiska förutsättningar. Det är därför viktigt att en sanktionsavgift blir kännbar, oaktat tjänsteleverantörens storlek och resurser. För att uppfylla kravet på effektiva, proportionella och avskräckande sanktioner bör därför sanktionsavgiften bestämmas inom ett beloppsintervall och intervallet bör vara förhållandevis stort. Den verkställande myndigheten får då möjlighet att göra en nyanserad bedömning när avgiftens storlek ska bestämmas.

Vid bestämmandet av vilka beloppsintervall som bör gälla finns det skäl att beröra hur avgiftsintervallerna ser ut i andra sanktionsavgiftssystem.

Enligt 9 § lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt ska en sanktionsavgift bestämmas till lägst

10 000 kronor och högst 15 000 000 kronor. Av 7 § lagen med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online följer att en sanktionsavgift ska bestämmas till lägst 5 000 kronor och högst 5 000 000 kronor eller, vid en systematisk eller fortgående underlåtenhet att fullgöra någon skyldighet enligt artikel 3.3 i TCO-förordningen, till ett sådant högre belopp som följer av artikel 18.3 i förordningen, dvs. fyra procent av värdtjänstleverantörens totala omsättning under det föregående räkenskapsåret.

De överträdelser av EU-förordningen som ska kunna leda till en sanktionsavgift kan vara av varierande art och karaktär. Att en mottagare inte följer en europeisk utlämnande- eller bevarandeorder kan få allvarliga konsekvenser och ytterst innebära att uppgifter som är avgörande ur bevissynpunkt kan gå helt förlorade. Beloppsintervallet bör därför vara förhållandevis stort för att ge den beslutande myndigheten ett vitt utrymme att göra en nyanserad bedömning av avgiftens storlek i det enskilda fallet.

Vi bedömer att det är rimligt att det lägsta belopp som ska kunna beslutas i sanktionsavgift är 10 000 kronor. Enligt artikel 15.1 har medlemsstaterna en skyldighet att säkerställa att sanktionsavgifter på upp till två procent av tjänstleverantörens totala globala årsomsättning föregående räkenskapsår kan åläggas. För att Sverige ska uppfylla denna skyldighet bör beloppsintervallets övre gräns bestämmas till detta belopp.

Sanktionsavgiftens storlek i det enskilda fallet

Av skäl 70 i EU-förordningen följer att vid bedömningen av lämpliga sanktionsavgifter i ett enskilt fall bör den behöriga myndigheten beakta alla relevanta omständigheter, såsom överträdelsens art, allvarlighetsgrad och varaktighet, om den begicks uppsåtligen eller genom försummelse, om tjänstleverantören har hållits ansvarig för liknande tidigare överträdelser och den finansiella styrkan hos den tjänstleverantör som hålls ansvarig. I undantagsfall kan den bedömningen enligt nämnda skäl leda till att den verkställande myndigheten beslutar att avstå från att ålägga sanktionsavgifter. I detta avseende ska särskild hänsyn tas till mikroföretag som i en nödsituation underlåter att efterleva en europeisk utlämnandeorder

eller en europeisk bevarandeorder på grund av bristande personalresurser utanför kontorstid, om uppgifterna överförs utan onödigt dröjsmål.

Till skillnad mot t.ex. TCO-förordningen, regleras de nämnda omständigheterna inte direkt i EU-förordningen. Mot denna bakgrund bör det i stället i den nationella kompletterande lagen regleras vilka omständigheter som kan påverka avgiftens storlek, vilket vår mening förutsätts i artikel 15.1. Detta är också särskilt viktigt eftersom sanktionsavgiftens storlek inte anges till ett fast belopp i lagen. En uppräknig av sådana omständigheter kan dock inte vara uttömmande utan bör ange de som är särskilt viktiga. Bestämmelsen bör lämna utrymme för att också beakta andra förmildrande eller försvårande omständigheter. Uppräkningen i skäl 70 i EU-förordningen av de omständigheter som ska beaktas bör tjäna som ledning för vilka som är relevanta i sammanhanget.

Särskild hänsyn bör tas till om överträdelsen varit avsiktlig eller berott på oaktsamhet. En avsiktlig överträdelse visar tydligt på nonchalans mot regleringen och utrymmet att underlåta att ta ut avgift eller att bestämma avgiften till ett lågt belopp bör vara mycket litet. Tvärtom talar avsiktliga överträdelser starkt för att sanktionsavgift ska tas ut och att den ska sättas högt. I många fall är dock överträdelser resultatet av mer eller mindre oaktsamma förfaranden, t.ex. missförstånd om hur regleringen ska tillämpas eller ursäktliga bedömningsfel. Även graden av oaktsamhet bör därför vägas in.

Det bör också beaktas vilken skada, fara eller kränkning som överträdelsen medfört. Ju större skadan, faran eller kränkningen är till följd av en order inte har följts, desto mindre blir utrymmet att bestämma avgiften till ett lågt belopp. Skadan kan t.ex. bestå i att en stor mängd elektronisk bevisning har gått eller riskerar att gå om intet.

Som följer av skäl 70 bör också överträdelsens karaktär, svårhetsgrad och varaktighet beaktas. Här är det t.ex. av betydelse om vägran att helt följa en europeisk utlämnande- eller bevarandeorder skett uppsåtligen och lett till att en stor mängd uppgifter som skulle kunna användas som bevis gått förlorade. Ju allvarligare överträdelse, desto starkare skäl talar för att beloppet ska sättas högt. I motsvarande riktning kan beaktas att ordern har bevarats

men att de svarstider som anges i artiklarna 10 och 11 inte har följts, dock utan att bevisning gått förlorad.

En ytterligare viktig faktor är om tjänsteleverantören tidigare gjort sig skyldig till överträdelser av regelverket. Det är särskilt allvarligt om någon vid upprepade tillfällen underlåtit att följa en europeisk utlämnande- eller bevarandeorder.

Slutligen bör även tjänsteleverantörens finansiella ställning beaktas vid bestämmandet av avgiftens storlek. Den finansiella ställningen indikeras genom t.ex. en juridisk persons totala omsättning eller en fysisk persons årsinkomst.

Som framgår ovan innebär förslaget att det i lagtexten anges en exemplifierande, men inte uttömmande, uppräknning av vilka omständigheter som ska beaktas. När sanktionsavgiftens storlek bestäms är alltså det många omständigheter som måste beaktas som antingen är hänförliga till den specifika överträdelser eller till den person, juridisk eller fysisk, som har begått överträdelser. Det innebär att det alltid måste göras en bedömning med hänsyn till alla omständigheter som är relevanta i det enskilda fallet. Sanktionsavgifter för juridiska personer bör normalt sett bestämmas till högre belopp än för fysiska personer för samma typ av överträdelser.⁹

En sanktionsavgift bör vidare vara rimlig i förhållande till överträdelsens allvarighet jämfört med andra typer av överträdelser. Det går inte att i lag ange vilken relativ vikt som ska tillmätas olika omständigheter eller hur de ska vägas i det enskilda fallet. Detta hindrar inte att den verkställande myndigheten som har i uppgift att besluta om sanktionsavgifter upprättar vägledande dokument för sin tillämpning av det spann inom vilket sanktionsavgift bör tas ut för olika typer av överträdelser.

I sammanhanget kan slutligen noteras att det i flera fall torde kräva att den beslutande myndigheten samråder med den myndighet som utfärdat den aktuella ordern, t.ex. för att avgöra vilken skada som en vägran att följa ordern haft i fråga om den brottsutredning i vilken ordern har utfärdats. En myndighet ska se till att ett ärende blir utrett i den omfattning som ärendets beskaffenhet kräver enligt den s.k. officialprincipen som kommer till uttryck i 23 § första stycket förvaltningslagen (2017:900), som är tillämplig i ärenden om administrativa sanktionsavgifter. Bestämmelsen innebär att det är myndigheten som har det yttersta ansvaret för att

⁹ Prop. 2016/17:22 s. 225.

underlaget i ett ärende är sådant att det leder till ett materiellt riktigt beslut. Kraven på myndighetens utredningsåtgärder varierar med hänsyn till ärendets karaktär och ett ingripande mot någon enskild kräver mer aktiva åtgärder.¹⁰

Det bör finnas en möjlighet att avstå från ingripande

Som konstaterats ovan bör strikt ansvar gälla för överträdelse av EU-förordningens bestämmelser. Om sanktionsbestämmelser bygger på ansvar utan krav på uppsåt eller oaktsamhet är det nödvändigt med ett utrymme för att sätta ned en sanktionsavgift helt eller delvis i vissa fall, genom eftergift eller jämkning. I annat fall riskerar avgiftssystemet att inte uppfylla de krav på rättssäkerhet som den ovan behandlade oskuldspresumtionen ger uttryck för. Sanktionsavgiftssystemen i svensk rätt som är baserade på strikt ansvar innehåller därför regler som möjliggör för kontrollmyndigheten att befria någon från sanktionsavgift om det framstår som oskäligt att ta ut en avgift. Även jämningsregler förekommer i de olika regelverken.

Det bör därför införas en bestämmelse som ger utrymme att jämka eller helt efterge avgiften om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

En sådan möjlighet utgör en säkerhetsventil i fall där det inte framstår som rimligt och proportionerligt att ta ut en avgift. Sanktionsavgiften bör kunna sättas ned helt eller delvis om exempelvis ett mindre företag inte har resurser att svara på en order i en nödsituation, vilket också tas upp som exempel i skäl 70 i EU-förordningen på en situation där sanktionsavgift inte bör påföras tjänstleverantören. Det bör alltså vara möjligt att jämka eller helt efterge sanktionsavgiften om det framkommer omständigheter som gör att överträdelsen är ursäktlig. Denna möjlighet bör tillämpas restriktivt och användas endast om det skulle te sig oskäligt att ta ut sanktionsavgift.

¹⁰ Prop. 2016/17:180 s. 148–149 och Kammarrätten i Stockholm, dom 2022-05-16 i mål nr 4471-21.

Vem ska betala sanktionsavgiften?

Enligt artikel 16.10 i EU-förordningen ska sanktionsavgift påföras om *mottagaren* inte har fullgjort sina skyldigheter. Enligt artikel 7 är mottagaren av en europeisk utlämnande- eller bevarandeorder det verksamhetsställe eller rättsliga ombud som tjänsteleverantören har utsett i enlighet med artikel 3.1 i EU-direktivet. Sanktionsavgiften ska således riktas mot någon av dessa aktörer. För svenskt vidkommande bör det således röra sig om verksamhetsställen eller rättsliga ombud i Sverige.

Av artikel 3.5 i EU-direktivet följer emellertid att medlemsstaterna ska säkerställa att både det utsedda verksamhetsstället eller det rättsliga ombudet och tjänsteleverantören kan hållas solidariskt ansvariga för bristande efterlevnad av de skyldigheter som följer av den tillämpliga rättsliga ramen vid mottagande av beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2, så att var och en av dem kan bli föremål för sanktioner för att någon av dem brustit i efterlevnad. Medlemsstaterna ska i synnerhet säkerställa att det inte är möjligt för tjänsteleverantören, det utsedda verksamhetsstället eller det rättsliga ombudet, att använda avsaknaden av lämpliga interna rutiner mellan tjänsteleverantören och verksamhetsstället eller det rättsliga ombudet för att rättfärdiga sin bristande efterlevnad av dessa skyldigheter. Solidariskt ansvar ska dock inte gälla för något som antingen tjänsteleverantören, det utsedda verksamhetsstället eller det rättsliga ombudet har gjort eller försummat att göra och som utgör ett brott i den medlemsstat som påför sanktionerna.

Artikel 3.5 i EU-direktivet stadgar alltså enligt vår mening ett solidariskt ansvar för tjänsteleverantören och dess utsedda verksamhetsställe eller rättsliga ombud för det fall en utfärdad europeisk utlämnande- eller bevarandeorder inte efterlevs. Tillsammans med artikel 16.10 i EU-förordningen bör det innebära att tjänsteleverantören och verksamhetsstället eller det rättsliga ombudet ska kunna vara solidariskt betalningsansvariga i fråga om en påförd sanktionsavgift om verksamhetsstället eller det rättsliga ombudet åsidosätter någon av sina skyldigheter enligt artiklarna 10, 11 eller 13.4 i EU-förordningen. Även skäl 70 i EU-förordningen indikerar en sådan solidarisk betalningsskyldighet eftersom det där talas om tjänsteleverantörens tidigare överträdelse och dess finansiella

ställning. En bestämmelse om ett sådant solidariskt ansvar bör föras in i den kompletterande lagen.

9.4 Sanktioner vid överträdelser av de bestämmelser som genomför EU-direktivet

9.4.1 Utgångspunkter i EU-direktivet

Artikel 5 i EU-direktivet innehåller också bestämmelser om sanktioner. Medlemsstaterna ska enligt bestämmelsen fastställa regler om sanktioner för överträdelse av nationella bestämmelser som antagits enligt artiklarna 3 och 4 och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas.

Artikel 3 innehåller bestämmelser om tjänsteleverantörernas skyldigheter varav av den viktigaste är att utse verksamhetsställen eller rättsliga ombud (artikel 3.1). I artikel 3.2 och 3.3 föreskrivs ytterligare skyldigheter för tjänsteleverantörerna, bl.a. att de utser ett verksamhetsställe som är etablerad i en medlemsstat där leverantören erbjuder sina tjänster. Av artikel 3.4 följer vidare en skyldighet för tjänsteleverantörerna att tillse att det utsedda verksamhetsstället eller rättsliga ombudet har tillräckliga befogenheter och resurser att svara på t.ex. en sådan europeisk utlämnandeorder eller bevarandeorder. I artikel 3.6 anges när en tjänsteleverantör senast ska ha utsett ett verksamhetsställe eller rättsligt ombud. Artikel 4.1–4.3 reglerar tjänsteleverantörernas skyldighet att underrätta centralmyndigheten om kontaktuppgifter till det utsedda verksamhetsstället eller rättsliga ombudet samt vilket språk som ska användas i kontakten med dessa aktörer (mer om artikel 3 och 4, se avsnitt 8.2).

Det är dock svårt att se att en sanktion enligt artikel 5 ska kunna beslutas vid bristande efterlevnad av artikel 3.5 eftersom den sistnämnda bestämmelsen syftar till att medlemsstaterna ska säkerställa att tjänsteleverantörer och verksamhetsställen eller rättsliga ombud kan hållas solidariskt ansvariga för andra brister, bl.a. genom sanktioner enligt EU-förordningen (se avsnitt 9.3.2).

Till skillnad från EU-förordningen överlåter direktivet till medlemsstaterna att fastställa nationella regler om vilka sanktioner som ska följa vid överträdelser av de aktuella artiklarna, dvs. även andra sanktioner än sanktionsavgifter kan aktualiseras.

Sanktionerna ska vara effektiva, proportionella och avskräckande (artikel 5). Sanktionerna bör inte under några omständigheter leda till ett permanent eller tillfälligt förbud mot tillhandhållande av tjänster (skäl 18). Av skäl 19 följer att vid fastställandet av lämpliga sanktioner för tjänsteleverantörers överträdelse bör de behöriga myndigheterna beakta alla relevanta omständigheter, såsom tjänsteleverantörens ekonomiska kapacitet, överträdelsens art, allvarlighetsgrad och varaktighet, huruvida den begåtts uppsåtligt eller av oaktsamhet samt huruvida tjänsteleverantören har hållits ansvarig för liknande tidigare överträdelse. I detta sammanhang bör enligt skälet särskild uppmärksamhet ägnas åt mikroföretag.

Medlemsstaterna ska enligt artikel 5 anmäla sina införda regler om sanktioner till kommissionen anmäla senast den 18 februari 2026 samt årligen informera kommissionen om tjänsteleverantörer som inte uppfyller kraven, relevanta verkställighetsåtgärder som vidtagits mot dem och påförda sanktioner.

9.4.2 Val av sanktioner vid överträdelse av de bestämmelser som genomför EU-direktivet

Förslag: Överträdelse av de nationella bestämmelser som genomför artiklarna 3 och 4 ska kunna leda till administrativa sanktioner i form av vitesföreläggande eller sanktionsavgift.

Bedömning: Några särskilda regler om handläggningen av ett ärende om vitesföreläggande behöver inte införas.

Skälen för förslaget och bedömningen

Överträdelse ska inte vara straffsanktionerad

Kriminalisering som metod för att försöka hindra överträdelse av olika normer i samhället bör användas med försiktighet. Regeringen har i detta sammanhang uttalat att rättsväsendet inte ska belastas med sådant som har ringa eller inget straffvärde. Kriminalisering är

heller inte det enda och inte alltid det mest effektiva medlet för att motverka oönskade beteenden.¹¹

De nationella bestämmelser som genomför EU-direktivets bestämmelser och som ska förenas med sanktioner innehåller skyldigheter som åläggs tjänsteleverantörer. En tjänsteleverantör kan enligt artikel 3.3 EU-förordningen vara antingen en fysisk eller juridisk person, även om det torde vara sällsynt att det rör sig om en fysisk person. Av artikel 3.1 i EU-direktivet följer dock att skyldigheten att utse ett verksamhetsställe eller rättsligt ombud endast omfattar tjänsteleverantörer som är juridiska personer. Det är därför av avgörande betydelse att de föreslagna sanktionerna är effektiva i förhållande till just juridiska personer. Juridiska personer kan inte åläggas ett straffansvar. En kriminalisering av överträdelser av de nationella bestämmelser som genomför artiklarna 3 och 4 skulle därför inte verka avskräckande för merparten av de tjänsteleverantörer som är skyldiga att följa.

Juridiska personer kan visserligen bli föremål för talan om företagsbot (36 kap. 23 § brottsbalken). En förutsättning för ansvar är dock att brottet har begåtts i utövningen av företagets verksamhet, vilket kan innebära bevisvärigheter.

Av nämnda skäl framstår inte straff som en lämplig sanktion eller som ett effektivt verktyg för att sanktionera de aktuella överträdelserna. Några straffbestämmelser föreslås därför inte.

Överträdelser ska leda till administrativa sanktioner

Vi har ovan gjort bedömningen att överträdelser av de nationella bestämmelser som genomför artiklarna 3 och 4 i EU-direktivet inte bör kriminaliseras. Det alternativ som återstår att överväga är därmed administrativa sanktioner.

Det finns flera fördelar med att välja administrativa sanktioner vid genomförandet av EU-direktivet, särskilt då det rör sig om juridiska personer. Förfarandet är snabbt och effektivt. Den ekonomiska avgiften kan bestämmas till relativt höga belopp och göras beroende av vilken skyldighet aktören åsidosatt och vilken aktör som ska påföras sanktionen, t.ex. kan aktörens storlek beaktas vilket också framhålls som angeläget i skäl 19 i EU-direktivet.

¹¹ Prop. 1994/95:23 s. 52–53.

Administrativa sanktioner är således ett effektivt och avskräckande styrmedel gentemot juridiska personer, oavsett verksamhetens storlek. Det är också vanligt att administrativa sanktioner införs i svensk rätt för att genomföra och komplettera EU-rättsakter.

I svensk rätt är, som utvecklas i avsnitt 9.2, vitesföreläggande, sanktionsavgift, återkallelse av tillstånd och förbud möjliga administrativa sanktioner. Återkallelse av tillstånd och förbud saknar här relevans med hänsyn till hur EU-direktivet är utformat, vilket också, som nämnts ovan, följer av skäl 18 till direktivet. De administrativa sanktioner som återstår att överväga är därmed beslut om vitesförelägganden och sanktionsavgifter. Utgångspunkten bör vid denna bedömning vara att sanktionen vid en överträdelse är handlingsdirigerande. Detta för att skapa ett incitament för tjänsteleverantörer att efterleva de skyldigheter som de ålagts genom direktivets bestämmelser, varav utseendet av ett verksamhetsställe eller ett rättsligt ombud får anses vara den huvudsakliga och viktigaste skyldigheten.

Som nämnts i avsnitt 9.2 är vitesföreläggande en framåtsyftande sanktion. Först om den vitesålagde inte uppfyller en skyldighet som en tillsynsmyndighet för dennes del har specificerat, döms vitet ut. Vitet är således särskilt lämpligt att använda när man vill förmå någon att vidta en åtgärd eller avstå från att vidta en åtgärd.

Centralmyndigheten bör få möjlighet att i sin tillsynsverksamhet, såsom vi föreslagit i avsnitt 8.6, att meddela förelägganden om t.ex. att få ta del av information eller få tillträde till utrymmen. Ett sådant föreläggande bör kunna förenas med vite för att ges erforderlig tyngd. Även de skyldigheter som tillkommer tjänsteleverantören enligt artikel 4.1–4.3, dvs. underrättelse om kontaktuppgifter och språk är av sådan karaktär att de är lämpliga att sanktionera med ett vitesföreläggande.

Vidare bör en tjänsteleverantör vid vite kunna föreläggas att följa skyldigheten att utse ett verksamhetsställe eller rättsligt ombud enligt artikel 3.1 i en stat i enlighet med artikel 3.2 eller att ge dessa nödvändiga befogenheter och resurser i enlighet med artikel 3.4. En sådan åtgärd har alltså ett framåtriktat syfte, dvs. att exempelvis förmå en tjänsteleverantör som inte har utsett ett verksamhetsställe eller rättsligt ombud att så göra.

Det förhållandet att vitet enbart är framåtsyftande medför att när denna metod används kan det dock många gånger finnas behov av att komplettera vitet med en tillbakaverkande sanktion.¹²

För det fall ett föreläggande med vite inte har en sådan åsytande verkan, bör det även kunna vara aktuellt att påföra en sanktionsavgift för en tjänsteleverantör som trots föreläggande inte har utsett ett verksamhetsställe eller rättsligt ombud eller gett dem erforderliga befogenheter och resurser. En sanktionsavgift riktar sig, som utvecklats ovan, mot en redan konstaterad överträdelse av en författningsbestämmelse. Om sanktionsavgiften innebär en risk för en kostnad eller förlust som väger tyngre än den besparing som görs genom att regelverket inte följs, skapar avgiften ett starkt incitament att undvika överträdelser. Det bör därför vara möjligt för centralmyndigheten att även kunna påföra sanktionsavgift för samma överträdelse, t.ex. om en tjänsteleverantör trots förelägganden inte utser ett verksamhetsställe eller rättsligt ombud eller att tidigare sådana aktörer inte längre företräder tjänsteleverantören.

Det bör också framhållas att en tjänsteleverantör som inte fullföljer en begäran i en europeisk utlämnandeorder respektive bevarandeorder kan bli föremål för påförande av sanktionsavgift enligt EU-förordningen. Sanktionsbestämmelserna enligt EU-direktivet avser i stället själva utseendet av ett verksamhetsställe eller rättsligt ombud eller frågan om dessa getts tillräckliga befogenheter och resurser. Att en tjänsteleverantör inte fullföljer en sådan order som omfattas av EU-förordningen kan bero på att denne inte har utsett ett verksamhetsställe eller rättsligt ombud eller inte gett det utsedda verksamhetsstället respektive det rättsliga ombudet tillräckliga befogenheter och resurser att besvara en order. I en sådan situation föreligger förutsättningar att besluta om sanktionsavgifter enligt både EU-förordningen och de nationella bestämmelser som genomför EU-direktivet. Vi återkommer till denna fråga i avsnitt 9.5.

I avsnitt 9.4.3 nedan redogörs för hur ett sanktionsavgiftssystem i denna del bör konstrueras.

¹² SOU 2013:38 s. 537.

Handläggning av ärenden om vitesförelägganden

Beslut om föreläggande ska kunna förenas med vite i de fall som redogjorts för ovan. Ett sådant beslut fattas av centralmyndigheten. Lagen (1985:206) om viten (viteslagen) innehåller bestämmelser om handläggningen av ärenden om vitesförelägganden och gäller enligt 1 § viten som enligt lag eller annan författning får föreläggas av myndigheter, såvida inte annat följer av vad som är särskilt föreskrivet. Av 2 § viteslagen följer att vitesförelägganden ska delges. Enligt 3 § viteslagen ska vite, när det föreläggs, fastställas till ett belopp som med hänsyn till vad som är känt om adressatens ekonomiska förhållanden och till omständigheterna i övrigt kan antas förmå honom att följa det föreläggande som är förenat med vitet. Frågor om utdömande av viten prövas av förvaltningsrätt på ansökan av den myndighet som har utfärdat vitesföreläggandet (6 §).

Bestämmelserna i viteslagen är ändamålsenligt utformade för handläggningen av ärenden om vitesförelägganden enligt förslaget ovan. Det finns därför inte skäl att införa några särskilda bestämmelser i den kompletterande lagen om handläggningen av vitesförelägganden. Vidare blir förvaltningslagen (2017:900) och förvaltningsprocesslagen (1971:291) tillämpliga på handläggningen hos centralmyndigheten respektive i förvaltningsdomstol. Inte heller i dessa delar finns skäl att införa några särskilda bestämmelser i den kompletterande lagen.

9.4.3 Utformningen av ett sanktionsavgiftssystem utifrån EU-direktivets bestämmelser

Förslag: Centralmyndigheten ska besluta att ta ut en sanktionsavgift av en tjänsteleverantör som åsidosätter någon av sina skyldigheter enligt de nationella bestämmelser som genomför artikel 3 EU-direktivet.

Sanktionsavgiften ska bestämmas till lägst 10 000 kronor och högst till ett sådant högre belopp som följer av artikel 15.1 i EU-förordningen.

Vid bedömningen av om någon sanktionsavgift ska tas ut och när storleken på avgiften ska bestämmas, ska särskild hänsyn tas till om överträdelsen varit uppsåtlig eller berott på oaktsamhet, den skada, fara eller kränkning som överträdelsen inneburit samt till överträdelsens karaktär, svårhetsgrad och varaktighet, om den tjänsteleverantör som har begått överträdelsen tidigare begått en liknande överträdelse samt den berörda tjänsteleverantörens finansiella ställning.

Sanktionsavgiften får sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgift.

Centralmyndigheten ska inte få besluta om sanktionsavgift om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömmande av vitet.

Skälen för förslaget

Utgångspunkter

Vi har i avsnitt 9.4.2 föreslagit att överträdelser av de nationella bestämmelser som genomför artikel 3 i huvudsak bör sanktioneras med sanktionsavgifter, medan överträdelser av artikel 4 endast bör kunna vara föremål för vitesföreläggande. Frågan är då hur ett sanktionssystem för överträdelser i denna del bör utformas.

Det sanktionsavgiftssystem som föreslås i avsnitt 9.3 beträffande överträdelser av EU-förordningens bestämmelser bör tjäna som förebild vid utformningen av sanktionsavgifter för de nu aktuella överträdelserna. På så sätt blir systemen enklare att överblicka för de tjänsteleverantörer som berörs av dem.

Utformningen av ett sanktionsavgiftssystem

Som har redogjorts för i avsnitt 9.2 är huvudregeln i svensk rätt att sanktionsavgifter bygger på strikt ansvar. Av samma skäl som anförts i fråga om utformningen av ett sanktionsavgiftssystem för överträdelse av EU-förordningens bestämmelser i avsnitt 9.3 bör ett system med sanktionsavgifter vid överträdelse av de nationella bestämmelser som genomför artikel 3 bygga på strikt ansvar.

Av de skäl som anförts i avsnitt 9.3 bör det vidare vara obligatoriskt att besluta om avgift om förutsättningarna för att ta ut avgift är uppfyllda. Som vi funnit i nämnda avsnitt bör dock en sådan bestämmelse förenas med en möjlighet att helt eller delvis efterge avgiften.

I likhet med vad som föreslås beträffande beslut om sanktionsavgifter vid överträdelse av EU-förordningen bör det inte vara förvaltningsdomstol som fattar beslut om sanktionsavgift. I stället bör avgiften beslutas av centralmyndigheten (se även avsnitt 8.6.3).

Sanktionerna ska enligt artikel 5 i EU-direktivet vara effektiva, proportionella och avskräckande. Som behandlats i avsnitt 9.4.1 följer det av skäl 19 till direktivet att alla relevanta omständigheter bör beaktas vid bestämmandet av sanktioner, såsom tjänsteleverantörens ekonomiska kapacitet, överträdelsens art, allvarlighetsgrad och varaktighet, huruvida den begåtts uppsåtligen eller av oakt-samhet samt huruvida tjänsteleverantören har hållits ansvarig för liknande tidigare överträdelse. I detta sammanhang bör det enligt skälet särskild uppmärksamhet ägnas åt mikroföretag.

Som konstaterats i avsnitt 9.3 kan det skilja stort mellan tjänsteleverantörer i fråga om storlek och ekonomiska förutsättningar, varför det är av vikt att en sanktionsavgift är kännbar för samtliga typer av tjänsteleverantörer, dvs. både ett mindre företag med små resurser, som t.ex. ett mikroföretag, och ett större företag med stora resurser. För att uppfylla kravet på effektiva, proportionella och avskräckande sanktioner bör intervallet för sanktionsavgiften därför vara förhållandevis stort för att möjliggöra en nyanserad bedömning.

I avsnitt 9.3 har vi redogjort för hur beloppsintervall är konstruerade i olika sanktionsavgiftssystem. De överträdelse av EU-direktivet som ska kunna leda till en sanktionsavgift enligt vår bedömning i avsnitt 9.4.2 är underlåtenhet att utse verksamhetsställe eller rätts-

ligt ombud i tid i en medlemsstat i vilken tjänsteleverantören erbjuder sina tjänster samt underlåtenhet att tillse att verksamhetsstället eller det rättsliga ombudet har fått de befogenheter och resurser som krävs för att kunna svara på t.ex. en europeisk utlämnande- eller bevarandeorder. För att samarbetet enligt EU-förordningen ska kunna fungera är det av största vikt att tjänsteleverantörerna efterlever de skyldigheter som följer av direktivet. Om en tjänsteleverantör t.ex. inte utser ett verksamhetsställe kommer en sådan order som omfattas av EU-förordningen inte kunna besvaras över huvud taget. Detta kan i sin tur leda till att brott inte kan utredas eller beivras, vilket får anses vara en allvarlig konsekvens av underlåtenheten att utse ett verksamhetsställe, vilket bör rendera i en kännbar avgift. Med hänsyn till att även tjänsteleverantörer av mindre storlek kan komma att omfattas av regelverket bör dock det lägsta belopp som ska kunna beslutas i sanktionsavgift vara 10 000 kronor. Till skillnad mot EU-förordningen innehåller inte direktivet någon bestämmelse om den övre gränsen för beloppsintervallet för sanktionsavgifter. Med hänsyn till de allvarliga konsekvenser som en överträdelse av EU-direktivets bestämmelser kan leda till bör den övre gränsen dock motsvara vad som gäller enligt EU-förordningen.

Som utvecklats i avsnitt 9.3 bör det i den kompletterande lagen regleras vilka omständigheter som i det enskilda fallet kan påverka avgiftens storlek. I skäl 19 anges, som behandlats ovan, ett antal omständigheter som bör beaktas vid bestämmandet av sanktioner. Dessa överensstämmer med vad som följer av skäl 70 i EU-förordningen. Samma omständigheter som ska beaktas i det enskilda fallet som föreslås gälla för påförande av sanktionsavgifter vid överträdelser av EU-förordningens bestämmelser bör därmed gälla även vid överträdelser av de nationella bestämmelser som genomför artikel 3 i EU-direktivet. Vid bestämmandet av sanktionsavgiftens storlek ska alltså särskild hänsyn tas till om överträdelser varit uppsåtlig eller berott på oaktsamhet, den skada, fara eller kränkning som överträdelser innebär. Vidare ska hänsyn tas till överträdelsens karaktär, svårhetsgrad och varaktighet, om den tjänsteleverantör som har begått överträdelser tidigare begått en liknande överträdelse samt den berörda tjänsteleverantörens finansiella ställning. Uppräkningen är som konstaterats i avsnitt 9.3 inte uttömmande, utan endast exemplifierande. Även andra omständigheter kan således beaktas vid bestämmandet av avgiftens storlek.

Slutligen bör det vara möjligt att jämka eller helt efterge sanktionsavgiften på samma sätt som utvecklats i avsnitt 9.3.3. I sammanhanget bör det framhållas att det kan förekomma att en tjänsteleverantör är etablerad i eller bedriver verksamhet i flera olika medlemsstater. Om tjänsteleverantören inte har utsett verksamhetsställe eller rättsligt ombud i någon medlemsstat föreligger förutsättningar för samtliga medlemsstater att påföra sanktionsavgift. I ett sådant fall bör, vilket har anförts i diskussioner mellan medlemsstater och kommissionen om genomförandet av rättsakten, endast en medlemsstat påföra sanktionsavgift, vilket kan koordineras genom det samarbete som enligt EU-direktivet ska ske mellan centralmyndigheterna. Detta eftersom tjänsteleverantören inte är skyldig att utse ett verksamhetsställe eller rättsligt ombud i varje medlemsstat där denne erbjuder tjänster, utan är fri att välja i vilken av dessa medlemsstater där verksamhetsställe eller rättsligt ombud ska utses (se avsnitt 8.3). Har en annan medlemsstat i en sådan situation redan påfört sanktionsavgift bör den svenska centralmyndigheten efterge sanktionsavgiften då det får anses oskäligt att ta ut avgift om annan medlemsstat redan har gjort detta. En ytterligare sanktion för samma underlåtenhet skulle även strida mot förbudet mot dubbelbestraffning.

Dubbelbestraffningsförbudet

I avsnitt 9.4.2 har vi föreslagit att både vitesföreläggande och sanktionsavgift ska kunna aktualiseras vid överträdelser av de nationella bestämmelser som genomför artikel 3 i EU-direktivet.

I det sjunde tilläggsprotokollet till Europakonventionen EU:s rättighetsstadga finns bestämmelser om rätten att inte bli lagförd eller straffad två gånger för samma brott (gärning), det s.k. förbudet mot dubbelbestraffning. Begreppet straff i den mening som avses i Europakonventionen och EU:s rättighetsstadga anses omfatta vite.¹³

Enligt Högsta domstolen är det inte enbart ett slutligt avgörande som utgör ett hinder mot ett andra förfarande, utan även en pågående prövning är ett sådant hinder (se NJA 2013 s. 502). Det innebär att det som avgör när ett hinder mot ett andra förfarande

¹³ Se t.ex. prop. 2007/08:107 s. 24, prop. 2012/13:143 s. 69 och prop. 2017/18:205 s. 72.

för samma gärning eller överträdelse uppkommer, får anses vara den tidpunkt när det inleds en domstolsprocess om utdömande om vite.¹⁴ En sanktionsavgift bör således inte kunna tas ut om överträdelsen har medfört att vite har dömts ut eller att en process om att döma ut vite har inletts. Om ett vitesföreläggande har överträtts ska alltså inte ha någon betydelse för frågan om en sanktionsavgift ska få beslutas. Sanktionsavgift bör kunna beslutas om ett föreläggande har överträtts men då åtgärder inte vidtagits för att vitet ska dömas ut. I stället kan det då bli aktuellt att besluta om sanktionsavgift. I ett sådant fall kan det dock inte komma i fråga att döma ut vitet i vid ett senare tillfälle. Förbudet mot dubbelbestraffning hindrar således både ett andra straff och en andra prövning av samma gärning. Ett förbud mot att både vite och sanktionsavgift tas ut för samma överträdelse bör därför följa av lag.

Solidariskt ansvar

En underlåtenhet att följa skyldigheten att utse ett verksamhetsställe eller rättsligt ombud enligt artikel 3.1 kan av naturliga skäl endast åläggas tjänsteleverantören. Detsamma gäller skyldigheten att förse ett verksamhetsställe eller rättsligt ombud med tillräckliga befogenheter och resurser enligt artikel 3.4. Något solidariskt betalningsansvar enligt det nu föreslagna sanktionssystemet på sätt som regleras i artikel 3.5 kan därför inte komma i fråga.

9.5 Gemensamma förfaranderegler avseende sanktionsavgifter

Förslag: 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.

Sanktionsavgiften ska betalas till den beslutande myndigheten 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

¹⁴ Prop. 2016/17:22 s. 228.

sanktionsavgiften inte betalas i tid, ska myndigheten lämna den obetalda avgiften för indrivning. Sanktionsavgiften tillfaller staten.

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

Ett beslut om sanktionsavgift vid bristande efterlevnad av de nationella bestämmelser som genomför direktivets bestämmelser om utseende av verksamhetsställen och rättsliga ombud och om tilldelning av tillräckliga befogenheter och resurser till verksamhetsställen eller rättsliga ombud för att besvara en order som omfattas av EU-förordningen ska ha företräde framför beslut om sanktionsavgifter vid bristande efterlevnad av EU-förordningens bestämmelser.

Beslut om sanktionsavgift ska få överklagas till allmän förvaltningsdomstol. Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Bedömning: Åklagarmyndigheten och centralmyndigheten bör inför beslut om sanktioner samråda med och informera varandra om de åtgärder som myndigheterna avser att vidta. Detta kan regleras i förordning.

Skälen för förslaget och bedömningen: Som föreslås ovan ska ett nationellt sanktionsavgiftssystem införas för överträdelser av artiklarna 10, 11 och 13.4 i EU-förordningen respektive för överträdelser av de nationella bestämmelser som genomför artikel 3 i EU-direktivet. I och med att det är den verkställande myndigheten, som vi föreslår ska vara Åklagarmyndigheten, respektive centralmyndigheten som ska besluta om sanktionsavgift kommer förvaltningslagen att gälla för förfarandet. Det behövs dock vissa ytterligare gemensamma förfarandebestämmelser.

På grund av sanktionsavgiftens ingripande natur bör det finnas en bortre tidsgräns för när en sanktionsavgift får beslutas. I likhet med vad som följer av bl.a. 13 § lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt och 9 § lagen med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online bör sanktionsavgift endast ska få tas ut om den som anspråket riktas mot har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Beslut om administrativa sanktionsavgifter är en ingripande åtgärd. Ett sådant beslut bör därför delges den betalningsskyldige enligt delgivningslagen (2010:1932).

EU-förordningen eller EU-direktivet innehåller inte några bestämmelser om att administrativa sanktioner ska tillfalla EU eller i övrigt om hur verkställighet ska ske. I avsaknad av en sådan reglering bör det framgå av den kompletterande lagen att sanktionsavgiften tillfaller staten. Vidare bör det anges att en sanktionsavgift ska betalas till den behöriga myndigheten 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 avgiften inte betalas i tid, bör den behöriga myndigheten vara skyldig att lämna den obetalda avgiften för indrivning. Det krävs inte någon särskild föreskrift för att beslutet om sanktionsavgift ska få verkställas enligt utsökningsbalken.¹⁵

I likhet med vad som i allmänhet gäller för sanktionsavgifter bör avgiften preskriberas till den del verkställighet inte har skett inom fem år från det att beslutet fick laga kraft.

Som har konstaterats i avsnitt 9.4.2 kan en situation uppstå att en vägran att följa en sådan order som omfattas av EU-förordningens bestämmelser beror på att tjänsteleverantören i fråga inte har utsett ett verksamhetsställe eller rättsligt ombud på föreskrivet sätt, vilket alltså innebär att det saknas en organisation att ta hand om ordern. Det kan också förhålla sig så att verksamhetsstället eller det rättsliga ombudet inte getts tillräckliga befogenheter eller resurser för att besvara en order enligt EU-förordningen. En sådan situation skulle innebära att det finns förutsättningar att fatta beslut om sanktioner både utifrån EU-förordningens och EU-direktivets bestämmelser. Med andra ord kan inte en europeisk utlämnande- eller bevarandeorder besvaras om tjänsteleverantören inte har utsett ett verksamhetsställe eller rättsligt ombud eller, om sådant har utsetts, inte gett den aktören tillräckliga befogenheter eller resurser att besvara en order. Det bör därför följa av lag att i en sådan situation ska beslut om sanktionsavgift vid bristande efterlevnad av de nationella bestämmelser som genomför direktivets bestämmelser om utseende av verksamhetsställen och rättsliga ombud respektive tilldelning av tillräckliga befogenheter och resurser till dessa aktörer ha företräde framför beslut om sanktionsavgifter vid bristande efterlevnad av EU-förordningens bestämmelser. Detta eftersom

¹⁵ Se 3 kap. 1 § utsökningsbalken och prop. 2021/22:206.

det är en förutsättning att det finns ett utsett verksamhetsställe eller rättsligt ombud med tillräckliga befogenheter och resurser för att en order enligt EU-förordningen över huvud taget ska kunna besvaras. Med hänsyn till att sanktioner kan bli aktuella enligt båda regelverken bör den verkställande myndigheten och centralmyndigheten inför beslut om sanktioner samråda med och informera varandra om de åtgärder som myndigheten avser att vidta. Detta kan dock regleras i förordning.

Eftersom vi föreslår att sanktionsavgifter ska beslutas av den verkställande myndigheten respektive centralmyndigheten, i stället för av en domstol, är det nödvändigt att lagen förses med en bestämmelse som anger att beslut om sanktionsavgift får överklagas. Artikel 16.10 i EU-förordningen stadgar vidare att ett effektivt rättsmedel ska finnas tillgängligt mot ett beslut att ålägga en sanktionsavgift. Med anledning av att det rör sig om en administrativ sanktionsavgift bör besluten kunna överklagas till allmän förvaltningsdomstol. Prövningstillstånd bör krävas vid överklagande till kammarrätten.

10 Övriga frågor

10.1 Inledning

Införandet av EU-förordningen och EU-direktivet kan enligt våra direktiv även medföra behov av andra författningsändringar än de förslag som behandlats i föregående kapitel. Vi ska därför analysera och vid behov lämna förslag om andra författningsändringar som bedöms nödvändiga med anledning av EU-förordningen och EU-direktivet.

I avsnitt 10.2 behandlas frågan om framställningar som skickas till Sverige ska godtas på andra språk än svenska (artiklarna 9.4 och 16.2 i EU-förordningen). Vidare behandlas tjänsteleverantörers möjligheter enligt artikel 14 i EU-förordningen att kräva ersättning av den utfärdande staten för kostnader som uppstår i samband med hanteringen av en europeisk utlämnande- eller bevarandeorder (avsnitt 10.3). Därefter analyseras hur rätten till effektiva rättsmedel ska kunna utövas på ett ändamålsenligt sätt enligt vad som anges i artikel 18 EU-förordningen (avsnitt 10.4). EU-förordningens regler om metoder för kommunikation enligt artiklarna 19.5 och 24 och om insamling av statistik enligt artikel 28 behandlas i avsnitten 10.5 och 10.6. Slutligen analyseras regelverkens förhållande till dataskyddsregleringen samt frågan om uppgiftslämnande och sekretess i avsnitten 10.7 och 10.8.

10.2 Intyg och språk

Förslag: Ett intyg om en europeisk utlämnande- eller bevarandeorder som översänds till Åklagarmyndigheten ska vara skrivet på eller översatt till svenska eller engelska.

Bedömning: Skyldigheten att upprätta intyg om en europeisk utlämnande- eller bevarandeorder följer direkt av EU-förordningen och kräver inga bestämmelser i lag.

Sverige bör avge en förklaring till artikel 27 i EU-förordningen i enlighet med förslaget.

Skälen för förslaget och bedömningen

EU-förordningens bestämmelser

Enligt artikel 9.1 ska den utfärdande myndigheten översända en utfärdad europeisk utlämnande- eller bevarandeorder till mottagaren i enlighet med artikel 7 (dvs. det utsedda verksamhetsstället eller det rättsliga ombudet). Det sker genom upprättande av ett intyg (eller formulär) som återfinns i bilaga I och II i förordningen. I intyget ska enligt artiklarna 9.2 och 9.3 alla de uppgifter som anges i artikel 5.5 respektive artikel 6.4 återfinnas. I artikel 9.4 finns bestämmelser om språk (se även skäl 55).

Intyget ska, om det behövs, enligt artikel 9.4 första stycket översättas till ett av unionens officiella språk som godtas av mottagaren i enlighet med det förfarande som anges i artikel 4 i EU-direktivet. Av artikel 4.2 i direktivet framgår att tjänsteleverantören ska informera den enligt direktivet utsedda centralmyndigheten vilket eller vilka språk som det utsedda verksamhetsstället eller det rättsliga ombudet accepterar, varav ett av de officiella språken i den stat i vilken verksamhetsstället är etablerat eller det rättsliga ombudet har sin hemvist ska inkluderas. Om tjänsteleverantören inte har angett något språk ska intyget enligt artikel 9.4 första stycket i EU-förordningen översättas till ett officiellt språk i den medlemsstat där det utsedda verksamhetsstället eller det rättsliga ombudet befinner sig.

Om en anmälan till den verkställande myndigheten krävs enligt artikel 8.1 ska intyget enligt artikel 9.4 andra stycket i EU-förord-

ningen översättas till ett officiellt språk i den verkställande staten eller till ett annat av unionens officiella språk som godtas av den staten. Detsamma gäller när den utfärdande myndigheten överlämnar ett intyg om en europeisk utlämnande- eller bevarandeorder enligt artikel 16.2.

Enligt artikel 27 kan en medlemsstat när som helst, dvs. även efter det att EU-förordningen har börjat tillämpas besluta att den godtar översättningar av intygen till ett eller flera av unionens officiella språk utöver dess officiella språk. Detta ska i en förklaring anmälas till kommissionen som i sin tur ska se till att göra förklaringarna tillgängliga för samtliga medlemsstater och för det europeiska rättsliga nätverket. Av artikel 31.1 d framgår slutligen att medlemsstaterna ska anmäla till kommissionen vilka språk som omfattas.

Upprättande av intyget

Skyldigheten att upprätta ett intyg med det innehåll som anges i de formulär som finns bilagda till EU-förordningen följer direkt av artikel 9.1–9.3 i förordningen och kräver inga bestämmelser i lag.

Vilka språk ska Sverige acceptera?

När det gäller EU-förordningens och EU-direktivets bestämmelser om språk i förhållande till tjänsteleverantören och det utsedda verksamhetsstället respektive det rättsliga ombudet behövs inga regler i svensk rätt eftersom språkkraven som en utfärdande myndighet har att förhålla sig till följer direkt av EU-förordningen. Däremot behövs regler om språk när ett intyg om en europeisk utlämnande- eller bevarandeorder enligt artikel 8.1 eller artikel 16.2 ska sändas över till Åklagarmyndigheten.

Sverige har vid genomförandet av flera andra EU-rättsakter som rör straffrättsligt samarbete ansett att svenska, norska, danska och – på senare år – engelska bör godtas. I samtliga fall ansågs det självklart att de språk som normalt godtas i det straffrättsliga samarbetet, nämligen svenska, danska och norska, ska vara godtagbara språk. Bakgrunden till att även engelska har godtagits i samband med genomförandet av vissa EU-rättsakter har varit att det kan

antas att många stater har begränsade möjligheter och resurser att ordna med översättningar till svenska, samtidigt som det finns skäl att anta kunskaperna i engelska och tillgången till översättare till engelska är god inom hela EU.¹

Vid genomförandet av direktivet om den europeiska skyddsordern uppställdes dock ett krav på att en skyddsorder som översänds till Sverige, ska vara översatt till svenska. Som skäl angavs att innehållet i det formulär som en skyddsorder ska utfärdas i enlighet med har en avgörande betydelse för bedömningen av såväl om en europeisk skyddsorder ska verkställas som hur verkställigheten ska gå till.²

I fråga om genomförandet av direktivet om en europeisk utredningsorder gjorde regeringen samma bedömning. Regeringen ansåg att en sådan order i vissa avseenden skiljer sig från de beslut och formulär som översänds enligt andra EU-rättsakter. Som exempel gavs att bl.a. en utredningsorder angående vissa åtgärder, t.ex. hemlig kameraövervakning eller hemlig rumsavlyssning, endast kan erkännas om samma förutsättningar som gäller för motsvarande åtgärd i en svensk förundersökning eller rättegång är uppfyllda. Det konstaterades att åklagarens och domstolens prövning då ska göras utifrån de uppgifter som lämnas i utredningsordern, vilka många gånger kan avse komplicerade förhållanden. I sammanhanget framhölls att ett förhör som ska hållas av en svensk myndighet ska som huvudregel hållas på svenska, varför frågor som är skrivna på engelska, norska eller danska måste översättas. Även i de fall då den svenska åklagaren eller domstolen ska pröva om förutsättningarna för åtgärden är uppfyllda, kan det enligt regeringen tänkas uppstå behov av översättning till svenska. Mot denna bakgrund fann regeringen att det framstod som mest lämpligt med ett krav på att en europeisk utredningsorder som översänds till Sverige ska vara skriven på eller översatt till svenska. Regeringen ansåg dock, att om omständigheterna i det enskilda fallet medger det, bör den åklagare eller tingsrätt som handlägger ärendet kunna godta att ordern i stället skrivs på eller översätts till engelska, vilket överensstämmer vad som gäller för en ansökan om rättslig hjälp enligt 2 kap. 5 § lagen om internationell rättslig hjälp i brottmål.³

¹ Se t.ex. prop. 2004/05:115 s. 39, prop. 2010/11:43 s. 65 och prop. 2014/15:29 s. 114–115.

² Prop. 2014/15:139 s. 46.

³ Prop. 2016/17:218 s. 165–166.

Det kan konstateras att varken Norge eller Danmark deltar i samarbetet kring den aktuella EU-förordningen. Det är därför överflödigt att föreskriva att en order som omfattas av förordningen kan vara skriven på eller översatt till norska och danska. Varken norska eller danska bör därför godtas. Samma bedömning gjordes vid genomförandet av direktivet om en europeisk utredningsorder.⁴

När det sedan gäller frågan om intyget om en europeisk utlämnandeorder eller bevarandeorder kan vara skriven på eller översatt till engelska kan konstateras att verkställighet av en order endast får nekas av de skäl som anges i artiklarna 16.4 och 16.5. Beträffande en europeisk utlämnandeorder ska vidare den verkställande myndigheten pröva vägransgrunder som avses i artikel 12.1. Någon prövning av om en order endast kan verkställas om samma förutsättningar som gäller för motsvarande åtgärd i en svensk förundersökning är uppfyllda ska således – till skillnad från vad som gäller för vissa åtgärder som omfattas av lagen om en europeisk utredningsorder – inte göras. Till det kommer att intyg om en europeisk utlämnande- eller bevarandeorder är utformat på ett sådant sätt att det endast lämnar begränsat utrymme för fritext. Det finns därför goda skäl att, i likhet med vad som gäller för förfarandet beträffande flera andra EU-rättsakter, godta även engelska när ett intyg om en europeisk utlämnande- eller bevarandeorder översänds hit enligt EU-förordningen.

Intyg om en europeisk utredningsorder respektive bevarandeorder som sänds över enligt EU-förordningen bör alltså vara skrivna på eller översatta till svenska och engelska. Detta bör framgå av den kompletterande lagen. Sverige bör med anledning härav i sin anmälan till kommissionen ange att utöver svenska accepteras engelska.

⁴ Prop. 2016/17:218 s. 165–166.

10.3 Ersättning för kostnader

Förslag: Bestämmelsen i 9 kap. 29 a § lagen om elektronisk kommunikation ska äga motsvarande tillämpning för en tjänsteleverantör som lämnar ut abonnentuppgifter eller andra användaruppgifter, trafikuppgifter eller innehållsdata till den svensk myndighet som har utfärdat en europeisk utlämnandeorder.

Skälen för förslaget: Artikel 14 i EU-förordningen reglerar möjligheten för en tjänsteleverantör att få ersättning för de kostnader som uppkommit vid svar på en europeisk utlämnande- eller bevarandeorder från den utfärdande staten (se även skäl 68). Av artikel 14.1 följer att tjänsteleverantören får kräva ersättning för sina kostnader från den utfärdande staten, om en sådan möjlighet föreskrivs i den utfärdande statens nationella rätt för inhemska förelägganden i liknande situationer, i enlighet med den statens nationella rätt. Medlemsstaterna ska informera kommissionen om sina nationella regler för ersättning, och kommissionen ska offentliggöra dessa. Finns inte några sådana bestämmelser i den utfärdande staten kan en tjänsteleverantör inte kräva ersättning även om det vore möjligt i den verkställande staten.

Enligt artikel 14.2 är artikeln inte tillämplig på ersättning av kostnader för det decentraliserade it-system som avses i artikel 25.

Som tidigare har behandlats i avsnitt 4.2.5 innehåller lagen (2022:482) om elektronisk kommunikation krav på att en verksamhet ska bedrivas så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs (9 kap. 29 §).

Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § nämnda lag har rätt till ersättning för kostnader som uppstår när uppgifter om abonnemang, innehållet i ett elektroniskt meddelande, eller en annan uppgift som angår ett särskilt elektroniskt meddelande lämnas ut till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott. I de fall det är särskilt föreskrivet ska ersättningen beräknas enligt schablon. Ersättningen ska betalas av den myndighet som har begärt uppgifterna (9 kap. 29 a § första stycket). Rätten till ersättning gäller

även för utlämnande av lokaliseringsuppgifter som inte är trafikuppgifter (andra stycket).

Post- och telestyrelsen får, efter samråd med Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket och Åklagarmyndigheten, meddela föreskrifter om ersättning och schablonberäkning enligt 9 kap. 29 a § lagen om elektronisk kommunikation, vilket följer av 9 kap. 12 § förordningen om elektronisk kommunikation.

I enlighet med våra bedömningar i avsnitten 6.8 och 6.9 motsvarar definitionerna av begreppen uppgifter om abonnemang, trafikuppgifter och lokaliseringsuppgifter av de begrepp som används i EU-förordningen; dvs. abonnentuppgifter och andra användaruppgifter och trafikuppgifter, medan innehållsdata får anses motsvaras av begreppet innehållet i ett elektroniskt meddelande.

Bestämmelsen i 9 kap. 29 a § lagen om elektronisk kommunikation om rätt till ersättning gäller för den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § lagen om elektronisk kommunikation. Den kan därför inte anses tillämplig på samtliga de tjänsteleverantörer som omfattas av EU-förordningens bestämmelser. De tjänsteleverantörer som mottar en europeisk utlämnandeorder avseende abonnentuppgifter eller andra användaruppgifter, trafikuppgifter eller innehållsdata från behörig utfärdande myndighet i Sverige bör ha rätt till ersättning för sina kostnader på samma sätt som en tjänsteleverantör som lämnar ut sådana uppgifter i ett inhemskt ärende har rätt till ersättning enligt 9 kap. 29 a § lagen om elektronisk kommunikation.

Det framstår därför som ändamålsenligt att en bestämmelse med motsvarande innehåll införs i den lag som kompletterar EU-förordningen. Regeringen eller den myndighet som regeringen bestämmer bör, i likhet med vad som gäller beträffande nämnda bestämmelse i lagen om elektronisk kommunikation, få meddela ytterligare föreskrifter om ersättningen och schablonberäkning av sådan ersättning.

Bestämmelsen kommer således endast träffa de utländska tjänsteleverantörer som vid en motsvarande tillämpning av 9 kap. 29 a § lagen om elektronisk kommunikation skulle ha rätt till ersättning. De utländska tjänsteleverantörer som bl.a. omfattas av artikel 3.3 b och c torde således inte kunna kräva någon ersättning eftersom det inte heller skulle vara möjligt i svenskt inhemskt förfarande. Inte

heller kan ersättnings krävas när en europeisk bevarandeorder har utfärdats eftersom någon rätt till ersättning inte föreskrivs i svensk rätt i dessa fall.

I det fall en utländsk behörig myndighet har begärt uppgifter från en tjänsteleverantör i Sverige är det enligt artikel 14.1 den utfärdande staten som ska svara för tjänsteleverantörens kostnader som uppkommit i samband med utlämnandet av uppgifter. Svenska tjänsteleverantörers rätt till ersättning styrs alltså av den andra statens nationella rätt och är beroende av den staten har föreskrivit om en rätt till ersättning. Det svenska ersättningssystemet bygger på tanken att tjänsteleverantörerna ska kompenseras för de kostnader de haft för att anpassa sina system till det nationella regelverket om lagring i lagen om elektronisk kommunikation. De kan te sig märkligt att den enskilde tjänsteleverantören i Sverige inte kan få ersättning för en förfrågan om den görs av en myndighet i en annan medlemsstat om en sådan regel inte finns i den medlemsstatens nationella rätt. Denna asymmetri följer dock av att lagstiftningarna i de olika medlemsstaterna kan skilja sig åt vad gäller ersättning för de kostnader som uppkommit i samband med en order.

10.4 Effektiva rättsmedel

10.4.1 Innehållet i artikel 18

Enligt artikel 18.1 i EU-förordningen ska varje person vars uppgifter har begärts genom en europeisk utlämnandeorder – utan att det påverkar andra rättsmedel som finns att tillgå enligt nationell rätt – ha rätt till effektiva rättsmedel mot den ordern. Om den personen är en misstänkt eller en tilltalad, ska personen ha rätt till effektiva rättsmedel under det straffrättsliga förfarande där uppgifterna användes. Den rätt till effektiva rättsmedel som avses i artikeln ska inte påverka rätten att söka rättsmedel enligt dataskyddsförordningen⁵ och dataskyddsdirektivet⁶. Se även skäl 80.

⁵ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

⁶ Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för

Rätten till effektiva rättsmedel ska enligt artikel 18.2 utövas vid en domstol i den utfärdande staten i enlighet med dess nationella rätt. Detta ska innefatta en möjlighet att bestrida åtgärdens lag-
enlighet, inklusive dess nödvändighet och proportionalitet, utan att det påverkar garantierna för de grundläggande rättigheterna i den verkställande staten. För att göra det möjligt att över huvud taget kunna använda sig av rättsmedel måste den person som berörs underrättas om att uppgifter har lämnats ut.

Av artikel 13.1 i EU-förordningen följer också att den utfärdande myndigheten utan onödigt dröjsmål ska informera den person vars uppgifter begärs genom en europeisk utlämnandeorder om utlämnandet av uppgifter, dock under förutsättning att det inte föreligger en sådan situation som anges i artikel 13.2 då en sådan underrättelseskyldighet kan begränsas. Enligt den sistnämnda bestämmelsen får den utfärdande myndigheten i enlighet med den utfärdande statens nationella rätt skjuta upp eller begränsa informationen till, eller underlåta att informera, den person vars uppgifter begärs, i den mån och så länge som villkoren i artikel 13.3 i dataskyddsdirektivet är uppfyllda. Den utfärdande myndigheten ska i ett sådant fall ange skälen till uppskjutandet, begränsningen eller underlåtelserna. En kort motivering ska också läggas till i intyget om en europeisk utlämnandeorder.

Enligt artikel 13.3 i EU-förordningen ska underrättelsen enligt artikel 13.1 innehålla information om tillgängliga rättsmedel enligt artikel 18. Därutöver följer det av artikel 18.3 att vid tillämpningen av artikel 13.1 ska information ges i god tid om möjligheterna enligt nationell rätt att utnyttja rättsmedel, och det ska säkerställas att de kan utövas på ett effektivt sätt.

Samma tidsfrister eller andra villkor för att utnyttja rättsmedel ska gälla vid tillämpning av EU-förordningen som i liknande inhemska ärenden och på ett sätt som garanterar att de berörda personerna kan utöva sin rätt till rättsmedel på ett effektivt sätt (artikel 18.4).

Utän att det påverkar nationella förfaranderegler ska den utfärdande staten och varje annan medlemsstat till vilken elektroniska bevis har överförts enligt EU-förordningen säkerställa att rätten till

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.

försvar och ett rättvist förfarande vid bedömningen av de bevis som inhämtats genom den europeiska utlämnandeordern respekteras (artikel 18.5).

10.4.2 Utgångspunkter för våra överväganden

Som konstaterats i avsnitt 6.9 motsvaras en europeisk utlämnandeorder som avser inhämtande av trafikuppgifter och innehållsdata i ett inhemskt motsvarande ärende av beslut om tillstånd till hemlig övervakning och hemlig avlyssning av elektronisk kommunikation.

I fråga om inhämtning av uppgifter om abonnentuppgifter eller andra användaruppgifter motsvaras en europeisk utlämnandeorder i ett inhemskt ärende av skyldigheten enligt 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation för den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, som inte är en Noik, att på begäran lämna ut uppgifter om abonnemang till de brottsbekämpande myndigheterna (se avsnitt 6.8). I de fall lagen om elektronisk kommunikation inte tillämplig kan motsvarande uppgifter inhämtas med stöd av bestämmelserna om beslag.

I det följande behandlas de rättsmedel som enligt nationell rätt står till buds i fråga om de inhemska förfaranden som motsvarar en europeisk utlämnandeorder. Därefter följer våra överväganden om dessa rättsmedel uppfyller EU-förordningens krav på effektiva rättsmedel. Slutligen behandlas översiktligt kraven i artikel 18.5 avseende rätten till försvar och ett rättvist förfarande.

10.4.3 Effektiva rättsmedel – en översikt

I Europakonventionen, inklusive de tilläggsprotokoll till konventionen som har tillkommit genom åren, anges de grundläggande materiella fri- och rättigheter som omfattas av konventionens tillämpningsområde. Europakonventionen införlivades som lag i svensk rätt år 1995. Genom 2 kap. 19 § regeringsformen har konventionen getts en särskild ställning i svensk rätt. Bestämmelsen innebär att lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av konventionen.

I konventionen finns bestämmelser om t.ex. vars och ens rätt till liv och om förbud mot tortyr och omänsklig och förnedrande behandling eller bestraffning. Det finns också artiklar om rätt till domstolsprövning och om rättssäkerhet. Vidare innehåller konventionen, inklusive dess tilläggsprotokoll, bestämmelser om skydd för egendom och om skydd för privat- och familjeliv, hem och korrespondens. Konventionen föreskriver även en rätt till tanke- och religionsfrihet. Sammantaget skyddar konventionen rättigheter som kan aktualiseras i många olika sammanhang.

Rätten till effektivt rättsmedel är fastslagen i artikel 13 i Europakonventionen. Enligt artikel 13 ska var och en, vars fri- och rättigheter enligt konventionen har kränkts, ha tillgång till ett effektivt rättsmedel inför nationell myndighet. I artikel 13 uppställs inga specifika krav på formerna för dessa rättsmedel och omfattningen av statens förpliktelse enligt artikeln varierar beroende på karaktären av det klagomål som ska bedömas. Det är i första hand respektive konventionsstat som ska fastställa de närmare villkoren i detta hänseende, och staterna ges här en viss bedömningsmarginal.

Europadomstolen har i sin praxis emellertid uppställt vissa principer för hur man ska bedöma vad som är ett effektivt rättsmedel. Dessa principer innebär i huvudsak följande⁷:

1. Rättsmedlet ska vara tillgängligt och praktiskt möjligt för den enskilde att använda och erbjuda reella möjligheter till prövning av den aktuella frågan. Det är således inte tillräckligt att det endast formellt sett finns ett rättsmedel i det nationella rättssystemet.
2. Rättsmedlet ska vara ägnat att leda till rättelse och ge rimliga utsikter till framgång. Ett effektivt rättsmedel är alltså ett medel som ger en tillfredsställande prövning av ett klagomål oavsett om det leder till framgång för klaganden. Ett rättsmedel måste inte garantera framgång för att det ska betraktas som effektivt.
3. Det prövande organets befogenheter och de rättssäkerhetsgarantier som gäller vid förfarandet inför det prövande organet ska vidare vara tillräckliga. Något krav på att prövningen måste ske av en domstol finns inte. Administrativa rättsmedel kan alltså vara tillräckliga för att uppfylla konventionens krav.

⁷ Prop. 2017/18:7 s. 17 och Danelius m.fl., *Mänskliga rättigheter i europeisk praxis* (2023, version 6, JUNO), s. 656–658.

4. Prövningen ska leda till beslut i rimlig tid och beslutet ska fattas medan det fortfarande kan få en praktisk effekt.
5. Slutligen måste det beslut som prövningen utmynnar i vara verkställbart.

Det är inte nödvändigt att ett enda rättsmedel ensamt uppfyller kravet på ett effektivt rättsmedel utan flera rättsmedel i den nationella lagstiftningen kan tillsammans uppfylla kravet.⁸

En motsvarande bestämmelse om rätt till effektiva rättsmedel finns i artikel 47 i EU:s rättighetsstadga. Enligt bestämmelserna i den artikeln har var och en vars unionsrättsligt garanterade rättigheter kränkts rätt till ett effektivt rättsmedel inför en domstol. Rätten till domstolsprövning gäller alltså i unionsrätten i fråga om varje unionsrättsligt garanterad rättighet.

En given utgångspunkt är att det i Sverige ska finnas ett regelverk och en tillämpning av det som lever upp till kraven i Europakonventionen och EU:s rättighetsstadga. T.ex. finns det i förvaltningslagen (2017:900), rättegångsbalken och annan lagstiftning ett antal regler som är avsedda att tillförsäkra en effektiv och rättssäker handläggning av mål och ärenden hos förvaltningsmyndigheter och i domstol.

Det kanske tydligaste exemplet på ett effektivt rättsmedel i svensk rätt är möjligheten att få ett avgörande överprövat eller omprövat genom överklagande. Har vissa processuella rättigheter åsidosatts finns också möjligheten att få ett avgörande ändrat eller upphävt på grund av rättegångsfel, se t.ex. 51 kap. 26 och 28 §§, 58 kap. 2 § och 59 kap. 1 § rättegångsbalken. Vid fel eller försumelse från det allmänna sidan finns vidare i svensk rätt möjlighet till skadestånd, som alltså utgör ett kompensatoriskt rättsmedel (om skadestånd, se nedan). Ett ytterligare exempel är Justitiekanslerns möjlighet att inom ramen för den frivilliga skaderegleringen reglera vissa skadeståndsanspråk som riktas mot staten, bl.a. sådana som grundar sig på att en statlig myndighet har fattat ett felaktigt beslut.

I sammanhanget bör EU-domstolens avgörande i mål C-852-19, Gavanozov II nämnas. I fallet avsåg en domstol i Bulgarien att utfärda en europeisk utredningsorder i ett nationellt förfarande för

⁸ Se t.ex. prop. 2006/07:133 s. 24 och SOU 2010:87 s. 157.

dels husrannsakan och beslag, dels vittnesförhör via videokonferens. I Bulgariens nationella rätt saknades möjligheter att få dessa beslut överprövade. Bulgarien hade också tidigare fällts i Europadomstolen för brott mot artikel 13 i Europakonventionen på grund av avsaknaden av rättsmedel mot domstolsbeslut om husrannsakan och beslag. EU-domstolen kom fram till att nationell lagstiftning som inte föreskriver något rättsmedel mot en europeisk utredningsorder för husrannsakan och beslag eller vittnesförhör via videokonferens inte är förenlig med direktivet och artikel 47 i EU:s rättighetsstadga. Vidare konstaterade EU-domstolen att avsaknaden av rättsmedel innebär att behöriga myndigheter inte kan utfärda en europeisk utredningsorder för aktuella utredningsåtgärder. När det gäller innebörden av rättsmedel ansåg EU-domstolen att prövningen ska avse dels lagenligheten och behovet av åtgärderna, dels lämplig kompensation om dessa åtgärder har beslutats eller verkställts.

Medlemsstaterna är oense om hur långtgående domen ska tolkas, men det finns dock tecken på att verkställande myndigheter i andra medlemsstater avser att vägra att verkställa en europeisk utredningsorder om sådana rättsmedel saknas.⁹

10.4.4 Effektiva rättsmedel i fråga om hemliga tvångsmedel i svensk rätt

Möjligheten att överklaga beslut om hemliga tvångsmedel

Hemlig avlyssning och hemlig övervakning av elektronisk kommunikation kräver tillstånd från rätten (27 kap. 21 § rättegångsbalken). Rättens beslut, som enligt 30 kap. 12 § rättegångsbalken genast går i verkställighet, är i likhet med andra tillståndsbeslut under förundersökningen ett beslut under rättegång. Mot ett sådant beslut ska talan föras särskilt enligt 49 kap. 5 § 6 rättegångsbalken. Enligt nämnda lagrum får domstolens beslut under rättegång överklagas i fråga om utredningsåtgärder som motsvarar åtgärder enligt 25–28 kap. rättegångsbalken. Om rätten under förundersökningsstadiet avslagit en framställning från åklagaren är beslutet att anse som slutligt och kan överklagas enligt 49 kap. 3 §

⁹ Wallentheim och Zetterstedt, Lagen om en europeisk utredningsorder (2 januari 2024, JUNO version 1B), kommentaren till 1 kap. 3 §.

första stycket rättegångsbalken. Ett avslagsbeslut kan alltså överklagas av åklagaren.

Enligt svensk rätt får den misstänkte i teorin överklaga ett beslut om användning av hemliga tvångsmedel. Den mot vilken beslutet riktar sig får emellertid av naturliga skäl inte del av beslutet och saknar därför praktisk möjlighet att överklaga det.¹⁰ Ett bifallande beslut kan dock – såvitt avser hemlig avlyssning av elektronisk kommunikation – överklagas av det offentliga ombud som ska bevaka enskildas integritetsintressen i sådant ärende (27 kap. 26 § rättegångsbalken). Det offentliga ombudet företräder dock inte den misstänkte eller någon annan särskild person som åtgärden kan komma att beröra, utan denne företräder enskildas intressen i allmänhet. Ombudet ska verka för att omständigheterna i ärendet blir så allsidigt belysta som möjligt och bevaka att domstolens beslut är förenligt med lag och att ett tillstånd att använda de aktuella tvångsmedlen utformas på ett sådant sätt att enskildas integritet inte i onödan kränks.¹¹ Det offentliga ombudet har full insyn i ärendet hos domstolen och har rätt att ta del av vad som förekommer i ärendet till dess det avslutats samt har rätt att yttra sig i ärendet och överklaga domstolens beslut. Skulle det offentliga ombudet uppmärksamma missförhållanden är det en naturlig följd av uppdraget att han eller hon påtalar det för Riksdagens ombudsmän (JO) eller Justitiekanslern.¹²

Endast i undantagsfall kan ett tvångsmedel, som redan har upphört, bli föremål för rättslig prövning. Enligt Högsta domstolens praxis kan s.k. deserta frågor inte kan vara föremål för rättslig prövning, dvs. beslut om tvångsmedel som redan har verkställts eller har hävts (se t.ex. NJA 1989 s. 502 och NJA 1977 s. 573). Det är alltså normalt inte möjligt att få ett beslut om tvångsmedel prövat när verkställigheten av beslutet väl har avslutats.

I NJA 2023 s. 143 konstaterade Högsta domstolen emellertid att det finns vissa slag av mål som typiskt sett når domstolen först i ett skede när beslutet redan har blivit desert. Detta gäller särskilt vissa slag av beslut som regelmässigt är fullt verkställda redan innan ett överklagande har kunnat prövas, exempelvis beslut om s.k. momentana tvångsmedel. För att Högsta domstolen ska ha en reell

¹⁰ Lindberg, *Straffprocessuella tvångsmedel* (2022, version 5, JUNO) s. 162.

¹¹ Prop. 2006/07:133 s. 33–34.

¹² Prop. 2005/06:177 s. 48.

möjlighet att fullgöra sin uppgift som prejudikatinstans bör det enligt domstolen i dessa fall finnas ett utrymme för domstolen att pröva ett överklagande av beslutet trots att beslutet genom den avslutade verkställigheten har förlorat sin omedelbara betydelse.

Utrymmet bör dock enligt Högsta domstolen vara begränsat och utnyttjas enbart där det finns en betydande risk för att den prejudikatintressanta frågan annars inte skulle komma under Högsta domstolens prövning. För att detta utrymme ska kunna utnyttjas bör hovrätterna enligt Högsta domstolen ha en motsvarande möjlighet att pröva beslut av dessa slag, när det är nödvändigt för att ett starkt prejudikatbehov ska kunna tillgodoses.¹³

Underrättelse i efterhand

Den misstänkte ska som huvudregel underrättas i efterhand om det tvångsmedel som denne varit utsatt för (27 kap. 31 § första stycket rättegångsbalken). Det finns dock flera undantag från underrättelse-skyldigheten. En underrättelse behöver inte lämnas till den som redan har fått del av eller tillgång till uppgifterna, t.ex. vid delgivning av misstanke enligt 23 kap. 18 § rättegångsbalken eller vid slutunderrättelse av förundersökning enligt 23 kap. 18 a § rättegångsbalken då den misstänkte och dennes försvarare har rätt att ta del av det som förekommit under förundersökningen. Någon underrättelse behöver inte heller lämnas om den med hänsyn till omständigheterna uppenbart är utan betydelse (27 kap. 31 § femte stycket rättegångsbalken). Gäller förundersökningssekretess eller annan sekretess för uppgifterna ska underrättelse skjutas upp till dess sekretess inte längre gäller (27 kap. 33 § första stycket rättegångsbalken). Har det inte på grund av sekretess kunnat lämnas någon underrättelse inom ett år och sex månader från det att tvångsmedelsanvändningen avslutades, ska frågan om underrättelse prövas slutligt. En underrättelse ska då bara lämnas om sekretess inte längre gäller och om det kan ske utan men för utredningen

¹³ När Högsta domstolen tar ställning till ett beslut av aktuellt slag, bör domstolens ställningstagande i prejudikatfrågan inte utmynna i ett fastställande eller upphävande av tingsrättens eller hovrättens beslut. I stället bör domstolen, sedan den har tagit ställning i prejudikatfrågan, skriva av målet. När en hovrätt i motsvarande situation prövar ett desert beslut bör den däremot skilja målet ifrån sig genom ett avgörande som avspeglar det ställningstagande som domstolen har gjort i sakfrågan och alltså inte skriva av målet. (NJA 2023 s. 143 p. 16).

(andra stycket nämnda paragraf). Vidare är de brottstyper som Säkerhetspolisen hanterar enligt tredje stycket undantagna från underrättelseskyldigheten.

Av 14 b § första stycket förundersökningskungörelsen (1947:948) följer att underrättelseskyldighet enligt 27 kap. 31 § rättegångsbalken ska fullgöras av den åklagare som är eller har varit förundersökningsledare. När en underrättelse har underlåtit enligt 27 kap. 33 § andra stycket rättegångsbalken, ska den åklagare som är eller har varit förundersökningsledare underrätta Säkerhets- och integritetsskydds-nämnden om detta (andra stycket samma paragraf), se vidare nedan om nämndens uppdrag.

Underrättelseskyldigheten syftar bl.a. till att den enskilde ska få möjlighet att bedöma vilket integritetsintrång som åtgärden har inneburit och att reagera mot vad han eller hon kan anse har varit en rättsstridig åtgärd. En skyldighet att lämna en sådan underrättelse kan även ha en återhållande verkan på användningen av hemliga tvångsmedel och bidra till att prövningen inför ett beslut sker på ett än mer noggrant sätt.¹⁴

Vidare innebär underrättelseskyldigheten en möjlighet för den enskilde att begära en kontroll av Säkerhets- och integritetsskydds-nämnden av om användningen av hemliga tvångsmedel har skett författningsenligt vilket följer av 3 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

En sådan begäran kan framställas av envar, oavsett medborgarskap eller hemvist. Även juridiska personer kan framställa en sådan begäran av om hemligt tvångsmedel har riktats mot en teleadress eller plats som den juridiska personen innehar. Nämnden är i dessa fall alltid skyldig att företa den kontroll som behövs och ska alltid underrätta den enskilde om att kontrollen har utförts. Vilka uppgifter som i övrigt kan lämnas beror på vilken sekretess som gör sig gällande i det enskilda fallet.¹⁵

Om Säkerhets- och integritetsskydds-nämnden vid en sådan kontroll uppmärksammar felaktigheter som kan medföra skadeståndsansvar för staten gentemot en fysisk eller juridisk person ska nämnden enligt 20 § andra stycket förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskydds-nämnden anmäla det till Justitiekanslern.

¹⁴ Prop. 2006/07:133 s. 30.

¹⁵ Prop. 2006/07:133 s. 81.

Skadestånd

För den enskilde kan en underrättelseskyldighet också innebära en möjlighet att själv reagera genom att t.ex. kräva ersättning för skada på grund av fel eller försummelse vid myndighetsutövning. I 3 kap. 1 § skadeståndslagen (1972:207) föreskrivs att den som har arbetstagare i sin tjänst ska ersätta personskada, sakskada eller sådan skada som föranleder särskild anhörigersättning enligt 2 kap. 3 a § som arbetstagaren vållar genom fel eller försummelse i tjänsten samt ren förmögenhetsskada som arbetstagaren i tjänsten vållar genom brott. I 3 kap. 2 § skadeståndslagen finns bestämmelser om det allmännas ansvar vid felaktig myndighetsutövning. Staten eller en kommun är skyldig att ersätta en enskild för personskada, sakskada, ren förmögenhetsskada eller sådan skada som föranleder särskild anhörigersättning enligt 2 kap. 3 a § som den enskilde har vållats genom begångna fel eller försummelser vid myndighetsutövning för vars fullgörande staten eller kommunen svarar. Det allmänna är även skyldigt att ersätta en enskild för allvarlig kränkning genom brott som innefattar angrepp mot dennes person, frihet, frid eller ära, om brottet innefattar fel eller försummelse vid myndighetsutövning (jfr 2 kap. 3 § skadeståndslagen).

Av 3 kap. 4 § skadeståndslagen följer vidare att staten eller en kommun ska ersätta personskada, sakskada, ren förmögenhetsskada och skada på grund av att någon kränks på sätt som anges i 2 kap. 3 §, om skadan uppkommit till följd av att den skadelidandes rättigheter enligt Europakonventionen överträtts från statens eller kommunens sida, och annan ideell skada som uppkommit till följd av en sådan rättighetsöverträdelse.

Den enskilde kan således ha rätt till ersättning för den kränkning som han eller hon drabbas av till följd av myndighetsutövning som t.ex. innefattar olovlig avlyssning. Skadeståndslagens regler innebär alltså ett skadeståndsrättsligt skydd i fråga om användning av hemliga tvångsmedel som varit obefogad. Det kan dock i sammanhanget konstateras att hemliga tvångsmedel som beslutas och verkställs i laga ordning inte torde kunna grunda en rätt till skadestånd. Det gäller även om användningen av tvångsmedlet inte på något mer avgörande sätt har kunnat föra brottsutredningen framåt

eller om det efter tvångsmedelsanvändningen skulle stå klart att den misstänkte är oskyldig.¹⁶

Tillsyn över användningen av hemliga tvångsmedel

Säkerhets- och integritetsskyddsnämnden har till uppgift att utöva tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel, vilket följer av ovan nämnda lagen om tillsyn över viss brottsbekämpande verksamhet. Tillsynen utförs genom inspektioner och andra undersökningar. Om nämnden i sin verksamhet uppmärksammar förhållanden som kan utgöra brott, ska nämnden anmäla det till Åklagarmyndigheten eller någon annan behörig myndighet (20 § första stycket förordning med instruktion för Säkerhets- och integritetsskyddsnämnden).

Nämnden är, som behandlats ovan, även skyldig att på begäran av en enskild kontrollera om han eller hon har varit utsatt för hemliga tvångsmedel och om denna användning har varit författningsenlig.

Förutom Säkerhets- och integritetsskyddsnämnden utövar både JO och Justitiekanslern tillsyn över de brottsbekämpande myndigheternas verksamhet och kan inom ramen för sin respektive tillsyn uttala sig i frågor om användningen av hemliga tvångsmedel.

Den svenska regleringen om hemliga tvångsmedel i förhållande till Europakonventionen

Europadomstolen har framhållit att det vid hemlig telefonavlyssning är svårt – eller ibland omöjligt – att använda normala rättsmedel. I rättsfallet *Klass m.fl. mot Tyskland* (1978-09-06, appl. 5029/71) fann domstolen att själva avsaknaden av en förhandsunderrättelse om avlyssningen i sig inte kan anses strida mot artikel 13, utan kravet på effektivt rättsmedel i konventionen måste i sammanhanget förstås så att det ska finnas ett så effektivt rättsmedel som möjligt med hänsyn till de särskilda omständigheterna. Enligt tysk rätt fanns det möjlighet att klaga över misstänkt telefonavlyssning till en särskild kommission och till Författningsdomstolen samt en skyldighet att i efterhand, när det kunde ske utan risk för skada,

¹⁶ Prop. 2006/07:133 s. 32–33.

underrätta den som avlyssnats om att avlyssning skett. När sådan underrättelse lämnats, blev ytterligare rättsmedel tillgängliga. Europadomstolen fann sammantaget att de tillgängliga rättsmedlen uppfyllde kraven i artikel 13.

Frågan huruvida rätten enligt artikel 13 i Europakonventionen till ett effektivt rättsmedel är tillgodosedd i fråga om hemliga tvångsmedel har behandlats i flera förarbeten till de aktuella bestämmelserna i rättegångsbalken. Ordningen med domstolsprövning, offentlig ombud, underrättelseskyldigheten till enskild, den tillsyn Säkerhets- och integritetsskyddsnämnden utövar över användningen av hemliga tvångsmedel samt den extraordinära tillsyn som utförs av JO och Justitiekanslern, den parlamentariska efterhandskontroll som utövas av riksdagen har sammantaget bedömts uppfylla det krav på effektiva rättsmedel som uppställs i artikel 13 för hemliga tvångsmedel.¹⁷

10.4.5 Inhämtning av uppgifter om abonnemang och effektiva rättsmedel

Skyldigheten enligt 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation för den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, som inte är en Noik, att på begäran lämna ut uppgifter om abonnemang till de brottsbekämpande myndigheterna är inte föremål för bestämmelserna om överklagande i lagen om elektronisk kommunikation. För det fall en tillhandahållare inte följer en begäran enligt nämnda lagrum kan Post- och telestyrelsen såsom tillsynsmyndighet, bl.a. besluta om sanktionsavgift. Till skillnad från ordningen beträffande hemliga tvångsmedel saknas regler om domstolsprövning, offentligt ombud, särskild tillsyn eller underrättelseskyldighet till enskild. Är den enskilde en misstänkt och har denne delgetts misstanke har den enskilde dock rätt att ta del av vad av som förekommit under förundersökningen enligt 23 kap. 18 § andra stycket rättegångsbalken, om det kan ske utan men för utredningen. När förundersökning är slutförd har den misstänkte och försvararen rätt att ta del av det som har förekommit vid förundersökningen (23 kap. 18 a § rättegångsbalken). Sådana uppgifter som den miss-

¹⁷ Se t.ex. prop. 2019/20:64 s. 97 beträffande det hemliga tvångsmedlet hemlig dataavläsning.

tänkte har rätt att ta del av enligt de aktuella bestämmelserna kan inkludera den omständighet att uppgifter om abonnemang har inhämtats enligt 9 kap. 33 § lagen om elektronisk kommunikation. Rätten till insyn enligt nämnda lagrum kan dock begränsas om sekretess gäller för uppgifterna. Har den enskilde fått kännedom om att uppgifter om dennes abonnemang inhämtats kan denne kräva ersättning för skada på grund av fel eller försummelse vid myndighetsutövning på sätt som utvecklats ovan vid obefogad inhämtning av de aktuella uppgifterna. En form av rättsmedel är ju, som angetts ovan, möjligheten att ge monetär kompensation till någon som har utsatts för en överträdelse av sina rättigheter enligt konventionen. För att den enskilde ska kunna tillgodogöra sig denna form av kompensatoriskt rättsmedel förutsätts dock att denne har fått kännedom om att uppgifterna har begärts ut.

I samband med att skyldigheten för operatörerna att lämna ut uppgifter om abonnemang till de brottsbekämpande myndigheterna utvidgades till att även avse brott som endast bedöms för- anleda böter prövades frågan om det skulle införas en underrättelse- skyldighet gentemot den enskilde i fråga om inhämtning av upp- gifter på abonnemang. Regeringen fann att inhämtning av sådana uppgifter inte innebär ett så betydande integritetsintrång att de bör medföra något krav på underrättelseskyldighet och gjorde således bedömningen att det inte fanns skäl att införa en underrättelse- skyldighet avseende inhämtande av abonnemangsuppgifter.¹⁸ Reger- ingen uttalade också i samma proposition att det finns ett starkt intresse av att införa en möjlighet för de brottsbekämpande myn- digheterna att få tillgång till abonnemangsuppgifter, vilket inklu- derar uppgift om IP-adresser, bl.a. för att lagföra brott som begås via internet såsom nätmobbing och trakasserier. Regeringen kon- staterade att detta innebär att utlämnandet utgör ett visst integritets- intrång, eftersom abonnentens identitet röjs. Vid denna intresse- avvägning bör enligt regeringen beaktas att privatpersoner oftast använder s.k. dynamiska IP-adresser, dvs. adresser som byts slump- vis och oregelbundet, vilket enligt regeringen innebär att en uppgift om att en viss person hade en viss IP-adress vid ett visst tillfälle i regel inte säger någonting om vem som hade den adressen vid ett annat tillfälle.¹⁹

¹⁸ Prop. 2011/12:55 s. 108.

¹⁹ Prop. 2011/12:55 s. 102. Prop. 2011/12:55 s. 108.

I de fall motsvarande uppgifter inhämtas med stöd av ett beslut om beslag kan den som drabbas av beslaget begära rättens prövning enligt 27 kap. 6 § rättegångsbalken.

10.4.6 Effektiva rättsmedel i fråga om en europeisk utlämnandeorder

Bedömning: Nationell rätt får anses uppfylla EU-förordningens krav på effektiva rättsmedel i fråga om en europeisk utlämnandeorder som avser inhämtning av abonnentuppgifter eller andra användaruppgifter. Vårt tidigare redovisade förslag i avsnitt 7.5.3 innebär att nationell rätt uppfyller kraven på effektiva rättsmedel även rörande en europeisk utlämnandeorder som avser inhämtning av trafikuppgift eller innehållsdata.

Skälen för förslaget och bedömningen

Effektiva rättsmedel vid en utlämnandeorder avseende inhämtning av abonnentuppgifter eller andra användaruppgifter

De svenska domstolarna tillämpar principen om fri bevisprövning. En central bestämmelse finns i 35 kap. 1 § rättegångsbalken. Enligt denna ska rätten, efter en samvetsgrann prövning av allt som förekommit, avgöra vad som är bevisat i målet. I det ligger att det råder fri bevisföring och fri bevisvärdering. Enligt svensk rätt är därför, som huvudregel, alla bevismedel tillåtna. Det förhållandet att ett bevis t.ex. åtkommit i strid mot en viss rättsregel utesluter i princip inte att det får läggas fram i en rättegång.

I vilken mån åtkomsten eller bevisets ursprung ska tillmätas någon betydelse, är ett förhållande som domstolen har att bedöma inom ramen för sin fria bevisprövning och gäller följaktligen inte frågan om beviset ska tillåtas eller ej (se t.ex. NJA 2011 s.638)

Skulle domstolen i sin fria bevisprövning finna att det finns anledning att ifrågasätta hur bevisningen inhämtats, har rätten skäl att beakta detta vid utvärderingen av beviset. Beroende på omständigheterna kan rätten komma fram till att bevisvärdet är lågt eller obefintligt (jämför t.ex. NJA 2003 s. 323). Den kränkning som det innebär att beviset tillkommit på ett felaktigt sätt kan också kom-

penseras genom t.ex. strafflindring, jämför NJA 2011 s. 638 och NJA 2012 s. 1038.

Som behandlats ovan har den enskilde också möjlighet att begära skadestånd vid felaktig myndighetsutövning eller om skadan uppkommit till följd av att den skadelidandes rättigheter enligt Europakonventionen har överträtts.

Det sagda innebär – även om det beträffande inhämtning av abonnemangsuppgifter enligt 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation saknas en sådan underrättelseskyldighet som gäller i fråga om hemliga tvångsmedel gentemot den enskilde – att nationell rätt får anses uppfylla krav på effektiva rättsmedel i fråga om en utlämnandeorder som avser inhämtning av abonnentuppgifter eller andra användaruppgifter.

Effektiva rättsmedel i fråga om en europeisk utlämnandeorder avseende inhämtning av trafikuppgifter eller innehållsdata

Som har redogjorts för i avsnitt 10.4.4 har de tillgängliga rättsmedlen för den enskilde i fråga om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation bedömts uppfylla kraven i artikel 13 i Europakonventionen på effektiva rättsmedel.

Det finns inte skäl att frånga denna bedömning, utan de rättsmedel som har behandlats ovan får alltså anses uppfylla EU-förordningens krav i artikel 18 på effektiva rättsmedel även i fråga om utfärdande av en europeisk utlämnandeorder avseende inhämtning av trafikuppgifter respektive innehållsdata, vilket i ett inhemskt ärende motsvaras av användningen av hemlig övervakning respektive hemlig avlyssning av elektronisk kommunikation. Dessa rättsmedel – dvs. ordningen med domstolsprövning, offentliga ombud, underrättelseskyldigheten till enskild samt den tillsyn som utövas – bör alltså vara tillämpliga i fråga om utfärdande av en sådan order. Därutöver gäller det som anförts ovan beträffande effektiva rättsmedel i fråga om en europeisk utlämnandeorder för inhämtning av abonnentuppgifter och andra användaruppgifter även i fråga om en europeisk utlämnandeorder för inhämtning av trafikuppgifter respektive innehållsdata.

Vårt förslag i avsnitt 7.5.3 innebär, som utvecklats i det avsnittet, att den ordning som gäller i rättegångsbalken för tvångsmedlen hemlig övervakning respektive hemlig avlyssning av elektronisk

kommunikation ska även tillämpas vid utfärdande av en europeisk utlämnandeorder för inhämtning av trafikuppgifter eller innehållsdata (jfr artikel 18.4). Domstolsprövning av en order följer dock direkt av artikel 4 i EU-förordningen och ska således inte regleras i nationell lag (se även avsnitt 7.5.3).

Som följer av förslaget i avsnitt 7.5.3 ska för domstolens handläggning vid ett godkännande av en europeisk utlämnandeorder för inhämtning av trafikuppgifter eller innehållsdata enligt artikel 4.2 b i tillämpliga delar gälla vad som är föreskrivet i rättegångsbalken. Detta innebär bl.a. att bestämmelserna om offentligt ombud i 27 kap. 26–30 §§ rättegångsbalken ska tillämpas i fråga om en order som i ett inhemskt ärende motsvaras av ett tillstånd till hemlig avlyssning av elektronisk kommunikation.

Den föreslagna regleringen i avsnitt 7.5.3 innebär även att domstolens beslut kan överklagas särskilt enligt 49 kap. 5 § rättegångsbalken. För överklagande av en europeisk utlämnandeorder för inhämtning av trafikuppgifter eller innehållsdata gäller således vad som är föreskrivet i rättegångsbalken för beslut angående den åtgärd som avses i ordern, dvs. de ovan behandlade bestämmelserna om överklagande i fråga om tillstånd till hemliga tvångsmedel ska äga motsvarande tillämpning för en sådan utlämnandeorder.

Förslaget i avsnitt 7.5.3 innebär vidare att bestämmelserna om underrättelse till enskild i 27 kap. 31–33 §§ ska äga motsvarande tillämpning i fråga om en europeisk utlämnandeorder av aktuellt slag.

I sammanhanget kan det noteras att det i avsnitt 7.5.3 behandlas vilka övriga förfaranderegler i 27 kap. rättegångsbalken som ska äga motsvarande tillämpning vid utfärdande av en europeisk utlämnandeorder för inhämtning av trafikuppgifter respektive innehållsdata.

Eftersom en europeisk utlämnandeorder av aktuellt slag motsvaras av ett tillstånd till hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation gäller den ovan behandlade nationella regleringen om tillsyn av användningen av dessa tvångsmedel utan att det särskilt anges i den nya lagen.

Det sagda innebär sammanfattningsvis att EU-förordningens krav på effektiva rättsmedel i fråga om en europeisk utlämnandeorder för inhämtning av trafikuppgifter respektive innehållsdata är uppfyllt.

10.4.7 Kraven på rätten till försvar och rättvist förfarande

Bedömning: Rätten till försvar och ett rättvist förfarande i fråga om prövning av de bevis som inhämtats genom EU-förordningen följer av befintlig lagstiftning och det finns inte behov av ytterligare reglering i detta avseende.

Skälen för bedömningen: Enligt artikel 18.5 ska medlemsstaterna säkerställa att rätten till försvar och ett rättvist förfarande vid bedömningen av de bevis som inhämtats med stöd av EU-förordningen respekteras. I det följande redogörs därför översiktligt för de rättigheter som tillkommer den som är misstänkt eller tilltalad för brott.

Var och en som är misstänkt eller tilltalad för brott garanteras flera processuella rättigheter. En rättighet som är av fundamental betydelse är rätten till en rättvis rättegång. Rätten till en rättvis rättegång garanteras inte minst genom artikel 6 i Europakonventionen. Artikel 6 i Europakonventionen ställer bl.a. krav på att var och en, när det gäller prövningen av civila rättigheter och skyldigheter eller av en anklagelse mot någon för brott, ska vara berättigad till en rättvis och offentlig förhandling inom skälig tid och inför en oavhängig och opartisk domstol som upprättats enligt lag. Rätten att ha en försvarare utgör även en grundläggande del av rätten till en rättvis rättegång enligt artikel 6 i Europakonventionen. Som nämnts ovan gäller Europakonventionen som lag i Sverige och lag eller föreskrift får inte meddelas i strid med Sveriges åtaganden på grund av konventionen (2 kap. 19 § regeringsformen).

I regeringsformen finns ett antal bestämmelser om brottmålsrättegången. Flera av dem har till huvudsakligt ändamål att säkerställa att domstolsprocessen är rättssäker för den enskilde. I 2 kap. 11 § andra stycket anges att en rättegång ska genomföras rättvist och inom skälig tid. Bestämmelsen har mycket nära anknytning till motsvarande reglering i Europakonventionen. Bestämmelsen kompletterar andra bestämmelser i regeringsformen som har till huvudsakligt ändamål att säkerställa en rättssäker domstolsprocess, t.ex. kravet på förhandlingsoffentlighet och kravet på saklighet i 1 kap. 9 §. I kravet på en rättvis rättegång ligger en rad processuella rättigheter som i materiellt hänseende redan är fastslagna i den svenska processordningen. Rättssäkerhetskraven innefattar bl.a. en grund-

läggande rätt för en part att bli hörd inför domstolen och att domstolen är opartisk och oavhängig. Av grundläggande betydelse är vidare att förfarandet är kontradiktoriskt och att parterna är likställda i processen. Kravet att en rättegång ska genomföras rättvist och inom skäligen tid kan inte inskränkas. Bestämmelsen gäller även för andra än svenska medborgare här i riket.

I sammanhanget kan också nämnas de bestämmelser om rätten till offentlig försvarare som i första hand finns i 21 kap. rättegångsbalken samt rätten att överklaga en tingsrätts dom, som regleras i 49 kap. rättegångsbalken.

De bestämmelser som redovisats ovan ger den misstänkte eller tilltalade rätt till försvar och ett rättvist förfarande i fråga om prövning av de bevis som inhämtats genom EU-förordningen och det finns således inte behov av ytterligare reglering i detta avseende.

10.5 Metoder för kommunikation

Bedömning: Bestämmelser behövs vad avser tillåtna metoder för kommunikation enligt artiklarna 19.5 och 24 i EU-förordningen. I förhållande till artikel 24 bör de dock upphävas när de artiklar i EU-förordningen som gäller det decentraliserade it-systemet ska börja tillämpas. Detta kan regleras i förordning.

Skälen för bedömningen

Det decentraliserade it-systemet

All skriftlig kommunikation mellan behöriga myndigheter och utsedda verksamhetsställen eller rättsliga ombud enligt EU-förordningen ska enligt artikel 19.4 ske genom ett säkert och tillförlitligt decentraliserat it-system, det s.k. decentraliserade it-systemet.

Varje medlemsstat och tjänsteleverantör ska säkerställa att de utsedda verksamhetsställena eller rättsliga ombuden i den medlemsstaten ges åtkomst till det decentraliserade it-systemet via sina respektive nationella it-system.

Skriftlig kommunikation mellan behöriga myndigheter, vilket innefattar utbyte av formulär och begärda uppgifter inom ramen för verkställighetsförfarandet enligt artikel 16, samt skriftlig kom-

munikation med behöriga unionsbyråer eller unionsorgan, ska också ske via det decentraliserade it-systemet.

Om kommunikation via det decentraliserade it-systemet inte är möjlig på grund av vissa angivna skäl ska överföringen ske på lämpligaste alternativa sätt, med beaktande av behovet av att säkerställa ett informationsutbyte som är snabbt, säkert och tillförlitligt och som gör det möjligt för mottagaren att fastställa äktheten (artikel 19.5).

Innan skyldigheten att kommunicera genom det decentraliserade it-systemet som avses i artikel 19 träder i kraft ska enligt artikel 24 den skriftliga kommunikationen mellan behöriga myndigheter och utsedda verksamhetsställen eller rättsliga ombud under en övergångsperiod ske på lämpligaste alternativa sätt, med beaktande av behovet av att säkerställa ett snabbt, säkert och tillförlitligt informationsutbyte. Om tjänsteleverantörer, medlemsstater eller unionsbyråer eller unionsorgan har inrättat särskilda plattformar eller andra säkra kanaler för hantering av framställningar om uppgifter från brottsbekämpande myndigheter och rättsliga myndigheter, får utfärdande myndigheter också välja att översända ett intyg om en europeisk utlämnandeorder eller ett intyg om en europeisk bevarandeorder via de kanalerna under övergångsperioden.

Kommissionen ska enligt artikel 25 anta de genomförandeakter som är nödvändiga för inrättandet och användningen av det decentraliserade it-systemet och då bl.a. fastställa tekniska specifikationer och mål för informationssäkerhet. Genomförandeakterna ska antas senast den 18 augusti 2025.

Sättet för kommunikation då det decentraliserade it-systemet inte kan användas

I dag används olika sätt att kommunicera i det internationella straffrättsliga samarbetet. Handlingar kan t.ex. skickas per post eller via Eurojust (Europeiska unionens byrå för straffrättsligt samarbete) som kan bistå medlemsstaterna i brottsutredningar vad gäller gränsöverskridande samarbete. Även Polismyndighetens SPOC-verksamhet kan användas för sådan kommunikation (se avsnitt 7.5.1 för en närmare beskrivning av denna verksamhet).

I de fall de ovan beskrivna undantagen i EU-förordningen är tillämpliga och det decentraliserade it-systemet inte kan användas

är det av vikt att handlingar, som ofta kan innehålla känslig information, vilket kan inkludera personuppgifter, kan överföras mellan parterna på ett säkert sätt. Detta kan exempelvis ske genom de system för kommunikation som beskrivs ovan eller på något annat sätt, t.ex. genom krypteringsnycklar eller liknande. Med hänsyn till handlingarnas känsliga innehåll bör det vara upp till parterna att avgöra vilken metod för kommunikation som ska användas i det enskilda ärendet. En bestämmelse med detta innehåll bör föras in i förordning, som meddelas med stöd av 8 kap. 7 § regeringsformen.

Den kompletterande regleringen om metoden för översändande av handlingar kommer att behöva upphävas när de artiklar i EU-förordningen som är hänförliga till det decentraliserade it-systemet ska börja tillämpas (dock inte i förhållande till artikel 19.5).²⁰

10.6 Insamling av statistik

Bedömning: Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten och övriga myndigheter som har till uppgift att ingripa mot brott eller brottslig verksamhet bör omfattas av den rapporteringsskyldighet som följer av artikel 28.2 i EU-förordningen. Detta kan regleras i förordning.

Skälen för bedömningen: Av artikel 28.2 i EU-förordningen följer att medlemsstaterna regelbundet ska samla in och bevara uttömmande statistik från de relevanta myndigheterna. Den statistik som samlas in ska varje år översändas till kommissionen och omfatta:

- a) Antalet intyg om en europeisk utlämnandeorder- eller bevarandeorder som utfärdats, indelat efter typen av uppgifter som begärts, mottagarna och situationen (nödsituation eller inte).
- b) Antalet intyg om en europeisk utlämnandeorder som utfärdats enligt det undantagsförfarande som gäller i en nödsituation.
- c) Antalet fullföljda respektive icke fullföljda intyg om en europeisk utlämnande- eller bevarandeorder, indelat efter typen av

²⁰ Se prop. 2021/22:142 s. 20–21 ang. EU:s bevisupptagningsförordning, enligt vilken också kommunikation ska ske enligt det decentraliserade it-systemet efter en övergångsperiod och 3 § förordningen (2022:625) med kompletterande bestämmelser till EU:s bevisupptagningsförordning.

uppgifter som begärts, mottagarna och situationen (nödsituation eller inte).

- d) Antalet anmälningar till verkställande myndigheter enligt artikel 8, och antalet intyg om en europeisk utlämnandeorder som vägrats, indelat efter typen av uppgifter som begärts, mottagarna och situationen (nödsituation eller inte) samt de åberopade vägransgrunderna.
- e) För fullföljda intyg om en europeisk utlämnandeorder, den genomsnittliga perioden mellan den tidpunkt då intyget utfärdades och den tidpunkt då de begärda uppgifterna erhöles, indelat efter typen av uppgifter som begärts, mottagarna och situationen (nödsituation eller inte).
- f) För fullföljda intyg om en europeisk bevarandeorder, den genomsnittliga perioden mellan den tidpunkt då intyget om en europeisk bevarandeorder utfärdades och den tidpunkt då den efterföljande framställan om utlämnande utfärdades, indelat efter typen av uppgifter som begärts och mottagarna.
- g) Antalet europeiska utlämnande- eller bevarandeorder som översänts till och mottagits av en verkställande stat för verkställighet, indelat efter typen av uppgifter som begärts, mottagarna och situationen (nödsituation eller inte) samt antalet sådana order som verkställdes.
- h) Antalet rättsmedel som använts mot europeiska utlämnandeorder i den utfärdande staten och i den verkställande staten, indelat efter typen av uppgifter som begärts.
- i) Antalet fall där efterhandsgodkännande, i enlighet med artikel 4.5, inte beviljades.
- j) En översikt över de kostnader som tjänsteleverantörer har begärt ersättning för fullföljande av intyg om en europeisk utlämnande- eller bevarandeorder samt de kostnader som de utfärdande myndigheterna gett ersättning för.

Artikel 28.2 ger således uttryck för ett långtgående åtagande för medlemsstaterna att förse kommissionen med statistiska uppgifter. Dessa uppgifter ska ligga till grund för den rapport som kommissionen årligen ska offentliggöra enligt artikel 28.5. Rapporterna

syftar till att övervaka EU-förordningens utfall, resultat och effekter (skäl 93).

Statistiska uppgifter av den karaktär som beskrivs i artikel 28.2 kommer främst att finnas hos Åklagarmyndigheten och Ekobrottsmyndigheten i egenskap av föreslagna behöriga myndigheter. Polismyndigheten samt övriga myndigheter som har till uppgift att ingripa mot brott eller brottslig verksamhet föreslås också vara behöriga myndigheter i vissa avseenden, och kan således inneha uppgifter av aktuellt slag. Vissa av uppgifterna skulle även kunna finnas hos domstolarna, då främst i fråga om de rättsmedel som har används. Sådana uppgifter torde dock även finnas tillgängliga hos de behöriga myndigheterna

Den föreslagna centralmyndigheten, Post- och telestyrelsen, torde dock inte komma att inneha uppgifter som omfattas av artikel 28.2, eftersom de uppgifter som krävs enligt artikeln inte berör utsedda verksamhetsställen och rättsliga ombud eller den tillsyn som ska bedrivas över dessa aktörer enligt EU-direktivet.

För att genomföra direktivets krav på rapportering av statistik bör de myndigheter som har tillgång till de uppgifter som EU-förordningen kräver, dvs. Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten och övriga myndigheter som har till uppgift att ingripa mot brott eller brottslig verksamhet ges i uppdrag att till kommissionen lämna de uppgifter som omfattas av artikel 28.2.

Artikel 28.2 kan i och för sig läsas som att medlemsstaterna ska samla in från myndigheterna och sedan skicka till kommissionen. För kommissionen är det naturligtvis också praktiskt att uppgifterna lämnas samlat. Vid genomförandet av andra rättsakter som ålägger medlemsstaterna att redovisa statistik till kommissionen, t.ex. EU-direktivet 2014/42 om frysning och förverkande av hjälpmedel vid och vinning av brott i EU, har det dock ansetts lämpligt att myndigheterna skickar direkt till kommissionen. I sammanhanget kan det framhållas att från och med den 18 augusti 2026 får den statistik som avses i artikel 28.2 samlas in automatiskt av nationella portaler när det gäller de utbyten av uppgifter som skett via det decentraliserade it-systemet (artikel 28.3). Informationen kan således sändas genom det decentraliserade it-systemet.

En bestämmelse om rapporteringsskyldighet för de aktuella myndigheterna till kommissionen bör lämpligen införas i förordning. Något särskilt bemyndigande för regeringen krävs inte, utan

sådana bestämmelser kan meddelas med stöd av 8 kap. 7 § regeringsformen. Av artikel 28.2 följer att redovisningen ska ske årligen och vilka uppgifter som ska lämnas, varför detta inte ska regleras i förordning.

10.7 Förhållandet till dataskyddsregleringen

10.7.1 Utgångspunkter i EU-förordningen

En europeisk utlämnandeorder ska enligt artikel 5.6 som huvudregel riktas till den tjänsteleverantör som agerar som personuppgiftsansvarig i enlighet med dataskyddsförordningen. Undantagsvis kan ordern riktas direkt till den tjänsteleverantör som lagrar eller på annat sätt behandlar uppgifterna på den personuppgiftsansvariges vägnar, om den personuppgiftsansvarige inte kan identifieras trots att rimliga ansträngningar gjorts från den utfärdande myndighetens sida, eller det kan vara till skada för utredningen att rikta sig till den personuppgiftsansvarige. Enligt skäl 14 till EU-förordningen bör medlemsstaterna vid genomförandet av förordningen säkerställa att personuppgifter skyddas och behandlas i enlighet med dataskyddsförordningen, dataskyddsdirektivets samt direktiv 2002/58²¹, även vid ytterligare användning, överföring och vidarebefordran av de uppgifter som inhämtats.

Av skäl 15 följer att personuppgifter som inhämtas enligt förordningen bör behandlas endast om det är nödvändigt och på ett sätt som är proportionellt i förhållande till ändamålen förebyggande, utredning, upptäckt och lagföring av brott eller verkställighet av straffrättsliga påföljder och utövande av rätten till försvar. Medlemsstaterna bör enligt skälet i synnerhet säkerställa att lämpliga strategier och åtgärder för dataskydd tillämpas på översändandet av personuppgifter från behöriga myndigheter till tjänsteleverantörer vid tillämpningen av EU-förordningen, inbegripet åtgärder för att säkerställa uppgifternas säkerhet. Tjänsteleverantörerna bör enligt samma skäl säkerställa att samma skyddsåtgärder tillämpas vid översändandet av personuppgifter till behöriga myndigheter. Endast behöriga personer bör enligt skälet ha tillgång till information som

²¹ 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).

innehåller personuppgifter, vilket kan uppnås genom förfaranden för autentisering.

Av skäl 34 till EU-förordningen följer att samtliga uppgiftskategorier innehåller personuppgifter och omfattas därmed av skyddsåtgärder enligt unionens dataskyddsregelverk. Graden av inverkan på de grundläggande rättigheterna varierar dock enligt skälet mellan kategorierna, i synnerhet mellan abonnentuppgifter och andra användaruppgifter, å ena sidan, och trafikuppgifter, med undantag för andra användaruppgifter, och innehållsdata, å andra sidan. Abonnentuppgifter och andra användaruppgifter (artikel 3.9 och 3.10), kan vara användbara för att vid en utredning få de första ledtrådarna om en misstänkt persons identitet, men trafikuppgifter och innehållsdata är i många fall mer relevanta som bevismaterial. Det är därför enligt samma skäl viktigt att samtliga uppgiftskategorier omfattas av förordningen, med införande av lämpliga skyddsåtgärder och villkor för inhämtande av sådana uppgifter.

När Åklagarmyndigheten i sin roll som utfärdande eller verkställande myndighet handlägger ärenden om verkställighet av en europeisk utlämnande- eller bevarandeorder behöver den behandla personuppgifter. Dessa kan finnas i det innehåll som är föremål för utlämnande eller bevarande, men även i exempelvis en sådan order som omfattas av EU-förordningens bestämmelser. Detsamma gäller för Polismyndigheten och övriga myndigheter i de fall de är behöriga att utfärda en sådan order som omfattas av EU-förordningen. Åklagarmyndigheten respektive centralmyndigheten kan också behöva behandla personuppgifter som avser berörda tjänstleverantörer i ärenden om påförande av sanktionsavgift samt, beträffande centralmyndigheten, i dess övriga tillsynsverksamhet.

10.7.2 Gällande rätt

Den generella regleringen för behandling av fysiska personers personuppgifter inom EU utgörs av dataskyddsförordningen. Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) innehåller generella nationella kompletteringar till dataskyddsförordningen.

Dataskyddsförordningen är inte tillämplig på den behandling av personuppgifter som behöriga myndigheter utför i syfte att före-

bygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder (artikel 2.2 d). För personuppgiftsbehandling inom detta område gäller i stället dataskyddsdirektivet. Direktivet har genomförts i svensk rätt genom brottsdatalagen (2018:1177).

Med personuppgifter avses varje upplysning som avser en identifierad eller identifierbar fysisk person. Avgörande är att uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en levande person. Exempel på personuppgifter är namn, adress, personnummer, telefonnummer och e-postadresser. Med personuppgiftsbehandling avses en åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter oavsett om det görs automatiserat eller inte, t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande, spridning eller tillhandahållande på annat sätt, justering, sammanföring, begränsning, radering eller förstöring (1 kap. 6 § brottsdatalagen).

En grundläggande princip för all personuppgiftsbehandling är att personuppgifter får samlas in endast för särskilda, uttryckligt angivna och berättigade ändamål. Principen kommer i dag till uttryck i både dataskyddsförordningen och brottsdatalagen. Både förordningen och lagen utgår också från att varje behandling av personuppgifter måste vila på en rättslig grund för att vara laglig.

Dataskyddsförordningen och brottsdatalagen gäller båda vid behandling av personuppgifter som är helt eller delvis automatiserat och för annan behandling av personuppgifter som ingår i eller kommer att ingå i ett register (artikel 2.1 i dataskyddsförordningen och 1 kap. 3 § brottsdatalagen). Båda regelverken innehåller grundläggande krav på behandling av personuppgifter, liksom bestämmelser om skyldigheter för personuppgiftsansvariga, enskildas rättigheter, tillsyn, sanktionsavgifter, skadestånd, rättsmedel samt överföring av personuppgifter till tredjeland och internationella organisationer.

Enligt 2 kap. 1 § första stycket brottsdatalagen får personuppgifter behandlas om det är nödvändigt för att en behörig myndighet ska kunna utföra sin uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. I 1 kap. 2 § andra stycket brottsdatalagen anges att med en behörig myndighets uppgift avses en uppgift som framgår av lag, förord-

ning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att utföra uppgiften. Personuppgiftsbehandlingen måste gå att härleda till den behöriga myndighetens uppgifter så som de kommer till uttryck i unionsrätten eller i nationell lagstiftning och andra för verksamheten bindande beslut om arbetsuppgifter. Unionsrätten är en del av den svenska rättsordningen. EU-förordningar är att jämställa med svensk lag. Den uppgift som den behöriga myndigheten ska utföra ska således ha stöd i unionsrätt eller nationell rätt, vilket utgör den rättsliga grunden för behandling av personuppgifter.²²

Det följer inte direkt av lagen vilka som är behöriga myndigheter (se 1 kap. 6 §). Avgörande är om myndigheten har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Myndigheten är behörig bara när den utför sådana uppgifter. I förarbetena till brottsdatalagen anges att Polismyndigheten, Tullverket, Kustbevakningen, Skatteverket, Ekobrottsmyndigheten, Åklagarmyndigheten, de allmänna domstolarna och Kriminalvården är behöriga myndigheter, men enbart när de behandlar personuppgifter för tidigare angivna syften. Även Säkerhetspolisen omfattas av brottsdatalagens respektive lagens (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område bestämmelser när Säkerhetspolisen behandlar personuppgifter som inte rör nationell säkerhet i syfte att bekämpa och lagföra brott. Säkerhetspolisens brottsutredande verksamhet är dock mycket liten och initieras endast undantagsvis genom anmälningar om brott. Säkerhetspolisens verksamhet rör i princip uteslutande nationell säkerhet. Den absoluta merparten av Säkerhetspolisens behandling av personuppgifter ligger därför utanför brottsdatalagens tillämpningsområde och regleras i lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter.

10.7.3 Det finns inget behov av ändringar i dataskyddsregleringen

Bedömning: EU-förordningen och den kompletterande lagen medför inget behov av ändringar i dataskyddsregleringen.

²² Prop. 2017/18:232 s. 117.

Skälen för bedömningen

Tillämpligt regelverk i ett ärende om utfärdande respektive verkställighet av en order som omfattas av EU-förordningen

För Åklagarmyndighetens personuppgiftsbehandling gäller antingen EU:s dataskyddsförordning, med den tillhörande lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen), eller brottsdatalagen (2018:1177) och lagen (2018:1697) om åklagarväsendets behandling av personuppgifter inom brottsdatalagens område (här kallad Åklagarväsendets brottsdatalag). För övriga behöriga myndigheter gäller även deras respektive registerlag. För Polismyndigheten gäller lagen om polisens behandling av personuppgifter inom brottsdatalagens område (Polisens brottsdatalag).

Avgörande för vilket regelverk som blir tillämpligt är, som utvecklats ovan, om behandlingen sker i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, eller utreda eller lagföra brott eller verkställa straffrättsliga påföljder (artikel 2.2 d i dataskyddsförordningen och 1 kap. 2 § brottsdatalagen). Är så fallet ska brottsdatalagen tillämpas, annars dataskyddsförordningen. Utfärdande respektive verkställighet av en europeisk utlämnande- eller bevarandeorder sker i syfte att utreda eller lagföra brott eller verkställa straffrättsliga påföljder, dvs. sådant brottsbekämpande syfte som följer av de nämnda bestämmelserna. Därmed är brottsdatalagen och myndigheternas respektive registerlag tillämpliga för den personuppgiftsbehandling som förekommer i ett sådant ärende.

EU-förordningen möjliggör inhämtning av elektronisk bevisning i form av abonnentuppgifter, andra användaruppgifter, trafikuppgifter och innehållsdata (se avsnitt 6.3.1). De uppgifter som de behöriga myndigheterna enligt EU-förordningen kan komma att behandla utgörs primärt av misstänkta, tilltalades eller dömda personers kontaktuppgifter, som t.ex. telefonnummer, e-postadress samt IP-nummer. I fråga om innehållsdata kan även känsliga personuppgifter förekomma, t.ex. som innehåll i ett meddelande (se nedan). Det är dock svårt att med någon mån av säkerhet uttala sig om omfattningen av personuppgiftsbehandlingen i anledning av EU-förordningen.

I 2 kap. 1 § brottsdatalagen anges de tillåtna rättsliga grunderna för myndigheternas personuppgiftsbehandling enligt lagen. Av

bestämmelsen framgår, som behandlats ovan, att myndigheterna bl.a. får behandla personuppgifter om det är nödvändigt för att myndigheten ska kunna förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda brott. Bestämmelsen ger den yttre ramen för när det är tillåtet att behandla personuppgifter enligt lagen. Personuppgifter får endast behandlas om det är nödvändigt för att fullgöra en sådan uppgift.

Känsliga personuppgifter, dvs. uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning får som huvudregel inte behandlas (2 kap. 11 § brottsdatalagen). Om uppgifter om en person behandlas får de dock kompletteras med sådana uppgifter som anges i första stycket när det är absolut nödvändigt för ändamålet med behandlingen (2 kap. 11 § andra stycket brottsdatalagen). Känsliga personuppgifter får dock enligt 2 kap. 13 alltid behandlas med stöd av 2 kap. 2 § brottsdatalagen, dvs. om det är nödvändigt för diarieföring eller, i fråga om uppgifter i en anmälan, ansökan eller liknande, om det är nödvändigt för myndighetens handläggning. I de enskilda registerförfattningarna finns också bestämmelser om behandling av personuppgifter.

Innan personuppgifter får behandlas för ett nytt ändamål inom brottsdatalagens tillämpningsområde ska det säkerställas att det finns en rättslig grund enligt 2 kap. 1 § brottsdatalagen för den nya behandlingen och att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet (2 kap. 4 § första stycket brottsdatalagen). Sådan rättslig grund för behandling av personuppgifter finns om det är nödvändigt för att en behörig myndighet ska kunna utföra sin uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. I den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning ska någon prövning enligt första stycket inte göras (2 kap. 4 § andra stycket brottsdatalagen).

När Åklagarmyndigheten respektive Polismyndigheten och övriga behöriga myndigheter agerar i sina respektive roller som utfärdande eller verkställande myndighet har de rättsligt stöd för den personuppgiftsbehandling som informationsutbytet enligt EU-förordningen ger upphov till. Det rättsliga stödet för behandlingen

kommer att finnas i 2 kap. 1 och 2 §§ i respektive registerförfattning tillsammans med 2 kap. 4 § brottsdatalagen. Bestämmelsen i 2 kap. 1 § 2 och 5 Åklagarväsendets brottsdatalag respektive 2 kap. 1 § 2 och 5 Polisens brottsdatalag innebär t.ex. att myndigheterna får behandla personuppgifter om det är nödvändigt för att myndigheterna ska kunna utreda och lagföra brott samt fullgöra förpliktelser som följer av internationella åtaganden. Av bestämmelsen i 2 kap. 2 § i respektive lag framgår att förutsättningarna för att behandla uppgifter som behandlas med stöd av 2 kap. 1 § respektive lag för nya ändamål regleras i bl.a. 2 kap. 4 § brottsdatalagen. Bedömningen görs att det kan anses vara både nödvändigt och proportionerligt att personuppgifter behandlas vid utfärdande eller verkställande av en europeisk utlämnandeorder respektive bevarandeorder. Förutsättningarna för att personuppgifter ska få behandlas för nya ändamål i enlighet med 2 kap. 4 § brottsdatalagen är därmed uppfyllda. Det finns därför inte behov av några kompletterande dataskyddsbestämmelser för hanteringen av en sådan order som omfattas av EU-förordningen.

*Personuppgifter i ärenden om vitesförelägganden
eller sanktionsavgifter*

Möjligheten att besluta om sanktionsavgift vid överträdelser av EU-förordningen syftar till att uppnå efterlevnad av förordningen, inte till att bestraffa begångna brott, och sanktionerna utgör inte straffrättsliga påföljder. Sanktionsavgift aktualiseras om en tjänsteleverantör inte hörsammar en europeisk utlämnande- eller bevarandeorder och således inte helt eller delvis lämnar ut eller bevarar de aktuella uppgifter eller inte följer de tidsfrister som anges i EU-förordningen. I den mån Åklagarmyndigheten kommer att hantera personuppgifter i ett sådant ärende som rör en tjänsteleverantör kan personuppgiftsbehandlingen därför i denna del inte anses ske primärt i brottsförebyggande eller brottsbekämpande syfte, även om effekterna i förlängningen kan bli positiva för det brottsförebyggande och brottsbekämpande arbetet. Detta innebär sammantaget att dataskyddsförordningen och dataskyddslagen blir tillämpliga på all behandling av personuppgifter som Åklagarmyndigheten vidtar inom ramen för ett ärende om påförande av sanktionsavgifter enligt EU-förordningen. Detsamma gäller för centralmyndig-

heten när den handlägger ett ärende om vitesföreläggande eller sanktionsavgift eller i övrigt bedriver tillsyn över utsedda verksamhetsställen eller rättsliga ombud i enlighet med förslagen i den kompletterande lagen.

Dataskyddsförordningen utgår från att varje behandling av personuppgifter måste vila på en rättslig grund (artikel 6). Den behandling av personuppgifter som myndigheter utför görs huvudsakligen med stöd av de rättsliga grunder som kommer till uttryck i artikel 6.1 c eller e, och som enligt artikel 6.3 ska fastställas i enlighet med unionsrätten eller nationell rätt. Den rättsliga grunden enligt artikel 6.1 c innebär att behandlingen är laglig om den är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Begreppet omfattar i första hand offentligrättsliga förpliktelser. Av 2 kap. 1 § dataskyddslagen följer att en rättslig förpliktelse utgör en rättslig grund för behandling av personuppgifter om förpliktelsen följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Den rättsliga grunden enligt artikel 6.1 e innebär att behandlingen är laglig om den är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

All verksamhet som en myndighet bedriver, inom ramen för sin befogenhet, anses vara av allmänt intresse.²³ Av 2 kap. 2 § 1 dataskyddslagen följer att en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning utgör en rättslig grund för behandling av personuppgifter. När Åklagarmyndigheten utför sina uppgifter som verkställande myndighet i fråga om beslut om sanktionsavgifter utför den en uppgift av allmänt intresse som följer av lag eller annan författning, dvs. av EU-förordningen och den kompletterande nationella lagen. Dessutom innehåller EU-förordningen och lagen rättsliga förpliktelser som innebär att personuppgifter kan komma att behandlas. Den personuppgiftsbehandling som är nödvändig för att utföra uppgifterna som verkställande myndighet i fråga om beslut om sanktionsavgifter har alltså rättslig grund enligt artikel 6.1 e och kan även ha det enligt artikel 6.1 c.

²³ Prop. 2017/18:105 s. 56–59.

Även personuppgifter som rör lagöverträdelser enligt artikel 10 i dataskyddsförordningen kan komma att behöva behandlas i ett ärende om sanktionsavgifter. Detta eftersom en europeisk utlämnande- eller bevarandeorder kan utfärdas för verkställighet av fängelsestraff eller annan frihetsberövande påföljd. Eftersom sådana personuppgifter enligt 3 kap. 8 § första stycket dataskyddslagen får behandlas av myndigheter finns rättsligt stöd också för denna personuppgiftsbehandling.

Det kan inte uteslutas att känsliga personuppgifter kan förekomma i ett ärende om sanktionsavgift. Det skulle t.ex. kunna vara fråga om innehåll i ett meddelande som inhämtats i det ärende som föranlett frågan om sanktionsavgift ska beslutas. Känsliga personuppgifter får behandlas under förutsättning att behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen (artikel 9.2 g). I förarbetena till dataskyddslagen gör regeringen bedömningen att det är ett viktigt allmänt intresse att myndigheterna kan sköta sitt uppdrag på ett korrekt, rättssäkert och effektivt sätt. När Åklagarmyndigheten behandlar känsliga personuppgifter som är nödvändiga för att utföra uppdraget som verkställande myndighet rör det sig således om en sådan behandling som omfattas av artikel 9.2 g.²⁴

Dataskyddsförordningen innehåller en mängd bestämmelser till skydd för den vars personuppgifter behandlas med stöd av förordningen. Av de allmänna principerna för behandling av personuppgifter i artikel 5 följer bl.a. att personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (ändamålsbegränsning), vara adekvata, relevanta och inte omfattande i förhållande till de ändamål för vilka de behandlas (uppgiftsminimering) och inte får förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas (s.k. lagringsminimering). Vid behandling av känsliga personuppgifter med stöd av artikel 9.2 g uppställer dataskyddsförordningen

²⁴ Prop. 2017/18:105 s. 85 och prop. 2022/23:71 s. 41.

även ett krav på lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen. En sådan åtgärd är den sökbegränsning som gäller enligt 3 kap. 3 § andra stycket dataskyddslagen.

Det sagda innebär sammanfattningsvis att det finns rättsligt stöd för den personuppgiftsbehandling som den verkställande myndigheten behöver vidta inom ramen för ett ärende om påförande av sanktionsavgift. Det gäller även för centralmyndigheten i den mån den myndigheten behandlar personuppgifter i ett tillsynsärende om vitesföreläggande eller påförande av sanktionsavgift. Det finns därför inte heller behov av några kompletterande dataskyddsbestämmelser i denna del.

10.8 Uppgiftslämnande och sekretess

Bedömning: Offentlighets- och sekretesslagens bestämmelser tillgodoser de behov av sekretess och uppgiftslämnande som kan förekomma när Sverige är utfärdande respektive verkställande stat av en europeisk utlämnande- eller bevarandeorder.

Skäl för bedömningen: EU-förordningen innehåller inte några särskilda bestämmelser om sekretess som riktar sig mot de behöriga utfärdande eller verkställande myndigheterna. Flera bestämmelser förutsätter dock ett visst informationsutbyte mellan dessa myndigheter, t.ex. anmälningsförfarande enligt artikel 8 och begäran om verkställighet enligt artikel 16. I ett sådant informationsutbyte kan det förekomma uppgifter som omfattas av sekretess. Även EU-direktivet innehåller bestämmelser om informationsutbyte mellan centralmyndigheterna.

I 18 kap. 17 § offentlighets- och sekretesslagen (2009:400) finns bestämmelser om sekretess i verksamhet som avser rättsligt samarbete på begäran av en annan stat, för uppgift som hänför sig till en utredning enligt bestämmelserna om förundersökning i brottmål eller en angelägenhet som angår tvångsmedel, om det kan antas att det varit en förutsättning för den andra statens begäran att uppgiften inte skulle röjas. Med hänsyn till den begränsade information som svenska myndigheter i normalfallet har om brottsutredningen i den andra staten är skaderekvisitet utformat på ett annat sätt än

vad som gäller vid förundersökningssekretess. Den svenska myndigheten ska pröva om det kan antas att uppgiften lämnats under förutsättning att uppgiften inte röjs. Mot bakgrund av att det inom det straffrättsliga samarbetet är en självklar utgångspunkt att känsliga uppgifter i den utländska brottsutredningen kan skyddas i den anmodade staten råder en stark presumtion för sekretess.²⁵ Regleringen kommer att vara tillämplig när Sverige är verkställande stat av en europeisk utlämnande- eller bevarandeorder.

När Sverige är utfärdande stat av en sådan order kommer bestämmelserna i 18 kap. 1 § offentlighets- och sekretesslagen om förundersökningssekretess att vara tillämpliga.

De grundläggande förutsättningarna för att en svensk myndighet ska kunna lämna ut sekretessbelagda uppgifter till en utländsk myndighet regleras i 8 kap. 3 § offentlighets- och sekretesslagen. En utgångspunkt i lagen är att en uppgift som omfattas av sekretess inte får röjas för en utländsk myndighet eller mellanfolklig organisation. I 8 kap. 3 § finns dock bestämmelser som innebär att en uppgift som omfattas av sekretess får röjas för en utländsk myndighet eller mellanfolklig organisation i två situationer. Den ena är när utlämnandet sker enligt en särskild föreskrift i lag eller förordning (punkt 1). En föreskrift i en EU-förordning är att jämställa med en föreskrift i lag eller förordning.²⁶ Den andra situationen är när uppgiften i motsvarande fall skulle få lämnas till en svensk myndighet och det enligt den utlämnande myndigheten står klart att det är förenligt med svenska intressen att uppgiften lämnas (punkt 2).

I de brottsbekämpande myndigheternas registerlagstiftningar finns uttryckliga sekretessbrytande bestämmelser som medger utlämnande av personuppgifter till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande, se t.ex. 2 kap. 7 § tredje stycket Polisens brottsdatalag. I vissa brottsbekämpande myndigheters registerlagstiftningar anges vidare vissa mera preciserade fall där personuppgifter får lämnas ut till en utländsk mottagare, trots att det gäller sekretess för uppgiften, se t.ex. 2 kap. 7 § första och andra stycket i Polisens brottsdatalag.

²⁵ Prop. 1999/2000:61 s.209 och prop. 2003/04:7 s. 216.

²⁶ Prop. 2018/19:38 s. 88 och prop. 1999/2000:126 s. 160 och 283.

Det finns även andra bestämmelser i offentlighets- och sekretesslagen som kan bli tillämpliga i de aktuella ärendena, t.ex. bestämmelserna om utrikessekretess i 15 kap. 1 §, och om sekretess till skydd för enskild i verksamhet som syftar till att förebygga eller beivra brott i 35 kap.

Sammanfattningsvis innebär det sagda att det behov av sekretess och uppgiftslämnande som kan följa vid tillämpning av EU-förordningen tillgodoses genom befintlig lagstiftning. Några kompletterande regler behöver således inte införas i detta avseende.

11 Säkrande av elektroniska bevis enligt Budapestkonventionen

11.1 Inledning

I november 1996 beslutade Europarådets straffrättsliga styrkommitté (CDPC) att uppdra åt en expertkommitté att utreda frågor rörande it-relaterad brottslighet. Efter beslut i ministerrådet påbörjades arbetet med en konvention om it-relaterad brottslighet i april 1997. Europarådets konvention om it-relaterad brottslighet (Budapestkonventionen, ETS 185) antogs av ministerrådet och öppnades för undertecknande 2001. Den trädde i kraft den 1 juli 2004. Hittills har 78 stater undertecknat konventionen och 76 stater ratificerat den. Konventionen trädde i kraft gentemot Sverige den 1 augusti 2021. Alla EU-stater utom en samt Island och Norge har ratificerat konventionen.

Budapestkonventionen har tre huvudsyften. Det första är att åstadkomma en tillnärmning av ländernas nationella straffrätt beträffande vissa it-relaterade brott. Det andra är att säkerställa att det finns nationella processrättsliga bestämmelser som tillgodoser behovet av att utreda och lagföra de brott som behandlas i konventionen och andra brott som begås med hjälp av datorer samt att kunna ta till vara bevisning i elektronisk form. Det tredje är att lägga grunden för ett snabbt och effektivt internationellt samarbete vid bekämpningen av it-relaterade brott.

Konventionen är indelad i fyra kapitel. Dessa innehåller definitioner (kapitel I), bestämmelser om straff- och processrättsliga åtgärder som ska vidtas på nationell nivå (kapitel II), bestämmelser om internationellt samarbete (kapitel III) och slutbestämmelser (kapitel IV). I kapitel II är bestämmelserna uppdelade i tre avsnitt. Bestämmelserna i avsnitt 1 ställer krav på kriminalisering av vissa gärningar som begås med hjälp av ett datorsystem. De process-

rättsliga reglerna finns i avsnitt 2. Där ställs krav på att medlemsstaterna ska kunna vidta olika former av åtgärder vid utredningen av de brott som omfattas av konventionen. I avsnitt 3 finns regler om domsrätt.

Bestämmelserna om internationellt samarbete i kapitel III utgör en betydande del av konventionen. Kapitlet är uppdelat i två avsnitt: ett allmänt avsnitt där de grundläggande principerna för samarbetet läggs fast och ett avsnitt med särskilda bestämmelser om rättslig hjälp med olika former av åtgärder.

I samband med att konventionen trädde i kraft inrättades The Cybercrime Convention Committee (T-CY). Kommittén har till uppgift att övervaka och främja efterlevnaden och effektiviteten av Budapestkonventionen.

Till konventionen finns ett första tilläggsprotokoll som trädde i kraft den 1 mars 2006 (ETS 189). Tilläggsprotokollet kriminaliserar gärningar av rasistisk och främlingsfientlig natur begångna med hjälp av datorsystem samt utvidgar konventionens processrättsliga bestämmelser och bestämmelser om internationellt samarbete också till att gälla brott som omfattas av tilläggsprotokollet. Hittills har 46 stater undertecknat tilläggsprotokollet och 36 stater ratificerat det.

Enligt artikel 16 i Budapestkonventionen ska konventionsstaterna se till att ha nationella processrättsliga bestämmelser om skyndsamt säkrande av lagrade uppgifter i elektronisk form. Vidare ställs krav enligt artikel 29 i konventionen att staterna även ska kunna samarbeta över gränserna när det gäller denna typ av åtgärd.

För att efterleva artikel 16 i Budapestkonventionen infördes i svensk rätt ett nytt tvångsmedel i 27 kap. 16 § rättegångsbalken om förelägganden om att bevara uppgifter i elektronisk form. När det gäller konventionens krav i artikel 29 om internationellt samarbete gjordes vissa tillägg i lagen (2000:562) om internationell rättslig hjälp i brottmål och lagen (2017:1000) om en europeisk utredningsorder så att samarbetet enligt dessa två lagar även omfattade en åtgärd enligt 27 kap. 16 § rättegångsbalken.

I december 2022 lämnade Åklagarmyndigheten in en framställan om förtydliganden i regleringen om det gränsöverskridande samarbetet beträffande förelägganden om att bevara uppgifter i elektronisk form. I framställan anges bl.a. att andra EU-stater inte anser att en europeisk utredningsorder ska användas vid förelägg-

anden enligt artikel 29 i Budapestkonventionen och att det medför problem i det rättsliga samarbetet som kan behöva åtgärdas genom lagändringar. Enligt direktiven ska vi därför analysera om det finns behov av att ändra eller komplettera bestämmelserna om gränsöverskridande hantering av förelägganden om att bevara lagrade uppgifter i elektronisk form, och lämna nödvändiga författningsförslag.

11.2 Närmare om Budapestkonventionens reglering om skyndsamt säkrande av lagrade uppgifter

Artikel 16 i Budapestkonventionen ålägger en stat att se till att dess behöriga myndigheter i inhemska straffrättsliga förfaranden skyndsamt kan säkra datorbehandlingsbara uppgifter som har lagrats med hjälp av ett datorsystem, dvs. en form av frysning av elektroniska lagrade uppgifter.

Syftet är att under en begränsad tid säkerställa att lagrade uppgifter inte går förlorade eller förändras. Frysningen innebär inte ett förbud för den som har ålagts att bevara uppgifterna att använda dem för legitima syften. Hur själva säkerställandet utförs är således upp till respektive stat, t.ex. att uppgifterna kopieras. En annan tanke med artikel 16 är att erbjuda en mindre ingripande åtgärd än t.ex. husrannsakan och beslag. Enligt artikel 16 ska ett säkrande ske under minst 90 dagar och tiden får förlängas. Efter det att uppgifterna har bevarats ska de brottsbekämpande myndigheterna ta ställning till om uppgifterna ska begäras ut av den som bevarat uppgifterna. (Se den förklarande rapporten till konventionen p. 155, 156 och 159.)

Ett annat och viktigt syfte med artikel 16 i konventionen är att möjliggöra motsvarande åtgärder i det internationella samarbetet och att de också vidtas skyndsamt (se den förklarande rapporten p. 157). Dessa bestämmelser återfinns i artikel 29.

I artikel 29.1 anges att en part får anmoda en annan part att skyndsamt säkra uppgifter som har lagrats med hjälp av ett datorsystem inom den sistnämnda partens territorium, vilka uppgifter den förstnämnda parten i ett senare led kommer att begära åtkomst till i någon form. Vilka uppgifter en framställning ska innehålla framgår av artikel 29.2. Efter det att en part mottagit en framställ-

ning ska den vidta alla lämpliga åtgärder för att skyndsamt säkra de angivna uppgifterna (artikel 29.3). Utgångspunkten är att ett krav på dubbel straffbarhet inte ska ställas upp, men en part kan i vissa situationer förbehålla sig rätten att ändå ställa upp ett sådant krav (artikel 29.3–29.4). En stat kan dock under alla förhållanden avslå en framställan med stöd av de vägransgrunder som anges i artikel 29.5 (t.ex. om gärningen utgör ett politiskt brott eller om en verkställighet skulle inkräkta på en stats suveränitet eller stå i strid mot allmänna rättsprinciper). Artikel 29.6 reglerar frågor om bl.a. sekretess. Ett säkerställande som verkställs i en stat ska enligt artikel 29.7 gälla dels minst 60 dagar så att den andra staten ges möjlighet att ansöka om att uppgifterna ska lämnas ut, dels under den tid sistnämnda ansökan prövas.

I den förklarande rapporten betonas flera gånger att det rör sig om en tillfällig åtgärd som ska vidtas mycket snabbare än en traditionell ansökan om rättslig hjälp (se p. 282 och 283), vilket också återspeglas av att ansökans innehåll är mer summarisk och att den prövning som ska ske är mer begränsad (se p. 284–287).

För att säkerställa att en begäran enligt bl.a. artikel 29 hanteras skyndsamt infördes genom artikel 35 i konventionen ett 24/7-nätverk som har, bland många andra, till uppgift att hantera och kommunicera framställningar enligt artikel 29.

11.3 Genomförandet av artiklarna 16 och 29 i Budapestkonventionen i svensk rätt

11.3.1 Rättegångsbalkens reglering

För att Sverige skulle leva upp till artikel 16 i Budapestkonventionen infördes bestämmelser om föreläggande om bevarande av lagrade uppgifter i 27 kap. 16 och 16 a §§ rättegångsbalken. Förutom att leva upp till åtagandet enligt aktuell artikel i konventionen sågs bestämmelserna även som ett mindre ingripande alternativ till åtgärder som husrannsakan och beslag, edition samt hemliga tvångsmedel.¹ Ett föreläggande innebär inte att uppgifterna ska lämnas ut utan det får prövas enligt andra regler, t.ex. enligt lagen (2022:482) om elektronisk kommunikation eller de om hemliga tvångsmedel.

¹ Prop. 2020/21:72 s. 24.

Bestämmelserna i 27 kap. 16 och 16 a §§ innebär sammanfattningsvis följande.

En åklagare eller undersökningsledare får förelägga den som i elektronisk form innehar en viss lagrad uppgift att bevara uppgiften om den skäligen kan antas ha betydelse för utredning av brott. Syftet är detsamma som i artikel 16 i Budapestkonventionen, dvs. att ge brottsutredande myndigheter möjlighet att under en begränsad tidsperiod se till att lagrade datorbehandlingsbara uppgifter inte raderas, förstörs eller ändras i avvaktan på ett eventuellt beslut om andra tvångsåtgärder.²

De uppgifter som avses kan vara av vilket slag som helst, t.ex. en digitalt lagrad bild, innehållet i ett meddelande eller uppgifter om ett meddelandes ursprung och adressat. Att uppgiften ska vara lagrad innebär att den ska finnas bevarad elektroniskt när föreläggandet meddelas. På vilken grund uppgiften har lagrats har ingen betydelse. Det spelar således ingen roll om uppgiften har lagrats på grund av regler om datalagring, kommersiella skäl eller av annan anledning. Reglerna om bevarande innebär inte en skyldighet för den som tar emot ett föreläggande att lagra eventuella framtida uppgifter. I föreläggandet måste anges vilken specifik elektronisk uppgift som ska bevaras, t.ex. en viss datafil eller trafikuppgifter hänförliga till ett visst meddelande. Ett föreläggande kan inte, utan närmare specificering, endast ange att alla uppgifter som mottagits under en tid ska bevaras.³

Ett föreläggande kan rikta sig mot vem som helst som innehar en lagrad uppgift. Både fysiska och juridiska personer omfattas av regleringen. Föreläggandet kan även avse lagrade uppgifter som innehas av flera olika personer samtidigt, t.ex. den som innehar ett e-postkonto eller den som innehar en server där uppgifterna också finns lagrade.⁴ Ett föreläggande får dock inte riktas mot den som skäligen kan misstänkas för brottet eller mot någon till honom eller henne sådan närstående person som avses i 36 kap. 3 § rättegångsbalken. Den som föreläggandet riktas emot kan åläggas en skyldighet att inte uppenbara att åtgärden har vidtagits.

Kravet på när ett föreläggande kan beslutas är relativt lågt ställt och motsvarar det krav som gäller för att beslagta föremål i bevis-

² Prop. 2020/21:72 s. 23–27.

³ Prop. 2020/21:72 s. 68.

⁴ Prop. 2020/21:72 s. 68.

syfte (27 kap. 1 § rättegångsbalken). Det krävs inte att någon är misstänkt för det brott som utreds.⁵

Ett föreläggande om bevarande får inte ske för en tid längre än 90 dagar. Om särskilda skäl föreligger kan dock fristen förlängas ytterligare 90 dagar. Särskilda skäl kan t.ex. vara att utredande myndighet måste vidta ytterligare åtgärder för att kunna besluta om de bevarande uppgifterna ska begäras ut. Det kan också vara fråga om mer komplicerade utredningar där en stor del av informationen är krypterad eller skyddas på annat sätt. Tiden för bevarande kan förlängas vid ett eller flera tillfällen så länge fristerna inte överskrids.⁶

Föreläggandet bör som huvudregel ges skriftligen. Situationer kan emellertid uppstå då det finns ett behov av att meddela ett föreläggande muntligt. I förarbetena ges som exempel att ett pågående dataintrång spåras till en dator i Sverige och det krävs ett omedelbart ingripande. Ett sådant föreläggande bör dock dokumenteras skriftligt och tillställas den som har förelagts åtgärden så snart det är möjligt.⁷

Den som har förelagts att bevara en viss uppgift får begära rättens prövning av föreläggandet. För rättens prövning gäller 27 kap. 6 § första stycket rättegångsbalken, vilket innebär att rätten så snart som möjligt och senast inom fyra dagar från begäran om prövning ska hålla förhandling.

Vid beslut om ett föreläggande om bevarande gäller proportionalitetsprincipen (27 kap. 1 § tredje stycket rättegångsbalken). Proportionalitetsprincipen innebär att en tvångsåtgärd ska stå i rimlig proportion till vad som står att vinna med den. Det innebär att ett föreläggande om bevarande inte kommer att kunna meddelas om det inte finns ett tillräckligt starkt behov av åtgärden med beaktande av motstående intressen.

11.3.2 Det gränsöverskridande samarbetet

För att leva upp till artikel 29 i Budapestkonventionen gjordes vissa ändringar i lagen om internationell rättslig hjälp i brottmål och lagen om en europeisk utredningsorder. Det ska noteras att be-

⁵ Prop. 2020/21:72 s. 68.

⁶ Prop. 2020/21:72 s. 69.

⁷ Prop. 2020/21:72 s. 27.

tänkandet om Sveriges anslutning till konventionen från 2013 inte hade några förslag på ändringar i sistnämnda lag då den trädde i kraft först 2017.

Av 5 § 3 förordningen (2022:1718) med instruktion för Polismyndigheten (bilaga, punkt 2.c) framgår att Polismyndigheten ska vara nationell kontaktpunkt för säkerställande av omedelbar hjälp enligt artikel 35 i Budapestkonventionen.

Lagen om internationell rättslig hjälp i brottmål

I 1 kap. 2 § lagen om internationell rättslig hjälp i brottmål kompletterades katalogen av de åtgärder som lagen omfattar med en åtgärd enligt 27 kap. 16 § rättegångsbalken. Vidare gjordes en ändring i 2 kap. 1 § så att de förutsättningar som gäller enligt rättegångsbalken för att besluta om ett föreläggande att bevara en lagrad uppgift ska gälla vid lämnande av rättslig hjälp med en sådan åtgärd. Hänvisningen till rättegångsbalken innebär att de ovan behandlade reglerna i 27 kap. 16 och 16 a §§ i samma balk gäller även vid rättslig hjälp i fråga om ett föreläggande om bevarande. En proportionalitetsbedömning ska alltid ske och den som drabbas av ett föreläggande kan begära rättens prövning och åläggas tystnadsplikt. Det tillägg som gjordes i 2 kap. 2 § lagen om internationell rättslig hjälp i brottmål innebär att ett krav på dubbel straffbarhet inte ska ställas upp.

Eftersom rättslig hjälp ska lämnas under samma förutsättningar som en motsvarande åtgärd under en svensk förundersökning får föreläggandet inte heller gälla längre än den tid som anges till 27 kap. 16 § andra och tredje styckena rättegångsbalken. Det innebär att tiden inte får bestämmas längre än nödvändigt och högst 90 dagar i ett första skede, med en möjlighet till förlängning, om det finns särskilda skäl, med ytterligare 90 dagar.

Slutligen infördes en ny bestämmelse i lagen om internationell rättslig hjälp i brottmål, 4 kap. 24 c §, som anger att åklagaren handlägger en ansökan enligt 27 kap. 16 § rättegångsbalken när åtgärden ska vidtas i Sverige.

När det gäller en ansökan utomlands om att bevara uppgifter i elektronisk form gjordes inga ytterligare tillägg än den i 1 kap. 2 § lagen om internationell rättslig hjälp i brottmål. Med stöd av den

bestämmelsen och 1 kap. 7 § kan åklagaren ansöka utomlands om en sådan åtgärd.

Lagen om en europeisk utredningsorder

Mellan EU:s medlemsstater tillämpas i huvudsak inte lagen om internationell rättslig hjälp i brottmål vid gränsöverskridande bevisinhämtning (se avsnitt 4.5.2). I stället tillämpas lagen om en europeisk utredningsorder (se 1 kap. 7 a § lagen om internationell rättslig hjälp i brottmål).

Genom att införa en möjlighet till föreläggande om bevarande av lagrade uppgifter i rättegångsbalken lades åtgärden till i 1 kap. 4 § lagen om en europeisk utredningsorder som anger vilka åtgärder som en europeisk utredningsorder kan avse eller motsvara. Enligt regeringen förelåg en skyldighet enligt direktivet att se till att lagen även omfattade nu aktuell åtgärd.⁸

Åklagaren utfärdar en europeisk utredningsorder om ett föreläggande om bevarande av lagrade uppgifter (2 kap. 1 § lagen om en europeisk utredningsorder). En sådan order får utfärdas om de förutsättningar som gäller för den aktuella utredningsåtgärden enligt svensk rätt är uppfyllda (2 kap. 3 §). Kraven på bl.a. att uppgiften skäligen kan antas ha betydelse för utredningen, tid för bevarande och vem ett föreläggande får riktas mot i 27 kap. 16 och 16 a §§ rättegångsbalken gäller alltså när en europeisk utredningsorder om att bevara en viss lagrad uppgift utfärdas (se även artikel 6.1 i direktivet om en europeisk utredningsorder). Detsamma gäller det proportionalitetskrav som finns i 27 kap. 1 § tredje stycket rättegångsbalken.

Erkännande och verkställighet av en europeisk utredningsorder för ett föreläggande om bevarande handläggs av åklagare (3 kap. 8 § lagen om en europeisk utredningsorder). Om den europeiska utredningsordern erkänns, ska åklagaren meddela en verkställbarhetsförklaring enligt 3 kap. 19 §. Förklaringen ska innehålla uppgifter av betydelse för verkställigheten, t.ex. hur länge de lagrade uppgifterna ska bevaras. Som utgångspunkt gäller samma förutsättningar för verkställigheten av en europeisk utredningsorder som för den aktuella utredningsåtgärden enligt svensk rätt (se

⁸ Prop. 2020/21:72 s. 35.

3 kap. 21 §). Det innebär bl.a. – liksom vid rättslig hjälp enligt lagen om internationell rättslig hjälp i brottmål – att tiden för bevarande inte får bestämmas till längre än nödvändigt och högst 90 dagar i ett första skede, med en möjlighet till förlängning med ytterligare högst 90 dagar om det finns särskilda skäl.

11.4 Åklagarmyndighetens framställan

I december 2022 lämnade Åklagarmyndigheten in en framställan till regeringen om förtydliganden i regelverket om gränsöverskridande hantering av förelägganden om att bevara uppgifter i elektronisk form (Ju2022/03650). I framställan anger myndigheten i huvudsak följande.

Vid handläggningen av ett gränsöverskridande föreläggande om bevarande enligt artikel 29 i Budapestkonventionen (artikel 29-begäran) måste en europeisk utredningsorder användas vid ett utgående föreläggande till ett annat EU-land, eftersom lagen om internationell rättslig hjälp i brottmål är subsidiär till lagen om en europeisk utredningsorder. Detta försvårar och försenar samarbetet eftersom andra EU-länder inte anser att en europeisk utredningsorder ska användas vid en artikel 29-begäran. Därmed riskerar uppgifterna som ska säkras att gå förlorade under handläggningstiden. I den förklarande rapporten till konventionen framhålls vikten av att länderna som tillträtt konventionen vidtar åtgärder för att tillräckligt skyndsamt kunna säkra elektroniska uppgifter, som till sin natur är mycket flyktiga och lätta att förstöra eller förvanska, och uppgifterna bör säkras genom en process mellan konventionsländerna som är betydligt snabbare än en än en formell begäran om ömsesidig rättslig hjälp (se punkt 282).

I dag handlägger Polismyndighetens 24/7-kontaktpunkt en inkommande artikel 29-begäran som en ansökan om rättslig hjälp enligt lagen om internationell rättslig hjälp i brottmål, även om begäran görs av ett annat EU-land. Detta utgör ett avsteg från övrig hantering av frågor om rättslig hjälp utan egentligt eller i vart fall utan uttryckligt lagstöd eftersom en artikel 29-begäran från ett annat EU-land ska handläggas enligt lagen om en europeisk utredningsorder. Det har enligt uppgift hänt att svensk åklagare har anmodat ansökande stat att inkomma med en europeisk utred-

ningsorder i fråga om en artikel 29-begäran, vilket är ett krav som enligt T-CY inte kan ställas⁹.

En inkommande artikel 29-begäran som är undertecknad av en polismyndighet i den ansökande staten accepteras. Begäran hanteras med vederbörlig skyndsamhet. Enligt Polismyndighetens metodstöd är endast åklagare behörig att fatta beslut om andra staters begäran om att bevara information och röja trafikuppgifter i Sverige. Polismyndigheten vänder sig alltså vid en inkommande artikel 29-begäran till åklagare för beslut om bevarandeföreläggande.

En artikel 29-begäran som skickas från Sverige till annan konventionsstat sker såsom en ansökan om rättslig hjälp. Åklagarmyndigheten har utvecklat en mall i överensstämmelse med Budapestkonventionen. Mallen anses möta kraven på en ansökan om rättslig hjälp och används vid utgående ansökan till länder som inte tillämpar direktivet om en europeisk utredningsorder. Ansökan kanaliseras via Polismyndighetens kommunikationskanaler. I fråga om en artikel 29-begäran som riktar sig till en annan EU-medlemsstat måste dock en europeisk utredningsorder utfärdas och skickas via gängse kanaler.

Med nuvarande lagstiftning är uppfattningen att Sverige inte lever upp till Budapestkonventionens tydliga krav på enkel och skyndsam hantering av en begäran om bevarande. Utgående förelägganden om bevarande bör därför undantas från lagen om en europeisk utredningsorder t.ex. genom ändring av 1 kap. 7 a § lagen om internationell rättslig hjälp i brottmål. Det bör vidare finnas lagstöd för att behandla en inkommande begäran om bevarande från en EU-medlemsstat som en begäran om rättslig hjälp och att det således inte ska krävas att en europeisk utredningsorder utfärdas i dessa fall. Det bör också finnas stöd för att handlägga en inkommande begäran från övriga konventionsstater och som utformats i enlighet med konventionens formulär och/eller undertecknats av polis som en begäran om rättslig hjälp.

Det bedöms att dagens ordning, att åklagare fattar beslut om i ett ärende om inkommande begäran om bevarande medan Polismyndigheten är kontaktpunkt i ärendet bör bestå. Det finns en struktur kring samarbetet mellan EU-stater reglerad i bl.a. lagen

⁹ T-CY: Opinion of the T-CY on the competent authority for issuing a preservation request Åklagarmyndigheten har här hänvisat till yttrande från under Articles 29 and 35 Budapest Convention, T-CY (2017)18.

om europeisk utredningsorder (1 kap. 3 §) och med andra stater i lagen om internationell rättslig hjälp i brottmål (1 kap. 3–4 §§). Avsteg från denna struktur och den kompetensfördelning som i normalfallet råder mellan polis och rättslig myndighet behöver inte ske för att möta Budapestkonventionens krav. Däremot kan det framhållas den effektivitets- och tidsvinst som ett rent polisiärt förfarande skulle medföra. Det lindriga intrång som ett föreläggande om bevarande innebär talar för en sådan lösning.

11.5 Överväganden och förslag

11.5.1 Tillämpliga regler vid en begäran enligt artikel 29 i Budapestkonventionen

Förslag: Lagen om en europeisk utredningsorder ska inte gälla vid skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter enligt artikel 29 i Budapestkonventionen. I stället ska lagen om internationell rättslig hjälp i brottmål tillämpas vid en sådan begäran.

Bedömning: Att en begäran enligt artikel 29 även i förhållande till annat EU-land som deltar i det straffrättsliga samarbetet ska handläggas enligt lagen om internationell rättslig hjälp i brottmål kräver inte några ytterligare ändringar av den lagen.

Skälen för förslaget och bedömningen

Lagen om en europeisk utredningsorder ska inte tillämpas vid en begäran enligt artikel 29 i Budapestkonventionen

Som redovisats ovan infördes föreläggande om att bevara lagrade uppgifter enligt 27 kap. 16 § rättegångsbalken för att genomföra artikel 16 i Budapestkonventionen. Artikel 29 i konventionen, som är motsvarigheten i det gränsöverskridande samarbetet, hanterades genom att såväl lagen om internationell rättslig hjälp i brottmål som lagen om en europeisk utredningsorder gjordes tillämplig vid ett föreläggande om bevarande enligt 27 kap. 16 § rättegångsbalken.

Att lagen om en europeisk utredningsorder, och inte enbart lagen om internationell rättslig hjälp i brottmål, omfattar nämnda åtgärd är en följd av de skyldigheter som direktivet om en europeisk utredningsorder ålägger en medlemsstat. Dessa skyldigheter innebär bl.a. att de åtgärder som finns i nationell rätt och som syftar till att hämta in bevis ska omfattas av aktuellt regelverk och att regelverket som huvudregel också ska gälla framför andra internationella avtal som reglerar motsvarande samarbete. Av sistnämnda skäl anges i 1 kap. 7 a § lagen om internationell rättslig hjälp i brottmål att den lagen inte gäller om lagen om en europeisk utredningsorder är tillämplig.

Artikel 29 i Budapestkonventionen tillhandahåller ett effektivt verktyg för en brottsbekämpande myndighet i en konventionsstat att snabbt säkra uppgifter i elektronisk form som finns lagrade i en annan konventionsstat. Det framgår tydligt av den förklarande rapporten att en artikel 29-begäran ska hanteras skyndsamt och utan tillämpning av det mer formella och tidsödande förfarandet som följer av en ansökan om rättslig hjälp (p. 282 och 283). Syftet med artikel 29 är helt enkelt att frångå en mer formell ordning och få till ett snabbt och effektivt förfarande så att lagrade uppgifter i elektronisk form, vilka är viktiga såsom bevisning, inte går förlorade. För att åstadkomma detta behöver, såsom redovisats ovan, en ansökan inte innehålla lika många uppgifter som en traditionell ansökan och den kan göras av en polismyndighet. Vidare skapades särskilda kommunikationskanaler för att snabba på förfarandet. Detta syfte gör sig gällande även i dag, trots att samarbetet har utvecklats, bl.a. genom direktivet om en europeisk utredningsorder som mellan EU-staterna i huvudsak har ersatt det mer traditionella samarbetet om ömsesidig rättslig hjälp i brottmål.

Åklagarmyndigheten har i sin framställan pekat på att en artikel 29-begäran från eller till en EU-stat som ska hanteras enligt lagen om en europeisk utredningsorder medför problem. Till att börja med finns en diskrepans gentemot andra EU-stater eftersom de anser att en europeisk utredningsorder inte ska utfärdas för att skyndsamt säkra datorbehandlingsbara uppgifter enligt artikel 29. Enligt Åklagarmyndigheten utfärdar inte heller andra stater en europeisk utredningsorder när de med stöd av artikel 29 vill få hjälp med att säkra nämnda uppgifter. En tillämpning av lagen om en europeisk utredningsorder medför även praktiska tillämpningsproblem och

en risk för att det tar längre tid eftersom regelverket kring en europeisk utredningsorder är mer formaliserat.

De problem som Åklagarmyndigheten lyfter fram bör rättas till, bl.a. mot bakgrund av hur pass viktigt det är att se till att betydelsefull bevisning inte går förlorad på grund av att svenska myndigheter tillämpar ett mer formaliserat förfarande än nödvändigt. Ett annat skäl är också den allmänna utgångspunkten att Sverige ska leva upp till de åtaganden som följer av Budapestkonventionen, vilket uppenbarligen andra EU-stater inte anser att Sverige gör när svenska myndigheter tillämpar regelverket om en europeisk utredningsorder.

Såvitt får förstås av myndighetens framställan fungerar en hantering av en artikel 29-begäran med stöd av lagen om internationell rättslig hjälp i brottmål utan några större problem (oaktat att samarbetet sker i en ”rättslig hjälp”-kontext, jfr den förklarande rapporten p. 282 och 283). Problemet ligger i stället i att myndigheterna ser sig skyldiga att tillämpa lagen om en europeisk utredningsorder eftersom den har företräde framför lagen om internationell rättslig hjälp i brottmål (se 1 kap. 7 a § i sistnämnda lag).

En lösning skulle kunna vara att undanta en åtgärd enligt 27 kap. 16 § rättegångsbalken från tillämpningsområdet för lagen om en europeisk utredningsorder. Då skulle endast lagen om internationell rättslig hjälp i brottmål vara tillämplig i det gränsöverskridande samarbetet. Som anförts ovan är dock detta inte möjligt med hänsyn till de åtaganden som följer av direktivet om en europeisk utredningsorder om att de straffprocessuella åtgärder som finns tillgängliga i nationell rätt även ska omfattas av nämnda regelverk.

Den lösning som i stället bör väljas är att begäran enligt artikel 29 i Budapestkonventionen undantas från tillämpningsområdet för lagen om en europeisk utredningsorder. Då undviks det mer formella förfarandet som följer av tillämpningen av denna lag. I stället bör lagen om internationell rättslig hjälp i brottmål tillämpas. Den lagen har en större flexibilitet när det gäller dels vad en ansökan ska innehålla, dels vem som kan ansöka om föreläggande att bevara lagrade uppgifter. Tillämpningen av lagen om internationell rättslig hjälp i brottmål torde således bättre möta de krav som följer av artikel 29. Den lagtekniska lösningen som bör väljas är att dels i lagen om en europeisk utredningsorder föreskriva att den lagen inte gäller vid en artikel 29-begäran och att i stället ska lagen om

internationell rättslig hjälp i brottmål tillämpas, dels i sistnämnda lag upplysa om att den lagen gäller vid en artikel 29-begäran. En motsvarande lagteknisk lösning används i förhållandet mellan lagen om en europeisk utredningsorder och lagen (2003:1174) om vissa former av internationellt samarbetet i brottsutredningar (se 1 kap. 5 § respektive 1 a §).

Den föreslagna lösningen hindrar inte heller en utfärdande myndighet i en medlemsstat i EU eller en svensk åklagare att utfärda en europeisk utredningsorder för föreläggande om bevarande av lagrade uppgifter enligt 27 kap. 16 § rättegångsbalken. Om den utfärdande myndigheten i den andra medlemsstaten eller en svensk åklagare ser ett behov av att tillämpa detta regelverk bör det inte finnas några hinder mot detta. Ett sådant säkrande sker dock inte med stöd av artikel 29 i Budapestkonventionen utan med stöd av direktivet om en europeisk utredningsorder.

Artikel 34 i direktivet om en europeisk utredningsorder

I sammanhanget bör noteras artikel 34 i direktivet om en europeisk utredningsorder som reglerar direktivets förhållande till andra internationella avtal.

Huvudregeln är att direktivet ska ersätta de rättsliga instrument som anges i artikel 34.1 och 34.2. Budapestkonventionen nämns inte. För att en EU-stat ska kunna tillämpa andra internationella avtal, bortsett från de som anges i artikel 34.1 och 34.2, ställs dock vissa krav upp. Till att börja med krävs att avtalet ytterligare stärker syftena med direktivet och bidrar till att förenkla eller ytterligare underlätta förfarandena för inhämtning av bevis och under förutsättning att de skyddsnivåer som anges i direktivet respekteras. För det andra krävs enligt artikel 34.4 av den medlemsstat som vill tillämpa ett sådant avtal att en anmälan har gjorts till kommissionen vid en viss tidpunkt.

Artikel 34 i direktivet ersätter dock endast ”motsvarande bestämmelser” i de rättsakter som räknas upp, vilket rimligen även måste avse andra internationella avtal som en EU-stat med stöd av artikel 34.3 vill tillämpa. Om ett sådant internationellt avtal reglerar en åtgärd som inte har ersatts eller har sin motsvarighet i direktivet

kan det i vart fall enligt artikel 34 inte finnas något hinder mot att tillämpa det andra avtalet.

Mellan medlemsstaterna i EU har det diskuterats om direktivet har ersatt bestämmelserna i Budapestkonventionen, dvs. om det rör sig om motsvarande bestämmelser. Andra EU-staters reaktioner, vilka framgår av Åklagarmyndighetens framställan, indikerar att den åtgärd som avses i artikel 29 i Budapestkonventionen inte har ersatts av direktivet. I slutändan är det dock EU-domstolen som avgör direktivets tillämpningsområde och tolkningen av artikel 34. För svenskt vidkommande torde det dock vara svårt att hävda att det inte rör sig om motsvarande bestämmelser med tanke på att bestämmelser om bevarandeföreläggande infördes i lagen om en europeisk utredningsorder just för att omhänderta samarbetet mellan medlemsstaterna enligt artikel 29 i Budapestkonventionen.

Artikel 29 i Budapestkonventionen får däremot under alla förhållanden anses utgöra en sådan bestämmelse som förstärker samarbetet mellan medlemsstaterna som artikel 34.3 i direktivet om en europeisk utredningsorder åsyftar. En artikel 29-begäran stärker syftena med direktivet och bidrar till att förenkla och effektivisera förfarandet för bevisinhämtning, vilket Åklagarmyndighetens framställan tydligt indikerar.

En aspekt att hantera är dock anmälningsskyldigheten enligt artikel 34.4 i direktivet. Enligt den bestämmelsen skulle en medlemsstat som ville tillämpa ett befintligt internationellt avtal ha anmält detta den senast den 22 maj 2017 eller, om det rör sig om ett avtal som ingås därefter, tre månader från det datum då överenskommelsen undertecknades av medlemsstaten i fråga. För Sveriges skulle således en anmälan senast ha skett i samband med genomförandet av direktivet 2017. Någon sådan anmälan har inte skett.

Vi anser emellertid att det förslag som lämnas om att lagen om en europeisk utredningsorder inte ska tillämpas vid en artikel 29-begäran, trots formaliabristen, är förenlig med grunderna för direktivet.

Ett viktigt syfte med direktivet är att effektivisera och förenkla det straffrättsliga samarbetet mellan medlemsstaterna, bl.a. genom att frånga det ofta formaliatunga och tidsödande samarbetet om rättslig hjälp i brottmål. Eftersom direktivet grundar sig på principen om ömsesidigt erkännande ställs dock vissa krav på innehållet i en europeisk utredningsorder, dvs. det formulär som ska fyllas i,

och förfarandet för att utfärda, erkänna och verkställa en sådan order. Samarbetet mellan medlemsstaterna vad gäller bevisinhämtning fungerar också väl enligt detta regelverk. Artikel 34.3 i direktivet ger dock den flexibilitet som behövs för de medlemsstater som vill gå än längre och effektivisera samarbetet, vilket en artikel 29-begäran gör. I sak kan det således inte finnas några invändningar mot att Sverige inte använder sig av lagen om en europeisk utredningsorder vid en artikel 29-begäran, utan tvärtom tillämpar ett smidigare förfarande som ökar förutsättningarna att bekämpa och beivra brott, vilket är ett övergripande mål för EU. Dessutom tycks medlemsstaterna inte heller använda sig av direktivet för en artikel 29-begäran, vilket ger ytterligare stöd för att Sverige bör kunna undanta direktivet, även om det kan vara så att en eller flera medlemsstater gör den bedömningen att direktivet över huvud taget inte ersätter artikel 29 i Budapestkonventionen.

Eftersom det föreslås att lagen om en europeisk utredningsorder och indirekt direktivet inte ska tillämpas vad avser en artikel 29-begäran, bör rådande formaliabrist kunna hanteras genom att det görs en anmälan i efterhand. En anmälan sker i syfte att anpassa Sveriges tillämpning av artikel 29 i Budapestkonventionen i enlighet med den praxis som övriga medlemsstater tillämpar. I annat fall skulle en diskrepans uppstå genom att Sverige och andra medlemsstater tillämpar olika regelverk, vilket inte kan vara avsett.

Sammanfattningsvis anser vi att förslaget om att en artikel 29-begäran alltid ska hanteras enligt lagen om internationell rättslig hjälp i brottmål och inte lagen om en europeisk utredningsorder är förenligt med direktivet.

Ytterligare ändringar i lagen om internationell rättslig hjälp i brottmål behövs inte

Som angetts i avsnitt 11.4.2 ska rättslig hjälp i form av föreläggande om att bevara lagrade uppgifter lämnas under samma förutsättningar som en motsvarande åtgärd under en svensk förundersökning. Det innebär att de förutsättningar som gäller enligt 27 kap. 16 § rättegångsbalken även gäller vid lämnande av rättslig hjälp, bl.a. om när en sådan åtgärd kan vidtas och hur länge uppgifterna kan vara bevarade (se 2 kap. 1 § lagen om internationell rättslig hjälp i brottmål).

I 2 kap. 2 § lagen om internationell rättslig hjälp i brottmål gjordes ett tillägg med innebörden att något krav på dubbel straffbarhet inte ställs upp för en åtgärd enligt 27 kap. 16 § rättegångsbalken, vilket motsvarar artikel 29.3 i Budapestkonventionen. Några ytterligare ändringar med hänsyn till övriga bestämmelser i artikel 29 i Budapestkonventionen om bl.a. ansökans innehåll, vägransgrunder och sekretess ansåg regeringen inte behövdes.¹⁰ Inte heller fanns det några behov av ändringar i lag när det gäller införandet av ett 24/7-nätverk enligt artikel 35 i konventionen.¹¹

Det är också denna ordning som i dag tillämpas när stater utanför EU gör en artikel 29-begäran. Att EU-staterna kommer förslagsvis inlemmas i samma regelverk medför inget behov av ytterligare ändringar i lagen om internationell rättslig hjälp i brottmål. Det innebär att bestämmelserna 2 kap. 3, 4 och 6 §§ i nämnda lag om vem kan göra en ansökan, om ansökans innehåll och om hur en ansökan sänds över även kan tillämpas i förhållande till en artikel 29-begäran från en annan EU-stat. Detsamma gäller tillämpningen av vägransgrunderna i 2 kap. 14 §. Bestämmelserna innebär bl.a. att en ansökan kan göras av en polisiär myndighet i en annan stat och att en ansökan kan skickas via 24/7-nätverket. I förhållande till 2 kap. 3 och 6 §§ lagen om internationell rättslig hjälp i brottmål bör en upplysning göras på regeringens hemsida om att Budapestkonventionen även är en sådan internationell överenskommelse som avses i nämnda bestämmelser.

11.5.2 Åklagare ska alltjämt besluta i ett ärende enligt artikel 29 i Budapestkonventionen

Bedömning: En ansökan om rättslig hjälp med ett föreläggande att bevara en viss lagrad uppgift enligt artikel 29 i Budapestkonventionen ska även fortsättningsvis handläggas av en åklagare.

Skälen för bedömningen: Enligt artikel 35.1 i Budapestkonventionen ska konventionsstaterna tillsätta en kontaktpunkt som ska vara tillgänglig 24 timmar om dygnet sju dagar i veckan för att säkerställa omedelbar hjälp vid utredning och lagföring av brott

¹⁰ Prop. 2020/21:72 s. 33–34.

¹¹ Prop. 2020/21:72 s. 64.

som är relaterade till datorsystem och datorbehandlingsbara uppgifter eller för insamling av bevis i elektronisk form om brott. Det krävs dock inte att den myndighet som mottar begäran enligt artikel 35.1 också fattar beslut om åtgärd. Av artikel 35.2 b följer att det är tillräckligt med skyndsam samverkan med den beslutande myndigheten.

Förordningen med instruktion för Polismyndigheten ger Polismyndigheten uppdrag att vara kontaktpunkt enligt artikel 35.1.

Som följer av avsnitt 11.3.2 handläggs en ansökan om ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken av åklagare (4 kap. 24 c § lagen om internationell rättslig hjälp i brottmål).

Åklagarmyndigheten har, som redovisats i avsnitt 11.4, väckt frågan om en ansökan av effektivitetsskäl bör kunna handläggas av Polismyndigheten.

Vid införandet av bestämmelsen i 27 kap. 16 § rättegångsbalken gjorde regeringen bedömningen att utgångspunkten bör vara att en ansökan om rättslig hjälp i fråga om en sådan åtgärd prövas av en åklagare, i likhet med vad som gäller motsvarande nationella ärenden.¹² Det har inte framkommit några bärande skäl att ändra denna ordning. Åklagarmyndigheten konstaterar också i sin framställan att avsteg från den kompetensfördelning som i normalfallet råder mellan Polismyndigheten och rättslig myndighet inte behöver ske för att möta Budapestkonventionens krav. Åklagare ska således även fortsättningsvis handlägga ansökan om rättslig hjälp avseende ett föreläggande att bevara viss lagrad uppgift.

¹² Prop. 2020/21:72 s. 33.

12 Det andra tilläggsprotokollet till Budapestkonventionen

12.1 Inledning

I november 2021 antog Europarådets ministerkommitté det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet (Budapestkonventionen). Sverige undertecknade protokollet den 12 maj 2022.

Det andra tilläggsprotokollet innehåller bestämmelser som syftar till att ge de brottsbekämpande myndigheterna nya och mera effektiva verktyg för gränsöverskridande åtkomst till elektroniska bevis. Det handlar om möjligheter för behöriga myndigheter i en stat att i brottsutredande syfte dels vända sig till privata aktörer i en annan stat för att få ut domän- och abonnemangsuppgifter, dels vända sig till behöriga myndigheter i den andra staten för verkställighet av en order om utlämnade av abonnemangs- och trafikuppgifter. Vidare finns bestämmelser som syftar till att stärka det rättsliga samarbetet mellan konventionsstaterna, bl.a. i nödsituationer och utökat användande av 24/7-nätverket som inrättades genom artikel 35 i Budapestkonventionen.

Bestämmelserna i det andra tilläggsprotokollet faller inom ett område som i stor utsträckning omfattas av EU-gemensamma regler och därmed unionens exklusiva externa befogenhet. Unionen kan emellertid inte underteckna protokollet, eftersom endast stater kan bli parter i det. Genom ett beslut av rådet den 14 februari 2023 bemyndigades medlemsstaterna att i unionens intresse ratificera protokollet.

Frågan om vilka ändringar av nationell rätt som kan krävas med anledning av det andra tilläggsprotokollet har i viss mån beröring med vilka ändringar i svensk rätt som krävs med anledning av de nya EU-rättsakterna om åtkomst till elektroniska bevis (se avsnitten 6–10).

De ändringar som kan krävas i nationell rätt kan vidare komma att påverkas av innehållet i nämnda rådsbeslutet. Vi ska därför kartlägga vilka svenska bestämmelser som berörs av det andra tilläggsprotokollet och analysera om de svenska bestämmelserna bör ändras eller kompletteras. Vidare ska vi föreslå de eventuella förbehåll och förklaringar som bör göras i samband med ett tillträde samt ta ställning till vilken eller vilka myndigheter som bör utses till behöriga myndigheter för förfarandena i det andra tilläggsprotokollet, och lämna nödvändiga författningsförslag.

I avsnitt 12.2 redogörs översiktligt för innehållet i det andra tilläggsprotokollet. Därefter följer i avsnitt 12.3 vår bedömning i fråga om Sveriges tillträde till det andra tilläggsprotokollet. I avsnitt 12.4–12.10 redogörs för våra överväganden och förslag i förhållande till de olika artiklarna i protokollet. Slutligen finns i avsnitt 12.11 våra överväganden och förslag i fråga om vilka förklaringar och under rättelser som Sverige bör lämna i anslutning till tillträdet till protokollet.

12.2 Kort om innehållet i det andra tilläggsprotokollet

För en kortare beskrivning av Budapestkonventionen och dess första tilläggsprotokoll hänvisas till avsnitt 11.1.

Mot bakgrund av den snabba teknikutvecklingen och inte minst den ökade användningen av s.k. molntjänster inleddes 2017 ett arbete med att ta fram ett nytt tilläggsprotokoll till Budapestkonventionen. Europarådet antog den 17 november 2021 det andra tilläggsprotokollet till Budapestkonventionen om it-brottslighet (ETS 224). Tilläggsprotokollet öppnades för undertecknande den 12 maj 2022 och träder i kraft efter att fem konventionsstater har ratificerat protokollet. Hittills har 45 stater undertecknat protokollet, däribland Sverige, och två stater har ratificerat det.

Som utvecklats inledningsvis syftar det andra tilläggsprotokollet till att ytterligare stärka samarbetet om it-brottslighet och insamling av bevis i elektronisk form för brott i samband med särskilda brottsutredningar eller straffrättsliga förfaranden. Protokollet innehåller därför bestämmelser om effektivare ömsesidig rättslig hjälp och andra former av samarbete mellan behöriga myndigheter samt om direkt samarbete mellan behöriga myndigheter och tjänste-

leverantörer och andra enheter som innehar eller kontrollerar relevant information.

Det andra tilläggsprotokollet är indelat i fyra kapitel. Dessa innehåller gemensamma bestämmelser (kapitel I), bestämmelser om åtgärder för utökat samarbete (kapitel II), bestämmelser om villkor och garantier vilket inkluderar detaljerade bestämmelser om dataskydd (kapitel III) och slutbestämmelser (kapitel IV).

I kapitel I (artiklarna 1–4) finns bestämmelser om tillämpningsområdet, definitioner och språk.

I kapitel II, som utgör protokollets huvudsakliga innehåll är bestämmelserna uppdelade i fem avsnitt.

Bestämmelserna i avsnitt 1 (artikel 5) innehåller allmänna principer som är tillämpliga på kapitel II.

Avsnitt 2 innehåller bestämmelser (artiklarna 6 och 7) om att behöriga myndigheter i en konventionsstat ska kunna vända sig till privata aktörer i en annan konventionsstat för att få ut domännamns- och abonnemangsuppgifter. Konventionsstaterna ska även se till att privata aktörer på dess territorium har möjlighet att svara på en sådan framställan.

I avsnitt 3 finns en bestämmelse om att behöriga myndigheter i en stat ska kunna vända sig till behöriga myndigheter i den andra staten för verkställighet av en order om utlämnade av abonnemangs- och trafikuppgifter med extra skyndsamhet (artikel 8). I avsnittet finns också en bestämmelse (artikel 9) om påskyndat utlämnande av lagrade datorbehandlingsbara uppgifter i en nödsituation via det 24/7-nätverk som inrättats genom artikel 35 i konventionen.

Bestämmelserna i avsnitt 4 reglerar under vilka omständigheter en stat kan ansöka om ömsesidig rättslig hjälp enligt ett skyndsamt förfarande om det föreligger en nödsituation (artikel 10).

Slutligen innehåller avsnitt 5 bestämmelser om förfarande för internationellt samarbete i avsaknad av tillämpliga internationella avtal. Bestämmelserna i det avsnittet behandlar frågor om videokonferens med vittnen eller sakkunniga (artikel 11) och om gemensamma utredningsgrupper och gemensamma utredningar (artikel 12).

Kapitel III innehåller bestämmelser om villkor och garantier samt dataskydd (artiklarna 13 och 14).

I det sista kapitlet finns slutbestämmelser (artiklarna 15–25).

12.3 Sverige ska tillträda det andra tilläggsprotokollet till Budapestkonventionen

Förslag: Riksdagen ska godkänna att Sverige tillträder det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet.

Skälen för förslaget: När Sverige tillträdde Budapestkonventionen och det första tilläggsprotokollet konstaterade regeringen att it-relaterade brott snabbt kan få stor omfattning och spridning, bevis kan utplånas och ekonomiskt utbyte av brott flyttas mellan länder på mycket kort tid samt att vissa it-relaterade brott bara kan utredas om de brottsbekämpande myndigheterna får tillgång till uppgifter om elektronisk kommunikation.¹ Regeringen menade vidare att det finns starka skäl att Sverige deltar aktivt i det internationella samarbetet mot it-brottslighet, varför det föreslogs att Sverige skulle ratificera Budapestkonventionen och tilläggsprotokollet.

Som framgår av föregående avsnitt syftar det andra tilläggsprotokollet till att ytterligare stärka samarbetet om it-brottslighet och insamling av bevis i elektronisk form i samband med särskilda brottsutredningar eller straffrättsliga förfaranden. Samma skäl som regeringen anförde inför att Sverige tillträdde Budapestkonventionen gör sig därför gällande i fråga om det andra tilläggsprotokollet.

Vidare följer det av rådets beslut (EU) 2023/436 av den 14 februari 2023 om bemyndigande för medlemsstaterna att i Europeiska unionens intresse ratificera det andra tilläggsprotokollet till konventionen om it-brottslighet om utökat samarbete och utlämnande av elektroniska bevis (rådsbeslutet 2023/436) att EU-länderna bemyndigas att i unionens intresse ratificera det andra tilläggsprotokollet. Rådsbeslutet är bindande för medlemsstaterna.

Eftersom ett tillträde medför lagändringar krävs riksdagens godkännande (se 10 kap. 3 § regeringsformen). Vi föreslår således att riksdagen godkänner att Sverige tillträder det andra tilläggsprotokollet till Budapestkonventionen.

I avsnitten 12.4–12.10 övervägs i vilken omfattning de olika artiklarna i det andra tilläggsprotokollet föranleder några ändringar

¹ Prop. 2020/21:72 s. 20–21.

i lag eller förordning. Sverige lämnade inga förbehåll vid under-tecknandet av tilläggsprotokollet. Möjligheten att göra det kvarstår emellertid fram till ratificeringen. I rådsbeslutet 2023/436 uppmanas eller rekommenderas medlemsstaterna att lämna eller avstå från vissa förbehåll eller förklaringar. Dessa frågor tas upp i anslutning till våra överväganden beträffande respektive artikel samt sammanfattningsvis i avsnitt 12.11. I sistnämnda avsnitt behandlas även frågan om att Sverige till kommissionen ska meddela att Sverige kommer att tillämpa det andra tilläggsprotokollet tillsammans med EU-förordningen och direktivet om en europeisk utredningsorder.

12.4 Inhämtande av information om domännamn (artikel 6)

12.4.1 Det närmare innehållet i artikel 6

I artikel 6 i det andra tilläggsprotokollet föreskrivs ett samarbete som innebär att en myndighet i en konventionsstat kan begära ut information om domännamnsregistrering hos en enhet som tillhandahåller domännamnsregistreringstjänster på en annan stats territorium. I det mellanstatliga samarbetet är artikel 6 (och artikel 7, se avsnitt 12.5) något nytt på så sätt att en myndighet i en stat kan vända sig direkt till en privat aktör i en annan stat för att hämta in bevis utan att först kontakta en myndighet i den sistnämnda staten. Samarbetet liknar i det avseende samarbetet enligt EU-förordningen.

Den information som artikel 6 avser innehas av enheter som tillhandahåller domännamnsregistreringstjänster. Sådana aktörer är enligt den förklarande rapporten dels regionala eller nationella registeroperatörer (ofta kallad ”registry” eller registreringsenhet för toppdomäner) vilka håller auktoritativa databaser över alla domännamn som är registrerade för en toppdomän och som accepterar registreringsförfrågningar, dels aktörer som säljer domännamn till allmänheten, även kallade ”registrarer” (p. 75).

Många it-relaterade brott sker genom att domäner skapas eller utnyttjas för skadliga och olagliga syften, t.ex. för spridning av skadlig programvara, nätfiske, bedrägerier, distribution av barnpornografi och för andra kriminella ändamål. Tillgång till information om vem som har registrerat en domän är därför enligt den

förklarande rapporten ofta ett första steg i en brottsutredning och avgörande för att identifiera en misstänkt i en specifik brottsutredning eller straffrättsligt förfarande (p. 73 och 74).

Enligt artikel 6.1 ska varje part anta den lagstiftning och de andra åtgärder som krävs för att ge sina behöriga myndigheter befogenhet att i samband med en brottsutredning rikta en framställning till en enhet som tillhandahåller tjänster för domännamnsregistrering på en annan parts territorium. Syftet är att tillhandahålla ett effektivt ramverk för att en brottsutredande myndighet i en konventionsstat snabbt ska få information som enheten innehar eller kontrollerar för att identifiera eller kontakta innehavaren² av ett domännamn, vilket också betonas i den förklarande rapporten (p. 76). En framställan enligt artikel 6.1 görs således utan att kontakta någon myndighet i den stat där enheten finns. De uppgifter som efterfrågas torde ofta vara namn, fysisk adress, e-postadress och telefonnummer. Det ska noteras att det är endast uppgifter som en enhet innehar som kan begäras ut.

I den förklarande rapporten framhålls att det är upp till varje part att avgöra på vilket sätt och av vem en framställan görs eftersom det kan variera mellan staterna så länge det görs av en behörig myndighet (p. 77). Med behörig myndighet avses enligt artikel 3.2 b en ”rättslig, administrativ eller annan brottsbekämpande myndighet som enligt nationell rätt har befogenhet att beordra, godkänna eller genomföra åtgärder enligt detta protokoll i syfte att samla in eller lägga fram bevis i samband med särskilda brottsutredningar eller straffrättsliga förfaranden”. I rapporten framhålls även att en framställan inte är bindande för den enhet som tar emot en framställan (p. 77). Slutligen kan noteras att med begreppet enhet som tillhandahåller tjänster för domännamnsregistrering avses såväl registreringsenhet för toppdomäner som återförsäljare av domännamn (p. 79).

Artikel 6.2 anger att varje part ska anta den lagstiftning och de andra åtgärder som krävs för att göra det möjligt för en enhet på dess territorium att lämna ut sådan information som svar på en framställning enligt artikel 6.1, med förbehåll för rimliga villkor i nationell rätt. Bestämmelsen kräver således inte att den enhet som

² I den svenska översättningen av artikel 6.1 har begreppet ”registrant” översatts till ”registraren”. Begreppet bör dock översättas till innehavare, vilket följer av den förklarande rapporten p. 74.

tar emot en framställan ska vara skyldig att lämna ut informationen, men i den förklarande rapporten betonas att protokollet innehåller krav på när och av vem en framställan kan göras samt regler om dataskydd som ska skapa förutsättningar för att kunna besvara en framställan (p. 82 och 83).

I artikel 6.3 finns bestämmelser om vilka uppgifter en framställan enligt artikel 6.1 ska innehålla; bl.a. uppgifter om den myndighet som gör framställan och att det sker enligt protokollets krav, det domännamn om vilket information söks samt om när uppgifterna behövs. Med stöd av artikel 6.4 kan en framställan göras i elektronisk form, om det är godtagbart för den enhet som tar emot framställan. I dessa fall får lämpliga säkerhets- och autentiseringsnivåer krävas. Parterna och enheterna kan vidare enligt den förklarande rapporten komma överens om säkra kanaler eller medel för överföring och om autentisering ska användas eller om särskilt säkerhetsskydd (inklusive kryptering) kan vara nödvändigt i ett särskilt känsligt fall (p. 86).

Om en enhet inte samarbetar får den ansökande staten enligt artikel 6.5 begära att enheten anger skälen till att den inte lämnar ut den begärda informationen. Som nämnts tidigare finns ingen skyldighet att lämna ut information, men i den förklarande rapporten anges att om förutsättningarna i protokollet är uppfyllda förväntas att informationen lämnas ut (p. 87). Om informationen inte lämnas ut får den ansökande staten, via den behöriga myndigheten enligt samma bestämmelse, samråda med en utsedd myndighet i den stat där enheten finns om vilka åtgärder som är tillgängliga för att få ta del av informationen. Varje stat ska utse en sådan myndighet och se till att hålla all relevant information uppdaterad, vilket följer av artiklarna 6.6 och 6.7.

12.4.2 Gällande rätt

Lagen (2006:24) om nationella toppdomäner för Sverige på internet (toppdomänlagen) reglerar teknisk drift av nationella toppdomäner för Sverige på internet samt tilldelning och registrering av domännamn under dessa toppdomäner (1 §). Termen domännamn definieras i 2 § som ett unikt namn sammansatt av domäner, där en i

domännamssystemet lägre placerad domän står före en domän som är högre placerad i systemet.

I 6 § nämnda lag anges att domänadministratören, dvs. den som ansvarar för administration av en nationell toppdomän för Sverige, ska föra ett register över tilldelade domännamn under toppdomänen och löpande upprätta säkerhetskopior av registeruppgifterna. Registret ska innehålla

- domännamnet,
- namnet på domännamnsinnehavaren och dennes postadress, telefonnummer och adress för elektronisk post,
- namnet på den som tekniskt administrerar domännamnet och dennes postadress, telefonnummer och adress för elektronisk post,
- uppgifter om de namnservrar som är knutna till domännamnet, samt
- övrig teknisk information som behövs för att administrera domännamnet.

Uppgifterna i registret ska kunna hämtas in utan avgift via internet. Personuppgifter får endast göras tillgängliga på detta sätt om den registrerade har samtyckt till det. Domänadministratören är personuppgiftsansvarig för behandling av personuppgifter i registret.

Enligt 9 § 2 toppdomänlagen får regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten meddela föreskrifter om register och säkerhetskopior enligt 6 § Post- och telestyrelsen (PTS) har denna behörighet enligt 3 § förordningen (2006:25) om nationella toppdomäner för Sverige på internet.

Ett av syftet med registret som regleras i toppdomänlagen är att det kan användas av rättsvårdande myndigheter på nationell nivå för att identifiera ansvariga för domännamn till vilka webbplatser med olagligt innehåll finns kopplade.

I Sverige ansvarar Stiftelsen för Internetinfrastruktur (Internetstiftelsen) för den svenska toppdomänen ".se", avseende registrering av domännamn, samt administration och teknisk drift av det nationella domännamnsregistret. Internetstiftelsen ska alltså i egen skap av domänadministratör för toppdomänen ".se" föra registret över tilldelade domännamn under toppdomänen. Internetstiftelsen

sköter också drift och administration av toppdomänen ".nu", som dock inte omfattas av toppdomänlagen. Internetstiftelsen är således den "registry" eller registreringsenhet för toppdomäner som beskrivs i den förklarande rapporten (p. 75). I det följande använder vi begreppet registreringsenhet för toppdomäner för att benämna en aktör som Internetstiftelsen, och således inte det nationella begreppet domänadministratör. Detta då begreppet registreringsenhet för toppdomäner används i EU-lagstiftningen (se avsnitt 12.4.3 nedan).

Återförsäljare av domännamn kallas ombud eller registrar (se även ovan). Dessa är ofta också värdtjänstleverantörer, som erbjuder både domännamn och webbhotell. För registrering av en ny domän krävs alltså kontakt med en återförsäljare. Ungefär 140 återförsäljare hanterar svenska domäner (enligt Internetstiftelsen hemsida). Dessa återförsäljare omfattas dock inte av toppdomänlagens bestämmelser.

Bakom varje domännamn finns en IP-adress, som används av datorer när de kommunicerar med varandra. IP-adressen utgörs av en rad siffror, och domännamnet kan sägas utgöra en översättning av siffrorna till bokstäver. En IP-adress kan alltså beskrivas som andra sidan av ett domännamn. I begreppet abonnemangsuppgifter i svensk rätt ingår uppgifter om IP-adresser. Enligt 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation är de tillhandahållare av elektroniska kommunikationstjänster som omfattas av bestämmelsen skyldiga att på begäran av brottsbekämpande myndigheter lämna ut uppgifter om abonnemang (se även avsnitt 4.4.2). Registreringsenheten för toppdomäner (dvs. Internetstiftelsen i Sverige) eller återförsäljare av domännamn omfattas emellertid inte av lagen om elektronisk kommunikation eftersom de inte anses tillhandahålla ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. De brottsbekämpande myndigheterna kan därför inte med stöd av nämnda lag begära ut uppgifter om domännamn från dessa aktörer. Inhämtning av sådana uppgifter sker i stället genom en förfrågan till Internetstiftelsen, som är ansvarig för att föra register över uppgifter om domännamn (se avsnitt 6.2.4). Internetstiftelsen, i dess egenskap av personuppgiftsansvarig för uppgifterna enligt EU:s dataskyddsförordning, lämnar ut uppgifter ur registret efter en prövning om det finns en rättslig grund för utlämnande av personuppgifter, enligt bestämmelserna i

dataskyddsförordningen. Utlämnande av uppgifter till brottsbekämpande myndigheter sker enligt Internetstiftelsen med stöd av den rättsliga grunden *berättigat intresse*. Vissa utredande och verkställande myndigheter kan förplikta Internetstiftelsen att lämna ut uppgifter. I dessa fall har Internetstiftelsen en rättslig förpliktelse att tillhandahålla myndigheten de uppgifter som efterfrågas.

Som påpekats inledningsvis innebär artikel 6 en ny form av samarbete eftersom en begäran skickas direkt till en privat aktör. Några sådana samarbetsbestämmelser finns sålunda inte i svensk lag (se även avsnitt 4.5).

12.4.3 Föreslagna ändringar i toppdomänlagen

I delbetänkandet *Nya regler om cybersäkerhet* (SOU 2024:18) föreslås, förutom en ny cybersäkerhetslag, vissa ändringar i toppdomänlagen för att genomföra Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS2-direktivet).

Inledningsvis kan nämnas att i betänkandets förslag till cybersäkerhetslag definieras vissa begrepp som har motsvarigheter i artikel 6 i andra tilläggsprotokollet. Definitionerna i den föreslagna lagen återfinns i artikel 6.21 och 6.22 i NIS2-direktivet. Begreppet *domännamnsregistreringstjänster* definieras som ”registrar eller en annan verksamhetsutövare som verkar som ombud eller återförsäljare av domännamn”. *Registreringsenhet för toppdomäner* definieras i sin tur i lagförslaget som ”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”.

För att anpassa toppdomänlagen till NIS2-direktivets krav föreslås i betänkandet bl.a. att det uttryckligen ska följa av toppdomänlagen att myndigheter och andra med offentligrättsliga uppgifter inom EES ska kunna begära ut uppgifter ur registret på annat sätt av domänadministratören (dvs. registreringsenheten för toppdomäner) än genom internet samt att sådana uppgifter ska

lämnas skyndsamt. Utredningen har vidare föreslagit att PTS ska föreskriva närmare hur och inom vilka tidsgränser uppgiftsskyldigheten ska fullgöras.

I betänkandet övervägdes om ansvaret för att föra register samt lämna ut uppgifter ur registret även skulle åvila återförsäljare av domännamnsregistreringstjänster. För att motverka dubblerad insamling av registreringsuppgifter gjordes emellertid bedömningen att det är tillräckligt att det är registreringsenheten för toppdomäner som har ansvar för att föra register och lämna ut förda uppgifter till myndigheter och andra med offentligrättsliga uppgifter inom EES (se s. 188).

Det kan i sammanhanget nämnas att utredningen också har föreslagit att toppdomänlagen ska ändras på så sätt att den inte endast ska omfatta nationella toppdomäner för Sverige, utan även toppdomänen ".nu" (se s. 392). Betänkandet bereds i skrivande stund inom Regeringskansliet.

12.4.4 En möjlighet att inhämta information om domännamn utomlands ska införas

Förslag: Svenska brottsutredande myndigheter ska kunna begära ut uppgifter från en registreringsenhet för toppdomäner eller återförsäljare av domännamn som erbjuder tjänster i en annan stat för att identifiera eller kontakta innehavaren av ett domännamn om uppgiften rör brottslig verksamhet eller misstanke om brott. De svenska myndigheter som ska omfattas är Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot ett brott eller brottslig verksamhet. En begäran ska endast kunna rikta sig till en aktör i en stat som har tillträtt det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet.

Bedömning: Bestämmelser om vilka uppgifter en begäran ska innehålla och vilket språk en begäran ska upprättas på eller översättas till samt sättet att sända över en begäran bör regleras i förordning.

Skälen för förslaget och bedömningen: Svenska brottsutredande myndigheter ska, som framgår ovan, enligt artikel 6 i andra tilläggsprotokollet till Budapestkonventionen ha möjlighet att begära ut uppgifter direkt från en registreringsenhet för toppdomäner (registry) eller en återförsäljare av domännamn (registrar) som erbjuder sina tjänster på sitt territorium för att identifiera eller kontakta innehavaren av ett domännamn. Sådana uppgifter torde i huvudsak omfatta namn, fysisk adress, e-postadress och telefonnummer.

I dag har svenska brottsutredande myndigheter inte någon möjlighet att direkt vända sig till en registreringsenhet för toppdomäner eller återförsäljare av domännamn utomlands. Ett sådant inhämtande sker på andra sätt, t.ex. genom rättslig hjälp i brottmål. För att uppfylla kraven i artikel 6.1 bör en sådan möjlighet införas i svensk rätt.

Mot bakgrund av att de uppgifter som avses i huvudsak motsvarar de uppgifter som inhämtas med stöd av 9 kap. 33 § första stycket 2 lagen (2022:482) om elektronisk kommunikation, bör de myndigheter som kan inhämta uppgifter med stöd av sistnämnda bestämmelse även vara behöriga att begära in uppgifter för att identifiera eller kontakta innehavaren av ett domännamn som innehas av en registreringsenhet för toppdomäner eller återförsäljare av domännamn utomlands. De myndigheter som avses är Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott eller brottslig verksamhet. En begäran bör emellertid endast kunna riktas till en aktör i en stat som tillträtt det andra tilläggsprotokollet till Budapestkonventionen.

När det gäller under vilka förutsättningar en begäran ska kunna göras anges i artikel 6.1 att uppgifter kan begäras i samband med särskilda brottsutredningar eller straffrättsliga förfaranden. Några ytterligare krav ställs inte, t.ex. att de inhämtade uppgifterna ska ha en viss betydelse för utredningen, vilket emellertid får antas då de begärs ut. Bestämmelsen får dock anses kräva att uppgifterna hämtas in i en specifik utredning eller förfarande och inte i största allmänhet.

Ett villkor för att hämta in uppgifter rörande ett domännamn bör vara att uppgifterna gäller brottslig verksamhet eller misstanke om brott, vilket skulle motsvara den reglering som finns i 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation. Ett

alternativ kan vara den reglering som finns om beslag i 27 kap. 1 § rättegångsbalken, dvs. en uppgift ska kunna begäras ut om det skäligen kan antas att den har betydelse för utredning av brott. Enligt vår mening bör det första alternativet väljas. Ett skäl är att de uppgifter som ska hämtas in är i mångt och mycket att likna vid abonnemangsuppgifter som hämtas in enligt lagen om elektronisk kommunikation och åtgärden bör således inte jämföras med tvångsmedel som beslag. Vidare bör uppgifterna kunna hämtas in även i de fall en förundersökning inte har inletts, t.ex. om en förutredning pågår och då kan en skrivning liknande den som finns i tvångsmedelbestämmelserna bli begränsande. Vårt förslag får anses leva upp till det krav som anges i artikel 6.1 om att det ska röra sig om särskilda brottsutredningar eller straffrättsliga förfaranden.

I artikel 6.3 och artikel 6.4 finns bestämmelser om dels vilka uppgifter en begäran enligt artikel 6.1 ska innehålla, dels om möjligheterna att översända en begäran i elektronisk form. Enligt vår uppfattning kan detta regleras i förordning. Detsamma gäller på vilket språk en begäran ska upprättad på eller översatt till (artikel 4.2).

12.4.5 Svenska aktörers skyldighet att lämna ut information om domännamn

Förslag: En registreringsenhet för toppdomäner eller återförsäljare av domännamn som erbjuder tjänster för domännamnregistrering i Sverige ska på begäran till en behörig myndighet i en annan stat som tillträtt det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet lämna ut uppgifter för att identifiera eller kontakta innehavaren av ett domännamn om uppgifterna rör brottslig verksamhet eller misstanke om brott. Uppgifterna ska lämnas ut om inte begäran är så bristfällig att den inte utan väsentlig olägenhet kan läggas till grund för ett utlämnande. Om en registreringsenhet för toppdomäner eller återförsäljare av domännamn inte lämnar ut några uppgifter ska den ange skälen för detta.

Åklagarmyndigheten ska utses till den myndighet som samråd ska ske med enligt artikel 6.5 i andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet.

En begäran som ställs till en registreringsenhet för domännamn eller återförsäljare av domännamn i Sverige ska vara skriven på eller översatt till svenska eller engelska eller det språk som godtas av mottagaren av begäran.

Bedömning: Bestämmelser om vilka uppgifter en begäran ska innehålla och sättet att sända över en begäran bör regleras i förordning.

Skälen för förslaget och bedömningen: På motsvarande sätt som i föregående avsnitt och för att leva upp till artikel 6.2 i andra tilläggsprotokollet till Budapestkonventionen bör det införas en bestämmelse i lag som ålägger en registreringsenhet för toppdomäner och återförsäljare av domännamn som erbjuder tjänster för domännamsregistrering i Sverige att på begäran lämna ut uppgifter för att identifiera eller kontakta innehavaren av ett domännamn. En sådan skyldighet bör endast gälla i förhållande till stater som har tillträtt den andra tilläggsprotokollet och avser endast uppgifter som innehas vid tidpunkten för begäran.

Artikel 6.2 innebär inte någon formell skyldighet en registreringsenhet för toppdomäner och återförsäljare av domännamn att lämna ut uppgifter. Bestämmelsen anger att information ska lämnas ut med förbehåll för rimliga villkor i nationell rätt. Tanken är dock att eftersom protokollet ställer upp villkor om att en begäran ska göras av en behörig myndighet i ett specifikt straffrättsligt förfarande, vilket myndigheten ska intyga, samt att staterna ska respektera de dataskyddsregler som åläggs genom artikel 14 (se avsnitt 12.9) bör några hinder mot att lämna ut uppgifterna inte föreligga i normalfallet.

Mot denna bakgrund bör de svenska bestämmelserna inte innebära ett absolut villkor att lämna ut uppgifter utan i vissa fall bör en svensk registreringsenhet för toppdomäner och återförsäljare av domännamn kunna neka detta. Samtidigt bör undvikas att dessa aktörer ska behöva göra ingående prövningar, vilket skulle förfela tanken med samarbetet enligt artikel 6. Dessutom ska påpekas att de uppgifter som kommer att begäras ut är för att identifiera eller kontakta innehavaren av ett domännamn. Av dessa skäl bör bestämmelsen formuleras på så sätt att uppgifterna ska lämnas ut om inte begäran är så bristfällig att den inte utan väsentlig olägenhet kan läggas till grund för ett utlämnande. En sådan bristfällighet kan

vara att det inte framgår klart vilket domännamn som avses. För en närmare beskrivning av dessa brister hänvisas till författningskommentaren (se avsnitt 15.4).

I föregående avsnitt har bedömningen gjorts att de aktuella uppgifterna ska kunna begäras ut av svenska behöriga myndigheter under förutsättning att uppgifterna gäller brottslig verksamhet eller misstanke om brott. Motsvarande gör sig gällande i fråga om skyldigheten för registreringsenheter för toppdomäner respektive återförsäljare av domännamn i Sverige att lämna ut uppgifter till myndigheter i annan stat som tillträtt det andra tilläggsprotokollet. Uppgifterna ska således lämnas ut om de gäller brottslig verksamhet eller misstanke om brott. Om den aktör som ska lämna ut uppgifterna anser att begäran har ett annat syfte så kan uppgifterna inte lämnas ut. I de fall några uppgifter inte lämnas ut ska registreringsenheten eller återförsäljaren ange skälen för detta, vilket följer av artikel 6.5.

Några sanktioner för att begärda uppgifter inte lämnas ut följer inte av artikel 6 och föreslås inte heller.

Enligt artikel 6.5 ska, för det fall begärda uppgifter inte lämnas ut, den behöriga myndighet som har begärt uppgifterna kunna vända sig till en myndighet i Sverige för att samråda om andra alternativ för att få tillgång till uppgifterna. Sverige ska enligt artikel 6.6 utse den myndighet som ska samråda med den utländska myndigheten. Med hänsyn till att det alternativ som främst torde stå till förfogande är internationell rättslig hjälp i brottmål eller utfärdande av en europeisk utredningsorder bör Åklagarmyndigheten utses till denna myndighet.

Av artikel 4.2 följer att en begäran enligt artikel 6 ska upprättas på eller översättas till ett språk som en registreringsenhet för toppdomäner och återförsäljare av domännamn godtar i ett jämförbart nationellt förfarande eller på ett annat språk som någon av dessa aktörer kan godta. Ett tydligt syfte med denna artikel är att skapa flexibilitet vad gäller språkkrav som ofta försvårar samarbetet i de fall stater kräver en översättning till sina nationella språk (se p. 47 och 48 i den förklarande rapporten).

Framställningar på svenska bör av förklarliga skäl accepteras. Eftersom det många gånger kommer att vara viktigt att snabbt få tillgång till uppgifterna och de begränsade möjligheter som många stater har att ordna översättning till svenska bör även framställ-

ningar på engelska accepteras. Förvisso har Sverige i samarbetet med andra stater tidigare accepterat framställningar på danska och norska men då har det rört sig om ett myndighetssamarbete. Nu är det privata aktörer som är mottagare och det bör därför inte uttryckligen föreskrivas att en begäran även kan vara upprättad på norska eller danska. Däremot bör en begäran kunna vara upprättad på ett annat språk – bl.a. danska eller norska – som en registreringsenhet för toppdomäner och återförsäljare av domännamn i Sverige kan godta. Om t.ex. en återförsäljare kan godta en begäran på ett annat språk än svenska och engelska bör några hinder mot detta inte föreligga.

I artikel 6.3 och artikel 6.4 finns bestämmelser om dels vilka uppgifter en begäran enligt artikel 6.1 ska innehålla, dels om möjligheterna att översända en begäran i elektronisk form. Enligt vår uppfattning kan detta regleras i förordning.

12.4.6 I vilket regelverk bör bestämmelserna föras in

Förslag: De ändringar i lag som krävs för att genomföra artikel 6 i andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet ska föras in i lagen om vissa former av internationellt samarbete i brottsutredningar.

Skälen för förslaget: Ett straffrättsligt samarbete som innebär att en brottsbekämpande myndighet i en stat vänder sig till en privat aktör i en annan stat för att få tillgång till viss information är något nytt och i svensk rätt finns inga regler om ett sådant samarbete (med undantag för det samarbetet EU-förordningen reglerar). Den reglering om straffrättsligt samarbete som finns bygger helt och hållet på ett samarbete mellan myndigheter i Sverige och en annan stat.

Som konstaterats i avsnitt 12.4.4 kan åtgärden att inhämta uppgifter som avser innehavaren av ett domännamn likställas med inhämtning av abonnemangsuppgifter enligt 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation. Det framstår emellertid mindre lämpligt att föra in nu aktuella bestämmelser i den lagen eftersom den inte omfattar registreringsenheter för toppdomäner eller återförsäljare av domännamn. I den lagen finns

inte heller i dag bestämmelser om gränsöverskridande straffrättsligt samarbete.

I avsnitt 12.4.3 redogörs för de ändringar som föreslås i SOU 2024:18, bl.a. att det i toppdomänlagen ska införas en bestämmelse som innebär att utländska myndigheter och andra med offentligrättsliga uppgifter inom EES ska kunna begära ut uppgifter ur registret på annat sätt än genom det register som domänadministratören tillhandahåller via internet. En sådan skyldighet motsvarar i sak av de uppgifter som kan begäras ut enligt artikel 6 i det andra tilläggsprotokollet. Toppdomänlagen reglerar den nationella toppdomänen och de skyldigheter som tillkommer domänadministratören i fråga om drift av nationella toppdomäner för Sverige samt tilldelning och registrering av domännamn och den uppgiftsskyldighet som föreslås i nämnda betänkande syftar främst till frågor om cybersäkerhet. Vidare omfattas den föreslagna regleringen inte återförsäljare av domännamn. Av dessa skäl bör de bestämmelser som genomför artikel 6 i det andra tilläggsprotokollet inte föras i toppdomänlagen.

Som nämnts ovan innefattar artikel 6 inte ett samarbete mellan olika staters rättsvårdande myndigheter och det ter sig därför mindre lämpligt att föreslå ändringar i lagen (2000:562) om internationell rättslig hjälp i brottmål eller lagen (2017:1000) om en europeisk utredningsorder. Inte heller är det lämpligt att föra in några bestämmelser i den reglering som ska komplettera EU-förordningen eller genomföra EU-direktivet.

I lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar regleras vissa former av samarbete som inte riktigt passar in i det straffrättsliga samarbetet, men inte heller i de Polismyndighetens eller andra myndigheters samarbete i brottsutredningar. Lagen reglerar ett samarbete i form av gemensamma utredningsgrupper, kontrollerade leveranser och brottsutredningar med användning av skyddsidentitet. Förvisso reglerar även denna lag ett samarbete mellan myndigheter, men enligt vår mening passar de bestämmelser som föreslås genomföra artikel 6 i det andra tilläggsprotokollet bäst i denna lag. I vart fall framstår det som ett bättre alternativ än att införa en helt ny lag med några få bestämmelser.

Sammanfattningsvis bör de nya bestämmelserna föras in i lagen om vissa former internationellt samarbete i brottsutredningar.

12.5 Inhämtande av abonnemangsuppgifter (artikel 7)

12.5.1 Det närmare innehållet i artikel 7

I artikel 7 finns bestämmelser som innebär att en brottsutredande myndighet i en stat kan begära ut abonnemangsuppgifter hos en tjänsteleverantör som finns i en annan stat. På samma sätt som anges i föregående avsnitt angående artikel 6 innebär artikel 7 något nytt i det mellanstatliga samarbetet då en myndighet i en stat kan vända sig direkt till en privat aktör i en annan stat för att hämta in bevis utan att först kontakta en myndighet i den sistnämnda staten.

I den förklarande rapporten – för att visa på behovet av bestämmelsen – anges att ett brottsutredningar i allt större omfattning kräver tillgång till elektroniska bevis som innehåller eller kontrolleras av tjänsteleverantörer i andra stater (se p. 91). Detta gäller även för brott som är helt av inhemsk karaktär, dvs. brottet begås i samma land som offret, förövaren och utredande myndighet befinner sig i. De mekanismer som finns tillgängliga, t.ex. internationell rättslig hjälp i brottmål, är ofta otillräckliga.

Artikel 7 rör abonnemangsuppgifter. Enligt artikel 3.1 i det andra tilläggsprotokollet ska definitionen av abonnemangsuppgifter enligt artikel 18.3 Budapestkonventionen även gälla för motsvarande uppgifter i tilläggsprotokollet. Enligt artikel 18.3 i konventionen definieras abonnemangsuppgifter som

varje information i form av datorbehandlingsbara uppgifter eller uppgifter i annan form som innehåller av en tjänsteleverantör och som hänförs till andra uppgifter om dennes abonnenter än trafikuppgifter eller innehållsuppgifter och genom vilka kan fastställas

- a) den typ av kommunikationstjänst som använts, de tekniska åtgärder som vidtagits för dem och tidsperioden för tjänsten,
- b) abonnentens identitet, postadress eller geografiska adress, telefonnummer och annat accessnummer, information om fakturering och betalning, som är tillgänglig genom tjänsteavtalet eller tjänstearrangemanget,
- c) övriga upplysningar om var kommunikationsutrustningen är belägen som är tillgängliga genom tjänsteavtalet eller tjänstearrangemanget.

I den förklarande rapporten anges att information för att identifiera en abonnent på en tjänst även kan inkludera information om IP-adresser, t.ex. vilken IP-adress som användes vid tidpunkten när ett konto skapades eller vid den senaste inloggningen eller annan spe-

cifik tidpunkt (p. 93). Vidare anges att eftersom abonnemangs-
uppgifter inte tillåter några exakta slutsatser om den enskildes
privatliv eller dagliga vanor kan ett utlämnande av sådana uppgifter
utgöra en lägre grad av intrång jämfört med utlämnande av andra
kategorier av uppgifter (p. 92).

Av artikel 7.1 följer att varje part ska anta den lagstiftning och
andra åtgärder som krävs för att ge sina behöriga myndigheter be-
fogenhet att utfärda en order som ska lämnas direkt till en tjänste-
leverantör på en annan parts territorium, i syfte att få till stånd
utlämnande av specificerade, lagrade abonnemangsuppgifter i den
tjänsteleverantörens besittning eller kontroll, om abonnemangs-
uppgifterna behövs för den utfärdande partens specifika brotts-
utredningar eller straffrättsliga förfaranden.

Enligt artikel 3.1 det andra tilläggsprotokollet ska definitionen i
artikel 1 c Budapestkonventionen av en tjänsteleverantör även gälla
i förhållande till protokollet. I konventionen definieras en tjänste-
leverantör som

en offentlig eller privat enhet som erbjuder användarna av dess tjänster
möjlighet att kommunicera med hjälp av ett datorsystem, och
varje annan enhet som behandlar eller lagrar datorbehandlingsbara
uppgifter för en sådan kommunikationstjänst eller för användarna av
en sådan tjänst.

Enligt artikel 7.2 ska varje part anta den lagstiftning och andra
åtgärder som krävs för att en tjänsteleverantör inom dess terri-
torium ska kunna svara på en order enligt artikel 7.1. Varje part får
avge en förklaring att en order enligt artikel 7.1 ska utfärdas av eller
under överinseende av en åklagare eller annan rättslig myndighet
eller på annat sätt utfärdas under oberoende tillsyn.

Artikel 7.3 anger vilken information som en order enligt artikel 7.1
ska innehålla, vilket bl.a. inkluderar utfärdande myndighet och
datum för utfärdande, en förklaring om att ordern utfärdas enligt
det andra tilläggsprotokollet, det eller de brott som är föremål för
brottsutredningen eller det straffrättsliga förfarandet samt en
detaljerad beskrivning av de specifika abonnemangsuppgifter som
sökts. I artikel 7.4 föreskrivs vilken kompletterande information
som en order enligt artikel 7.1 ska åtföljas av. Sådan information är
enligt artikeln t.ex. de rättsliga grunderna enligt nationell rätt för
myndighetens befogenhet att utfärda ordern och den tidsram inom
vilken och det sätt på vilket abonnemangsuppgifterna ska skickas.

En part får enligt artikel 7.5 a, i varje enskilt fall eller under vissa villkor, kräva samtidig underrättelse om ordern, den kompletterande informationen och en sammanfattning av de sakförhållanden som har samband med utredningen eller förfarandet. Oavsett om en part kräver en sådan underrättelse, får den kräva att tjänsteleverantören under vissa fastställda omständigheter samråder med partens myndigheter innan uppgifter lämnas ut (artikel 7.5 b).

Den myndighet som har underrättats eller med vilka samråd har skett får enligt artikel 7.5 c utan onödigt dröjsmål uppmana tjänsteleverantören att inte lämna ut abonnemangsuppgifterna. Detta kan ske om ett utlämnande kan skada en brottsutredning eller ett straffrättsligt förfarande, eller om villkor eller vägransgrunder skulle vara tillämpliga enligt artikel 25.4 och artikel 27.4 i Budapestkonventionen för det fall abonnemangsuppgifterna hade begärts inom ramen för ömsesidig rättslig hjälp.

Enligt artikel 7.5 d får den myndighet som avses i artiklarna 7.5 a och 7.5 b begära kompletterande information från den myndighet som har beslutat om ordern, vilken information får inte lämnas till tjänsteleverantören utan sistnämnda myndighets samtycke. Denna myndighet ska också informeras om tjänsteleverantören har uppmanats att inte lämna ut uppgifterna och skälen till detta.

Varje part ska enligt artikel 7.5 e i en underrättelse utse den myndighet som avses i artiklarna 7.5 a och 7.5 b.

Artikel 7.6 innehåller bestämmelser om sättet att sända över en order enligt artikel 7.1.

Av artikel 7.7 följer att för det fall en tjänsteleverantör underrettar den behöriga myndigheten om att den inte kommer att lämna ut de begärda abonnemangsuppgifterna, eller om den inte lämnar ut uppgifterna inom viss tid får den utfärdande partens behöriga myndigheter söka verkställa ordern med stöd av artikel 8 eller genom andra former av ömsesidig rättslig hjälp. Parterna får enligt artikeln begära att tjänsteleverantören anger skälen för vägran att lämna ut uppgifterna, t.ex. att uppgifterna inte längre finns tillgängliga (se p. 119 i den förklarande rapporten).

En part får enligt artikel 7.8 förklara att en utfärdande part ska begära att abonnemangsuppgifter lämnas ut från tjänsteleverantören med stöd av artikel 7.2 innan en begäran görs enligt artikel 8, om det inte lämnas en rimlig förklaring till varför detta inte gjorts.

En part får enligt artikel 7.9 a förbehålla sig rätten att inte tillämpa artikel 7. Enligt artikel 7.9 b i protokollet får en part, om utlämnande av vissa typer av åtkomstnummer enligt artikeln skulle strida mot de grundläggande principerna i det nationella rättssystemet, förbehålla sig rätten att inte tillämpa artikel 7 på sådana nummer. I den förklarande rapporten anges beträffande sistnämnda förbehåll att i vissa stater kan dessa uppgifter motsvara trafikuppgifter och inte abonnemangsuppgifter (p. 93).

Av bilagan till rådsbeslutet 2023/436 anges hur medlemsstaterna ska förhålla sig de förbehåll som är möjliga att göra samt vidare vilka förklaringar och underrättelser som ska lämnas av medlemsstaterna i anslutning till artikel 7.

12.5.2 Gällande rätt

Med uppgift om abonnemang i svensk rätt avses främst uppgifter om abonnentens nummer, namn, titel och adress, men även uppgifter om exempelvis avtal och fakturering. Vidare innefattas uppgift om vem som använt en fast eller dynamisk IP-adress samt IMSI-nummer (se avsnitt 4.2.2). Mot denna bakgrund får begreppet abonnemangsuppgifter i det andra tilläggsprotokollet, såsom det beskrivits föregående avsnitt, anses överensstämma med vad som innefattas i begreppet uppgifter om abonnemang i svensk rätt.

Begreppet tjänsteleverantör i det andra tilläggsprotokollet har samma innebörd som motsvarande begrepp i artikel 1 c i Budapestkonventionen. Det begreppet har vid genomförande av den konventionen i huvudsak bedömts vara en leverantör som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.³

Som utvecklats i avsnitt 4.4.2 är den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst (Noik) enligt 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation skyldig att på begäran lämna en uppgift om abonnemang och som gäller brottslig verksamhet eller misstanke om brott till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon

³ SOU 2013:39 s. 68.

annan myndighet som ska ingripa mot brottet eller den brottsliga verksamheten. Som behandlats i avsnitt 4.2.6 har 2021 års data-lagringsutredning föreslagit att även tillhandahållare av Noik ska omfattas av denna reglering i lagen om elektronisk kommunikation. Regleringen innebär att de brottsbekämpande myndigheterna i princip har rätt att hämta in abonnemangsuppgifter för att beivra alla typer av brott utom sådana som åtalas enbart av målsäganden.

När det gäller det gränsöverskridande samarbetet finns i dag inga svenska regler som innebär att en svensk brottsutredande myndighet kan vända sig direkt till en tjänsteleverantör utomlands eller tvärtom. I stället inhämtas dessa uppgifter med stöd av bestämmelser om internationell rättslig hjälp i brottmål eller genom att utfärda en europeisk utredningsorder.

12.5.3 En möjlighet att inhämta abonnemangsuppgifter utomlands ska införas

Förslag: Svenska brottsutredande myndigheter ska kunna begära ut uppgifter om abonnemang från en tjänsteleverantör som erbjuder tjänster i en stat som har tillträtt det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet, om uppgifterna rör brottslig verksamhet eller misstanke om brott. De svenska myndigheter som ska omfattas är Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot ett brott eller brottslig verksamhet. En begäran om att få ut uppgifter om abonnemang ska godkännas av åklagare i de fall ett sådant krav har ställts upp av den andra staten.

Bedömning: Bestämmelser om vilka uppgifter en begäran ska innehålla och vilket språk en begäran ska upprättas på eller överlämnas till samt sättet att sända över en begäran bör regleras i förordning. En skyldighet att underrätta en av den andra staten utsedd myndighet om att en begäran har sänds över, bör också regleras i förordning.

Skälet för förslaget och bedömningen: Som nämnts innebär artikel 7 något nytt i det mellanstatliga samarbetet, dvs. ett beslut av en behörig myndighet i en stat om att en tjänsteleverantör i en annan stat ska lämna ut abonnemangsuppgifter. Motsvarande regler finns i EU-förordningen, vilka ska tillämpas från och med augusti 2026, och systemet med europeiska utlämnandeorder respektive bevarandeorder för inhämtning av elektronisk bevisning riktade direkt till tjänsteleverantörer har därför ännu inte prövats. Bara av den anledningen skulle det kunna argumenteras att motsvarande samarbete med stater utanför EU fick avvakta till dess vissa erfarenheter inhämtats från EU-samarbetet.

Som följer av bilagan till rådsbeslutet 2023/436 (p. 1) ska dock EU-staterna avstå från att använda sig av förbehållet i artikel 7.9 a. Eftersom rådsbeslutet är bindande för Sverige bör en bestämmelse som ger svenska brottsbekämpande myndigheter en möjlighet till gränsöverskridande inhämtning av abonnemangsuppgifter på det sätt som föreskrivs i artikel 7.1 införas i svensk rätt.

Enligt 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation är det flera myndigheter som kan begära ut uppgifter om abonnemang från en svensk tjänsteleverantör som omfattas av bestämmelsen. Enligt vår mening bör samma myndigheter kunna begära ut motsvarande uppgifter från en tjänsteleverantör i en annan stat som tillträtt det andra tilläggsprotokollet. Det ska röra sig om tjänsteleverantörer som omfattas av artikel 3.1 i protokollet (som hänvisar till artikel 1 c i Budapestkonventionen). Några skäl att exkludera en myndighet finns inte så länge ett inhämtande begärs i en specifik brottsutredning eller ett straffrättsligt förfarande (se nedan om när ett inhämtande ska kunna ske).

Enligt bilagan till rådsbeslutet 2023/436 (p. 2) ska medlemsstaterna, med avseende på en order som utfärdats gentemot en tjänsteleverantör inom deras territorium, avge den förklaring som anges i artikel 7.2 b, dvs. att en order enligt artikel 7.1 ska utfärdas av eller under överinseende av en åklagare eller annan rättslig myndighet eller på annat sätt utfärdas under oberoende tillsyn. Denna förklaring som ska avges enligt rådsbeslutet kommer troligen inte att ha någon bäring på samarbetet mellan medlemsstaterna eftersom det får förutsättas att EU-förordningen ska tillämpas i dessa fall (jfr dock artikel 32 i EU-förordningen). Även om rådsbeslutet inte innebär att en medlemsstat måste begränsa vilka nationella

myndigheter som enligt artikel 7.1 kan begära ut uppgifter, kan det argumenteras att samma bör gälla när Sverige agerar som begärande part, dvs. om Sverige ställer krav på andra stater i detta avseende bör vi själva endast utse myndigheter som lever upp till nämnda förklaring. Enligt vår mening finns det emellertid inga bärande skäl att begränsa vilka svenska myndigheter som kan begära ut uppgifter så länge det är förenligt med det andra tilläggsprotokollet.

Om däremot en annan stat har avgett en förklaring enligt artikel 7.2 b är Sverige förstås bunden av en sådan förklaring. Den staten kommer således inte att acceptera att t.ex. Polismyndigheten begär ut uppgifter om abonnemang utan ett förfarande som är förenligt med en förklaring enligt artikel 7.2 b bör införas. Enligt vår mening bör i dessa fall en åklagare godkänna en sådan begäran. Ett skäl till det är att åklagare är den instans som är behörig att ansöka om rättslig hjälp för att få ut dessa uppgifter. Vidare överensstämmer en sådan ordning i huvudsak med det som föreslås i avsnitt 7.5.1 om att åklagaren ska godkänna Polismyndighetens utfärdande av europeisk utlämnandeorder enligt EU-förordningen för utlämnande av abonnemangsuppgifter. Att utse domstol att godkänna en sådan begäran enligt artikel 7.1 är därför inte behövlig och en ordning med att åklagare gör detta, får anses vara förenligt med en förklaring enligt artikel 7.2 b. Förvisso medför detta ytterligare arbetsmoment för Polismyndigheten och övriga myndigheter men Åklagarmyndigheten tillsammans med övriga myndigheter bör kunna finna en ordning som motsvarar det godkännandeförfarande som blir aktuellt enligt avsnitt 7.5.1.

Enligt 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation ska en uppgift om abonnemang lämnas ut om uppgiften gäller brottslig verksamhet eller misstanke om brott. Samma krav bör gälla för att begära ut uppgifter om abonnemang enligt nu föreslagna bestämmelse. Av samma skäl som anges i avsnitt 12.4.4 bör kravet för att begära ut uppgifter inte motsvara det som gäller för beslag. En begäran om att få ut en uppgift som gäller brottslig verksamhet eller misstanke om brott anser vi uppfyller det krav som ställs upp i artikel 7.1 om att ett inhämtande ska ske i en specifik brottsutredning eller ett straffrättsligt förfarande.

I artikel 7.3 och 7.4 samt artikel 7.6 finns bestämmelser dels om vilka uppgifter en order om att begära ut abonnemangsuppgifter enligt artikel 7.1 ska innehålla, dels om möjligheterna att översända

en order i elektronisk form, vilka vi anser kan regleras i förordning. Bestämmelser på vilket språk en begäran ska upprättad på eller översatt till bör också regleras i förordning (artikel 4.2). Detsamma gäller den skyldighet som följer av artikel 7.5 a att underrätta en av den andra staten utsedd myndighet om att en begäran har sänts över.

Bestämmelsen i artikel 7.8 kräver inga bestämmelser i författning. Om en stat har lämnat en sådan förklaring som anges i den artikeln, har de svenska myndigheterna att förhålla sig det. I sådana fall får en ansökan om att få ut abonnemangsuppgifter med stöd av artikel 8 ske först efter det att behörig myndighet i Sverige begärt ut uppgifterna enligt artikel 7.1 men att det inte har lyckats.

12.5.4 Svenska tjänsteleverantörers skyldighet att lämna ut uppgifter om abonnemang

Förslag: En tjänsteleverantör som är skyldig att lämna ut uppgift om abonnemang enligt lagen om elektronisk kommunikation, ska på begäran av behörig myndighet i en stat som har tillträtt det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet lämna ut motsvarande uppgifter, om de rör brottslig verksamhet eller misstanke om brott. Uppgifterna ska lämnas ut senast 30 dagar från mottagandet av begäran eller inom den tidsfrist som anges i begäran om fristen är längre än 30 dagar. Uppgifterna ska lämnas ut om inte begäran är så bristfällig att den inte utan väsentlig olägenhet kan läggas till grund för ett utlämnande.

En sådan begäran ska vara beslutad av en åklagare eller annan rättslig myndighet eller på annat sätt vara utfärdad under oberoende tillsyn.

En tjänsteleverantör ska vid behov samråda med Åklagarmyndigheten innan några uppgifter lämnas ut.

Åklagarmyndigheten får besluta att tjänsteleverantören inte får lämna ut begärda uppgifter om det finns skäl att anta att ett utlämnande kan skada en pågående utredning om brott eller det finns förutsättningar att vägra att lämna ut motsvarande uppgifter om de hade begärts ut enligt lagen om internationell rättslig hjälp i brottmål.

En begäran som ställs till en tjänsteleverantör i Sverige ska vara skriven på eller översatt till svenska eller engelska eller det språk som godtas av tjänsteleverantören, medan en underrättelse till Åklagarmyndigheten ska vara skriven på eller översatt till svenska, danska, norska eller engelska.

Bedömning: Bestämmelser om innehållet i begäran, sättet att sända över den, kompletteringar av begäran och underrättelser bör regleras i förordning.

Skälen för förslaget och bedömningen

Svenska tjänsteleverantörer ska lämna ut abonnemangsuppgifter

Mot bakgrund av artikel 7.2 i det andra tilläggsprotokollet till Budapestkonventionen och bilagan till rådsbeslutet 2023/436 (p. 1), som innebär att Sverige inte ska förbehålla sig att inte tillämpa artikel 7 i protokollet, bör en bestämmelse i lag införas som ger utländska brottsbekämpande myndigheter en möjlighet att hämta in abonnemangsuppgifter i Sverige på det sätt som föreskrivs i artikel 7.2. Skyldigheten att lämna ut uppgifter ska bara gälla i förhållande till en stat som har tillträtt det andra tilläggsprotokollet. Med hänsyn till artikel 7.7 bör det vidare framgå av lag att den svenska tjänsteleverantören ska lämna ut uppgifterna senast 30 dagar efter mottagandet av begäran, om inte den myndighet som har utfärdat ordern har angett en längre tidsfrist.

De tjänsteleverantörer som bör omfattas av bestämmelsen är de som enligt 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation är skyldiga att lämna motsvarande uppgifter om abonnemang. Vi ser inga skäl till att utvidga eller inskränka kretsen av tjänsteleverantörer.

I föregående avsnitt har bedömningen gjorts att de aktuella uppgifterna hos en utländsk tjänsteleverantör ska kunna begäras ut av svenska behöriga myndigheter under förutsättning att uppgifterna gäller brottslig verksamhet eller misstanke om brott. Motsvarande överväganden gör sig gällande i fråga om skyldigheten för tjänsteleverantörer i Sverige att lämna ut uppgifter till myndigheter i annan stat som tillträtt det andra tilläggsprotokollet. Uppgifterna ska således lämnas ut om de gäller brottslig verksamhet eller miss-

tanke om brott. Om den tjänsteleverantör som ska lämna ut uppgifterna anser att begäran har ett annat syfte så kan uppgifterna inte lämnas ut.

I bilagan till rådsbeslutet 2023/436 (p. 2) uppmanas medlemsstaterna att avge en förklaring med det innehåll som framgår av artikel 7.2 b i det andra tilläggsprotokollet, dvs. att en order enligt artikel 7.1 ska utfärdas av eller under överinseende av en åklagare eller annan rättslig myndighet eller på annat sätt utfärdas under oberoende tillsyn. I lag bör därför införas en bestämmelse av denna innebörd. Se även avsnitt 12.11.

Utgångspunkten är att de begärda uppgifterna ska lämnas ut, men den skyldigheten ska inte vara absolut. Av de skäl som angetts i avsnitt 12.4.5 om skyldigheten för registreringsenheter för toppdomäner respektive återförsäljare av domännamn att lämna ut uppgifter till myndighet i annan stat som tillträtt det andra tilläggsprotokollet bör bestämmelsen formuleras på så sätt att uppgifterna ska lämnas ut om inte begäran är så bristfällig att den inte utan väsentlig olägenhet kan läggas till grund för ett utlämnande. En given utgångspunkt är vidare att endast de uppgifter som tjänsteleverantören har lagrade kan lämnas ut.

Inga sanktioner bör således införas för att tjänsteleverantören inte efterkommer en begäran. Utgångspunkten får dock vara att uppgifterna ska lämnas ut, på samma sätt som förutsätts enligt lagen om elektronisk kommunikation. Om uppgifterna trots detta inte lämnas ut får den andra statens myndigheter i stället enligt artikel 7.7 ansöka om rättslig hjälp via svensk åklagare för att få ut uppgifterna. Om en åklagare då anser att det inte finns skäl för att vägra lämna ut uppgifterna, kommer tjänsteleverantören vara förpliktigade att bistå.

Underrättelse till Åklagarmyndigheten och tjänsteleverantörernas skyldighet att samråda med denna myndighet

Artikel 7 i det andra tilläggsprotokollet är något nytt i det mellanstatliga samarbetet i och med att en begäran görs direkt till en tjänsteleverantör. I artikel 7.5 finns bestämmelser som ändå möjliggör för en stat att ha en viss kontroll över de framställningar som sänds över till den staten.

Enligt artikel 7.5 a kan en stat i en förklaring ange att samtidigt som en begäran skickas till en tjänsteleverantör ska en underrättelse om begäran tillsammans med viss information skickas till behörig myndighet i den stat där tjänsteleverantören finns. Vidare kan en stat med stöd av artikel 7.5 b kräva att tjänsteleverantören ska samråda behörig myndighet i den staten. Sistnämnda myndighet kan också enligt artikel 7.5 d begära kompletteringar för att kunna ta ställning till om tjänsteleverantören ska uppmanas att inte lämna ut några uppgifter med stöd av artikel 7.5 c.

Enligt vår uppfattning bör dessa möjligheter användas just mot bakgrund av att samarbetsformen är ny i förhållande till stater utanför EU.

En förklaring som innebär att behörig myndighet i Sverige ska underrättas i samtliga fall kan vid en första anblick ses som betungande. Det bör dock noteras att merparten av Sveriges straffrättsliga samarbete sker med EU-staterna och i förhållande till dem (förutom Danmark) kommer samarbetet i allt väsentligt ske med stöd av EU-förordningen (se avsnitt 3). Vidare anser vi att det finns skäl att en svensk myndighet mot bakgrund av kretsen av länder som samarbetet avser, kan agera i de fall det finns skäl att hindra att lämna ut uppgifter. Det ska också noteras att i bilagan till rådsbeslutet 2023/436 (p. 3) anges att medlemsstaterna ska använda sig av den förklaring som föreskrivs i artikel 7.5 a. I avsnitt 12.11 redogörs närmare för Sveriges förklaringar till det andra tilläggsprotokollet. Det som anges i bilagan till rådsbeslutet 2023/436 (p. 4) om att Sverige får låta en begäran granskas av en åklagare när den behörig myndigheten mottar en samtidig underrättelse av begäran blir överflödigt eftersom vi gör bedömningen att Åklagarmyndigheten ska vara behörig myndighet att ta emot en underrättelse (se nedan).

En tjänsteleverantör som tvekar att lämna ut uppgifterna ska med stöd av artikel 7.5 b ha en möjlighet att samråda med en svensk myndighet om uppgifterna ska lämnas ut. En skyldighet att samråda i samtliga fall bör inte införas eftersom det i onödan skulle tynga samarbetet, utan ett samråd bör kunna ske vid behov. Ett sådant behov kan exempelvis vara om det är tveksamt om uppgifterna begärs ut i ett straffrättsligt förfarande eller om det är en myndighet som avses i artikel 7.2 b som har sänt över begäran.

Sammanfattningsvis bör Sverige avge en förklaring med det innehåll som anges i artikel 7.5 a. Vidare bör en bestämmelse med det innehåll som anges i artikel 7.5 b införas.

I artikel 7.5 e anges att varje stat i en förklaring ska ange vilken myndighet som ska vara behörig att ta emot underrättelse, samråda med tjänsteleverantörerna samt begära kompletteringar från den myndighet som har sänt över en begäran. Den myndighet som bör utses anser vi vara Åklagarmyndigheten. Förvisso kommer andra svenska myndigheter ha möjlighet att begära ut uppgifter om abonnemang från andra staters tjänsteleverantörer, men de överväganden som ska ske enligt artikel 7.5, motsvarar dem som görs vid en ansökan om rättslig hjälp. Dessutom anges i bilagan till rådsbeslutet 2023/436 (p. 3) att medlemsstaterna ska utse endast en myndighet. Se även avsnitt 12.11.

Åklagaren ska kunna besluta om att uppgifterna inte får lämnas ut

En behörig myndighet som underrättats om en begäran enligt artikel 7.5 a, eller via ett samråd enligt artikel 7.5 b, kan med stöd av artikel 7.5 c uppmana tjänsteleverantören att inte lämna ut några uppgifter. Det kan ske dels om ett utlämnande skulle skada en pågående brottsutredning eller straffrättsligt förfarande (i), dels om de vägransgrunder som anges i artikel 25.4 och 27.4 i Budapestkonventionen hade varit tillämpliga om uppgifterna hade begärts ut inom ramen för ömsesidig rättslig hjälp i brottmål (ii).

Den möjlighet som föreskrivs i artikel 7.5 c i det andra tilläggsprotokollet bör Sverige använda sig av. Bestämmelsen i lag bör dock utformas på så sätt att en åklagare kan besluta om att uppgifterna inte får lämnas ut, vilket beslut tjänsteleverantören ska följa. Artikel 7.5 c kan inte tolkas på så sätt att en tjänsteleverantör ändå ska kunna lämna ut uppgifter, trots en uppmaning från en brottsbekämpande myndighet att inte göra det för att t.ex. en pågående brottsutredning skadas.

Sammanfattningsvis bör åklagaren kunna besluta om att tjänsteleverantören inte får lämna ut uppgifter om abonnemang dels om ett utlämnande skulle skada en pågående utredning om brott, dels om det hade förelegat hinder enligt lagen om internationell rättslig hjälp i brottmål om motsvarande uppgifter hade begärts ut med

stöd av en ansökan om rättslig hjälp. Hänvisningen till nämnda lag får anses vara förenlig med artikel 7.5 c ii.

Språk

När det gäller språkraven för en begäran enligt artikel 7.1 i det andra tilläggsprotokollet tillämpas artikel 4.2 i protokollet, dvs. begäran ska upprättas på eller vara översatt till ett språk som tjänsteleverantören godtar i ett jämförbart nationellt förfarande eller på ett annat språk som leverantören kan godta. Av de skäl som anges i avsnitt 12.4.5 bör samma krav på översättningar även gälla beträffande en begäran enligt artikel 7.1, dvs. en begäran ska vara upprättat på eller översatt till svenska eller engelska eller något annat språk som tjänsteleverantören kan godta.

Av artikel 4.1 följer att en underrättelse enligt artikel 7.5 a ska vara upprättat på eller översatt till ett språk som Sverige kan godta. I detta fall sker således kommunikationen mellan den andra statens behöriga myndighet och Åklagarmyndigheten. Mot bakgrund av att samarbetet har nära kopplingar till rättslig hjälp och bestämmelsen i 2 kap. 5 § lagen om internationell rättslig hjälp i brottmål bör en underrättelse vara upprättat på eller översatt till svenska, danska eller norska. Vidare bör även engelska accepteras.

Övriga bestämmelser i artikel 7

I artikel 7.3 och 7.4 finns bestämmelser om vad en begäran ska innehålla. I artikel 7.5 d i finns en bestämmelse som innebär åklagaren ska kunna hämta in kompletterande information från den myndighet som har sänt över begäran för att kunna ta ställning till om uppgifterna ska få lämnas ut samt att den kompletterande informationen inte får lämnas ut till tjänsteleverantören utan den utfärdande myndighetens samtycke. Innebörden av artikel 7.5 d ii är att åklagaren ska underrätta den utfärdande myndigheten om sitt beslut att tjänsteleverantören inte får lämna ut begärda uppgifter. Motsvarande skyldighet för tjänsteleverantören föreskrivs i artikel 7.7. Vidare finns bestämmelser i artikel 7.6 om möjligheterna att sända över en begäran och annan information i elektronisk form. Vi bedömer att dessa bestämmelser bör kunna regleras i förordning.

Förbehållen enligt artiklarna 7.8 och 7.9

Enligt artikel 7.8 i det andra tilläggsprotokollet kan Sverige i en förklaring ange att innan en stat ansöker om att få ut uppgifter om abonnemang enligt artikel 8, ska den först ha använts av det förfarande som föreskrivs i artikel 7, om inte den andra staten anger en rimlig förklaring varför det inte har skett.

Vi anser att Sverige inte behöver avge en sådan förklaring. Det får vara upp till den andra statens myndigheter att avgöra om den vill tillämpa artikel 7 eller artikel 8 i det enskilda fallet. I vissa fall kan det vara enklare för en stat att via svenska myndigheter få ut uppgifter om abonnemang. Att kräva ett förfarande enligt artikel 7 innan en ansökan enligt artikel 8 får göras framstår som onödigt betungande och bör således undvikas.

Med stöd av artikel 7.9 b i protokollet kan Sverige förbehålla sig att artikel 7 inte ska tillämpas beträffande vissa åtkomstnummer om ett utlämnande av dessa skulle strida mot grundläggande principer i det svenska rättssystemet. I den förklarande rapporten till protokollet (p. 93) klagörs att IP-adresser i de flesta fall ses som uppgifter om abonnemang, medan i vissa stater likställs dessa uppgifter som trafikuppgifter. Av det skälet finns den möjlighet till förbehåll som föreskrivs i artikel 7.9 b. I bilagan till rådsbeslutet 2023/436 (p. 1) anges att medlemsstaterna får göra ett sådant förbehåll, men endast när det gäller andra åtkomstnummer än dem som är nödvändiga för att identifiera användaren. Eftersom uppgift om IP-adress i Sverige ses som en uppgift om abonnemang, och inte som en trafikuppgift, ser vi inget behov att avge ett förbehåll enligt artikel 7.9 b.

12.5.5 I vilket regelverk bör bestämmelserna föras in

Förslag: De ändringar i lag som krävs för att genomföra artikel 7 i andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet ska föras in i lagen om vissa former av internationellt samarbete i brottsutredningar.

Skälen för förslaget: På de skäl som anförs i avsnitt 12.4.6 anser vi att de ändringar i lag som krävs för att leva upp till de skyldigheter som följer av artikel 7 i det andra tilläggsprotokollet inte bör föras in i lagen om elektronisk kommunikation eller lagen om internationell rättslig hjälp i brottmål utan i stället i lagen om vissa former av internationellt samarbete i brottsutredningar tillsammans med de ändringar som behövs för att genomföra artikel 6 i protokollet.

12.6 Skyndsamt framtagande av abonnemangs- och trafikuppgifter (artikel 8)

12.6.1 Det närmare innehållet i artikel 8

Enligt artikel 8.1 ska staterna anta den lagstiftning och andra åtgärder som krävs för att ge sina behöriga myndigheter befogenhet att utfärda en order som ska överlämnas som en del av en framställning till en annan stat i syfte att få ut abonnemangs- och trafikuppgifter från en tjänsteleverantör som denne har sin besittning eller under kontroll. Uppgifterna får begäras ut när de behövs för specifika brottsutredningar eller straffrättsliga förfaranden.

Termen trafikuppgifter definieras i artikel 1 d i Budapestkonventionen som ”datorbehandlingsbara uppgifter som hänför sig till ett meddelande som förmedlas med hjälp av ett datorsystem, vilka alstrats av ett datorsystem som ingick i kommunikationskedjan och anger meddelandets ursprung, destination, färdväg, tid, datum, storlek, varaktighet eller typ av underliggande tjänst”. Definitionen av abonnemangsuppgifter behandlas i avsnitt 12.5.1.

Ett krav enligt artikel 8.1 är att tjänsteleverantören är fysiskt närvarande i den mottagande staten. Enbart den omständigheten att

t.ex. en tjänsteleverantör har ingått ett avtalsförhållande med ett företag i en part, men tjänsteleverantören själv inte är fysiskt närvarande i den parten, innebär inte att tjänsteleverantören befinner sig på den partens territorium (se den förklarande rapporten p. 128).

Artikel 8 kompletterar enligt den förklarande rapporten Budapestkonventionens bestämmelser om ömsesidig rättslig hjälp och skapar ett mer effektivt förfarande för att få tillgång till abonnemangs- och trafikuppgifter (p. 125). Bestämmelsen i artikel 8 påverkar inte heller eller andra multilaterala eller bilaterala avtal som en part har rätt att åberopa. Det framhålls vidare att varje stat får avgöra om nämnda uppgifter ska begäras ut med stöd av artikel 8 eller ingå i en traditionell ansökan om rättslig hjälp innefattande även utfående av innehållsdata.

Enligt artikel 8.2 ska varje part anta den lagstiftning som krävs för att kunna verkställa en sådan order som avses i artikel 8.1. Enligt den förklarande rapporten får varje stat själv avgöra på vilket sätt en sådan order verkställs (se p. 129).

Artikel 8.3 innehåller bestämmelser om vilken information som en order enligt artikel 8.1 ska innehålla. I sin framställning ska den ansökande parten bifoga ordern, informationsunderlaget och eventuella särskilda förfarandeanvisningar för den anmodade parten. Ordern ska enligt artikel 8.3 a ange bl.a. namn på och adress till den eller de tjänsteleverantörer som ska delges ordern, det eller de brott som är föremål för brottsutredningen eller det straffrättsliga förfarandet samt en detaljerad beskrivning av den specifika information eller de specifika uppgifter som begärs.

I det informationsunderlag som tillhandahålls för att hjälpa den anmodade parten att verkställa ordern ska enligt artikel 8.3 b bl.a. anges de rättsliga grunderna för myndighetens befogenhet att utfärda ordern, en sammanfattning av de faktiska omständigheterna bakom utredningen eller förfarandet samt uppgifternas relevans för undersökningen eller förfarandet. Dessa uppgifter får inte lämnas ut till tjänsteleverantören utan den ansökande partens samtycke.

Enligt artikel 8.3 c får den ansökande parten begära att den anmodade parten följer särskilda instruktioner om förfarandet. I den förklarande rapporten nämns som exempel att ordern inte ska lämnas ut till abonnenten eller att autentiseringsformulär ska fyllas i för bevisningen (p. 135).

Av artikel 8.4 följer att en part får förklara att ytterligare informationsunderlag krävs för att verkställa en order. Enligt den förklarande rapporten kräver vissa parter nationella lagstiftning ytterligare information för att ta fram trafikuppgifter (p. 137).

Den anmodade parten ska enligt artikel 8.5 godta framställningar i elektronisk form. Den får kräva lämpliga säkerhets- och autentiseringsnivåer innan framställningen godtas.

Artikel 8.6 a innehåller bestämmelser om tidsfrister. Den anmodade parten ska, från och med dagen för mottagandet av framställningen delge tjänsteleverantören inom 45 dagar, men helst tidigare, och ska beordra att begärd information eller uppgifter lämnas senast inom 20 dagar för abonnemangsuppgifter och 45 dagar för trafikuppgifter. Den anmodade parten ska se till att den information eller de uppgifter som tagits fram översänds till den ansökande parten utan onödigt dröjsmål (artikel 8.6 b). Av den förklarande rapporten framgår dock att tidsfristerna inte är absoluta utan avtalsstaterna ska vidta rimliga åtgärder för att hålla tidsfristerna (p. 139).

Artikel 8.7–8.9 reglerar underrättelseskyldighet för parterna samt under vilka villkor verkställighet av en framställning kan vägras. Artikel 8.10–8.12 innehåller bl.a. bestämmelser om kontaktuppgifter till behöriga myndigheter och om centralmyndigheter.

En part får enligt artikel 8.13 förbehålla sig rätten att inte tillämpa artikeln på trafikuppgifter. Enligt bilagan till rådsbeslutet 2023/436 (p. 1) uppmantras medlemsstaterna att avstå från att göra ett sådant förbehåll.

12.6.2 Gällande rätt

I avsnitt 4.4.2 och 4.4.3 redogörs för hur svenska brottsbekämpande myndigheter kan få tillgång till abonnemangsuppgifter med stöd av 9 kap. 33 § lagen om elektronisk kommunikation och historiska trafikuppgifter genom hemlig övervakning av elektronisk kommunikation.

Vidare redogörs för det internationella samarbetet i avsnitt 4.5, bl.a. lagen om internationell rättslig hjälp i brottmål och lagen om en europeisk utredningsorder.

Vi hänvisar till dessa avsnitt.

12.6.3 Inhämtande av abonnemangs- och trafikuppgifter utomlands

Förslag: I lagen om internationell rättslig hjälp i brottmål ska det anges att en order enligt artikel 8 i det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet ska jämföras med en ansökan om rättslig hjälp.

Bedömning: Bestämmelser om åklagarens skyldighet att underätta den anmodade staten i vissa fall bör regleras i förordning.

Skälen för förslaget och bedömningen

En order om att hämta in abonnemangs- och trafikuppgifter ska jämföras med en ansökan om rättslig hjälp

Insamling av uppgifter om abonnemang från tjänsteleverantörer i Sverige kan i svensk rätt ske med stöd av bestämmelsen i 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation. Beträffande historiska trafikuppgifter gäller bestämmelserna om hemlig övervakning av elektronisk kommunikation, närmare bestämt 27 kap. 19–19 b §§ rättegångsbalken. I dessa bestämmelser anges de närmare förutsättningarna, t.ex. att brottet ska vara en viss svårhetsgrad samt att det är domstol som prövar om förutsättningarna är uppfyllda (se avsnitt 4.4.3).

I förhållande till EU:s medlemsstater (utom Danmark och Irland) tillämpas lagen om en europeisk utredningsorder. Enligt den lagen kan en europeisk utredningsorder utfärdas för inhämtande av aktuella uppgifter (se 1 kap.4 §). Vi anser att bestämmelserna i lagen, som genomför direktivet om en europeisk utredningsorder, lever upp till de åtagande som följer av artikel 8 i det andra tilläggsprotokollet. När det gäller samarbetet med dessa stater behövs därför inga ändringar i lag i samband med att en svensk åklagare utfärdar en utredningsorder för inhämtande av abonnemangs- eller trafikuppgifter.

När det gäller samarbetet med övriga länder kan rättslig hjälp med såväl inhämtning av abonnemangsuppgifter som lagrade trafikuppgifter ansökas med stöd av lagen om internationell rättslig hjälp i brottmål (se 1 kap. 7 §). Det förfarande som anges i artikel 8 är

visserligen inte att jämställa med en traditionell ansökan om rättslig hjälp i brottmål, utan myndigheten ska i stället besluta om att uppgifterna ska lämnas ut, vilket beslut sedan verkställs i den andra staten. Å andra sidan kan noteras att samma uppgifter kan inhämtas genom en ansökan om rättslig hjälp i brottmål och den andra staten som tar emot en order från en svensk åklagare kan vid sin prövning i huvudsak tillämpa de förutsättningar som gäller för detta samarbete. Det bör vara upp till åklagare att avgöra vilket förfarande som är att anse som mest effektivt i förhållande till de stater som tillträtt det andra tilläggsprotokollet, dvs. det bör vara möjligt för en åklagare att kunna utfärda en order enligt artikel 8. Med hänsyn till de ovan beskrivna likheterna mellan en order enligt artikel 8.1 och en traditionell ansökan om rättslig hjälp bör samma regelverk gälla för en order som för en ansökan om rättslig hjälp. Det bör därför följa av lagen om internationell rättslig hjälp i brottmål att en order enligt artikel 8 i det andra tilläggsprotokollet till Budapestkonventionen ska jämföras med en ansökan om rättslig hjälp.

Bestämmelsen kan föras in i 3 kap. 1 § lagen om internationell rättslig hjälp i brottmål. Det ska noteras att den andra staten kan komma att kräva att åklagaren inhämtar ett tillstånd från domstol i Sverige innan en order sänds över till den andra staten för att inhämta trafikuppgifter. Bestämmelser om detta finns i 4 kap. 26 § lagen om internationell rättslig hjälp i brottmål.

Med stöd av artikel 8.10 a bör Åklagarmyndigheten utses som behörig myndighet att inge en sådan order (se även 12.11).

Enligt artikel 8.13 kan en stat förbehålla sig att inte tillämpa artikel 8 när det gäller trafikuppgifter. I bilagan till rådsbeslutet 2023/436 (p. 1) uppmanas medlemsstaterna att inte göra ett sådant förbehåll, även om det inte finns något hinder mot detta. Artikel 8 ger de brottsbekämpande myndigheterna ett nytt verktyg i samarbetet och tanken med bestämmelsen är att snabbare komma åt uppgifterna (t.ex. genom de tidsfrister som föreskrivs i artikel 8.6). Vi föreslår således – i överensstämmelse med rådsbeslutet 2023/436 – att Sverige inte lämnar ett allmänt förbehåll om att inte tillämpa artikel 8 beträffande trafikuppgifter. Däremot bör ett förbehåll lämnas med vissa begränsningar när det gäller trafikuppgifter (se avsnitt 12.6.5).

Övriga bestämmelser i artikel 8

Artiklarna 8.3 och 8.4 anger närmare vad en order ska innehålla för uppgifter. I 3 kap. 1 § lagen om internationell rättslig hjälp i brottmål, som hänvisar till 2 kap. 4 § i lagen, och 10–12 §§ förordningen (2000:704) om internationell rättslig hjälp i brottmål, finns bestämmelser om vad en ansökan om rättslig hjälp ska innehålla. Bland annat anges att en ansökan ska ha det innehåll som följer av en internationell överenskommelse som Sverige är bunden av, vilket även kommer att gälla i förhållande till det andra tilläggsprotokollet till Budapestkonventionen. Artiklarna 8.3 och 8.4 kräver således inga ändringar i lag.

Några ändringar i lag behövs inte heller när det gäller sättet att sända över en order eftersom det i artikel 8.5 endast anges vad den anmodade staten ska acceptera.

Bestämmelserna i artikel 8.6–8.8 reglerar endast den anmodade statens skyldigheter. I artikel 8.9 finns bestämmelser om att den ansökande staten har en skyldighet dels att underrätta den anmodade staten i vissa fall, dels att efterleva villkor som sistnämnda stat har ställt upp. När det gäller underrättelseskyldigheten kan det regleras i förordning. En skyldighet att följa uppställda villkor följer av 5 kap. 1 § lagen om internationell rättslig hjälp i brottmål. Några ändringar i lag beträffande artikel 8.9 föreligger därför inte.

Med stöd av artikel 8.10 a bör Åklagarmyndigheten utses till behörig myndighet att utfärda en order enligt artikel 8.1. Se även avsnitt 12.11 om att även Europeiska åklagarmyndigheten ska utses till behörig myndighet i enlighet med bilagan till rådsbeslutet 2023/436 (p. 3).

Övriga bestämmelser i artikel 8 föranleder inga ändringar i lag.

12.6.4 Verkställighet i Sverige av en order om inhämtande av abonnemangs- och trafikuppgifter

Bedömning: Några ändringar i lag behövs inte vid verkställighet i Sverige av en order om inhämtande av abonnemangs- och trafikuppgifter. Bestämmelser om underrättelse i vissa fall till den ansökande staten bör regleras i förordning.

Skälen för bedömningen

Samarbetet enligt lagen om en europeisk utredningsorder

Inledningsvis gör vi – på samma sätt som i föregående avsnitt – den bedömningen att i samarbetet med EU:s medlemsstater (utom Danmark och Irland) är bestämmelserna i lagen om en europeisk utredningsorder förenliga med de krav som följer av artikel 8 i det andra tilläggsprotokollet. Av 1 kap. 4 § i nämnda lag följer att inhämtande av abonnemangs- och trafikuppgifter omfattas av samarbetet.

En utredningsorder som utfärdas av en annan medlemsstat är jämförbar med en order som utfärdas enligt artikel 8.1 och som ska verkställas enligt artikel 8.2. Innehållet i utredningsordern överensstämmer i allt väsentligt med de uppgifter som anges i artikel 8.3 och 8.4. På sikt kommer all kommunikation mellan medlemsstaterna ske elektroniskt (jfr artikel 8.5).

I samarbetet med EU-staterna anges särskilda tidsfrister för att dels besluta om att vidta åtgärden, dels att verkställa den (se 3 kap. 16 och 23 §§ lagen om en europeisk utredningsorder). I vissa särskilda fall kan beslut och verkställighet ske inom några dagar (se 3 kap. 32 §). Dessa bestämmelser får anses vara förenliga med de tidsfrister som framgår av artikel 8.6 och det särskilt med beaktande av vad som sägs i den förklarande rapporten om att tidsfristerna inte är absoluta utan att avtalsstaterna ska vidta rimliga åtgärder för att hålla fristerna.

Möjligheterna att inte tillämpa ett visst förfarande eller att vägra hjälpa till, ställa upp särskilda villkor eller skjuta upp verkställigheten är inte mer långtgående utan ofta mer begränsade i lagen om en europeisk utredningsorder än vad som anges i artikel 8.7 och 8.8.

Några ändringar i lagen om en europeisk utredningsorder behövs därför inte.

Artiklarna 8.1–8.5, 8.7 och 8.8 kräver inga lagstiftningsåtgärder i samarbetet enligt lagen om internationell rättslig hjälp i brottmål

För att en svensk myndighet ska kunna lämna rättslig hjälp med en åtgärd krävs att den finns tillgänglig i nationell rätt och omfattas av lagen om internationell rättslig hjälp i brottmål. Utgångspunkten är

att alla åtgärder som är möjliga att vidta i en svensk förundersökning eller rättegång även ska vara tillgängliga för en annan stat efter en ansökan om rättslig hjälp, oavsett om bistånd med åtgärden föreskrivs i en internationell överenskommelse eller inte.⁴ Denna utgångspunkt kommer till uttryck i 2 kap. 1 § i lagen.

Insamling av uppgifter om abonnemang från tjänsteleverantörer i Sverige kan i svensk rätt ske med stöd av den ovan behandlade bestämmelsen i 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation. Trafikuppgifter inhämtas genom hemlig övervakning av elektronisk kommunikation (se 27 kap. 19–19 b §§ rättegångsbalken). Detta tvångsmedel kan användas för att samla in sådana trafikuppgifter som avses i artikel 8 (se även avsnitt 4.2.2 om den nationella definitionen av begreppet trafikuppgifter). Rättslig hjälp med såväl inhämtning av abonnemangsuppgifter som trafikuppgifter via hemlig övervakning av elektronisk kommunikation kan således lämnas med stöd av lagen om internationell rättslig hjälp i brottmål.

Som påpekats i föregående avsnitt är ett utfärdande av en order enligt artikel 8.1 visserligen något annat än en traditionell ansökan om rättslig hjälp, i vart fall när det gäller den stat som ska utfärda en order. När det däremot gäller den anmodade parten – eller den verkställande staten – anges i förklaranderapporten beträffande artikel 8.2 att det är upp till varje stat att avgöra vilka regler som ska tillämpas för att verkställa en order, t.ex. genom att behöriga myndigheter själva beslutar om att vidta åtgärden (se p. 129). Något särskilt förfarande för att verkställa nu aktuella order föreskrivs därför inte i artikel 8. När åklagaren beslutar om att inhämta abonnemangsuppgifter eller inhämtar domstolens beslut om hemlig övervakning av elektronisk kommunikation så upprätthålls de krav som följer av artikel 8.2 och några lagstiftningsåtgärder krävs därför inte. I avsnitt 12.6.5 föreslås dock vissa begränsningar vad gäller historiska trafikuppgifter.

Den information som ska följa en framställning enligt artikel 8.3 och 8.4 överensstämmer i allt väsentligt med bestämmelserna om vad en ansökan om rättslig hjälp bör innehålla enligt 2 kap. 4 § första stycket lagen om internationell rättslig hjälp i brottmål. Bestämmelsen är också så formulerad att den ska kunna ta hänsyn de krav som ställs upp i olika internationella överenskommelser

⁴ Prop. 1999/2000:61 s. 79.

eftersom det inte är möjligt att ha en heltäckande regel om vad en ansökan ska innehålla.⁵ Möjligheten för den ansökande staten att enligt artikel 8.3 c anvisa ett särskilda förfarande överensstämmer med 2 kap. 11 § lagen om internationell rättslig hjälp i brottmål. Den underrättelseskyldighet som följer artikel 8.7 kan regleras i förordning. Artikel 8.3, 8.4 och 8.7 kräver därmed inte några lagstiftningsåtgärder. Enligt artikel 8.4 kan en stat i en förklaring ange att ytterligare underlag krävs för att verkställa en order enligt artikel 8.1. Enligt bilagan till rådsbeslutet 2023/436 (p. 4) ska medlemsstaterna avge en sådan förklaring, vilket Sverige således bör göra (se avsnitt 12.11). Förklaringen kräver inga ändringar i lag eftersom nu gällande bestämmelser gör det möjligt för åklagaren att begära kompletteringar (se t.ex. 2 kap. 9 § lagen om internationell rättslig hjälp i brottmål).

Regeln i artikel 8.5 om att en ansökande stat ska kunna göra framställningar i elektronisk form är förenlig med svenska regler om möjliga kommunikationssätt (se 2 kap. 4 § fjärde stycket lagen om internationell rättslig hjälp i brottmål).

Bestämmelsen i artikel 8.8 om rätten att vägra rättslig hjälp hänvisar till artiklarna 25.4 eller 27.4 i Budapestkonventionen. Dessa artiklar anger allmänna principer som ska gälla för rättslig hjälp mellan de stater som tillträtt nämnda konventionen. Bestämmelserna ger huvudsakligen uttryck för etablerade allmänna principer för internationellt rättsligt samarbete (se bl.a. 2 kap. 14 § lagen om internationell rättslig hjälp i brottmål). Lagen om internationell rättslig hjälp i brottmål är redan anpassad till regleringen i Budapestkonventionen i samband med att Sverige tillträdde konventionen.⁶ Möjligheten att ställa upp villkor för att kunna verkställa en order framgår av 2 kap. 9 § nämnda lag. Inte heller artikel 8.8 i det andra tilläggsprotokollet kräver lagstiftningsåtgärder.

Med stöd av artikel 8.10 b bör Åklagarmyndigheten utses som mottagare av en order enligt artikel 8.1. Se även avsnitt 12.11 om att även Europeiska åklagarmyndigheten ska utses till behörig myndighet i enlighet med bilagan till rådsbeslutet 2023/436 (p. 3).

⁵ Prop. 1999/2000:61 s. 94.

⁶ Prop. 2020/21:72 s. 61–62 och 193.

Skyndsambetskravet i artikel 8.6

Artikel 8.6 i det andra tilläggsprotokollet ställer krav på ett skyndsamt förfarande och anger särskilda tidsfrister inom vilka en tjänsteleverantör ska delges respektive lämna ut den begärda informationen. Informationen ska sedan lämnas ut utan dröjsmål till den ansökande parten. Det ska emellertid noteras att i den förklarande rapporten anges att tidsfristerna inte är absoluta utan avtalsstaterna ska vidta rimliga åtgärder för att iaktta dessa tidsfrister.

En ansökan om rättslig hjälp ska enligt 2 kap. 10 § lagen om internationell rättslig hjälp i brottmål behandlas skyndsamt. Några särskilda tidsfrister föreskrivs inte i lagen. De tidsfrister som uppställs i rättegångsbalken eller i annan författning när en motsvarande åtgärd ska vidtas i ett inhemskt förfarande blir direkt tillämpliga vid verkställandet av en ansökan om rättslig hjälp genom den generella hänvisningen till förfarandet vid en svensk förundersökning eller rättegång.

Med hänsyn till skyndsambetskravet i 2 kap. 10 § lagen om internationell rättslig hjälp i brottmål får förutsättas att åklagaren beträffande abonnemangsuppgifter eller domstolen efter en begäran från åklagaren om hemlig övervakning av elektronisk kommunikation beslutar i så pass god tid att berörd tjänsteleverantör underrättas om beslutet inom den tidsfrist om 45 dagar som anges i artikel 8.6.

När det sedan gäller kravet i artikel 8.6 om att tjänsteleverantören ska lämna ut de begärda abonnemangs- och trafikuppgifterna inom vissa angivna tidsfrister (20 respektive 45 dagar) har tjänsteleverantörer en anpassningsskyldighet enligt lagen om elektronisk kommunikation. Anpassningsskyldigheten enligt 9 kap. 29 och 29 b §§ innebär att de ska bedriva sin verksamhet så att beslut om bl.a. hemlig övervakning av elektronisk kommunikation kan verkställas utan att verkställigheten röjs samt att uppgifterna lämnas ut utan dröjsmål (9 kap. 29 b §). Samma skyndsambetskrav gäller för uppgifter om abonnemang som lämnas ut enligt 9 kap. 33 § första stycket 2. Några särskilda angivna tidsfrister föreskrivs däremot inte.

Av förarbetena till anpassningsskyldigheten kan följande noteras.⁷ Utgångspunkten är att arbetet med att lämna ut information med anledning av en begäran som inkommer under kontorstid ska in-

⁷ Prop. 2021/22:183 s. 74 och prop. 2010/11:46 s. 80.

ledas inom mycket kort tid. Skyndsamhetskravet innebär att leverantören kan också komma att behöva arbeta med verkställigheten utanför kontorstid. Om det tar olika lång tid att få fram uppgifterna ur leverantörens system, bör utlämnandet ske successivt så snart uppgifterna blir tillgängliga för leverantören. Hur snabbt ett utlämnande ska ske i det enskilda fallet är en fråga som får avgöras av den aktuella brottsbekämpande myndigheten och leverantören i varje situation. Post- och telestyrelsen har bemyndigats att meddela närmare föreskrifter om skyndsamhetskravet (se 9 kap. 29 b § femte stycket lagen om elektronisk kommunikation och 9 kap. 13 § förordningen (2022:511) om elektronisk kommunikation). Några sådana föreskrifter har dock inte meddelats.

Bestämmelserna i lagen om internationell rättslig hjälp i brottmål och lagen om elektronisk kommunikation bör enligt vår mening vara tillräckliga för att leva upp till de tidsfrister som anges i artikel 8.6, särskilt med beaktande av förarbetsuttalandena om skyndsamhetskravet. Vi gör bedömningen att tjänsteleverantörerna i de allra flesta fallen med god marginal kommer att lämna ut uppgifter inom föreskrivna tidsfrister. Dessutom ska beaktas vad som sägs i den förklarande rapporten om att avtalsstaterna ska vidta rimliga åtgärder för att hålla tidsfristerna, vilket vi anser nuvarande regelverk gör. Några särskilda regler i nämnda lagar för att omhänderta tidsfristerna enligt nämnda artikel behövs därför inte.

Vi menar också att åklagaren kan i samband med att beslutet om att lämna ut uppgifter sänds över till tjänsteleverantören påminna om de tidsfrister som gäller. Därutöver ska påpekas att nationella bestämmelser – bl.a. skyndsamhetskravet i 9 kap. 29 b § lagen om elektronisk kommunikation – alltid ska tolkas konformt med Sveriges internationella åtaganden, vilket även gäller tjänsteleverantörernas åligganden. Slutligen är det inget som hindrar Post- och telestyrelsen att med stöd av sitt bemyndigande föreskriver närmare om skyndsamhetskravet om det skulle visa sig att tjänsteleverantörerna inte respekterar tidsfristerna.

12.6.5 Partiellt förbehåll beträffande historiska trafikuppgifter

Bedömning: Artikel 8 i det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet bör endast tillämpas när det gäller insamling av trafikuppgifter på de brott och brottstyper som avses i 27 kap. 19 a § andra stycket och 19 b § andra stycket rättegångsbalken. Artikel 8 bör inte tillämpas vid insamling av trafikuppgifter inom en tjänsteleverantörs datorsystem som dels drivs för en sluten användargrupp, dels inte använder allmänna kommunikationsnät och inte är anslutet till ett annat datorsystem. Sverige bör avge en förklaring med detta innehåll.

Skälen för bedömningen: I fråga om trafikuppgifter får hemlig övervakning av elektronisk kommunikation endast användas vid en förundersökning om vissa särskilt angivna brott (se 27 kap. 19 a § andra stycket och 19 b § andra stycket rättegångsbalken). En annan begränsning är att hemlig övervakning av elektronisk kommunikation inte får avse meddelanden som endast överförs eller har överförts i ett elektroniskt kommunikationsnät som med hänsyn till sin begränsade omfattning och omständigheterna i övrigt får anses vara av mindre betydelse från allmän kommunikationssynpunkt (se 27 kap. 20 § tredje stycket rättegångsbalken). Några motsvarande begränsningar framgår inte av det andra tilläggsprotokollet.

Artikel 8 kommer att tillämpas gentemot stater vars rättssystem avsevärt torde avvika från svenska bestämmelser, t.ex. att trafikuppgifter kan inhämtas för mindre allvarliga brott än vad som följer av svenska bestämmelser eller avse elektroniska kommunikationsnät som inte kan bli föremål för hemlig övervakning av elektronisk kommunikation enligt rättegångsbalkens regler.

Av såväl lagen om en europeisk utredningsorder (3 kap. 4 §) som lagen om internationell rättslig hjälp i brottmål (2 kap. 1 §) följer att Sverige samarbetar med andra stater utifrån samma förutsättningar som gäller för en motsvarande åtgärd i ett inhemskt ärende. Ett samarbete som innebär att Sverige ska bistå andra stater med åtgärder som svenska myndigheter inte hade kunnat vidta, trots att någon sådan skyldighet inte finns, bör därför undvikas.

Enligt artikel 8.13 i det andra tilläggsprotokollet kan en stat förbehålla sig att över huvud taget inte tillämpa artikel 8 på trafik-

uppgifter. Vi menar att det då inte bör föreligga något hinder att lämna ett partiellt förbehåll som överensstämmer med nu gällande bestämmelser. Bilagan till rådsbeslutet 2023/436 (p. 1) kan inte heller anses hindra ett sådant förbehåll.

Sverige bör därför lämna en förklaring i vilken Sverige förbehåller sig att artikel 8 endast kan tillämpas på de brott och brottstyper som avses i 27 kap. 19 a § andra stycket och 19 b § andra stycket rättegångsbalken. Vidare bör Sverige förbehålla sig rätten att inte tillämpa artikel 8 vad avser insamling av trafikuppgifter inom en tjänsteleverantörs datorsystem som dels drivs för en sluten användargrupp, dels inte använder allmänna kommunikationsnät och inte är anslutet till ett annat datorsystem.

12.7 Utlämnande av uppgifter i nödsituationer (artiklarna 9 och 10)

12.7.1 Det närmare innehållet i artiklarna 9 och 10

Innehållet i artikel 9

Artikel 9 föreskriver ett påskyndat utlämnande av lagrade datorbehandlingsbara uppgifter i en nödsituation.

En nödsituation definieras i artikel 3.2 c som ”en situation där det föreligger en betydande och överhängande risk för en fysisk persons liv eller säkerhet”. Enligt den förklarande rapporten kan en nödsituation t.ex. avse en gisslansituation där det finns en trolig risk för omedelbar förlust av liv eller allvarlig skada för brottsoffret, pågående sexuella övergrepp mot barn, de omedelbara efterdyningarna av en terroristattack och hot mot säkerheten för kritisk infrastruktur där det finns en betydande och överhängande risk för en fysisk persons liv eller säkerhet (p. 42). Andra exempel på en nödsituation som nämns är en ransomware-attack som riskerar att lamslå ett sjukhusystem eller en kidnappningssituation där ett e-postkonto används av kidnappare för att ställa krav och kommunicera med offrets familj (p. 148).

Artikeln påverkar enligt rapporten inte annat samarbete mellan parterna, eller mellan parterna och tjänsteleverantörer, som sker genom andra tillämpliga avtal, arrangemang, praxis eller nationell

lagstiftning i vilket samarbete uppgifter begärs ut i en nödsituation (p. 150).

Varje part ska enligt artikel 9.1 a anta den lagstiftning och de andra åtgärder som krävs för att dess kontaktpunkt inom det 24/7-nätverk av kontaktpunkter som har inrättats genom artikel 35 i Budapestkonventionen i nödsituationer ska kunna vidarebefordra en framställning till och ta emot en framställning från en kontaktpunkt i en annan part som begär omedelbar hjälp med att få ut lagrade datorbehandlingsbara uppgifter som en tjänsteleverantör innehar eller kontrollerar, utan någon framställning om ömsesidig rättslig hjälp.

Nätverket är enligt den förklarande rapporten särskilt väl lämpat för att hantera de brådskande förfrågningar som avses i artikeln (se p. 151). Nätverket är bemannat med kontaktpunkter som kommunicerar skyndsamt och utan behov av skriftliga översättningar. Kontaktpunkterna kan verkställa framställningar från andra parter, antingen genom att vända sig direkt till leverantörer på deras territorium eller genom att begära hjälp från andra behöriga myndigheter, om detta krävs enligt partens nationella lagstiftning. Dessa kontaktpunkter kan också ge råd till begärande parter om frågor som de kan ha om leverantörer och insamling av elektroniska bevis, t.ex. genom att förklara den nationella lagstiftning som måste vara förenlig för att inhämta bevis.

Termen "specificerade, lagrade datorbehandlingsbara uppgifter" omfattar alla specificerade datorbehandlingsbara uppgifter enligt definitionen i artikel 1 b i Budapestkonventionen. Enligt den artikeln avser termen "framställning av fakta, information eller begrepp i en form som lämpar sig för behandling i ett datorsystem, inklusive program som utformats för att få ett datorsystem att utföra en viss funktion". Begreppet omfattar enligt den förklarande rapporten lagrat innehåll och befintliga trafikuppgifter, och inte endast abonnemangsuppgifter, men inte trafikuppgifter och innehållsuppgifter som avser framtida kommunikation (p. 155).

En part får enligt artikel 9.1 b förklara att den inte kommer att verkställa framställningar enligt artikel 9.1 a som endast avser utlämnande av abonnemangsuppgifter. I den förklarande rapporten anges som skäl att en begäran enligt artikeln om enbart om abonnemangsuppgifter kan riskera att överbelasta kontaktpunkterna i 24/7-nätverket genom att avleda resurser och energi från för-

frågningar om innehåll eller trafikuppgifter (p. 157). I sådana fall får parter som endast vill ha abonnentuppgifter använda sig av artiklarna 7 eller 8. Enligt bilagan till rådsbeslutet 2023/436 (p. 2) uppmuntras medlemsstaterna dock att avstå från att avge en sådan förklaring.

Vidare ska varje part enligt artikel 9.2 anta den lagstiftning och de andra åtgärder som krävs för att dess myndigheter kan begära ut uppgifter från en tjänsteleverantör, vilken begäran leverantören ska kunna besvara, samt översända inhämtade uppgifter till den ansökande staten.

I artikel 9.3 anges den information som ska lämnas i en begäran enligt artikel 9.1. Detta omfattar bl.a. namn på och adress till den eller de tjänsteleverantörer som innehar eller kontrollerar de begärda uppgifterna, det eller de brott som är föremål för brottsutredningen eller det straffrättsliga förfarandet och en hänvisning till de rättsliga bestämmelser och tillämpliga påföljder som gäller för brottet samt tillräckliga fakta för att visa att det föreligger en nödsituation och hur de begärda uppgifterna förhåller sig till den. Det är enligt den förklarande rapporten den anmodade parten som har att avgöra om det föreligger en nödsituation i samband med en framställning med hjälp av de upplysningar som lämnas enligt artikel 9.3 (p. 154).

Den anmodade parten ska enligt artikel 9.4 godta en framställning i elektronisk form. En part får också godta en muntlig framställning och kan då kräva bekräftelse i elektronisk form. Den får kräva lämpliga säkerhets- och autentiseringsnivåer innan framställningen godtas.

Enligt artikel 9.5 får en part avge en förklaring om att den ansökande parten, efter det att begäran har verkställts och uppgifterna har översänts, ska lämna in framställningen och eventuell kompletterande information som översänts till stöd för denna i ett sådant format och via en sådan kanal, vilket kan inbegripa ömsesidig rättslig hjälp.

Den anmodade parten ska enligt artikel 9.6 underrätta den ansökande parten om sitt beslut om framställningen enligt artikel 9.1 och, i tillämpliga fall, ange på vilka villkor den skulle tillhandahålla uppgifterna och varje annan form av samarbete som kan komma i fråga. Bestämmelsen innebär enligt den förklarande rapporten att den anmodade parten i ett särskilt fall får besluta att ömsesidig

rättslig hjälp i nödsituationer enligt artikel 10 eller någon annan form av samarbete skulle vara lämpligast (p. 169).

I artikel 9.7 beskrivs de tillämpliga förfarandena när den anmodade staten har enligt artikel 9.6 specificerat villkor för att lämna ut de begärda uppgifterna.

Innehållet i artikel 10

Artikel 10 i syftar till att tillhandahålla ett påskyndat förfarande för framställningar om ömsesidig rättslig hjälp i nödsituationer. Begreppet ”nödsituation” har samma innebörd som i artikel 9.

Varje part får enligt artikel 10.1 ansöka om ömsesidig rättslig hjälp enligt ett skyndsamt förfarande om den anser att det föreligger en nödsituation. En framställning ska, utöver det övriga innehåll som krävs, innefatta en beskrivning av de fakta som visar att en nödsituation föreligger och hur den begärda hjälpen förhåller sig till den. En anmodad part ska enligt artikel 10.2 godta en sådan framställning i elektronisk form. Den får kräva lämpliga säkerhets- och autentiseringsnivåer innan framställningen godtas.

Den anmodade parten får enligt artikel 10.3 begära kompletterande information enligt ett skyndsamt förfarande för att kunna bedöma framställningen. Den ansökande parten ska tillhandahålla sådan kompletterande information enligt ett skyndsamt förfarande. När den anmodade parten har förvissat sig om att en nödsituation föreligger och övriga krav för ömsesidig rättslig hjälp är uppfyllda ska den besvara framställningen enligt ett skyndsamt förfarande (artikel 10.4).

Varje part ska säkerställa att en person från dess centralmyndighet eller andra myndigheter med ansvar för att besvara framställningar om ömsesidig rättslig hjälp är tillgänglig dygnet runt för att besvara en framställning (artikel 10.5). I den förklarande rapporten erinras om att 24/7-nätverket i enlighet med artikel 35 i Budapestkonventionen är tillgängligt för samordning med de myndigheter som ansvarar för ömsesidig rättslig hjälp (p. 177).

Centralmyndigheten eller andra myndigheter med ansvar för ömsesidig rättslig hjälp får enligt artikel 10.6 besluta att inhämtade uppgifter får lämnas till den ansökande parten via en annan kanal än den som används för framställningen. I den förklarande rapporten

anges att i en nödsituation kan myndigheterna t.ex. besluta om översändande av bevis direkt till en utredande myndighet eller åklagarmyndighet i den ansökande parten snarare än genom den kedja av myndigheter genom vilken sådan bevisning normalt skulle färdas (p. 177).

I artikel 10.7 föreskrivs att när de berörda parterna inte är ömsesidigt bundna av ett tillämpligt avtal eller arrangemang om ömsesidig rättslig hjälp, ska parterna tillämpa vissa angivna punkter i artiklarna 27 och 28 i Budapestkonventionen (om ömsesidig rättslig hjälp i avsaknad av ett avtal). Av artikel 10.8 följer att när de berörda parterna är ömsesidigt bundna av ett sådant avtal eller arrangemang, ska artikel 10 kompletteras med bestämmelserna i det avtalet eller arrangemanget, såvida inte de berörda parterna ömsesidigt beslutar att tillämpa någon eller alla av de bestämmelser i konventionen som det hänvisas till i artikel 10.7.

Slutligen får varje part enligt artikel 10.9 förklara att framställningar också kan sändas direkt till dess rättsliga myndigheter eller via Internationella kriminalpolisorganisationens (Interpol) kanaler eller till 24/7-nätverket som har inrättats enligt artikel 35 i Budapestkonventionen.

Förhållandet mellan artiklarna 9 och 10

Att använda det förfarande som följer av artikel 9 kan enligt den förklarande rapporten vara mer fördelaktigt än det förfarande för ömsesidig rättslig hjälp i nödsituationer som anges i artikel 10 (p. 152). Fördelen med att använda sig av artikel 9 är t.ex. att det inte finns något behov av att göra en begäran om ömsesidig rättslig hjälp i förväg. När det gäller rättslig hjälp kräver de anmodade parterna ofta att den kompletterande informationen ska lämnas i skriftlig och mer detaljerad form, medan det genom 24/7-nätverket kan ske utbyte av information i realtid. Å andra sidan erbjuder artikel 10 fördelar i vissa situationer. T.ex. kan liten eller ingen tid gå förlorad genom att använda detta förfarande om det finns särskilt nära arbetsrelationer mellan de berörda centrala myndigheterna. Ömsesidig rättslig hjälp i nödsituationer får även användas för att få till stånd ytterligare former av samarbete utöver inhämtning av lagrade behandlingsbara uppgifter som tjänsteleverantörer

innehar eller kontrollerar. Det är upp till parterna att, på grundval av sin samlade erfarenhet och de specifika rättsliga och faktiska omständigheterna, avgöra vilken kanal som är bäst att använda i ett visst fall.

12.7.2 Gällande rätt

I varken lagen om internationell rättslig hjälp i brottmål eller lagen om en europeisk utredningsorder finns särskilda bestämmelser om rättslig hjälp i brottmål eller verkställighet av en europeisk utredningsorder i nödsituationer.

I 2 kap. 10 § lagen om internationell rättslig hjälp i brottmål finns en bestämmelse om att en ansökan om rättslig hjälp ska handläggas skyndsamt. Lagen om en europeisk utredningsorder anger också att prövningen ska skyndsamt samt inom vissa angivna tidsfrister (3 kap. 16 och 23 §§).

När det gäller sättet att sända över en ansökan om rättslig hjälp är huvudregeln enligt 2 kap. 6 § och 3 kap. 2 § lagen om internationell rättslig hjälp i brottmål att en ansökan skickas centralmyndigheten på Justitiedepartementet. En ansökan kan emellertid enligt samma bestämmelser sändas över från eller till åklagare om det framgår av en internationell överenskommelse som är bindande för Sverige. I samarbetet enligt lagen om en europeisk utredningsorder ska en utfärdad utredningsorder skickas från eller till handläggande åklagare (2 kap. 7 § och 3 kap. 13 §). Oaktat vilken lag som tillämpas finns inga hinder att en åklagare sänder eller tar emot en ansökan eller utredningsorder via 24/7-nätverket.

I Sverige är Polismyndigheten utsedd som kontaktpunkt för 24/7-nätverket enligt 5 § förordningen (2022:1718) med instruktion för Polismyndigheten.

12.7.3 Översändande av framställningar enligt artikel 9 och dess innehåll

Bedömning: Inga ändringar i lag behövs.

Skälen för bedömningen: Huvudsyftet med artikel 9 är att till skapa ett mer skyndsamt förfarande när det gäller inhämtning av lagrade datorbehandlingsbara uppgifter från en tjänsteleverantör på den anmodade statens territorium. Några specifika tidsfrister anges dock inte i artikel 9. För att uppnå syftet med bestämmelsen åläggs avtalsparterna dels att använda sig av 24/7-nätverket som har inrättats enligt artikel 35 i Budapestkonventionen för att skicka och ta emot framställningar avseende ett sådant inhämtande, dels att dessa framställningar, med det innehåll som framgår av artikel 9.3, ska accepteras i stället för en ansökan om rättslig hjälp. Slutligen åläggs den anmodade parten att skyndsamt underrätta den ansökande parten om sitt beslut.

Artikel 9 innebär således inte några krav på att en anmodad part ska lämna ut lagrade datorbehandlingsbara uppgifter under andra förutsättningar än dem som gäller för ömsesidig rättslig hjälp eller vid erkännande och verkställighet av en europeisk utredningsorder, vilket tydliggörs i den förklarande rapporten (se t.ex. p. 160). Några ändringar i lag i detta avseende behövs därför inte.

Bestämmelserna i 2 kap. 3 och 4 §§ lagen om internationell rättslig hjälp i brottmål innebär att en framställning kan göras av den som enligt en internationell överenskommelse som är bindande för Sverige får göra en sådan ansökan samt att innehållet i ansökan kan anpassas till vad som framgår eller krävs av en sådan överenskommelse. Med stöd av dessa bestämmelser bör en anmodad part kunna sända över en framställning – oaktat att det i bestämmelserna talas om en ansökan om rättslig hjälp – via sin kontaktpunkt i 24/7-nätverket till Sverige med det innehåll som framgår av artikel 9.3. Även i det motsatta förhållandet, dvs. då Sverige är ansökande part bör bestämmelserna i 3 kap. 1 och 2 §§ vara tillräckliga för att en framställning, med det innehåll som anges i artikel 9.3, ska kunna skickas till den andra statens kontaktpunkt i nämnda nätverk.

I 2 kap. 6 § och 3 kap. 2 § lagen om internationell rättslig hjälp i brottmål anges att en ansökan (eller en framställning) kan skickas direkt till eller från en åklagare om det följer en internationell

överenskommelse. Bestämmelserna utgör således inget uttryckligt stöd för att framställningar enligt artikel 9.1 kan skickas direkt till eller från Sveriges kontaktpunkt i 24/7-nätverket (dvs. Polismyndigheten).

När nätverket inrättades genom Budapestkonventionen var tanken att staternas kontaktpunkter skulle kunna kommunicera med varandra skyndsamt men även att utsedd kontaktpunkt skulle kunna samverka skyndsamt med den myndighet som är ansvarade för frågor om internationell rättslig hjälp.⁸ Motsvarande framgår av den förklarande rapporten till konventionen (p. 298). Vid Sveriges tillträde till konventionen ansågs det inte föreligga något behov av lagändringar i förhållande till lagen om internationell rättslig hjälp i brottmål och lagen om en europeisk utredningsorder.⁹ Vi gör ingen annan bedömning i förhållande till artikel 9 i det andra tilläggsprotokollet. Polismyndigheten får i detta avseende i rollen som kontaktpunkt i 24/7-nätverket mer ses som en brevlåda som framställningar skickas från och till, vilket inte behöver regleras i lag. Redan i dag samverkar Polismyndigheten i rollen som kontaktpunkt med Åklagarmyndigheten när det gäller Budapestkonventionen.

En ändring i lagen om internationell rättslig hjälp i brottmål att Polismyndigheten skulle vara behörig att skicka och ta emot framställningar enligt nämnda lag för att enbart leva upp till artikel 9 (framställningar i nödsituationer) skulle vidare kunna leda till motsatsvisa tolkningar beträffande det övriga samarbetet. Detta bör således undvikas.

Sammanfattningsvis anser vi att artikel 9 inte föranleder något behov av att ändra i lagen om internationell rättslig hjälp i brottmål på så sätt att även Polismyndigheten inkluderas uttryckligen i 2 kap. 6 och 3 kap. 2 §.

Med beaktande av 2 kap. 4 § tredje stycket lagen om internationell rättslig hjälp i brottmål behövs inga ändringar i lag när det gäller artikel 9.4 om sättet att sända över en ansökan.

Enligt artikel 9.5 kan en stat avge en förklaring att en ansökande part efter det att framställning verkställts ska lämna in framställningen med eventuell kompletterande information på det sätt som anges av den anmodade parten. Eftersom en framställning som ges

⁸ SOU 2013:39 s. 200.

⁹ Se prop. 2020/21:72 s. 64.

in till Polismyndigheten enligt artikel 9.1 a kommer att vidarebefordras till åklagare för en prövning om efterfrågade uppgifter ska lämnas ut med stöd av de sedvanliga förutsättningarna i lagen om internationell rättslig hjälp i brottmål ser vi inget behov av att Sverige avger en sådan förklaring.

En avtalspart kan vidare enligt artikel 9.1 b i en förklaring ange att den inte kommer verkställa framställningar enligt artikel 9.1 a som enbart avser abonnemangsuppgifter. Mot bakgrund av bilagan till rådsbeslutet 2023/436 (p. 2) i vilken medlemsstaterna uppmuntras att inte avge en sådan förklaring gör vi den bedömningen att någon sådan förklaring inte ska avges. Dessutom torde artikel 9 i sig inte ändra de brottsbekämpande myndigheternas behov av tillgång till abonnemangsuppgifter, dvs. fler framställningar just på grund av nämnda artikel kan inte förutses. Vidare så är artikel 9 endast tillämplig på nödsituationer, dvs i undantagsfall.

Bestämmelserna i artikel 9 om översändande av en framställning eller dess innehåll föranleder inte heller några ändringar i lagen om en europeisk utredningsorder. Vår bedömning är att det inte finns något hinder mot att använda sig av 24/7-nätverket för att sända över en europeisk utredningsorder (se ovan angående förarbetena om användandet av nätverket i förhållande till Budapestkonventionen). Inom EU pågår dock ett arbete som innebär att europeiska utredningsorder på sikt kommer att skickas snabbt och säkert via digitala plattformar. När det gäller bestämmelserna i artikel om en framställnings innehåll kan de inte påverka vad en europeisk utredningsorder ska innehålla. Om en behörig myndighet i medlemsstat i en nödsituation vill använda sig av detta regelverk har myndigheten inte val annat än att leva upp till de krav som gäller för en sådan orders innehåll. När det gäller en medlemsstats möjlighet att i stället använda sig av artikel 9 och förfarandet enligt lagen om internationell rättslig hjälp i brottmål hänvisas till avsnitt 12.11.

12.7.4 Skyndsamhetskravet i artiklarna 9 och 10

Förslag: Om det föreligger en omedelbar fara för liv, hälsa eller egendom, ska särskild hänsyn tas till kravet om skyndsamhet vid handläggningen av ett ärende enligt lagen om internationell rättslig hjälp i brottmål.

Motsvarande bestämmelse ska föras in i lagen om en europeisk utredningsorder.

Skälen för förslaget: Artikel 9 ställer, som nämnts i föregående avsnitt, inte något krav på att en framställning enligt artikeln ska hanteras inom en viss tidsfrist, men anger dock att förfarandet ska vara skyndsamt med hänvisning till att uppgifterna behövs för att hantera en nödsituation.

Enligt 2 kap. 4 § lagen om internationell rättslig hjälp i brottmål kan den som gör en framställning ange om ärendet är brådskande eller om verkställigheten önskas inom en viss tidsfrist. Vidare föreskrivs i 2 kap. 10 § i samma lag att ärendet ska handläggas skyndsamt. Dock föreskrivs inga direkta tidsfrister i lagen. När det gäller skyndsamhetskravet är utgångspunkten att samma skyndsamhet ska iakttas som när motsvarande åtgärd vidtas i ett inhemskt ärende.¹⁰

Föreligger en nödsituation, dvs. en omedelbar fara för liv, hälsa eller egendom, är behovet av extra skyndsamhet stor. Vi anser att nuvarande lagstiftning inte tillräckligt tydligt beaktar dessa situationer.

Ett krav på skyndsamt handläggning kan utformas på olika sätt, antingen som ett allmänt utformat krav eller i form av en särskild angiven tidsfrist. När det konstateras att en måltyp har behov av extra skyndsamhet bör alltid den minst ingripande åtgärd som kan möta behovet användas. Ett krav på skyndsamt handläggning med närmare bestämda tidsfrister är förbehållen situationer där skyndsamhetskravet korresponderar med ett särskilt starkt skyddsintresse (se avsnitt 7.5.7). Ett sådant skyddsintresse bör anses vara för handen när det föreligger en sådan nödsituation som avses i artikel 10.

Med hänsyn till att nödsituationer som faller inom artikelns tillämpningsområde kan vara av vitt skild natur är det dock svårt att

¹⁰ Se prop. 1999/2000:61 s. 103.

formulera en tidsfrist som kan vara användbar i samtliga situationer som kan uppstå. För att emellertid säkerställa att en framställning som rör nödsituationer behandlas skyndsamt, bör det framgå av 2 kap. 10 § lagen om internationell rättslig hjälp i brottmål att det vid handläggningen av en ansökan ska särskild hänsyn tas till om det är fråga om en omedelbar fara för liv, hälsa eller egendom, vilket får anses motsvara begreppet nödsituation såsom det beskrivs i den förklarande rapporten. Som framgår av den förklarande rapporten till artikeln är det den handläggande myndigheten, dvs. åklagaren, som avgör om det föreligger en nödsituation (p. 154). Åklagaren kommer således med hänsyn till omständigheterna i det enskilda fallet kunna bedöma behovet av skyndsamhet. Med denna bestämmelse kan det särskilda skyndsamhetskravet i artikel 9 iakttas.

Vi anser att den föreslagna bestämmelsen om att särskild hänsyn ska tas till skyndsamhetskravet i 2 kap. 10 § lagen om internationell rättslig hjälp i brottmål om det föreligger en omedelbar fara för liv, hälsa eller egendom även bör vara generell tillämplig i förhållande till ansökningar om rättslig hjälp. Förutom att en sådan generell regel omhändertar motsvarande skyndsamhetskrav i artikel 10 i det andra tilläggsprotokollet, se vi inga hinder mot att den kan tillämpas även i andra situationer. Rör det sig om en nödsituation bör svenska myndigheter bistå så fort det är möjligt oaktat vilken åtgärd som avses eller vilken stat som ansöker om rättslig hjälp. Eftersom det är åklagaren som kommer att avgöra om det föreligger en nödsituation, kan eventuellt ett överanvändande undvikas.

En motsvarande ändring bör göras i 3 kap. 23 § lagen om en europeisk utredningsorder på de skäl som angetts ovan.

12.7.5 Lagstiftningsbehovet beträffande övriga bestämmelser i artikel 10

Bedömning: Inga ändringar i lag behövs.

Skälen för förslaget: Bestämmelsen i artiklarna 10.2 och 10.3 i det andra tilläggsprotokollet om sättet att sända över en ansökan om rättslig hjälp och möjligheterna att begära kompletterande infor-

mation kräver med hänsyn till 2 kap. 4 och 9 §§ lagen om internationell rättslig hjälp i brottmål inga ändringar i lag.

Kravet på sådan dygnet-runt bemanning som avses i artikel 10.5 får anses vara uppfyllt genom den inrättande kontaktpunkten enligt artikel 35 i Budapestkonventionen samt den jourverksamhet som Åklagarmyndigheten bedriver och det samarbete som finns mellan denna myndighet och Polismyndigheten som är utsedd kontaktpunkt.

Artikel 10.7 rör förfarandet vid ömsesidig rättslig hjälp när det saknas ett fördrag eller arrangemang. I artikeln anges att vissa bestämmelser i artiklarna 27 och 28 i Budapestkonventionen ska vara tillämpliga på artikel 10.

Artikel 27 i Budapestkonventionen reglerar ömsesidig rättslig hjälp när tillämpliga internationella avtal saknas. Där regleras bland annat vilken parts lagar som styr förfarandet, vilka skäl som ska vara giltiga för ett avslag och vad som ska gälla vid en begäran om hemlighållande. Artikeln innehåller också bestämmelser om att parterna ska utse och anmäla en centralmyndighet.

I svensk rätt finns, som tidigare behandlats, regler om förfarandet, skäl för avslag och sekretess m.m. i ärenden om internationell rättslig hjälp i bl.a. lagen om internationell rättslig hjälp i brottmål och offentlighets- och sekretesslagen (2009:400). Om en konventionsstat som Sverige inte har några avtal med begär att reglerna i artikel 10.7 i tilläggsprotokollet och artikel 27 i Budapestkonventionen ska tillämpas på en framställan om rättslig hjälp kan Sverige tillmötesgå en sådan begäran med stöd av befintlig lagstiftning och det skulle inte uppstå någon konflikt mellan regelverken. Artikeln kräver därför inte några lagstiftningsåtgärder.¹¹

I artikel 28 i Budapestkonventionen finns en möjlighet för den anmodade staten att ställa upp dels krav på sekretess, dels begränsningar i fråga om användningen.

Svenska myndigheter kan i dag frivilligt lämna information till en annan stat, med de begränsningar som gäller med hänsyn till sekretess, se t.ex. 8 kap. 3 § offentlighets- och sekretesslagen. De kan då ställa villkor som begränsar den mottagande statens användning av uppgifterna¹². Möjligheten att ställa villkor som begränsar den mottagande statens användning av uppgifterna finns även i

¹¹ Se prop. 2020/21:72 s. 61–62.

¹² Se bl.a. prop. 2012/13:170 s. 23 och prop. 2009/10:78 s. 37.

annan lagstiftning (5 kap. 2 § lagen om internationell rättslig hjälp i brottmål). Det finns också bestämmelser om bindande villkor för hur uppgifterna får användas när en svensk myndighet är mottagare av informationen (se 5 kap. 1 § i samma lag).

Svenska myndigheter kan således tillmötesgå en begäran om användningsbegränsningar från en annan fördragsslutande stat med stöd av nämnda bestämmelser och det krävs därför inte några lagstiftningsåtgärder för att uppfylla kraven i artikel 10.7 som hänvisar till artikel 28 i Budapestkonventionen.¹³

Av artikel 10.8 följer att om det finns ett fördrag eller arrangemang om ömsesidig rättslig hjälp ska artikel 10 kompletteras med de bestämmelserna, om inte parterna beslutar att tillämpa de bestämmelser som anges i artikel 10.7. Bestämmelsen kräver inte heller några lagstiftningsåtgärder.

För att underlätta samarbetet bör en förklaring med det innehåll som föreskrivs i artikel 10.9 avges. Det innebär att framställningar kan sändas direkt till eller från svenska rättsliga myndigheter utan att behöva involvera centralmyndigheten. Med stöd av 2 kap. 6 § och 3 kap. 2 § lagen om internationell rättslig hjälp i brottmål kan framställningar redan skickas direkt på det sätt som anges i nämnda artikel.

Vår bedömning är vidare att några ändringar i lagen om en europeisk utredningsorder inte behövs när det gäller artikel 10 (förutom skyndsamhetskravet). Samarbetet enligt nämnda lag (och det bakomliggande direktivet) följer en viss struktur beträffande en utredningsorders innehåll och sättet att sända över en sådan order. Några ändringar kan inte ske i nämnda lag för att efterleva vissa bestämmelser i det andra tilläggsprotokollet men som samtidigt inte är förenligt med direktivet om en europeisk utredningsorder. Dock kan vi konstatera att inget hindrar att en utredningsorder sänds över i elektronisk form eller att möjligheten att begära kompletteringar av en utfärdad utredningsorder (se 2 kap. 7 § och 3 kap. 13 och 14 §§ lagen om en europeisk utredningsorder). Det 24/7-nätverk som upprättats i och med artikel 35 i Budapestkonventionen bör på samma sätt som vid internationell rättslig hjälp i brottmål kunna hantera en utfärdad europeisk utredningsorder. Övriga bestämmelser anser vi inte påverkar bestämmelserna i lagen om en europeisk utredningsorder.

¹³ Se prop. 2020/21:72 s. 62.

12.8 Förfarandet för internationellt samarbete i avsaknad av avtal (artiklarna 11 och 12)

12.8.1 Innehållet i artiklarna 11 och 12

Avsnitt 5 i det andra tilläggsprotokollet består av artiklarna 11 och 12 som innehåller bestämmelser om videokonferenser och gemensamma utredningsgrupper.

Artiklarna 11 och 12 är enligt artikel 5.5 tillämpliga (förutom artikel 12.7) om det inte finns ett fördrag eller arrangemang om ömsesidig rättslig hjälp mellan den ansökande och den anmodade parten. Det samarbete som föreskrivs i artiklarna 11 och 12 kan enligt den förklarande rapporten föreskrivas i andra internationella överenskommelser, t.ex. det andra tilläggsprotokollet till Europarådskonventionen om ömsesidig rättslig hjälp i brottmål (SÖ 2014:6) eller avtal om ömsesidig rättslig hjälp mellan Europeiska unionen och Amerikas förenta stater (p. 183). Sådana avtal kan också enligt rapporten ge mer detaljer angående de omständigheter och villkor under vilka sådant samarbete får äga rum. Även om en sådan internationell överenskommelse finns får de berörda parterna ömsesidigt besluta att i stället tillämpa bestämmelserna i artiklarna 11 och 12, om överenskommelsen inte förbjuder det.

Artikel 11 innehåller bestämmelser om upptagande av vittnesmål och andra utsagor genom videokonferens. Av artikel 11.1 följer att en ansökande part får begära och den anmodade parten får medge att vittnesmål och utsagor inhämtas från ett vittne eller en sakkunnig genom videokonferens. Parterna ska samråda för att underlätta lösningen av eventuella problem som kan uppstå i samband med verkställigheten av framställningen, t.ex. i fråga om vem som ska leda videokonferensen, vilka myndigheter och personer som ska närvara eller om den ena eller båda parterna ska ansvara för att ta upp särskilda eder från vittnen och sakkunniga. I artikel 11 finns i övrigt bestämmelser om bl.a. processuella förfaranden för genomförande av videokonferens samt ansvar för kostnader som uppkommit i samband med en videokonferens.

Artikel 12 innehåller bestämmelser om gemensamma utredningsgrupper och gemensamma utredningar. Genom en ömsesidig överenskommelse får två eller flera parters behöriga myndigheter enligt artikel 12.1 inrätta och driva en gemensam utredningsgrupp på sina territorier för att underlätta brottsutredningar eller straffrättsliga

förfaranden, om en förstärkt samordning anses vara av särskilt stor nytta.

Förfarandena och villkoren för en gemensam utredningsgrupps verksamhet, bl.a. gruppens ändamål, sammansättning och varaktighet och dess lokalisering, organisation och villkoren för en parts deltagande samt villkor för insamling, överföring och användning av information eller bevis ska vara de som överenskommits mellan dessa behöriga myndigheter (artikel 12.2). Artikel 12.4–12.6 innehåller i övrigt bestämmelser om bl.a. kommunikation mellan de behöriga myndigheterna, vidtagande av utredningsåtgärder, användning av information och bevisning. Enligt artikel 12.7 får gemensamma utredningar genomföras enligt överenskomna villkor från fall till fall vid avsaknad av en sådan överenskommelse som beskrivs i artikel 12.1–2. Artikeln är tillämplig oavsett om det finns ett fördrag eller arrangemang om ömsesidig rättslig hjälp på grundval av gällande enhetlig eller gemensam lagstiftning mellan de berörda parterna.

12.8.2 Gällande rätt

Enligt svensk rätt får rättslig hjälp lämnas i fråga om förhör genom videokonferens under såväl rättegång som under förundersökning (1 kap. 2 §, 4 kap. 11 och 12 §§ lagen om internationell rättslig hjälp i brottmål). Om ansökan gäller ett förhör under rättegång ska den handläggas av en tingsrätt, varvid ärendet ska ses som en bevisupptagning utom huvudförhandling. Om ansökan gäller förhör under förundersökning ska ärendet handläggas av svensk åklagare.

Även svenska domstolar och åklagare får ansöka om rättslig hjälp vid utländsk myndighet med förhör genom videokonferens, om det avtalats om sådan rättslig hjälp i en internationell överenskommelse eller om den andra staten annars ger sådan hjälp (4 kap. 13 § lagen om internationell rättslig hjälp i brottmål).

Rättslig hjälp med förhör genom videokonferens ska i huvudsak lämnas enligt samma förutsättningar som om åtgärden skulle ha vidtagits i en svensk förundersökning eller rättegång (2 kap. 1 § lagen om internationell rättslig hjälp i brottmål). När det gäller vittnesförhör som tas upp inom ramen för rättslig hjälp uppstår t.ex. frågor om vittnesplikt och om straffansvar för oriktiga vittnes-

utsagor. Visserligen sker vittnesförhöret som en del av ett utländskt förfarande men samtidigt innebär rättslig hjälp att förhöret genomförs vid en domstol i den anmodade staten och det är den senare domstolen som har kallat vittnet att infinna sig för att avlägga sitt vittnesmål. Det innebär t.ex. att frågor om vittnesplikt och rätt att vägra att yttra sig bestäms av svenska rättegångsregler. Frågor om ansvar för vägran att vittna trots vittnesplikten och ansvar för oriktiga eller ofullständiga uppgifter ska alltså avgöras enligt de regler som gäller i Sverige (som anmodad stat). Reglerna i 36 kap. 21 § rättegångsbalken om sanktioner vid vittnes vägran att avlägga ed, avge vittnesmål, besvara en fråga eller följa ett föreläggande att vidta vissa förberedande åtgärder gäller liksom straffbestämmelserna om mened m.m. i 15 kap. brottsbalken som gäller utsagor inför svensk domstol.

I förordningen om internationell rättslig hjälp i brottmål finns regler om återkrav av kostnader som uppstått med anledning av en ansökan om rättslig hjälp.

Lagen om en europeisk utredningsorder innehåller motsvarande regler om förhör genom videokonferens, vilket i lagen benämns förhör genom ljud- och bildöverföring (se 1 kap. 1 § 4, 2 kap. 1–3, 10 och 11 §§ samt 3 kap. 2 §).

I svensk rätt finns regler om gemensamma utredningsgrupper i lagen om vissa former av internationellt samarbete i brottsutredningar. Lagen innehåller regler om bl.a. inrättande av en gemensam utredningsgrupp, utredningsåtgärder som en sådan grupp vidtar i Sverige samt villkor för användning av uppgifter som erhållits genom en utredningsgrupp. Till skillnad från vad som gäller för samarbetsformerna som stadgas i lagen om internationell rättslig hjälp i brottmål är inte reglerna om gemensamma utredningsgrupper i ovan nämnda lag generellt tillämpliga. Lagen gäller endast för sådana gemensamma utredningsgrupper för brottsutredningar som inrättas mellan myndigheter i Sverige och myndigheter i en eller flera stater med stöd av de internationella överenskommelser som anges i 1 § nämnda lag, bl.a. konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater samt det andra tilläggsprotokollet till Europarådskonventionen om ömsesidig rättslig hjälp i brottmål.

12.8.3 Lagstiftningsbehovet beträffande artiklarna 11 och 12

Förslag: Det ska införas en möjlighet att inrätta en gemensam utredningsgrupp även i förhållande till stater som tillträtt det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet.

Bedömning: Det andra tilläggsprotokollets föreskrifter om rättslig hjälp i fråga om videokonferens kräver inte några lagändringar.

Skälen för förslaget och bedömningen: Sverige har bl.a. tillträtt Europarådskonventionen om ömsesidig rättslig hjälp i brottmål och dess tilläggsprotokoll, bl.a. det andra tilläggsprotokollet som nämns i den förklarande rapporten (p. 183). Regleringen i lagen om internationell rättslig hjälp i brottmål har anpassats efter innehållet i denna och andra internationella överenskommelser, som innehåller regler om rättslig hjälp med förhör genom videokonferens vilka överensstämmer med innehållet i artikel 11 i det andra tilläggsprotokollet till Budapestkonventionen. Svenska åklagare och domstolar kan alltså redan i dag både lämna och söka rättslig hjälp med förhör genom videokonferens på sätt som föreskrivs i nämnda artikel. Som behandlats i föregående avsnitt är utgångspunkten för rättslig hjälp enligt lagen om internationell rättslig hjälp i brottmål och verkställighet enligt lagen om en europeisk utredningsorder att bistånd som huvudregel ska lämnas under förutsättning att åtgärden skulle varit möjlig att vidta i ett motsvarande svenskt förfarande. Det sagda innebär att svensk rätt redan är förenlig med tilläggsprotokollet i denna del och något behov av författningsändringar finns därmed inte.

Beträffande gemensamma utredningsgrupper bör det andra tilläggsprotokollet till Budapestkonventionen läggas till i den uppräkningslista av internationella överenskommelser som finns i 1 § lagen om vissa former av internationellt samarbete i brottsutredningar för att samarbete enligt artikel 12 i protokollet ska omfattas av lagen.

12.9 Skydd för personuppgifter (artikel 14)

12.9.1 Innehållet i artikel 14

Artikel 14 reglerar skydd för personuppgifter. Om inte annat föreskrivs i artiklarna 14.1 b och 14.1 c ska vardera parten enligt artikel 14.1 a behandla de personuppgifter som parten tar emot enligt protokollet i enlighet med artikel 14.2–14.15.

Om parterna är ömsesidigt bundna av ett internationellt avtal om för skydd av personuppgifter, och som är tillämpligt på överföring av personuppgifter i syfte att förebygga, förhindra, upptäcka, utreda och lagföra brott, och där det anges att behandlingen av personuppgifter enligt det avtalet uppfyller kraven i de berörda parternas uppgiftsskyddslagstiftning, ska villkoren i ett sådant avtal tillämpas på personuppgifter som mottas enligt det andra tilläggsprotokollet i stället för artikel 14.2–14.15, om inte annat överenskommit mellan de berörda parterna (artikel 14.1 b).

Om parterna däremot inte är ömsesidigt bundna av ett avtal får de gemensamt besluta att överföringen av personuppgifter kan ske på grundval av andra avtal eller överenskommelser mellan de berörda parterna i stället för artikel 14.2–14.15 (artikel 14.1 c).

I artikel 14.2 behandlas de ändamål för vilka parterna får behandla personuppgifter enligt protokollet. Av artikel 14.2 a följer att personuppgifter endast får behandlas för särskilda brottsutredningar eller straffrättsliga förfaranden som gäller brott med anknytning till datorsystem och data och för insamling av bevis i elektronisk form för ett brott, och för särskilda brottsutredningar eller straffrättsliga förfaranden som rör brott som straffbeläggs i enlighet med det första tilläggsprotokollet.

Enligt artikel 14.3 ska varje part vidta rimliga åtgärder för att säkerställa att personuppgifter bevaras med sådan precision och fullständighet och är så aktuella som är nödvändigt och lämpligt för en laglig behandling av personuppgifterna, med beaktande av de ändamål för vilka de behandlas. Artikel 14.4 innehåller bestämmelser om behandling av känsliga personuppgifter, vilka endast får behandlas om det finns garantier som skyddar mot risker för skadliga effekter vid användningen av uppgifterna, särskilt i fråga om olaglig diskriminering. Enligt artikel 14.5 ska personuppgifter lagras endast så länge som är nödvändigt och lämpligt. Av artikel 14.6 följer att beslut som har en betydande negativ inverkan på den

berörda personens intressen får inte grunda sig enbart på automatisk behandling av personuppgifter, om det inte är tillåtet enligt nationell rätt och det finns lämpliga garantier som innefattar möjligheten till mänskligt ingripande.

Enligt artikel 14.7 a ska varje part säkerställa att den har infört lämpliga tekniska, fysiska och organisatoriska åtgärder för skydd av personuppgifter, särskilt mot förlust eller oavsiktlig eller obehörig åtkomst, utlämnande, ändring eller förstöring (säkerhetsincident). Vid upptäckt av en säkerhetsincident som innebär en betydande risk för fysisk eller icke-fysisk skada för enskilda personer eller för den andra parten, ska den mottagande parten enligt artikel 14.7 b omgående bedöma sannolikheten för och omfattningen av skadan och omgående vidta åtgärder för att minimera skadan. Sådana åtgärder ska som huvudregel innefatta underrättelse till den överförande myndigheten eller den myndighet som utsetts enligt artikel 14.7 c att motta en sådan underrättelse samt även till den berörda personen, om inte parten har vidtagit lämpliga åtgärder så att det inte längre föreligger någon betydande risk för skada.

Artikel 14.8 föreskriver att varje part ska föra register eller ha andra lämpliga metoder för att visa hur en enskilds personuppgifter görs tillgängliga, används och lämnas ut i ett specifikt fall. Av artikel 14.9 a följer att när en parts myndighet tillhandahåller personuppgifter som ursprungligen mottagits enligt protokollet till en annan myndighet i den parten, ska den andra myndigheten som huvudregel behandla dem i enlighet med artikel 14. Enligt artikel 14.10 a får den mottagande parten överföra personuppgifterna till en annan stat eller till en internationell organisation endast med förhandstillstånd från den överförande myndigheten eller den eller de myndigheter som utsetts enligt artikel 14.10 b. Artikel 14.11 innehåller bestämmelser om underrättelse till den person vars uppgifter har samlats in och innehållet i en sådan underrättelse.

Varje part ska enligt artikel 14.12 a säkerställa att envar vars personuppgifter har mottagits enligt protokollet har rätt att, i enlighet med förfaranden som fastställs i dess nationella regelverk och utan onödigt dröjsmål, begära och erhålla

- en skriftlig eller elektronisk kopia av den dokumentation som bevaras om personen i fråga, vilken innehåller dennes personuppgifter och tillgänglig information som anger den rättsliga grunden för och syftet med behandlingen, lagringsperioderna

och mottagarna av uppgifterna, samt information om möjligheter till prövning,

- rättelse, om den enskildes personuppgifter är felaktiga eller har behandlats på ett felaktigt sätt som normalt ska innefatta korrigering, komplettering, radering eller anonymisering, begränsning av behandling eller blockering.

Om åtkomst eller rättelse vägras eller medges endast i begränsad omfattning ska parten enligt artikel 14.12 b utan onödigt dröjsmål lämna ett svar till den enskilde om vägran eller begränsningen. Skälen för en sådan vägran eller begränsning ska anges tillsammans med information om tillgängliga möjligheter till prövning.

Enligt artikel 14.13 ska varje part ska ha effektiva rättsmedel och prövningsförfaranden utanför domstol för att ge möjlighet till prövning vid överträdelse av artikel 14. Av artikel 14.14 följer vidare att varje part ska ha en eller flera myndigheter som utövar oberoende och effektiva tillsynsfunktioner och tillsynsbefogenheter med avseende på de åtgärder som anges i artikel 14.

Slutligen följer det av artikel 14.15 att en part får avbryta överföringen av personuppgifter till en annan part om den har konkreta bevis för att den andra parten systematiskt eller väsentligt bryter mot villkoren i artikel 14 eller att ett väsentligt brott mot villkoren är nära förestående. Den ska som huvudregel inte avbryta överföringar utan rimligt varsel och inte förrän efter det att de berörda parterna har inlett en rimlig samrådsperiod utan att nå en lösning. Den avbrytande parten ska häva avbrytandet så snart den överträdelse som motiverar avbrytandet har åtgärdats. Personuppgifter som överförts före avbrytandet ska fortsätta att behandlas i enlighet med protokollet.

12.9.2 Gällande rätt

I avsnitt 10.7 behandlas den nationella regleringen avseende skydd för personuppgifter. Som utvecklats i det avsnittet är dataskyddsförordningen inte tillämplig på den behandling av personuppgifter som behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga på-

följder (artikel 2.2 d). För personuppgiftsbehandling inom detta område gäller i stället brottsdatalagen (2018:1177).

Utbyte av personuppgifter i enlighet med det andra tilläggsprotokollets bestämmelser får anses ske i brottsbekämpande syfte. Därmed är brottsdatalagen och respektive behörig myndighets registerlag tillämpliga för den personuppgiftsbehandling som förekommer i ett sådant ärende. Behöriga myndigheter enligt brottsdatalagen som kan komma att behandla personuppgifter enligt tilläggsprotokollet torde främst vara Polismyndigheten, Tullverket, Ekobrottsmyndigheten, Åklagarmyndigheten och de allmänna domstolarna.

I detta sammanhang behandlas översiktligt de bestämmelser i brottsdatalagen som är av relevans. Om registerlagstiftningarna innehåller avvikande reglering tas de bestämmelserna upp.

Personuppgifter får enligt 2 kap. 3 § första stycket brottsdatalagen behandlas endast för särskilda, uttryckligt angivna och berättigade ändamål. Personuppgifter som behandlas ska vara korrekta och, om det är nödvändigt, uppdaterade (2 kap. 7 §). Känsliga personuppgifter som huvudregel inte behandlas. Om uppgifter om en person behandlas får de dock kompletteras med sådana uppgifter när det är absolut nödvändigt för ändamålet med behandlingen (2 kap. 11 §). Biometriska uppgifter och genetiska uppgifter får behandlas endast om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen (2 kap. 12 §). I bl.a. Polismyndighetens respektive Åklagarväsendets registerlagstiftning finns avvikande bestämmelser. Personuppgifter får enligt 2 kap. 17 § första stycket brottsdatalagen inte behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

I fråga om automatiserade beslut följer det av 2 kap. 18 § första stycket brottsdatalagen att om ett beslut enbart grundas på automatiserad behandling av sådana personuppgifter som är avsedda att bedöma hans eller hennes egenskaper, ska personen ha möjlighet att under vissa förutsättningar på begäran få beslutet prövat på nytt av någon person.

I 3 kap. finns bestämmelser om personuppgiftsansvarigas skyldigheter.

Den personuppgiftsansvarige ska enligt 3 kap. 2 § genom lämpliga tekniska och organisatoriska åtgärder säkerställa och kunna

visa att behandlingen av personuppgifter är författningsenlig och att den registrerades rättigheter skyddas. I 3 kap. 8 § regleras säkerhetsåtgärder. Den personuppgiftsansvarige ska enligt bestämmelsen vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada.

I 3 kap. 9–10 §§ regleras hanteringen av personuppgiftsincidenter. En personuppgiftsincident definieras som en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till personuppgifter (1 kap. 6 §). Av 9 § första stycket följer att senast 72 timmar efter det att den personuppgiftsansvarige fått kännedom om en personuppgiftsincident ska den anmälas till tillsynsmyndigheten, utom i de fall där incidenten ska rapporteras enligt säkerhetsskyddslagen (2018:585) eller föreskrifter som har meddelats i anslutning till den lagen. Om en personuppgiftsincident som ska anmälas har medfört eller kan antas medföra särskild risk för otillbörligt intrång i registrerades personliga integritet, ska den personuppgiftsansvarige som huvudregel utan onödigt dröjsmål underrätta den registrerade om incidenten (3 kap. 10 § brottsdatalagen). Enligt 3 kap. 20 § är två eller flera behöriga myndigheter gemensamt personuppgiftsansvariga om de gemensamt bestämmer ändamålen med och medlen för personuppgiftsbehandlingen.

I 4 kap. regleras enskildas rättigheter. Enligt 4 kap. 1 § ska den personuppgiftsansvarige göra bl.a. följande allmänna information tillgänglig för den registrerade: kategorier av ändamål för behandlingen, rätten att begära att få information om behandling av personuppgifter och att få del av uppgifterna och att begära rättelse, radering eller begränsning av behandlingen. Av 4 kap. 2 § följer att den registrerade, om det behövs för att han eller hon ska kunna ta till vara sina rättigheter, ska få information om:

1. den rättsliga grunden för behandlingen,
2. kategorier av mottagare av personuppgifterna, även i tredjeland eller internationella organisationer,

3. hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det, och
4. övrig nödvändig information.

Rätten till information är dock i vissa fall begränsad av lag eller annan författning (4 kap. 5 §).

Den personuppgiftsansvarige ska på begäran av den registrerade enligt 4 kap. 9 § utan onödigt dröjsmål rätta eller komplettera personuppgifter som rör honom eller henne, om de är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen. Den registrerade kan också enligt 4 kap. 10 § begära att uppgifterna utan onödigt dröjsmål raderas om uppgifterna behandlats i strid med vissa bestämmelser i lagen.

I 5 kap. finns bestämmelser om tillsyn. Tillsynsmyndigheten ska enligt 5 kap. 2 § bl.a. utöva allmän tillsyn över personuppgiftsbehandling och handlägga klagomål från registrerade. Av 5 kap. 3 § följer att tillsynsmyndigheten ska på begäran kontrollera om uppgifter om en fysisk person behandlas författningsenligt. I 5 kap. 5–7 §§ finns bestämmelser om de undersökande, förebyggande och korrigerande befogenheter som tillsynsmyndigheten har i sitt arbete. Integritetsskyddmyndigheten (IMY) är tillsynsmyndighet i fråga om brottsdatalogens bestämmelser.

I 7 kap. finns bestämmelser om den enskildes rätt till skadestånd vid felaktig personuppgiftsbehandling (7 kap. 1 §) samt den enskildes rätt att överklaga den personuppgiftsansvariga myndigheters beslut bl.a. rättelse (7 kap. 2 §).

Bestämmelser om överföring av personuppgifter till tredjeland och internationella organisationer finns i 8 kap. En behörig myndighet får enligt 8 kap. 1 § överföra personuppgifter till ett tredjeland eller en internationell organisation. Överföring för dock endast ske om den är nödvändig för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet och riktas till en behörig myndighet i ett tredjeland eller till en internationell organisation som är en behörig myndighet samt omfattas av adekvat skyddsnivå, tillräckliga skyddsåtgärder, eller ett undantag för särskilda situationer. Personuppgifter som en svensk myndighet har fått från en annan medlemsstat får överföras till ett tredjeland eller en internationell organisation endast om den

medlemsstat som lämnat uppgifterna till en svensk myndighet har medgett att de överförs (8 kap. 2 § första stycket). En svensk behörig myndighet får inte tillåta att sådana personuppgifter som anges i 8 kap. 2 § första stycket, och som överförts till ett tredjeland eller en internationell organisation, vidareöverförs till ett tredjeland eller en internationell organisation, om inte någon behörig myndighet i den andra medlemsstaten har medgett att uppgifterna får vidareöverföras (8 kap. 6 § första stycket).

I bl.a. Polismyndighetens registerlagstiftning finns bestämmelser om att utlämning av uppgifter får ske till Interpol, Europol, eller en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol (2 kap. 7 §).

12.9.3 Svensk rätt uppfyller de krav som följer av artikel 14

Bedömning: Svensk rätt uppfyller det andra tilläggsprotokollets krav på skydd för personuppgifter.

Integritetsskyddsmyndigheten ska motta underrättelse om säkerhetsincidenter enligt artikel 14.7 b. Åklagarmyndigheten ska ge förhandstillstånd till vidareöverföring av personuppgifter enligt artikel 14.10 a.

Skälen för bedömningen

Svensk rätt uppfyller kraven om skydd för personuppgifter enligt artikel 14

Rådet har i rådsbeslutet 2023/436 konstaterat att tilläggsprotokollet föreskriver lämpliga skyddsåtgärder i linje med kraven för internationella överföringar av personuppgifter enligt dataskyddsförordningen och dataskyddsdirektivet (skäl 11 i beslutet). Ikraftträdandet kommer därför enligt nämnda skäl i beslutet att bidra till att främja unionens dataskyddsstandarder på global nivå, underlätta dataflöden mellan medlemsstater som är parter och tredjeländer som är parter och säkerställa att medlemsstater som är parter fullgör sina skyldigheter enligt unionens dataskyddsregler. Tilläggsprotokollets bestämmelser om dataskydd i artikel 14 motsvarar således i allt väsentligt dataskyddsförordningen samt bestämmel-

serna i brottsdatalagen och behöriga myndigheters registerförfattningar, genom vilka dataskyddsdirektivet har genomförts. De nu genomgångna bestämmelserna i det nationella regelverket uppfyller således det andra tilläggsprotokollets krav i artikel 14 avseende skydd för personuppgifter.

I sammanhanget kan framhållas att artikel 14.10 a anger krav på förhandstillstånd från den överförande myndigheten innan den mottagande parten överför personuppgifter till annan stat eller internationell organisation. I brottsdatalagen finns, som redogjorts för ovan, ett krav på förhandstillstånd i dessa situationer i fråga om personuppgifter som förts över från en annan medlemsstat i EU. Lagen reglerar inte frågan om förhandstillstånd från tredjeland för överföring av personuppgifter. De länder som tillträtt det andra tilläggsprotokollet är inte endast EU-medlemsstater. Samtliga länder som tillträtt protokollet omfattas således inte av brottsdatalagens bestämmelser som förhandstillstånd vid vidareöverföring av personuppgifter.

Av 5 kap. 1 § första stycket lagen om internationell rättslig hjälp i brottmål följer att om en svensk myndighet i ett ärende om rättslig hjälp har fått uppgifter eller bevisning från en annan stat för att användas vid utredning av brott eller i ett rättsligt förfarande med anledning av brott och gäller på grund av en internationell överenskommelse som är bindande för Sverige villkor som begränsar möjligheten att använda uppgifterna eller bevisningen, ska svenska myndigheter följa villkoren oavsett vad som annars är föreskrivet i lag eller annan författning.

Bestämmelserna ska även tillämpas beträffande villkor som en annan stat ställer upp för att på eget initiativ, utan samband med ett ärende, lämna rättslig hjälp i form av uppgifter eller bevisning för att användas vid utredning av brott eller i rättsligt förfarande med anledning av brott (andra stycket nämnda paragraf).

Av 5 § lagen om vissa former av internationellt samarbete i brottsutredningar följer att om en svensk myndighet har fått uppgifter genom en gemensam utredningsgrupp som inrättats med stöd av den lagen och gäller på grund av en överenskommelse som anges i 1 § första stycket villkor som begränsar möjligheten att använda uppgifterna ska myndigheten följa villkoren oavsett vad som annars är föreskrivet i lag eller annan författning.

De nu nämnda bestämmelserna får tillsammans anses uppfylla kravet på förhandstånd för överföring av personuppgifter som erhållits i ett ärende enligt det andra tilläggsprotokollets bestämmelser från ett land som tillträtt det protokollet. Visserligen skulle det i 5 kap. 1 § första stycket lagen om internationell rättslig hjälp i brottmål uttryckligen kunna anges att bestämmelsen även avser överföring av personuppgifter. Bestämmelsens nuvarande lydelse för dock anses omfatta även en sådan hantering av personuppgifter. Det krävs således inte någon ytterligare reglering vad gäller frågan om förhandstillstånd från stater utanför EU och som tillträtt det andra tilläggsprotokollet för överföring av personuppgifter till annan stat eller internationell organisation.

Protokollets bestämmelser om skydd för personuppgifter kräver sammanfattningsvis inte några lagstiftningsåtgärder.

I sammanhanget kan framhållas att de nationella reglerna om tillsyn enligt brottsdatalagen aktualiseras i de fall svenska behöriga myndigheter behandlar personuppgifter enligt det andra tilläggsprotokollet. Det är således IMY som, på sätt som angetts i avsnitt 12.9.2, som utövar tillsyn över denna behandling.

Myndigheter som ska utses enligt artikel 14.7 c respektive 14.10 b

Enligt artikel 14 ska varje part utse myndigheter för vissa i artikeln angivna ändamål. Enligt artikel 14.7 c ska varje part meddela Europarådets generalsekreterare den eller de myndigheter som ska underrättas om en säkerhetsincident enligt artikel 14.7 b för de ändamål som avses i artiklarna 6 och 7. En säkerhetsincident på sätt begreppet definieras i artikel 14.7 a får anses ha motsvarande innebörd som begreppet personuppgiftsincident i brottsdatalagen. Den nationella tillsynsmyndigheten på området, IMY, bör utses till den myndighet som ska motta underrättelse om säkerhetsincidenter enligt artikel 14.7 b eftersom denna myndighet erhåller motsvarande underrättelser enligt 3 kap. 9 § brottsdatalagen på sätt som beskrivits i avsnitt 12.9.2.

Det är den myndighet till vilken personuppgifterna har överförts som enligt artikel 14.7 b ska hantera en säkerhetsincident och som ska underrätta den överförande myndigheten eller den myndighet som utsetts enligt artikel 14.7 c. IMY ska således i sin roll som

mottagande myndighet av en underrättelse enligt artikel 14.7 b inte hantera själva säkerhetsincidenten, men får dock begära samråd och kompletterande information om den incidenten och de åtgärder som mottagits (artikel 14.7 b).

Vidare ska varje part meddela Europarådets generalsekreterare den eller de myndigheter som ska ge förhandstillstånd att överföra personuppgifterna till en annan stat eller till en internationell organisation enligt artikel 14.10 a för de ändamål som avses i artiklarna 6 och 7 (artikel 14.10 b). Det framstår som mest lämpligt att den myndighet som deltar i ett samråd enligt artikel 6 samt godkänner en begäran enligt artikel 7 och mottar underrättelse samt samrådet om en sådan begäran ger tillstånd till vidareöverföring av uppgifterna. I avsnitten 12.4.5 och 12.5.4 har Åklagarmyndigheten föreslagits till den myndighet som ska utses i angivna syften, varför även den myndigheten bör ge förhandstillstånd till vidareöverföring av personuppgifter enligt artikel 14.10 a.

Enligt bilagan till rådsbeslutet 2023/436 (p. 3) ska medlemsstaterna avge en förklaring enligt artikel 14.7 c och 14.10 b i det andra tilläggsprotokollet.

12.10 Övriga artiklar

Bedömning: Artiklarna 1–5, 13 och 15–25 kräver inte några lagstiftningsåtgärder.

Skälen för bedömningen: Artiklarna 1–5 innehåller bestämmelser om syfte, tillämpningsområde, definitioner, språk samt allmänna principer som är tillämpliga avseende kapitel II. Artiklarna kräver inte några lagstiftningsåtgärder.

Artikel 13 innehåller bestämmelser om villkor och garantier. Bestämmelsen, som hänvisar till artikel 15 i Budapestkonventionen, syftar till att garantera proportionalitet och rättssäkerheten vid införandet och användningen av tvångsmedel och andra åtgärder. Artiklarna kräver i sig inga lagstiftningsåtgärder men ska beaktas vid genomförandet av övriga processrättsliga bestämmelser.

Slutbestämmelserna i artiklarna 15–25 kräver inte heller några lagstiftningsåtgärder.

12.11 Förklaringar och underrättelser

12.11.1 Förklaringar till det andra tilläggsprotokollet

Förslag: Sverige ska med stöd av artikel 19 i det andra tilläggsprotokoll till Europarådets konvention om it-relaterad brottslighet avge förklaringar angående

- artikel 6.6 om att Åklagarmyndigheten är behörig myndighet att samråda med enligt artikel 6.5,
- artikel 7.2 b om att en order enligt artikel 7.1 ska utfärdas av eller under överinseende av en åklagare eller annan rättslig myndighet eller på annat sätt under oberoende tillsyn,
- artikel 7.5 a om att när en order utfärdas enligt artikel 7.1 till en tjänsteleverantör på Sveriges territorium, ska i varje enskilt fall samtidig underrättelse om ordern, den kompletterande informationen och en sammanfattning av de sakförhållanden som har samband med utredningen eller förfarandet lämnas till Åklagarmyndigheten,
- artikel 7.5 e om att Åklagarmyndigheten är den behöriga myndigheten i Sverige när det gäller tillämpningen av vissa bestämmelser i artikel 7,
- artikel 8.4 om att ytterligare informationsunderlag krävs för att verkställa en order enligt artikel 8.1 samt att vad som krävs kommer att vara beroende av omständigheterna bakom ordern och därmed sammanhängande utredning eller förfarande,
- artikel 8.10 om att Sverige, utöver Åklagarmyndigheten, i egenskap av medlemsstat i Europeiska unionen som deltar i det fördjupade samarbetet om inrättande av Europeiska åklagarmyndigheten, utser Europeiska åklagarmyndigheten till behörig myndighet vad gäller utövandet av dess befogenheter som föreskrivs i artiklarna 22, 23 och 25 i rådets förordning (EU) 2017/1939 av den 12 oktober 2017 om genomförande av fördjupat samarbete om inrättande av Europeiska åklagarmyndigheten,
- artikel 8.13 om att artikel 8 dels ska endast tillämpas på de brott och brottstyper som avses i 27 kap. 19 a § andra stycket

och 19 b § andra stycket rättegångsbalken, dels inte kommer att tillämpas vad avser meddelanden som överförs inom en tjänsteleverantörs datorsystem som dels drivs för en sluten användargrupp, dels inte använder allmänna kommunikationsnät och inte är anslutet till ett annat datorsystem,

- artikel 10.9 om att framställningar enligt artikel 10 kan sändas direkt till svenska rättsliga myndigheter eller via Interpol eller den kontaktpunkt i det 24/7-nätverk som har inrättats genom artikel 35 i Europarådets konvention om it-relaterad brottslighet,
- artikel 14.7 c om att Integritetsskyddsmyndigheten ska utses till den myndighet som ska motta underrättelse om säkerhetsincidenter enligt artikel 14.7 b, och
- artikel 14.10 b om att Åklagarmyndigheten ska ge förhandstillstånd att överföra personuppgifterna till en annan stat eller till en internationell organisation enligt artikel 14.10 a.

Skälen för förslaget

Förklaringar med hänsyn till rådsbeslutet 2023/436

Som framgår av avsnitten 12.5–12.7 åläggs Sverige enligt rådsbeslutet 2023/436 att avge en mängd olika förklaringar som främst rör de olika artiklarnas tillämpning.

När det gäller artikel 7 ska Sverige avge en förklaring enligt artikel 7.2 b om att en order enligt artikel 7.1 ska utfärdas av eller under överinseende av en åklagare eller annan rättslig myndighet eller på annat sätt under oberoende tillsyn. Vidare ska Sverige enligt artikel 7.5 a lämna en förklaring om att när en order utfärdas enligt artikel 7.1 för verkställighet i Sverige, ska i varje enskilt fall samtidigt underrättelse om ordern, den kompletterande informationen och en sammanfattning av de sakförhållanden som har samband med utredningen eller förfarandet lämnas till Åklagarmyndigheten.

I förhållande till artikel 8 ska Sverige avge en förklaring enligt artikel 8.4 att ytterligare informationsunderlag krävs för att verkställa en order enligt artikel 8. Vidare ska Sverige avge en förklaring

enligt artikel 8.10 som inkluderar Europeiska åklagarmyndigheten bland de myndigheter som är behöriga enligt nämnda artikel.

Beträffande artikel 14.7 c bör IMY utses till den myndighet som mottar underrättelser om säkerhetsincidenter enligt artikel 14.7 b. Slutligen bör Åklagarmyndigheten utses enligt artikel 14.10 b till den myndighet som ger förhandstillstånd till att överföra personuppgifterna till en annan stat eller till en internationell organisation enligt.

Med hänsyn till Sveriges åtagande som medlemsstat i EU bör Sverige avge de förklaringar och med det innehåll som framgår av rådsbeslutet 2023/436 (bilagan, punkt 1–3).

Övriga förklaringar

Enligt flera artiklar i det andra tilläggsprotokollet ska Sverige utse en myndighet som ska vara behörig att vidta de åtgärder som framgår av de olika bestämmelserna. Det rör sig om samråd med den andra statens myndigheter om uppgifter inte lämnas ut enligt artikel 6.1 (artikel 6.6) eller tillämpning av vissa bestämmelser i artikel 7 (artikel 7.5 e). Enligt artikel 8.10 ska avtalsstaterna utse behörig myndighet att inge respektive motta en order enligt artikel 8.1

Av avsnitten 12.4.5, 12.5.4, 12.6.3 och 12.6.4 framgår att denna myndighet bör vara Åklagarmyndigheten. Sverige bör därför avge förklaringar om att Åklagarmyndigheten är behörig myndighet i dessa avseenden. När det gäller behörig myndighet ska Europeisk åklagare också vara behörig.

Som redogjorts för i avsnitt 12.6.5 görs bedömningen att en förklaring bör lämnas beträffande artikel 8 om att den endast kommer att tillämpas på de brott och brottstyper som avses i 27 kap. 19 a § andra stycket och 19 b § andra stycket rättegångsbalken samt att bestämmelsen inte kommer att tillämpas vad avser meddelanden som överförs inom en tjänsteleverantörs datorsystem som dels drivs för en sluten användargrupp, dels inte använder allmänna kommunikationsnät och inte är anslutet till ett annat datorsystem.

Enligt avsnitt 12.7.5 bör Sverige avge en förklaring med det innehåll som framgår av artikel 10.9, dvs. en framställning ska

kunna sändas direkt till svenska rättsliga myndigheter eller via Interpol eller den kontaktpunkt som inrättats genom artikel 35 i Budapestkonventionen.

12.11.2 Underrättelser till kommissionen

Förslag: Sverige ska till kommissionen meddela att Sverige kommer att tillämpa det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet tillsammans med Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden och Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området. Ett sådant meddelande ska endast gälla artiklarna 6–10 i det andra tilläggsprotokollet.

Skälen för förslaget: Bestämmelserna i det andra tilläggsprotokollet har flera beröringspunkter med vissa EU-rättsliga regelverk. Artiklarna 6 och 7 har likartade regler som EU-förordningen, medan artikel 8–12 berör främst direktivet om en europeisk utredningsorder.

I artikel 15.1 b i det andra tilläggsprotokollet anges att när det gäller EU-stater får de i sina ömsesidiga förbindelser tillämpas det EU-rättsliga regelverket vad gäller frågor som behandlas i detta protokoll. I den förklarande rapporten anges att protokollet inte hindrar att EU-staterna tillämpar det EU-rättsliga regelverk i frågor som regleras i protokollet (p. 290).

Det kan vidare konstateras att radsbeslutet 2023/436 inte hindrar att EU:s medlemsstater sinsemellan tillämpar bestämmelserna i det andra tilläggsprotokollet även om det rör sig om frågor som regleras i de EU-rättsliga regelverken. Det ska även konstateras att i skäl 5 anges att genom att kommissionen deltog i förhandlingarna såg den till att protokollets bestämmelser överensstämde med unionsrätten.

De regelverk som berörs är som nämns ovan EU-förordningen och direktivet om europeisk utredningsorder.

I artikel 32.1 i EU-förordningen anges att EU-förordningen inte påverkar andra internationella överenskommelser beträffande bevisinhämtning som omfattas av denna förordnings tillämpningsområde. Om en medlemsstat avser att tillämpa en sådan överenskommelse ska den enligt artikel 32.1 senast den 18 augusti 2026 till kommissionen meddela att den avser att fortsatt tillämpa den internationella överenskommelsen. För framtida internationella överenskommelser har en medlemsstat tre månader på sig att meddela kommissionen.

Motsvarande bestämmelser finns i artikel 34 i direktivet om en europeisk utredningsorder. En skillnad är dock att en sådan internationell överenskommelse får tillämpas endast i den mån den gör det möjligt att ytterligare stärka syftena med detta direktiv och bidra till att förenkla eller ytterligare underlätta förfarandena för bevisinhämtning och under förutsättning att de skyddsnivåer som anges i detta direktiv respekteras (artikel 34.3).

För att skapa en flexibilitet för de svenska brottsbekämpande myndigheterna anser vi att Sverige bör meddela kommissionen att Sverige avser att tillämpa vissa bestämmelser i det andra tilläggsprotokollet till Budapestkonvention i förhållande till såväl EU-förordningen och direktivet om en europeisk utredningsorder. En åklagare kan då välja att använda det regelverk som är mest effektivt i stället för att låsa in sig på ett regelverk som andra medlemsstater inte förväntar sig ska tillämpas (jfr avsnitt 11.5.1).

Vår bedömning är att när det gäller EU-förordningen är det artiklarna 6 och 7 i det andra tilläggsprotokollet som kan fortsätta att tillämpas i förhållande till förordningen. Beträffande direktivet om en europeisk utredningsorder bör bestämmelserna i artiklarna 8–10 i det andra tilläggsprotokollet kunna fortsätta att tillämpas. När det gäller artikel 11 i protokollet ser vi inga vinster med att tillämpa den i stället för bestämmelserna om videokonferens i lagen om en europeisk utredningsorder.

Om en åklagare väljer att tillämpa nämnda bestämmelser i det andra tilläggsprotokollet är det lagen om vissa former av internationellt samarbete i brottsutredningar och lagen om internationell rättslig hjälp i brottmål som i stället ska tillämpas.

En tillämpning av bestämmelserna i det andra tilläggsprotokollet kommer dock endast att vara möjlig gentemot medlemsstater som har lämnat samma meddelande till kommissionen. I de fall EU-stat t.ex. inte vill tillämpa artikel 7 i det andra tilläggsprotokollet utan i stället, med stöd av artikel 15.1 b i protokollet, väljer att tillämpa EU-förordningen har svenska myndigheter inte något annat val än använda sig av sistnämnda regelverk.

13 Konsekvenser av utredningens förslag

13.1 Inledning

Av kommittéförordningen (1998:1474) följer att en utredning ska redovisa vilka konsekvenser de förslag som utredningen lämnar kan ha i flera olika avseenden. Utöver bestämmelserna i kommittéförordningen finns i förordningen om konsekvensutredningar (2024:183) bestämmelser om vad en utredning ska redovisa. Den förordningen trädde i kraft den 6 maj 2024 och gäller enligt övergångsbestämmelserna inte de utredningar som tillsatts före ikraftträdandet. För sådana utredningar gäller i stället kommittéförordningens bestämmelser i 14–15 a § i den äldre lydelsen samt 6 och 7 § i den numera upphävda förordningen (2007:1244) om konsekvensutredning vid regelgivning.

Vi ska enligt dessa bestämmelser redovisa vilka konsekvenser i olika avseenden som förslagen i betänkandet kan få (1 § andra stycket kommittéförordningen). Om förslagen påverkar kostnaderna eller intäkterna för staten, kommuner, regioner, företag eller andra enskilda, ska vi redovisa en beräkning av dessa konsekvenser i betänkandet (14 §). Innebär förslagen samhällsekonomiska konsekvenser i övrigt ska utredningen även redovisa dessa. Om våra förslag leder till kostnadsökningar eller intäktsminskningar för staten, kommuner eller regioner ska vi föreslå hur förslagen ska finansieras.

I 15 § anges att om förslagen i ett betänkande har betydelse för den kommunala självstyrelsen, för brottsligheten och det brottsförebyggande arbetet, för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företag, för jämställdheten mellan kvinnor och män eller för möjligheterna att

nå de integrationspolitiska målen ska konsekvenserna i det avseendet också anges i betänkandet.

Om ett betänkande innehåller förslag till nya eller ändrade regler, ska enligt 15 a § kommittéförordningen förslagets kostnadsmissiga och andra konsekvenser anges i betänkandet. Konsekvenserna ska anges på ett sätt som motsvarar de krav på innehållet i konsekvensutredningar som finns i 6 och 7 §§ förordningen om konsekvensutredning vid regelgivning.

EU-förordningen reglerar skyldigheter för tjänsteleverantörer och för behöriga myndigheter i flera avseenden. De bindande och direkt tillämpliga bestämmelserna i EU-förordningen har, av skäl som hänför sig till hur EU-rätt ska hanteras i de nationella rättsordningarna, inte föranlett några lagförslag. Konsekvenserna av sådana EU-bestämmelser är således inte föremål för denna konsekvensbedömning. Därmed berörs inte vilka konsekvenser EU-förordningens direkt tillämpliga bestämmelser medför för de berörda aktörerna.

Våra förslag hänför sig till genomförande av EU-direktivet respektive det andra tilläggsprotokollet till Budapestkonventionen samt kompletterande lagstiftning till EU-förordningen. Det finns därför inte skäl att beskriva alternativa lösningar eller effekterna om någon reglering inte kommer till stånd. Sverige är skyldigt att genomföra EU-direktivet samt att följa förordningen och vidta åtgärder för att densamma ska få fullt genomslag. Underlåtenhet att vidta erforderliga åtgärder skulle innebära att Sverige blir föremål för ett överträdelseärende.

13.2 Konsekvenser för brottsbekämpande myndigheter

13.2.1 Förslag avseende EU-förordningen som berör brottsbekämpande myndigheter

Vi föreslår att åklagare ska vara behöriga att utfärda en europeisk utlämnandeorder respektive europeisk bevarandeorder i Sverige. En utlämnandeorder avseende inhämtning av trafikuppgifter respektive innehållsdata kräver dock domstols tillstånd. Polismyndigheten och övriga brottsbekämpande myndigheter föreslås vara behöriga att utfärda en utlämnandeorder avseende abonnemangs-

uppgifter eller andra användaruppgifter samt en bevarandeorder. En sådan order måste dock godkännas av åklagare.

Åklagarmyndigheten föreslås vidare vara verkställande myndighet enligt EU-förordningen. Denna uppgift innebär bl.a. att Åklagarmyndigheten ska verkställa en order på sätt EU-förordningen föreskriver samt besluta om att ta ut en sanktionsavgift vid överträdelse av vissa av EU-förordningens bestämmelser.

Vi föreslår också att den som innehar en viss lagrad elektronisk uppgift som behövs för att lokalisera en person för verkställighet av en frihetsberövande påföljd att ska kunna föreläggas att bevara uppgiften.

Vidare föreslås att åklagare och övriga brottsbekämpande myndigheten ska samla in och rapportera statistik till kommissionen.

13.2.2 Förslag avseende det andra tilläggsprotokollet till Budapestkonventionen samt artikel 29 i konventionen som berör brottsbekämpande myndigheter

Vi har föreslagit att åklagare och övriga brottsbekämpande myndigheter ska ha rätt att från en registreringsenhet för toppdomäner eller återförsäljare av domännamn och från en tjänsteleverantör i en annan stat som tillträtt det andra tilläggsprotokollet till Budapestkonventionen begära ut uppgifter för att identifiera eller kontakta innehavaren av ett domännamn respektive uppgifter om abonnemang som skäligen kan antas ha betydelse för utredningen om ett brott.

Vidare har vi föreslagit att Åklagarmyndigheten utses till den myndighet som utländsk behörig myndighet ska kunna samråda med i de fall uppgifter för att identifiera eller kontakta innehavaren av ett domännamn har begärts ut från en svensk aktör.

Vi har också föreslagit att Åklagarmyndigheten ska underrättas om begäran om uppgifter om abonnemang som riktats till en tjänsteleverantör i Sverige samt att tjänsteleverantören vid behov ska kunna samråda med Åklagarmyndigheten innan uppgifterna lämnas ut.

Åklagarmyndigheten föreslås vidare utses till den myndighet som ska ge förhandstillstånd till vidareöverföring av personuppgifter enligt artikel 14.10 a i det andra tilläggsprotokollet.

Det föreslås vidare att det i 2 kap. 10 § lagen (2000:562) om internationell rättslig hjälp i brottmål ska anges att i fråga om skyndsam-

hetskravet särskild hänsyn tas till att om det föreligger en omedelbar fara för liv, hälsa eller egendom. Motsvarande bestämmelse föreslås föras in i 3 kap. 23 § lagen (2017:1000) om en europeisk utredningsorder.

Slutligen har vi föreslagit att lagen om en europeisk utredningsorder inte ska gälla vid skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter enligt artikel 29 i Budapestkonventionen. I stället ska lagen om internationell rättslig hjälp i brottmål tillämpas vid en sådan begäran.

13.2.3 Konsekvenser för Åklagarmyndigheten och Ekobrottsmyndigheten

I dag finns ett samarbete mellan Polismyndigheten och flertalet större internationella tjänsteleverantörer. Samarbetet innebär att tjänsteleverantörerna, efter förfrågan från Polismyndigheten, på frivillig basis lämnar ut sådana uppgifter som enligt förordningen motsvarar abonnentuppgifter eller uppgifter som begärs med det enda syftet att identifiera användaren. Enligt uppgift i utredningen hanterar Polismyndigheten drygt 7 000 ärenden per år gällande sådana förfrågningar. I de fall en tjänsteleverantör i ett annat land inte vill lämna ut uppgiften på frivillig basis kan en åklagare i stället utfärda en europeisk utredningsorder eller skicka en framställan om rättslig hjälp. Åklagarmyndigheten har inte någon statistik över hur vanligt det är att en europeisk utredningsorder eller framställan om rättslig hjälp görs till annat land med detta syfte, men enligt uppgift från myndigheten det går med säkerhet att säga att det är betydligt färre än de ärenden Polismyndigheten hanterar genom det beskrivna samarbetet.

Våra förslag innebär att åklagare kommer att involveras i samtliga ärenden enligt EU-förordningen om att utfärda en europeisk utlämnande- eller bevarandeorder; antingen genom utfärdande av orden samt ansökan om rättens godkännande att utfärda en utlämnandeorder avseende trafikuppgifter eller innehållsdata eller genom godkännande en order utfärdad av annan myndighet. I fråga om inhämtning av abonnemangsuppgifter enligt de bestämmelser som genomför det andra tilläggsprotokollet till Budapestkonventionen ska en sådan utgående order enligt våra förslag godkännas av

åklagare om den är utfärdad av annan behörig myndighet och så begärs av den andra staten.

Behörigheten att utfärda en europeisk utlämnande- eller bevarandeorder eller en begäran för inhämtning av abonnemangsuppgifter respektive uppgifter hänförliga till domännamn enligt de nationella bestämmelser som genomför det andra tilläggsprotokollet kommer sannolikt inte i sig att öka myndigheternas arbetsbörda, eftersom motsvarande uppgifter i dag kan inhämtas med stöd av lagen om internationell rättslig hjälp i brottmål respektive lagen om en europeisk utredningsorder. Detsamma gäller i fråga om godkännande av order enligt EU-förordningen eller en begäran om abonnemang som utfärdats av annan behörig myndighet. Dessa myndigheter kan i dag inte självständigt utfärda en ansökan om rättslig hjälp eller europeisk utredningsorder för inhämtning av dessa uppgifter, utan sådan inhämtning sker genom åklagare. Att i stället godkänna en order eller en begäran torde därför inte innebära någon ökad arbetsbörda för åklagarna i denna del.

Om tjänsteleverantörerna även fortsättningsvis och i samma utsträckning väljer att på frivillig basis lämna ut de uppgifter som i dag överlämnas till Polismyndigheten, kommer förslagen sannolikt inte innebära någon kostnadsökning för Åklagarmyndigheten respektive Ekobrottsmyndigheten i fråga om utfärdande respektive godkännande av order enligt EU-förordningen och enligt övriga föreslagna bestämmelser.

Samtidigt finns det enligt Åklagarmyndigheten starka skäl att tro att tjänsteleverantörerna inte kommer acceptera dubbla lösningar i form av dels det decentraliserade it-systemet, i vilket uppgifter ska föras över mellan tjänsteleverantörer och behöriga myndigheter, dels utlämnande på frivillig basis. Det kan därför enligt Åklagarmyndigheten antas att åtminstone flertalet tjänsteleverantörer kommer kräva att ansökan görs genom det decentraliserade it-systemet och det förfarande som följer av EU-förordningen. Det innebär att åklagare kommer behöva involveras i betydligt högre utsträckning än i dag vid den här typen av förfrågningar. Detta medför en ökad arbetsbelastning för åklagarna, vilket medför ökade kostnader.

Därutöver kommer det enligt Åklagarmyndigheten att vara nödvändigt med anpassningar av myndighetens it-system, vilket

också kommer innebära en kostnad för myndigheten som i dag är svår att uppskatta.

EU-förordningen och de bestämmelser som genomför det andra tilläggsprotokollet till Budapestkonventionen möjliggör för utländska behöriga myndigheter att vända sig direkt till tjänsteleverantörer i bl.a. Sverige för att få ut uppgifter om abonnemang, trafikuppgifter och innehållsdata i stället för att vända sig till behörig myndighet i Sverige för bistånd med inhämtning. Detta kommer sannolikt att minska arbetsbördan och därmed kostnaden för svenska åklagare vad avser hantering av sådana ansökningar om rättslig hjälp eller verkställande av europeisk utredningsorder. Det är dock svårt att uttala sig med säkerhet om hur stor denna minskning av inkommande ansökningar om rättslig hjälp respektive utfärdande av en europeisk utredningsorder kommer att bli.

Åklagarmyndighetens uppgift att besluta om sanktionsavgifter innebär helt nya arbetsuppgifter för myndigheten, som kommer att medföra vissa ökade kostnader. Dels krävs inledande arbetsinsatser för att ta fram handläggningsrutiner, utbildningsinsatser och framtagande av administrativt stöd för att få systemet på plats, dels krävs i varje ärende arbetsinsatser för utredning och beslut. Hur stor den årliga kostnaden blir i denna del beror på flera faktorer; hur många tjänsteleverantörer som omfattas av förordningens bestämmelser som kommer att vara representerade i Sverige (genom verksamhetsställe eller rättsligt ombud), hur många förfrågningar som riktas till dem och hur många av dessa förfrågningar som inte kommer att höras.

Uppgiften att samla in statistik är en ny arbetsuppgift för åklagarna och kan därför innebära ökade kostnader. I EU-förordningen anges dock att statistikinsamling ska kunna ske genom det decentraliserade it-systemet, varför denna kostnad endast torde vara marginell i sammanhanget.

Övriga förslag bedöms inte påverka åklagarnas arbetsbörda annat än i marginell mån.

Åklagarmyndigheten har uppgett att den ökade arbetsbördan i anledning av förslagen kommer att vara betydande och inte rymmas inom befintligt anslag. Detta även med beaktande av att förslaget också innebär att åklagare i lägre utsträckning än i dag kan komma att involveras i ärenden där annat land önskar bistånd med att inhämta trafikuppgifter eller innehållsdata.

Hur stora konsekvenser uppdraget som verkställande myndighet kommer att innebära i fråga om antal ärenden för Åklagarmyndigheten är, som vi konstaterat ovan, mycket svårt att uppskatta. Det är inte heller möjligt att med någon form av säkerhet bedöma om tjänsteleverantörerna, som Åklagarmyndigheten befarat, till följd av EU-förordningen inte längre kommer att godta frivillig utlämning av uppgifter, vilket skulle kunna resultera i en ökad mängd ärenden att hantera för myndigheten i förhållande till dagsläget. Det är således inte möjligt att göra några bedömningar av vilka resursökningar som kan bli aktuella i dessa avseenden. De ökade kostnader som våra förslag kan komma att innebära för Åklagarmyndigheten får under angivna förutsättningar anses rymmas inom befintliga anslag. Om det skulle visa sig att uppdraget innebär större ekonomiska konsekvenser än vad vi nu kan överblicka har Åklagarmyndigheten möjlighet att återkomma inom ramen för myndighetens ordinarie budgetdialoger.

Ekobrottsmyndigheten ser i nuläget inte att våra förslag medför sådana kostnadsökningar för myndigheten som inte rymms inom befintliga budgetramar. Vi gör ingen annan bedömning än myndigheten i denna fråga.

13.2.4 Konsekvenser för övriga behöriga myndigheter

Som beskrivits inledningsvis ska Polismyndigheten, Säkerhetspolisen, Tullverket och övriga brottsbekämpande myndigheter enligt våra förslag ha rätt att utfärda en europeisk utlämnandeorder för vissa uppgiftsslag respektive en bevarandeorder samt begära ut uppgifter om abonnemang respektive domännamn direkt från en aktör i annan stat som tillträtt det andra tilläggsprotokollet till Budapestkonventionen.

När det gäller brottsbekämpande myndigheter, utöver åklagarna, så kan det antas att de i många fall är involverade i processen att ansöka om rättslig hjälp respektive att utfärda en europeisk utredningsorder för inhämtning av de aktuella uppgifterna. Den tillkommande uppgiften att utfärda en order av aktuellt slag kan komma att öka arbetsbördan, men det kan antas att det inte medför någon sådan ökning att den inte kan hanteras inom befintliga budgetramar. Övriga förslag bedöms inte heller ha en sådan inverkan på

myndigheternas arbetsbörda att det inte ryms inom befintliga budgetramar.

Polismyndigheten har i sammanhanget framhållit frågan om kostnader för det decentraliserade it-systemet som utbyte av uppgifterna ska genom enligt EU-förordningen och då angett att denna kostnad inte kan anses rymmas inom befintliga budgetramar. Åtkomstpunkterna i det decentraliserade it-systemet ska enligt skäl 83 i EU-förordningen baseras på e-Codex-systemet, som inrättades genom Europaparlamentets och rådets förordning (EU) 2022/850, och som är ett EU-gemensamt it-system. Systemet ska bidra till ett effektivare rättsligt samarbete mellan medlemsstaterna och avser alltså inte endast kommunikation som sker enligt EU-förordningen. Kostnaden för inrättandet av it-systemet är således inte endast hänförlig till EU-förordningen och förslaget att utse Polismyndigheten till behörig myndighet enligt förordningen, utan ska alltså användas även i annan kommunikation medlemsstaterna emellan.

Vidare är investeringar i system att se som en verksamhetsinvestering. Verksamhetsinvesteringar är anläggningstillgångar som används i statens verksamhet och kan t.ex. avse it-system.¹ Verksamhetsinvesteringar ska som huvudregel finansieras genom lån i Riksgäldskontoret.²

I fråga om insamling av statistik enligt EU-förordningen görs ingen annan bedömning än beträffande motsvarande skyldighet för åklagarna, se resonemanget ovan.

Övriga förslag bedöms inte påverka myndigheternas arbetsbörda annat än i marginell mån.

Vår bedömning är sammantaget att förslagen kan komma att medföra kostnadsökningar för de berörda myndigheterna, men att dessa inte är större än att de ryms inom ramen för befintliga anslag.

¹ Förordningen (2000:605) om årsredovisning och budgetunderlag, 5 kap, 1–2 §§ och ESV, Ekonomistyrningsverkets föreskrifter och allmänna råd om årsredovisning och budgetunderlag (ESVFA 2022:1), 5 kap. 1–3 §§.

² 7 2 kap. 1 § kapitalförsörjningsförordningen (2011:210) samt ESV, Verksamhetsinvesteringar finansieras enligt lånemodellen, www.esv.se.

13.3 Konsekvenser för domstolarna och övriga myndigheter

Förslaget att Stockholms tingsrätt ska vara behörig enligt artikel 17 i EU-förordningen kommer sannolikt att öka kostnaderna för domstolen i någon mån. Det är dock svårt att uttala sig med något mått av säkerhet i frågan, eftersom den är beroende av hur många tjänsteleverantörer i Sverige som kommer att åberopa artikel 17 enligt EU-förordningen. Det kan antas att sådana ärenden inte kommer att vara frekvent förekommande och den eventuella kostnadsökningen som förslaget medför för Stockholms tingsrätt torde kunna rymmas inom ramen för domstolens budgetramar. Detsamma gäller för Svea hovrätt, dit ett ärende enligt förslaget kan överklagas.

För domstolarna i övrigt kommer våra förslag tillsammans med regleringen i EU-förordningen innebära att de under vissa förutsättningar ska godkänna en europeisk utlämnandeorder. Detta förfarande torde i stort motsvara vad som i dag gäller för en motsvarande ansökan om rättslig hjälp eller utfärdande av en europeisk utredningsorder. Våra förslag bör därför ha högst en marginell påverkan på domstolarnas arbetsbörda och kostnader och torde kunna hanteras inom befintliga anslag.

Vi föreslår ett sanktionssystem vid överträdelse av EU-förordningen och de nationella bestämmelserna som genomför EU-direktivet. Detta system som innehåller bestämmelser om sanktionsavgifter och vitesförelägganden. Vi föreslår också att sanktionsavgifter som beslutas med stöd av den kompletterande lagen ska få överklagas till allmän förvaltningsdomstol. Utöver de beslut som överklagas till domstolen kommer måltillströmningen även att bestå av ansökan om utdömande av vite. Det kommer med all säkerhet att röra sig om enstaka mål varför uppgiften bör rymmas inom förvaltningsdomstolarnas befintliga anslag.

Integritetsskyddsmyndigheten föreslås utses till den myndighet som ska motta underrättelse om säkerhetsincidenter enligt artikel 14.7 b i det andra tilläggsprotokollet till Budapestkonventionen. Förslaget torde endast i mindre mån ha en påverkan på myndighetens arbetsbörda och uppgiften bör därför kunna hanteras inom befintliga anslag.

Bestämmelserna om sanktionsavgifter och viten kan komma att generera enstaka ärenden hos Kronofogdemyndigheten. Uppgiften kan hanteras inom myndighetens befintliga anslag. Detsamma gäller för Kronofogdemyndighetens föreslagna uppgift att biträda centralmyndigheten i dess tillsynsverksamhet.

13.4 Konsekvenser för den utsedda centralmyndigheten

Uppgiften som centralmyndighet

Centralmyndigheten ska enligt våra förslag bedriva viss tillsyn över de tjänsteleverantörer som är skyldiga att utse verksamhetsställen eller rättsliga ombud i Sverige eller annan medlemsstat där tjänsteleverantören erbjuder tjänster. Centralmyndigheten föreslås ges möjlighet att i sin tillsyn bl.a. meddela förelägganden i förening med vite gentemot de tjänsteleverantörer som inte följer de nationella bestämmelser som genomför EU-direktivet. Centralmyndigheten ska även besluta om sanktionsavgifter vid överträdelse av dessa bestämmelser. För att avgöra om en tjänsteleverantör är skyldig att utse ett verksamhetsställe eller rättsligt ombud kommer det sannolikt ofta krävas att centralmyndigheten samråder med centralmyndigheter i andra medlemsstater för att avgöra om det föreligger en sådan skyldighet.

Vi har föreslagit att Post- och telestyrelsen (PTS) ska utses till centralmyndighet enligt EU-direktivet.

PTS har i dag tillsynsansvar för bl.a. området elektronisk kommunikation och bedriver enligt lagen (2022:482) om elektronisk kommunikation tillsyn över flera av de tjänsteleverantörer som omfattas av våra förslag. Uppgiften som centralmyndighet innebär som en tillkommande arbetsuppgift för PTS.

Denna tillkommande arbetsuppgift kommer att innebära en kostnadsökning för myndigheten som är beroende av flera parametrar; hur många tjänsteleverantörer som omfattas, hur många av dessa som är skyldiga att utse verksamhetsställen eller rättsliga ombud i Sverige samt hur många av dessa som inte följer denna skyldighet.

PTS har i fråga om tjänsteleverantörer som erbjuder tjänster i Sverige uppskattat antalet tjänsteleverantörer av elektroniska kom-

munikationstjänster till cirka 700. I denna siffra ingår nationella leverantörer som endast erbjuder tjänster inom Sverige, och således inte omfattas av kravet på att utse verksamhetsställe eller rättsliga ombud. Tjänsteleverantörer som tillhandahåller tjänster för internet-domännamn och IP-numrering, såsom tjänster för tilldelning av IP-adresser, tjänster för domännamnsregister, tjänster för domännamnsregistratorer och domännamnsrelaterade integritets- och proxytjänster har av myndigheten uppskattats till 100. Slutligen har antalet tjänsteleverantörer av Noik angetts uppgå till drygt 35. Det är alltså fråga om tjänsteleverantörer som erbjuder tjänster i Sverige och flertalet av dem torde vara etablerade i annat land samt även erbjuda tjänster i andra medlemsstater. Samtliga av dessa tjänsteleverantörer kommer därför sannolikt inte att utse verksamhetsställen i Sverige, eftersom många inte är etablerade här. De tjänsteleverantörer som erbjuder tjänster inom EU men som inte är etablerade inom unionen, kan också välja att utse ett rättsligt ombud i annan medlemsstat där de erbjuder tjänster.

PTS har uppskattat att kostnaden i fråga om personalresurser till följd av uppgiften som centralmyndighet uppgår till cirka två årsarbetskrafter, vilket motsvarar en sammanlagd årlig kostnad om tre miljoner kronor.

Den årliga kostnaden kan inte anses rymmas inom myndighetens befintliga budgetramar. Den bör därför huvudsakligen finansieras genom att medel tillförs från andra utgiftsområden.

Förslaget om tjänsteleverantörers rätt till ersättning för kostnader

Vi har föreslagit att bestämmelsen i 9 kap. 29 a § lagen om elektronisk kommunikation ska ha motsvarande tillämpning i fråga om tjänsteleverantörers rätt till ersättning enligt EU-förordningen. Förslaget innebär att när en uppgift begärs av en svensk behörig myndighet av en tjänsteleverantör i en annan medlemsstat har tjänsteleverantören rätt till ersättning för kostnaden hänförlig till de utlämnande uppgifterna. Det är PTS som beslutar om sådan ersättning i dag. Det kan antas att ansökningar om ersättning kommer att öka till följd av förslaget. Det är dock svårt att uttala sig i vilken mån detta kommer att ske och hur stora ersättningar som kommer att betalas ut i varje enskilt ärende samt hur stor arbets-

belastning detta medför för myndigheten. Detta är beroende av hur många europeiska utlämnandeorder eller bevarandeorder som svenska behöriga myndigheter kommer att utfärda, eftersom det alltså är den utfärdande staten som ska svara för tjänsteleverantörens kostnader.

Sammantaget görs bedömningen eventuella kostnadsökningar inte blir mer omfattande än att de ryms inom myndighetens befintliga ekonomiska ramar.

13.5 Konsekvenser för företagen

En tjänsteleverantör som är etablerad i Sverige och som är en juridisk person ska enligt vårt förslag utse ett eller flera verksamhetsställen i Sverige eller annan medlemsstat där denne erbjuder tjänster för mottagande, efterlevnad och verkställighet av beslut och förelägganden som omfattas av EU-förordningen och övriga rättsakter som anges i artikel 1.2 i EU-direktivet. För motsvarande ändamål föreslås att en tjänsteleverantör som inte är etablerad i någon av unionens medlemsstater och som är juridisk person, men som erbjuder tjänster i Sverige ska utse ett eller flera rättsliga ombud i Sverige eller annan medlemsstat där denne erbjuder tjänster.

Vidare föreslår vi att en registreringsenhet för toppdomäner eller återförsäljare av domännamn som erbjuder tjänster för domännamnregistrering i Sverige respektive en tjänsteleverantör i Sverige som omfattas av lagen om elektronisk kommunikation ska på begäran av en myndighet i en annan stat som tillträtt det andra tilläggsprotokollet till Budapestkonventionen lämna ut uppgifter om domännamn respektive abonnemang.

Att utse ett verksamhetsställe eller rättsligt ombud är givetvis förenat med kostnader. Hur stora kostnader det innebär för den enskilde tjänsteleverantören är dock mycket svårt att svara på och beror på olika faktorer, t.ex. om tjänsteleverantören väljer att driva verksamheten i egen regi eller uppdrar åt någon annan aktör att uppfylla åtagandena.

En ytterligare fråga i sammanhanget är hur många tjänsteleverantörer som kommer att utse verksamhetsställen respektive rättsliga ombud i Sverige. Samtliga tjänsteleverantörer som omfattas av skyldigheten att utse en sådan aktör kan komma att välja att utse

den i något annat EU-land eftersom tjänsteleverantörer som endast är etablerade och erbjuder tjänster i Sverige inte omfattas av förslaget.

Våra förslag om utseende av verksamhetsställen eller rättsliga ombud kan vidare ha en sådan påverkan för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags som anges i 15 § kommittéförordningen. Detta eftersom skyldigheten för tjänsteleverantörer att utse verksamhetsställen eller rättsliga ombud kan vara mer betungande för små företag än för större företag, vilket kan påverka små företag negativt i de aktuella avseendena. Det går dock inte att med någon mån av säkerhet uttala sig hur stora dessa konsekvenser kan vara, varken i fråga för den enskilde tjänsteleverantören eller för mindre tjänsteleverantörer som grupp.

Våra förslag innebär också ökade kostnader i form av vite och sanktionsavgifter för de tjänsteleverantörer som inte följer bestämmelserna i EU-förordningen respektive den kompletterande lagen. Avgifterna kan dock differentieras så att hänsyn kan tas till företagens storlek.

Ett föreläggande om bevarande i verkställighetssyfte ska enligt vårt förslag kunna riktas mot såväl fysiska som juridiska personer och mot leverantörer av elektroniska kommunikationsnät och elektroniska kommunikationstjänster. Det är svårt att med någon säkerhet uppskatta hur många beslut om förelägganden som kommer att fattas men det antas det är fråga om ett begränsat antal per år. Förslaget bedöms därmed endast ha en marginell påverkan på berörda företags kostnader.³

I sammanhanget bör framhållas att skyldigheten att lämna ut uppgifter enligt EU-förordningen respektive de bestämmelser som genomför det andra tilläggsprotokollet till Budapestkonventionen som sådan inte är ny. Det är fråga om uppgifter som tjänsteleverantörer redan i dag ska tillhandahålla inom ramen för det internationella rättsliga samarbetet, men skillnaden är att en förfrågan enligt EU-förordningen respektive de nationella bestämmelser som genomför det andra tilläggsprotokollet görs direkt av en utländsk myndighet och av inte en svensk åklagare. Däremot är tjänsteleverantörernas rätt till ersättning för utlämnande av uppgifter

³ Se motsvarande bedömning avseende bevarandeföreläggande enligt 27 kap. 16 § rättegångsbalken i prop. 2020/21:72 s. 67.

beroende av om en sådan rätt till ersättning följer av det utfärdade landets rätt eller inte.

13.6 Konsekvenser för brottsligheten och det brottsförebyggande arbetet

Vi ska, som framgår inledningsvis, enligt 15 § kommittéförordningen bedöma vilka konsekvenser våra förslag har på brottsligheten och det brottsförebyggande arbetet. EU-förordningen och övriga rättsakter syftar till att effektivisera arbetet med att inhämta bevisning och bekämpa brott. Det är sannolikt att våra förslag kommer att ha en sådan verkan, eftersom EU-förordningen och övriga rättsakter syftar till att underrätta arbetet med att utreda och lagföra brott genom att effektivisera gränsöverskridande inhämtning av elektronisk bevisning. Det är dock svårt att ha någon mer välgrundad uppfattning om i vilken utsträckning förslagen kan bidra till att minska antalet brott eller vilken påverkan de har på det brottsförebyggande arbetet.

Polismyndigheten har i sammanhanget framfört att det finns en risk för att tjänsteleverantörer prioriterar en begäran som sker genom EU-regelverket framför en inhemsk begäran, eftersom de sanktioner som kan aktualiseras vid en överträdelse av EU-förordningens regler är strängare än de sanktioner som kan bli aktuella i ett nationellt ärende.

13.7 Övriga konsekvenser

Vi bedömer att våra förslag i övrigt inte får några sådana konsekvenser som anges i 15 § kommittéförordningen som ska redovisas i betänkandet, dvs. konsekvenser för den kommunala självstyrelsen, för sysselsättning och offentlig service i olika delar av landet, för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen.

14 Ikraftträdande- och övergångsbestämmelser

14.1 Ikraftträdande

Förslag: Lagen om inhämtande av elektronisk bevisning inom Europeiska unionen ska träda i kraft den 18 augusti 2026. Övriga bestämmelser ska träda i kraft den 1 juli 2026.

Mellan den 18 februari 2026 och den 18 augusti 2026 ska en tillfällig lag gälla som reglerar tjänsteleverantörernas skyldighet att utse verksamhetsställen eller rättsliga ombud.

Skälen för förslaget: EU-förordningen ska tillämpas i alla medlemsstater från och med den 18 augusti 2026. Den föreslagna lagen om inhämtande av elektronisk bevisning inom Europeiska unionen bör därför träda i kraft samma datum.

De bestämmelser som är nödvändiga för att följa EU-direktivet ska dock enligt artikel 7.1 träda i kraft senast den 18 februari 2026. Vidare anges i artikel 3.6 i EU-direktivet att medlemsstaterna ska säkerställa att tjänsteleverantörer som erbjuder tjänster i unionen den 18 februari 2026 är skyldiga att utse utsedda verksamhetsställen eller rättsliga ombud senast den 18 augusti 2026 och att tjänsteleverantörer som börjar erbjuda tjänster i unionen efter den 18 februari 2026 är skyldiga att utse utsedda verksamhetsställen eller rättsliga ombud inom sex månader efter den dag då de börjar erbjuda tjänster i unionen. Mot denna bakgrund bör de nationella bestämmelser som genomför direktivets regler om att tjänsteleverantörer som erbjuder tjänster inom unionen är skyldiga att utse verksamhetsställen eller rättsliga ombud träda i kraft den 18 februari 2026. Detta bör ske genom att införa en tillfällig lag, som upphör att gälla den 18 augusti 2026 när lagen om inhämtande

av elektronisk bevisning inom Europeiska unionen föreslås träda i kraft. Den tillfälliga lagen ska endast vara tillämplig på de tjänsteleverantörer som vid tidpunkten för den tillfälliga lagens ikraftträdande erbjuder tjänster inom unionen. Eftersom tjänsteleverantörer har sex månader på sig att utse ett verksamhetsställe eller rättsligt ombud från den 18 februari 2026 bör den tillfälliga lagen endast reglera skyldigheten att utse ett verksamhetsställe eller rättsligt ombud, och således inte innehålla bestämmelser om tillsyn eller sanktioner. I fråga om de tjänsteleverantörer som börjar erbjuda tjänster från ett senare datum än den 18 februari 2026, bör centralmyndigheten i sin tillsynsverksamhet beakta fristen om sex månader för utseende av verksamhetsställe eller rättsligt ombud när den permanenta lagen föreslås träda i kraft. För dessa övergångssituationer behövs inga särskilda bestämmelser i lag.

Övriga bestämmelser, dvs. förslaget att i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder införa en möjlighet att bevara uppgifter i verkställighetssyfte samt de nationella bestämmelser som genomför det andra tilläggsprotokollet till Budapestkonventionen, bör med hänsyn till den tid som kan beräknas gå åt för remissförfarande, fortsatt beredning inom Regeringskansliet och riksdagsbehandling kunna träda i kraft den 1 juli 2026.

14.2 Övergångsbestämmelser

Bedömning: De föreslagna lagändringarna kräver inte några särskilda övergångsbestämmelser.

Skälen för bedömningen: Enligt allmänna principer får ny lag inte retroaktiv verkan. När det gäller processrättslig lagstiftning är utgångspunkten att nya regler ska tillämpas genast efter ikraftträdandet. Det innebär att nya regler ska tillämpas på varje processuell företeelse som inträffar efter det att regleringen har trätt i kraft. De processrättsliga lagändringar vi föreslår kommer i enlighet med huvudprincipen att tillämpas från och med att de träder i kraft och då även i förundersökningar som har inletts innan de föreslagna bestämmelserna träder i kraft. Vi bedömer därför att det inte behövs några övergångsbestämmelser.

15 Författningskommentar

15.1 Förslaget till tillfällig lag (2026:000) om utseende av verksamhetsställen eller rättsliga ombud

1 § Denna lag genomför vissa bestämmelser i Europaparlamentets och rådets direktiv (EU) 2023/1544 av den 12 juli 2023 om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden, i denna lag kallat EU-direktivet.

Lagen innehåller tillfälliga bestämmelser om en skyldighet för tjänsteleverantörer att utse ett verksamhetsställe eller rättsligt ombud i enlighet med EU-direktivet.

Paragrafen anger lagens innehåll. Övervägandena finns i avsnitt 14.1.

I *första stycket* anges att lagen genomför vissa bestämmelser i EU-direktivet.

Av *andra stycket* följer att lagen innehåller tillfälliga bestämmelser om en skyldighet för tjänsteleverantörer att utse ett verksamhetsställe eller rättsligt ombud i enlighet med EU-direktivet.

2 § I lagen avses med tjänsteleverantör en juridisk person som tillhandahåller en tjänst i enlighet med artikel 2.1 i EU-direktivet.

Paragrafen anger vad som i lagen avses med tjänsteleverantör och hänvisar här till 2.1 i EU-direktivet. Övervägandena finns i avsnitt 14.1. En närmare beskrivning av vilka tjänsteleverantörer som avses finns i avsnitt 6.2. Denna lag är endast tillämplig på de tjänsteleverantörer som vid tidpunkten för lagens ikraftträdande erbjuder tjänster inom unionen.

3 § En tjänsteleverantör som är etablerad i Sverige ska utse ett verksamhetsställe i Sverige eller i en annan medlemsstat för mottagande,

efterlevnad och verkställighet av beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet.

Om tjänsteleverantören utser ett verksamhetsställe i en annan medlemsstat är tjänsteleverantören inte skyldig att utse ett verksamhetsställe i Sverige under förutsättning att verksamhetsstället är etablerat i en medlemsstat där tjänsteleverantören erbjuder sina tjänster och att den staten tillämpar en av de rättsakter som anges i artikel 1.2.

Skyldigheten att utse ett verksamhetsställe gäller inte om tjänsteleverantören endast är etablerad i Sverige och enbart erbjuder tjänster inom Sveriges territorium.

Paragrafen anger under vilka omständigheter det finns en skyldighet för en tjänsteleverantör att utse ett verksamhetsställe i Sverige eller i annan medlemsstat. Övervägandena finns i avsnitt 8.3.1, 8.4 och 14.1.

I 3 kap. 2 § lagen (2026:000) om inhämtande av elektronisk bevisning inom Europeiska unionen finns en likalydande bestämmelse. Det hänvisas därför till kommentaren till den paragrafen i avsnitt 15.2 där bestämmelsens innehåll och tillämpning beskrivs.

4 § En tjänsteleverantör som inte är etablerad i någon medlemsstat, men som erbjuder tjänster i Sverige, ska utse ett rättsligt ombud med hemvist i Sverige för mottagande, efterlevnad och verkställighet av beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet.

Första stycket gäller inte om tjänsteleverantören har utsett ett rättsligt ombud med hemvist i en annan medlemsstat i vilken tjänsteleverantören erbjuder sina tjänster och att den staten tillämpar en av de rättsakter som anges i artikel 1.2.

Paragrafen anger under vilka omständigheter det föreligger en skyldighet för en tjänsteleverantör att utse ett rättsligt ombud i Sverige eller i annan medlemsstat. Övervägandena finns i avsnitt 8.3.1, 8.4 och 14.1.

I 3 kap. 3 § lagen om inhämtande av elektronisk bevisning inom Europeiska unionen finns en bestämmelse med likalydande innehåll. Det hänvisas därför till kommentaren till den paragrafen i avsnitt 15.2 där bestämmelsens innehåll och tillämpning beskrivs.

15.2 Förslaget till lag (2026:000) om inhämtande av elektronisk bevisning inom Europeiska unionen

1 kap. Allmänna bestämmelser

1 § Denna lag innehåller bestämmelser som kompletterar Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden, i denna lag kallad EU-förordningen.

Denna lag genomför också Europaparlamentets och rådets direktiv (EU) 2023/1544 av den 12 juli 2023 om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden, i denna lag kallat EU-direktivet.

Paragrafen anger lagens innehåll. Övervägandena finns i avsnitt 5.3.

I *första stycket* anges att lagen innehåller bestämmelser som kompletterar EU-förordningen. Lagen måste alltså läsas tillsammans med förordningen.

Av *andra stycket* följer att lagen också innehåller bestämmelser som genomför EU-direktivet.

2 § Termer och uttryck i bestämmelser i denna lag som kompletterar EU-förordningen har samma betydelse som i EU-förordningen.

Paragrafen anger att de termer och uttryck som används i lagen ska förstås på samma sätt som i EU-förordningen. Övervägandena finns i avsnitt 5.5.

Av paragrafen framgår bl.a. att definitionerna i artikel 3 i EU-förordningen även gäller vid tillämpningen av lagen. Hänvisningen till förordningen är i huvudsak dynamisk och avser alltså förordningen i den vid varje tidpunkt gällande lydelsen. I några fall är hänvisningen statisk, dvs. EU-förordningen i dess ursprungliga lydelse.

2 kap. Bestämmelser som kompletterar EU-förordningen

Utfärdande i Sverige av en europeisk utlämnandeorder eller bevarandeorder

1 § Åklagare är behörig enligt EU-förordningen att utfärda en europeisk utlämnandeorder och en europeisk bevarandeorder.

Polismyndigheten, Säkerhetspolisen, Tullverket, eller någon annan myndighet som ska ingripa mot brott eller brottslig verksamhet är behörig enligt EU-förordningen att utfärda en europeisk utlämnandeorder för att inhämta abonnentuppgifter och uppgifter som begärts med det enda syftet att identifiera användaren samt en europeisk bevarandeorder.

En order som har utfärdats enligt andra stycket ska godkännas av åklagare.

I paragrafen anges vilka myndigheter som är behöriga att utfärda en europeisk utlämnande- eller bevarandeorder. Övervägandena finns i avsnitt 7.5.1.

Av *första stycket* följer att åklagare är behörig att utfärda en europeisk utlämnande- eller bevarandeorder enligt EU-förordningen. Behörigheten omfattar alltså samtliga uppgiftsslag som kan inhämtas eller bevaras med hjälp av en sådan order enligt EU-förordningen, dvs. abonnentuppgifter, andra uppgifter som begärts med det enda syftet att identifiera användaren (andra användaruppgifter), trafikuppgifter samt innehållsdata. En europeisk utlämnandeorder för inhämtning av trafikuppgifter respektive innehållsdata ska dock godkännas av domstol innan den sänds över till mottagaren, se kommentaren till 2 §.

Enligt *andra stycket* är även Polismyndigheten, Säkerhetspolisen, Tullverket och annan myndighet som ska ingripa mot brott eller brottslig verksamhet behöriga att utfärda en order enligt EU-förordningen i vissa avseenden. Behörigheten omfattar utfärdande av en europeisk utlämnandeorder för inhämtning av abonnentuppgifter och andra användaruppgifter samt en europeisk bevarandeorder för samtliga uppgiftskategorier som omfattas av EU-förordningen. Behörigheten för de nämnda myndigheterna gäller även i fråga om en sådan nödsituation som avses i artikel 4.5 i EU-förordningen. De aktuella myndigheterna är således också behöriga att i en sådan situation besluta om utfärdande av en europeisk utlämnandeorder för inhämtning av abonnentuppgifter och annan användarinformation samt av en europeisk bevarandeorder.

Av *tredje stycket* följer att order som utfärdats av enligt andra stycket ska godkännas av åklagare. En order som utfärdats i en nödsituation ska enligt artikel 4.5 i EU-förordningen godkännas av åklagare innan den i artikeln angivna tidsfristen om 48 timmar löper ut. Det bör enbart vara en åklagare inom det svenska åklagarväsendet som kan ge ett sådant godkännande som avses i bestämmelsen.

2 § För domstolens handläggning av ett godkännande av en europeisk utlämnandeorder för inhämtning av trafikuppgifter eller innehållsdata enligt artikel 4.2 b i EU-förordningen gäller det som föreskrivs i rättegångsbalken vid rättens lämnande av tillstånd till hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation. Vid utfärdande av en sådan order ska även 27 kap. 22, 23–24, 31–33 och 35 §§ rättegångsbalken tillämpas.

Paragrafen innehåller bestämmelser om förfarandet vid utfärdande av en europeisk utlämnandeorder för inhämtning av trafikuppgifter respektive innehållsdata. Övervägandena finns i avsnitt 7.5.3 och 10.4.6.

EU-förordningen innehåller detaljerade regler om villkoren för utfärdande av en order som omfattas av förordningen samt under vilka förutsättningar som domstolsprövning krävs innan en utlämnandeorder översänds till mottagaren och formerna för översändandet av en order till mottagaren. Det följer direkt av artikel 4.2 b i EU-förordningen att en domstol ska godkänna en europeisk utlämnandeorder som avser trafikuppgifter och innehållsdata. Paragrafen anger dock vilka nationella regler som ska gälla för domstolens godkännande.

En europeisk utlämnandeorder av aktuellt slag motsvaras i nationell rätt av ett beslut om hemlig avlyssning av elektronisk kommunikation respektive hemlig övervakning av elektronisk kommunikation. För domstolens handläggning gäller därför vad som är föreskrivet i rättegångsbalken vid rättens lämnande av tillstånd till sådana hemliga tvångsmedel.

Detta innebär att de regler som anges i 27 kap. 21 § andra, tredje och sjätte stycket rättegångsbalken ska tillämpas. Dessa regler avser att det i tillståndet ska ange vilken tid tillståndet gäller, vilket telefonnummer, adress, kommunikationsutrustning eller geografiskt område tillståndet avser samt att tillståndet ska innehålla uppgift

om villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Vidare innebär hänvisningen till rättegångsbalken att reglerna i 27 kap. 26–30 §§ om sammanträde och förordnande av offentligt ombud är tillämpliga. Av hänvisningen till rättegångsbalken följer även att tingsrättens beslut får överklagas särskilt enligt 49 kap. 5 §. Även 27 kap. 34 § rättegångsbalken, som innehåller en alternativ forumregel för prövning av vissa frågor om hemliga tvångsmedel, är tillämplig.

Bestämmelserna i 27 kap. 22 och 23–24 §§ rättegångsbalken har vidare enligt paragrafen motsvarande tillämplighet vid utfärdande av en europeisk utlämnandeorder för inhämtning av trafikuppgifter och innehållsdata. Dessa paragrafer uppställer bl.a. vissa begränsningar när det gäller vem eller vilka hemlig avlyssning av elektronisk kommunikation kan riktas mot. Detta innebär bl.a. att det inte är tillåtet att genomföra hemlig avlyssning av elektronisk kommunikation av telefonsamtal eller andra meddelanden där någon som yttrar sig inte skulle ha kunnat höras som vittne om det som sagts eller på annat sätt kommit fram (se 27 kap. 22 § första stycket och 36 kap. 5 § andra–sjätte styckena). Vidare regleras under vilka förutsättningar uppgifter som framkommit om ett annat brott än det som legat till grund för beslutet om avlyssning eller övervakning får användas (27 kap. 23 a §). Därutöver finns bestämmelser om granskning och bevarande av upptagning eller uppteckning som har gjorts (27 kap. 24 §). Vidare anges i paragrafen att bestämmelserna om underrättelse till enskild i 27 kap. 31–33 §§ är tillämpliga vid utfärdande av en europeisk utlämnandeorder för inhämtning av trafikuppgifter och innehållsdata.

3 § Bestämmelserna i 9 kap. 29 a § lagen (2022:482) om elektronisk kommunikation ska tillämpas i de fall en motsvarande tjänsteleverantör i en annan medlemsstat lämnar ut elektronisk bevisning till en myndighet som med stöd av 1 § har utfärdat en europeisk utlämnandeorder.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om ersättningen och schablonberäkningen.

Paragrafen reglerar frågan om ersättning för kostnader som uppstått för tjänsteleverantören vid utlämnande av uppgifter. Övervägandena finns i avsnitt 10.3.

Av *första stycket* följer att bestämmelserna i 9 kap. 29 a § lagen om elektronisk kommunikation om rätt till ersättning ska tillämpas

i de fall en motsvarande tjänsteleverantör i en annan medlemsstat lämnar ut elektronisk bevisning till en svensk myndighet som med stöd av 1 § har utfärdat en europeisk utlämnandeorder för inhämtning av abonnentuppgifter eller andra användaruppgifter, trafikuppgifter eller innehållsdata.

Nämnda paragraf i lagen om elektronisk kommunikation gäller för den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § lagen om elektronisk kommunikation och är således inte tillämplig på samtliga de tjänsteleverantörer som omfattas av EU-förordningens bestämmelser. De tjänsteleverantörer som omfattas av bestämmelsen och således har rätt till ersättning är leverantörer av elektroniska kommunikationstjänster, dvs. de leverantörer som omfattas av artikel 3.3 a i EU-förordningen. Övriga tjänsteleverantörer som omfattas av EU-förordningen har inte rätt till ersättning enligt bestämmelsen.

Enligt *andra stycket* får regeringen eller den myndighet som regeringen bestämmer, i likhet med vad som gäller beträffande 9 kap. 29 a § andra stycket lagen om elektronisk kommunikation, meddela ytterligare föreskrifter om ersättningen och schablonberäkning av sådan ersättning.

Verkställighet i Sverige av en europeisk utlämnandeorder eller bevarandeorder

4 § Åklagarmyndigheten är verkställande myndighet enligt EU-förordningen.

I paragrafen anges att Åklagarmyndigheten är verkställande myndighet enligt EU-förordningen. Övervägandena finns i avsnitt 7.5.4.

Uppgifterna som verkställande myndighet innebär bl.a. att, efter en anmälan enligt artikel 8, ta ställning till det finns skäl enligt artikel 12 att vägra verkställighet av en europeisk utlämnandeorder. Vidare ska den verkställande myndigheten enligt artikel 16 besluta om verkställighet av en order som omfattas av EU-förordningen, för det fall ordern inte följs. Den verkställande myndigheten har vidare till uppgift att enligt artikel 15.1 ålägga tjänsteleverantören en sanktionsavgift för det fall denne inte fullgör sina skyldigheter (se vidare kommentaren till 4 kap. 1 §). Slutligen ska den verk-

ställande myndigheten ta del av information som rör en prövning enligt artikel 17.

5 § Ett beslut av åklagare att en europeisk utlämnandeorder ska vägras enligt artikel 12.1 i EU-förordningen eller att verkställighet av en europeisk utlämnande- eller bevarandeorder inte ska ske enligt artikel 16 i EU-förordningen ska innehålla skälen för beslutet.

Av paragrafen följer att Åklagarmyndighetens beslut i fråga om återopande av vägransgrunder samt om vägrande av verkställighet ska motiveras. Övervägandena finns i avsnitt 7.5.5.

6 § Ett intyg om en europeisk utlämnandeorder eller en europeisk bevarandeorder ska vara skrivet på svenska eller engelska eller åtföljas av en översättning till något av dessa språk.

I paragrafen anges vilka språk som ett intyg om en europeisk utlämnandeorder respektive bevarandeorder ska vara skrivet på eller översatt till. Övervägandena finns i avsnitt 10.2.

Förfarandet enligt artikel 17 i EU-förordningen

7 § Stockholms tingsrätt är behörig domstol enligt artikel 17 i EU-förordningen.

Av paragrafen följer att Stockholms tingsrätt är behörig domstol att pröva ärenden enligt artikel 17 i EU-förordningen, som innehåller bestämmelser om lagkonflikter. Övervägandena finns i avsnitt 7.5.7.

8 § Vid rättens handläggning av ett ärende enligt artikel 17 i EU-förordningen tillämpas reglerna om domstols handläggning i brottmål, om inte annat sägs i denna lag.

Handläggningen ska ske skriftligen. Sammanträde ska hållas endast om mottagaren av ordern begär det, om det inte är uppenbart att den europeiska utlämnandeordern ska upphävas.

Domstolen ska avgöra ett ärende inom 30 dagar efter det att den myndighet som har utfärdat den europeiska utlämnandeordern har begärt domstolens prövning. Endast om det finns särskilda skäl får denna tidsfrist överskridas.

Paragrafen innehåller bestämmelser om handläggningen av ett ärende enligt artikel 17 i EU-förordningen. Övervägandena finns i avsnitt 7.5.7.

Enligt *första stycket* tillämpas vid rättens handläggning av ett ärende enligt artikel 17 reglerna om domstols handläggning i brottmål, om inte annat sägs i lagen. För rättens prövning gäller alltså de allmänna reglerna i brottmål. Med det avses i första hand de för brottmål gällande bestämmelserna i rättegångsbalken. Ett sådant ärende handläggs alltså som ett ärende enligt rättegångsbalken, och inte som ett ärende enligt lagen (1996:242) om domstolsärenden. Eftersom det inte ska hållas någon huvudförhandling är tingsrätten enligt 1 kap. 3 § rättegångsbalken domför med en lagfaren domare. Övriga regler som kan bli tillämpliga, är t.ex. reglerna om jäv, anteckningar vid sammanträde, bevisupptagning och offentlighet och ordning. Rättegångsbalkens regler om domstols handläggning i brottmål innebär vidare bl.a. att reglerna i 30 kap. rättegångsbalken om motivering av beslut gäller för domstolen. Vidare ska de vanliga reglerna för överklagande tillämpas. Tingsrättens beslut överklagas till hovrätten inom tre veckor och hovrättens beslut till Högsta domstolen inom fyra veckor från hovrättens beslut.

Handläggningen av ett ärende ska enligt *andra stycket* som huvudregel ske skriftligen. Om det begärs av mottagaren, dvs. tjänsteleverantörens utsedda verksamhetsställe eller rättsliga ombud, ska emellertid sammanträde hållas. Sammanträde behöver dock inte hållas om det är uppenbart att den europeiska utlämnandeordern ska upphävas. Till sammanträdet bör mottagaren av ordern och den utfärdande myndigheten kallas.

Av *tredje stycket* följer att ett ärende enligt artikel 17 som huvudregel ska avgöras inom 30 dagar efter det att den utfärdande myndigheten har begärt rättens prövning. Föreligger det särskilda skäl får dock tidsfristen överskridas. Sådana skäl kan t.ex. vara att domstolen inte fått svar på en begäran enligt artikel 17.7 om innehållet i tredjelandets rätt inom tidsfristen eller fått svar först kort tid innan tidsfristen löper ut.

3 kap. Bestämmelser som genomför EU-direktivet

Centralmyndighet

1 § Den myndighet regeringen bestämmer är centralmyndighet enligt EU-direktivet.

Paragrafen anger att regeringen bestämmer vilken myndighet i Sverige som ska utses som centralmyndighet enligt EU-direktivet. Övervägandena finns i avsnitt 8.6.2.

Skyldighet att utse verksamhetsställe eller rättsligt ombud

2 § En tjänsteleverantör som är etablerad i Sverige ska utse ett verksamhetsställe i Sverige eller i en annan medlemsstat för mottagande, efterlevnad och verkställighet av beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet.

Om tjänsteleverantören utser ett verksamhetsställe i en annan medlemsstat är tjänsteleverantören inte skyldig att utse ett verksamhetsställe i Sverige under förutsättning att verksamhetsstället är etablerat i en medlemsstat där tjänsteleverantören erbjuder sina tjänster och att den staten tillämpar en av de rättsakter som anges i artikel 1.2.

Skyldigheten att utse ett verksamhetsställe gäller inte om tjänsteleverantören endast är etablerad i Sverige och enbart erbjuder tjänster inom Sveriges territorium.

Paragrafen anger under vilka omständigheter det finns en skyldighet för en tjänsteleverantör att utse ett verksamhetsställe i Sverige eller i annan medlemsstat. Övervägandena finns i avsnitt 8.3.1 och 8.4.

Av första stycket följer att en tjänsteleverantör som är etablerad i Sverige ska utse ett verksamhetsställe i Sverige eller annan medlemsstat för mottagande, efterlevnad och verkställighet av beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet. En tjänsteleverantör är etablerad i Sverige eller annan medlemsstat om det finns en betydande anknytning till landet genom ett verksamhetsställe. Med verksamhetsställe avses i denna kontext – enligt artikel 2.4 i direktivet – en enhet som de facto utövar ekonomisk verksamhet under en obegränsad tid genom en stabil infrastruktur varifrån tillhandahållandet av tjänster genomförs eller verksamheten förvaltas. Begreppet verksamhetsställe i denna kontext ska alltså inte förväxlas med ett sådant utsett verksamhetsställe som avses i paragrafen (och artikel 2.5 i EU-

direktivet), utan åsytftar själva etableringen. Kan en sådan etablering konstateras infaller således en skyldighet för tjänsteleverantören att utse ett verksamhetsställe enligt paragrafen för mottagande av de beslut och förelägganden som anges i bestämmelsen. Bestämmelsen omfattar tjänsteleverantörer som är juridiska personer.

Av *andra stycket* följer att en tjänsteleverantör som är etablerad i Sverige inte är skyldig att utse ett verksamhetsställe i landet, om leverantören utsett ett verksamhetsställe i en annan medlemsstat. Det står alltså tjänsteleverantören fritt att välja i vilken medlemsstat denne utser ett verksamhetsställe (vilket följer av skäl 13 i EU-direktivet). En förutsättning för att tjänsteleverantören ska kunna utse ett verksamhetsställe i en annan stat är dock att denne erbjuder tjänster i den i staten. Begreppet erbjuda tjänster innefattar, utöver en bedömning av huruvida tjänsteleverantören gör det möjligt för fysiska eller juridiska personer i en eller flera medlemsstater att använda dess tjänster, ett krav på att det finns en betydande anknytning till unionen. En sådan betydande anknytning till unionen ska anses föreligga om tjänsteleverantören har ett verksamhetsställe (i enlighet med artikel 2.4 i direktivet) i en medlemsstat, eller i avsaknad av verksamhetsställe, att det finns ett betydande antal användare i en eller flera medlemsstater eller om verksamheten är inriktad på en eller flera medlemsstater. Vidare krävs att den medlemsstaten också tillämpar en av de rättsakter som anges i artikel 1.2 i EU-direktivet, dvs. EU-förordningen, direktivet om en europeisk utredningsorder eller EU-konventionen från 2000 om ömsesidig rättslig hjälp i brottmål.

Enligt *tredje stycket* gäller inte skyldigheten i första stycket om tjänsteleverantören enbart är etablerad och erbjuder tjänster inom Sveriges territorium.

3 § En tjänsteleverantör som inte är etablerad i någon medlemsstat, men som erbjuder tjänster i Sverige ska utse ett rättsligt ombud med hemvist i Sverige för mottagande, efterlevnad och verkställighet av beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet.

Första stycket gäller inte om tjänsteleverantören har utsett ett rättsligt ombud med hemvist i en annan medlemsstat i vilken tjänsteleverantören erbjuder sina tjänster och att den staten tillämpar en av de rättsakter som anges i artikel 1.2.

Paragrafen anger under vilka omständigheter det föreligger en skyldighet för en tjänsteleverantör att utse ett rättsligt ombud i Sverige eller i annan medlemsstat. Övervägandena finns i avsnitt 8.3.1 och 8.4.

Av *första stycket* följer att en tjänsteleverantör som inte är etablerad i någon av unionens medlemsstater men som erbjuder tjänster i Sverige ska utse ett rättsligt ombud med hemvist i Sverige för mottagande, efterlevnad och verkställighet av beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet. Avseende begreppet erbjuda tjänster, se kommentaren till 2 §. Med begreppet hemvist i fråga om en juridisk person avses vanligen dess stadgeenliga säte, dess huvudkontor eller där det bedriver sin huvudsakliga verksamhet (se t.ex. 10 kap. 1 § andra stycket rättegångsbalken och artikel 63 i den s.k. Bryssel I-förordningen¹). Det rättsliga ombudet ska alltså ha en sådan anknytning till Sverige för att kravet på hemvist ska vara uppfyllt. Paragrafen omfattar tjänsteleverantörer som är juridiska personer.

Enligt *andra stycket* gäller inte skyldigheten i första stycket om tjänsteleverantören har utsett ett rättsligt ombud med hemvist i en annan medlemsstat i vilken tjänsteleverantören erbjuder sina tjänster och att den staten tillämpar en av de rättsakter som anges i artikel 1.2. Det står alltså en tjänsteleverantör, som inte är etablerad i någon medlemsstat, fritt att välja i vilken eller vilka stater som det rättsliga ombudet ska utses, dock under förutsättning att tjänsteleverantören erbjuder tjänster i staten och att staten tillämpar en av de rättsakter som anges i artikel 1.2.

4 § De verksamhetsställen och rättsliga ombud som har utsetts i Sverige ska ta emot sådana beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet.

Paragrafen reglerar skyldigheten för de verksamhetsställen och rättsliga ombud som har utsetts i Sverige att ta emot sådana beslut och förelägganden som omfattas av det tillämpningsområde som anges i artikel 1.2 i EU-direktivet. Övervägandena finns i avsnitt 8.4.

En europeisk utlämnande- eller bevarandeorder som utfärdas med stöd av bestämmelserna i EU-förordningen ska enligt EU-förordningen riktas till det av tjänsteleverantören utsedda verk-

¹ Europaparlamentets och rådets förordning (EU) nr 1215/2012 av den 12 december 2012 om domstols behörighet och om erkännande och verkställighet av domar på privaträttens område.

samhetsstället eller rättsliga ombudet och dessa ska alltså enligt bestämmelsen ta emot sådana förelägganden och beslut som omfattas av EU-förordningen, men även av övriga rättsakter som anges artikel 1.2. Paragrafen omfattar de verksamhetsställen som utsetts enligt 2 och 3 §§, men även sådana verksamhetsställen som utsetts i Sverige av en tjänsteleverantör som är etablerad i en annan medlemsstat, se även 5 § andra stycket.

Artikel 1.2 i EU-direktivet omfattar som nämnts EU-förordningen, men även direktivet om en europeisk utredningsorder och EU-konventionen från 2000 om ömsesidig rättslig hjälp i brottmål samt inhemska förfaranden. I fråga om dessa två sistnämnda rättsakter finns bestämmelser i lagen (2000:562) om internationell rättslig hjälp i brottmål respektive i lagen (2017:1000) om en europeisk utredningsorder. Beträffande inhemska förfaranden finns bestämmelser i lagen om elektronisk kommunikation och rättegångsbalken.

En begäran om rättslig hjälp enligt lagen om internationell rättslig hjälp i brottmål hanteras av åklagare och beslutas av domstol om det blir aktuellt med hemliga tvångsmedel. Bestämmelsen ger svensk åklagare möjlighet att vid en ansökan om rättslig hjälp avseende t.ex. inhämtning av abonnentuppgifter att vända sig till ett utsett verksamhetsställe eller rättsligt ombud i Sverige. Motsvarande gäller i fråga om en svensk åklagare som ska erkänna och verkställa en utfärdad europeisk utredningsorder som mottagits enligt lagen om en europeisk utredningsorder om att inhämta abonnentuppgifter. Samma gäller i inhemska förfaranden.

Bestämmelsen påverkar dock inte de nationella myndigheternas befogenheter att i enlighet med unionsrätten och nationell rätt rikta framställningar direkt till tjänsteleverantörer som är etablerade i landet i syfte att samla in elektroniska bevis i straffrättsliga förfaranden, vilket följer av artikel 1.3 i EU-direktivet. Vill t.ex. en svensk åklagare vända sig direkt till tjänsteleverantören i fråga om en ansökan om rättslig hjälp eller en mottagen europeisk utredningsorder är detta möjligt. Bestämmelsen hindrar inte detta utan ger endast ett alternativ för de brottsbekämpande myndigheterna.

5 § En tjänsteleverantör som utser ett verksamhetsställe enligt 2 § ska ge verksamhetsstället de befogenheter och resurser som krävs för att svara på sådana beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet.

Ett verksamhetsställe, som inte har utsetts enligt 2 §, eller ett rättsligt ombud i Sverige ska ha de befogenheter och resurser som krävs för att svara på sådana beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet.

Paragrafen anger krav på befogenheter och resurser som ska ges till ett verksamhetsställe eller rättsligt ombud. Övervägandena finns i avsnitt 8.4.

Av *första stycket* följer att en tjänsteleverantör som utsett ett verksamhetsställe enligt 2 § ska ge sitt utsedda verksamhetsställe de befogenheter och resurser som krävs för att svara på sådana beslut och förelägganden som avses i artikel 1.2 i EU-direktivet. En tjänsteleverantör som är etablerad i Sverige omfattas alltså av bestämmelsen, även om denne utsett ett verksamhetsställe i en annan medlemsstat enligt 2 § andra stycket. Skyldigheten att förse verksamhetsstället med tillräckliga befogenheter och resurser gäller således även om verksamhetsstället utses i en annan medlemsstat, under förutsättning att de krav som anges i 2 § andra stycket är uppfyllda.

Enligt *andra stycket* gäller skyldigheten att ge utsedda verksamhetsställen och rättsliga ombud de befogenheter och resurser som krävs för att svara på sådana beslut och förelägganden som avses i artikel 1.2 i EU-direktivet även för den tjänsteleverantör som utsett ett verksamhetsställe eller rättsligt ombud i Sverige. Andra stycket reglerar således en skyldighet gentemot tjänsteleverantörer som inte är etablerade i Sverige, men som erbjuder tjänster här och har utsett ett verksamhetsställe eller rättsligt ombud i landet.

Vilka befogenheter och resurser som krävs enligt paragrafen kan variera mellan olika tjänsteleverantörer och karaktären på dess verksamhet. Det får därför avgöras i det enskilda fallet – och då ytterst av centralmyndigheten i egenskap av tillsynsmyndighet – vilka befogenheter och resurser som är tillräckliga.

Tillsyn

6 § Centralmyndigheten ska ha tillsyn över att 2–5 §§ och de föreskrifter som har meddelats i anslutning till lagen följs.

Paragrafen anger centralmyndighetens tillsynsområde. Övervägandena finns i avsnitt 8.6.3.

Tillsynsområdet omfattar bestämmelserna i 2–5 §§ om att utse ett verksamhetsställe eller rättsligt ombud samt att tjänsteleverantören har gett dessa aktörer tillräckliga resurser och befogenheter att besvara sådana beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet. Tillsynsobjekten innefattar de tjänsteleverantörer som är etablerade eller erbjuder tjänster i Sverige, oavsett om de utsett verksamhetsställen i landet eller i någon annan medlemsstat, samt verksamhetsställen och rättsliga ombud som andra tjänsteleverantörer har utsett i Sverige.

Centralmyndigheten har alltså i uppgift att utöva tillsyn över att tjänsteleverantörer som är etablerade i Sverige har utsett ett verksamhetsställe i Sverige eller i en annan medlemsstat i enlighet med de krav som följer av 2 § och att dessa verksamhetsställen fullföljer den uppgift som anges i 4 § samt har getts tillräckliga resurser och befogenheter enligt 5 §. För att fullgöra denna uppgift kan det bli aktuellt för den svenska centralmyndigheten att samråda med centralmyndigheter i andra medlemsstater.

Centralmyndigheten har också till uppgift att utöva tillsyn över att tjänsteleverantörer som inte är etablerade i någon medlemsstat fullföljer sina skyldigheter enligt 3 §. Vidare omfattar tillsynen kontroll av att de verksamhetsställen och rättsliga ombud, som utsetts av andra tjänsteleverantörer än de som avses i 2 §, och som ska verka i Sverige på samma sätt kan fullfölja den uppgift som anges i 4 § samt har getts tillräckliga resurser och befogenheter enligt 5 §. Om tjänsteleverantören är etablerad i en annan medlemsstat får det dock anses primärt vara den medlemsstatens centralmyndighet som ska vidta åtgärder mot tjänsteleverantören, t.ex. vad gäller beslut om sanktioner. Den svenska centralmyndigheten kan dock bistå i detta arbete genom att samråda med centralmyndigheten i den andra staten.

Vidare omfattar tillsynsområdet föreskrifter som i förordning meddelats med stöd av lagen, vilket avser de nationella bestämmelser som genomför artikel 4 i EU-direktivet om tjänsteleverantörens skyldighet att förse centralmyndigheten med kontaktuppgifter till verksamhetsstället eller det rättsliga ombudet och uppgifter om de språk som godtas i kommunikationen med dessa.

7 § Centralmyndigheten har rätt att för tillsynen få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som omfattas av denna lag bedrivs.

Paragrafen ger tillsynsmyndigheten rätt att få tillträde till vissa utrymmen för att kunna bedriva en effektiv tillsyn. Övervägandena finns i avsnitt 8.6.3.

Bestämmelsen avser områden, lokaler och andra utrymmen, med undantag för bostäder, där tjänsteleverantören eller dess utsedda verksamhetsställe eller rättsliga ombud bedriver sin verksamhet. Bestämmelsen bör tillämpas med särskild försiktighet i fråga om tillträde till lokaler och andra utrymmen för verksamhet som omfattas av grundlagsskydd, t.ex. redaktionslokaler för massmedia. Centralmyndighetens befogenheter enligt bestämmelsen kan endast utövas i Sverige. Skulle centralmyndigheten behöva utöva sådan tillsyn, t.ex. om ett verksamhetsställe som utsetts i en annan medlemsstat av en tjänsteleverantör som är etablerad i Sverige ska anses etablerat där eller har getts tillräckliga resurser eller befogenheter, får myndigheten vända sig till centralmyndigheten i den staten för bistånd och samråd.

8 § Centralmyndigheten får förelägga den som bedriver verksamhet som omfattas av denna lag att tillhandahålla myndigheten de upplysningar eller handlingar som behövs för tillsynen.

Ett föreläggande enligt första stycket får förenas med vite.

Paragrafen innehåller en rätt för centralmyndigheten att besluta om föreläggen. Övervägandena finns i avsnitt 8.6.3 och 9.4.2.

Enligt *första stycket* får centralmyndigheten kräva in de upplysningar eller handlingar som behövs för tillsynen av bestämmelserna i 2–5 §§. Centralmyndigheten kan t.ex. behöva tillgång till handlingar eller upplysningar från en enskild tjänsteleverantör för att kunna avgöra om den är skyldig att utse ett verksamhetsställe eller rättsligt ombud, t.ex. vad avser bedömningen om en tjänsteleverantör ska anses vara etablerad inom unionen eller erbjuder tjänster på den enskilda medlemsstatens territorium. Centralmyndigheten kan också behöva upplysningar eller handlingar för att kunna avgöra om ett i Sverige utsett verksamhetsställe eller rättsligt ombud har getts tillräckliga befogenheter och resurser för att besvara sådana föreläggen och beslut som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet.

Av *andra stycket* följer att ett föreläggande enligt första stycket får förenas med vite. Lagen (1985:206) om viten (viteslagen) innehåller bestämmelser om handläggningen av ärenden om vitesförelägganden och gäller enligt 1 § viten som enligt lag eller annan författning får föreläggas av myndigheter, såvida inte annat följer av vad som är särskilt föreskrivet. Av 2 § viteslagen följer att vitesförelägganden ska delges. Enligt 3 § viteslagen ska vite, när det föreläggs, fastställas till ett belopp som med hänsyn till vad som är känt om adressatens ekonomiska förhållanden och till omständigheterna i övrigt kan antas förmå honom att följa det föreläggande som är förenat med vitet. Frågor om utdömande av viten prövas av förvaltningsrätt på ansökan av den myndighet som har utfärdat vitesföreläggandet (6 §).

Förvaltningslagen (2017:900) och förvaltningsprocesslagen (1971:291) ska tillämpas vid handläggningen hos centralmyndigheten respektive i förvaltningsdomstol.

9 § Centralmyndighetens beslut som avser åtgärder som krävs för tillsynen enligt denna lag får verkställas av Kronofogdemyndigheten. Då gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

Paragrafen behandlar möjligheten till verkställighet av centralmyndighetens beslut om åtgärder. Övervägandena finns i avsnitt 8.6.3.

Centralmyndigheten kan enligt bestämmelsen begära handräckning av Kronofogdemyndigheten. Det skulle t.ex. kunna bli aktuellt om myndigheten behöver avlägsna fysiska hinder för att kunna genomföra sin tillsyn. I fråga om förfarandet hos Kronofogdemyndigheten gäller utsökningsbalken i tillämpliga delar. Sådant bistånd som anges i paragrafen kan endast begäras inom Sverige. För behov av motsvarande åtgärder i ett annat land, får centralmyndigheten samråda med centralmyndigheten i det landet.

10 § Centralmyndigheten får meddela de förelägganden som behövs för att 2–5 §§ eller de föreskrifter som har meddelats i anslutning till lagen ska följas.

Ett föreläggande enligt första stycket får förenas med vite.

Paragrafen innehåller bestämmelser om förelägganden för att komma till rätta med överträdelser av bestämmelserna i 2–5 §§ och de före-

skrifter som meddelats med stöd av lagen. Övervägandena finns i avsnitt 8.6.3 och 9.4.2.

Enligt *första stycket* får centralmyndigheten meddela de förelägganden som behövs för att bestämmelserna i 2–5 §§ eller i de föreskrifter som meddelats med stöd av lagen ska följas. Ett sådant föreläggande kan t.ex. bli aktuellt när centralmyndigheten efter en tillämpning av 7 eller 8 § kan konstatera att en tjänsteleverantör inte lever upp till de åtaganden som följer av 2–5 §§. Ett föreläggande enligt förevarande paragraf innebär således att tjänsteleverantören ska vidta de rättelser som krävs för att leva upp till sistnämnda bestämmelser.

Av *andra stycket* följer att ett föreläggande enligt första stycket får förenas med vite. Om handläggningen av vitesförelägganden, se kommentaren till 9 § ovan.

4 kap. Gemensamma bestämmelser om sanktionsavgifter

1 § Åklagarmyndigheten ska besluta att ta ut en sanktionsavgift av ett utsett verksamhetsställe eller rättsligt ombud i Sverige som åsidosätter någon av sina skyldigheter enligt artikel 10, 11 eller 13.4 i EU-förordningen, i den ursprungliga lydelsen.

Åklagarmyndigheten får besluta att den tjänsteleverantör som har utsett det verksamhetsställe eller rättsliga ombudet som ska betala en sanktionsavgift enligt första stycket ska ha ett solidariskt betalningsansvar för avgiften.

I paragrafen regleras sanktionsavgifter som följer efter överträdelse av angivna bestämmelser i EU-förordningen. Övervägandena finns i avsnitt 9.3.2.

Av *första stycket* följer att det är Åklagarmyndigheten, i egenkap av verkställande myndighet enligt EU-förordningen som beslutar om sanktionsavgift. I paragrafen anges de överträdelser av regelverket som kan föranleda att en sanktionsavgift ska tas ut av den som har gjort sig skyldig till överträdelsen. Enligt artikel 15.1 ska överträdelse av artiklarna 10, 11 och 13.4 kunna leda till beslut om sanktionsavgift med anledning av att ett verksamhetsställe eller rättsligt ombud inte har efterlevt ett beslut om att en europeisk utlämnande- eller bevarandeorder ska verkställas (se artikel 16.10). Bestämmelserna i artiklarna 10, 11 och 13.4 avser dels huruvida en utlämnandeorder eller bevarandeorder har följts på det sätt som

anges i artikel 10 respektive artikel 11, dels om mottagaren av en sådan order har säkerställt konfidentialiteten, sekretessen och integriteten för intyget om en europeisk utlämnande- eller bevarandeorder för de uppgifter som lämnas ut eller bevaras. Hänvisningen till förordningen är utformad så att den avser förordningen i den ursprungliga lydelsen, s.k. statisk hänvisning.

Strikt ansvar för överträdelser gäller. Det innebär att det inte krävs att det föreligger någon form av uppsåt eller vårdslöshet hos den som gjort sig skyldig till överträdelsen. Det är obligatoriskt för den verkställande myndigheten att besluta om sanktionsavgift vid en konstaterad överträdelse, vilket följer av formuleringen att avgift ska tas ut. Av 4 § framgår att den verkställande myndigheten ska beakta olika försvårande och förmildrande omständigheter vid prövningen av avgiftens storlek. Avgiften ska tas ut av tjänsteleverantörens utsedda verksamhetsställe eller rättsliga ombud i Sverige.

Av *andra stycket* följer dock att åklagaren får även vända sig till tjänsteleverantören för betalningen av avgiften. Åklagarmyndigheten kan således vända sig mot både tjänsteleverantören och det utsedda verksamhetsstället eller någon av dem för uttagande av sanktionsavgift, dvs. betalningsansvaret kan göras solidariskt.

2 § Centralmyndigheten ska besluta att ta ut en sanktionsavgift av den tjänsteleverantör som åsidosätter någon av sina skyldigheter enligt 3 kap. 2–5 §§.

I paragrafen regleras sanktionsavgifter som följer efter överträdelse av de nationella bestämmelser som genomför vissa av EU-direktivets bestämmelser. Övervägandena finns i avsnitt 9.4.3.

Det är centralmyndigheten som beslutar om sanktionsavgift enligt paragrafen. Av bestämmelsen följer att överträdelser av bestämmelserna i 3 kap. 2–5 §§ kan föranleda att en sanktionsavgift ska tas ut av den som har gjort sig skyldig till överträdelsen, dvs. tjänsteleverantören. Det handlar sammanfattningsvis om en skyldighet för tjänsteleverantörer som omfattas av 3 kap. 2 och 3 §§ att enligt dessa bestämmelser utse ett verksamhetsställe eller rättsligt ombud samt förse verksamhetsstället eller det rättsliga ombudet med tillräckliga resurser och befogenheter att besvara de förelägganden och beslut som omfattas av det tillämpningsområde som fastställs i artikel 1.2 i EU-direktivet.

Strikt ansvar för överträdelser gäller. Det innebär att det inte krävs att det föreligger någon form av uppsåt eller vårdslöshet hos den som gjort sig skyldig till överträdelser. Det är obligatoriskt för centralmyndigheten att besluta om en sanktionsavgift vid en konstaterad överträdelse, vilket följer av formuleringen att avgift ska tas ut. Av 4 § framgår att myndigheten ska beakta olika försvårande och förmildrande omständigheter vid prövningen av avgiftens storlek.

3 § Sanktionsavgiften enligt 1 och 2 §§ ska bestämmas till lägst 10 000 kronor och högst till ett sådant högre belopp som följer av artikel 15.1 i EU-förordningen, i den ursprungliga lydelsen.

Paragrafen reglerar vilka belopp som sanktionsavgiften ska bestämmas till. Övervägandena finns i avsnitt 9.3.2 och 9.4.3.

I paragrafen fastställs det lägsta och det högsta beloppet för en sanktionsavgift. Det högsta beloppet får, i enlighet med vad som anges i artikel 15.1 i EU-förordningen, uppgå till två procent av tjänsteleverantörens totala globala årsomsättning föregående räkenskapsår. Hänvisningarna till förordningen är utformade så att de avser förordningen i den ursprungliga lydelsen, s.k. statisk hänvisning. Det är den verkställande myndigheten respektive centralmyndigheten som beslutar om sanktionsavgiftens storlek. Hur avgiften ska bestämmas i det enskilda fallet regleras i 4 och 5 §§.

4 § När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till

1. om överträdelser varit uppsåtlig eller berott på oaktsamhet,
2. den skada, fara eller kränkning som överträdelser inneburit,
3. överträdelserns karaktär, svårhetsgrad och varaktighet,
4. om den tjänsteleverantör som har begått överträdelser tidigare begått en överträdelse, och
5. den berörda tjänsteleverantörens finansiella ställning.

Paragrafen reglerar hur sanktionsavgiften i det enskilda fallet ska bestämmas. Övervägandena finns i avsnitt 9.3.2 och 9.4.3.

Av paragrafen följer att den verkställande myndigheten respektive centralmyndigheten ska beakta dessa omständigheter när sanktionsavgiftens storlek bestäms. Uppräkningen är inte uttömmande, vilket innebär att hänsyn kan tas även till andra relevanta omständigheter.

I *punkt 1* föreskrivs att det ska beaktas om överträdelser varit uppsåtlig eller berodde på oaktsamhet. En avsiktlig överträdelse

visar tydligt på nonchalans mot regleringen och utrymmet att underlåta att ta ut avgift eller att bestämma avgiften till ett lågt belopp bör vara mycket litet. Avsiktliga överträdelse talar starkt för att sanktionsavgift ska tas ut med ett högt belopp. Om överträdelsen haft sin grund i oaktsamhet, t.ex. missförstånd om hur regleringen ska tillämpas eller ursäktliga bedömningsfel, talar det för en lägre sanktionsavgift, såvida inte oaktsamheten är grov. Det kan dock inte uteslutas att en sanktionsavgift i vissa fall bör tas ut med högre belopp även om överträdelsen skett med oaktsamhet. Det kan vara fallet om överträdelsen fått eller riskerat att få allvarliga konsekvenser, t.ex. att en större mängd uppgifter som begärts ut har gått förlorade till följd av en order enligt EU-förordningen inte har följts.

Enligt *punkt 2* ska det beaktas vilken skada, fara eller kränkning som överträdelsen inneburit. Det behöver inte konstateras att skada uppstått utan det räcker att det funnits risk för skada. Som regel blir det fråga om att göra en helhetsbedömning av de potentiella skadeverkningarna. En faktisk skada behöver inte heller vara allvarligare än risken för skada, särskilt om risken varit mycket hög och skadan – om den hade inträffat – skulle ha fått stora konsekvenser. Risken för skada kan t.ex. vara mycket stor om en tjänstleverantör som är etablerad eller erbjuder i tjänster i Sverige har underlåtit att utse ett verksamhetsställe eller rättsligt ombud i Sverige eller någon annan medlemsstat, vilket försvårar eller omöjliggör mottagandet och hanteringen av en order som omfattas av EU-förordningen.

Även överträdelsens karaktär, svårhetsgrad och varaktighet ska enligt *punkt 3* beaktas. Här är det t.ex. av betydelse om vägran att helt följa en europeisk utlämnande- eller bevarandeorder skett uppsåtligt och lett till att en stor mängd uppgifter som skulle kunna användas som bevis gått förlorade. Ju allvarligare överträdelse, desto starkare skäl talar för att beloppet ska sättas högt. I motsvarande riktning kan beaktas att ordern har bevarats men att de svarstider som anges i artiklarna 10 och 11 inte har följts, dock utan att bevisning har gått förlorad. Ett annat exempel på olika svårhetsgrader är om tjänstleverantören inte gett sitt utsedda verksamhetsställe eller rättsliga ombud de befogenheter och resurser som krävs för att besvara förelägganden och beslut och denna underlåtenhet varit bestående under en längre tid, vilket talar för att avgiften ska

sättas högre än om det endast varit fråga om en underlåtenhet som varit begränsad i tiden.

Av *punkt 4* följer att det också ska beaktas om den som har begått överträdelsen tidigare har begått en överträdelse. Det är t.ex. särskilt allvarligt om tjänsteleverantören vid upprepade tillfällen har underlåtit att följa en europeisk utlämnande- eller bevarandeorder. Om tjänsteleverantören tidigare har ålagts att betala sanktionsavgift för samma typ eller liknande överträdelser bör det också ses som försvårande.

Enligt *punkt 5* ska även tjänsteleverantörens finansiella ställning beaktas vid bestämmandet av avgiftens storlek. Den finansiella ställningen indikeras genom t.ex. en juridisk persons totala omsättning eller en fysisk persons årsinkomst. Hänsyn ska tas till om det är fråga om en mindre aktör i sammanhanget, som inte ska påföras en avgift som är mer betungande än för en större aktör i fråga om samma typ av överträdelse. Sanktionsavgifter för juridiska personer bör normalt sett bestämmas till högre belopp än för fysiska personer för samma typ av överträdelse. Det ska dock noteras att det torde vara sällsynt det blir aktuellt med sanktioner mot fysiska personer även om dessa omfattas av EU-förordningens definition av tjänsteleverantörer. Det kan också framhållas att fysiska personer inte omfattas av bestämmelserna i 3 kap. 2 och 3 §§, dvs. dessa bestämmelser gäller endast för tjänsteleverantörer som är juridiska personer, se kommentaren till respektive paragraf.

5 § Sanktionsavgiften får sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut en avgift.

I paragrafen regleras jämkning av sanktionsavgift. Övervägandena finns i avsnitt 9.3.2 och 9.4.3.

Det kan ibland finnas omständigheter som gör att det framstår som oskäligt eller stötande att ta ut en sanktionsavgift, trots att förutsättningarna för att ta ut en avgift är uppfyllda. Paragrafen ger möjlighet att sätta ned sanktionsavgiften, helt eller delvis, om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut en avgift. Bestämelsen avser undantagssituationer och ska tillämpas restriktivt.

Sanktionsavgiften bör t.ex. kunna sättas ned helt eller delvis om exempelvis ett mindre företag inte har resurser att svara på en order

i en nödsituation. Det kan också röra sig om fall där det har gått så lång tid sedan överträdelsen att det skulle vara oskäligt att ta ut en sanktionsavgift. Andra omständigheter att beakta i mildrande riktning kan vara att den avgiftsskyldige har samarbetat med den verkställande myndigheten eller med centralmyndigheten för att komma till rätta med överträdelsen eller skyndsamt har vidtagit rättelse för att minska skadan eller risken för skada. Det är däremot inte oskäligt att ta ut en avgift när överträdelsen exempelvis har berott på att okunskap om regelverket eller på dålig ekonomi, tidsbrist, glömska eller undermåliga rutiner.

Det kan förekomma att en tjänsteleverantör är etablerad i eller bedriver verksamhet i flera olika medlemsstater. Om tjänsteleverantören inte har utsett verksamhetsställe eller rättsligt ombud i någon medlemsstat föreligger förutsättningar för samtliga medlemsstater att påföra sanktionsavgift. I ett sådant fall bör endast en medlemsstat påföra sanktionsavgift, eftersom tjänsteleverantören kan välja i vilken medlemsstat som verksamhetsstället eller det rättsliga ombudet ska utses. Har en annan medlemsstat i en sådan situation redan påfört en sanktionsavgift bör den svenska centralmyndigheten efterge sanktionsavgiften då det får anses oskäligt att ta ut avgift om annan medlemsstat redan har gjort detta.

Regleringen i 3 § om sanktionsavgifternas storlek hindrar inte ett beslut om jämkning som innebär att sanktionsavgift tas ut med ett belopp som är lägre än 10 000 kronor.

6 § En sanktionsavgift får inte beslutas enligt 2 § om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömmande av vitet.

En sanktionsavgift får inte beslutas enligt 1 § om överträdelsen omfattas av ett beslut om sanktionsavgift enligt 2 §.

I paragrafen regleras ett förbud mot beslut om sanktionsavgifter i vissa fall. Övervägandena finns i avsnitt 9.4.3 och 9.5.

Enligt *första stycket* får en sanktionsavgift inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömmande av vitet. Paragrafen syftar till att förhindra att samma överträdelse blir föremål för dubbla prövningar och sanktioner. Regleringen avser det förhållande att ett föreläggande med vite har meddelats med stöd av 3 kap. 10 §. De aktuella bestämmelserna i EU-förordningen kan inte vara

föremål för ett sådant vitesföreläggande enligt lagen. Om ett beslut om vitesföreläggande har meddelats och en domstolsprocess inletts om utdömning av vitet är centralmyndigheten enligt bestämmelsen förhindrad att besluta om sanktionsavgift för samma överträdelse. Bestämmelsen hindrar dock inte att en överträdelse först kan bli föremål för ett vitesföreläggande och i ett senare skede beslut om sanktionsavgift, under förutsättning att någon ansökan om utdömning av vitet inte har gjorts.

Av *andra stycket* följer att en sanktionsavgift inte får beslutas enligt 1 § om överträdelsen omfattas av ett beslut om sanktionsavgift enligt 2 §. Bestämmelsen tar sikte på en sådan situation där det finns förutsättningar för både den verkställande myndigheten och centralmyndigheten att fatta beslut om sanktionsavgift. En vägran att följa en sådan order som omfattas av EU-förordningens bestämmelser kan ju bero på att tjänsteleverantören i fråga inte har utsett ett verksamhetsställe eller rättsligt ombud på föreskrivet sätt, vilket alltså innebär att det saknas en organisation att ta hand om ordern. Med andra ord kan inte en utlämnande- eller bevarandeorder besvaras om inte tjänsteleverantören har utsett ett verksamhetsställe eller rättsligt ombud. I ett sådant fall får den verkställande myndigheten inte fatta beslut om sanktionsavgift, om överträdelsen omfattas av ett beslut om sanktionsavgift av centralmyndigheten. I 6 § förordningen (2026:000) med kompletterande bestämmelser om inhämtande av elektronisk bevisning inom Europeiska unionen föreslås bestämmelser om samråd mellan de berörda myndigheterna.

7 § 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 bl.a. preskriptionstiden för beslut om sanktionsavgift. Övervägandena finns i avsnitt 9.5.

Första stycket innebär att kommunikation enligt 25 § förvaltningslagen måste ske inom två år för att en sanktionsavgift ska få beslutas. Tidsfristen räknas från när överträdelsen ägde rum. Den verkställande myndigheten respektive centralmyndigheten ska självant beakta att kommunikation har skett.

Andra stycket innebär att ett beslut om sanktionsavgift ska delges den avgiftsskyldige med hjälp av något av de förfaranden för delgivning som regleras i delgivningslagen (2010:1932).

8 § En sanktionsavgift ska betalas till Åklagarmyndigheten eller Centralmyndigheten 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 tid, ska myndigheten lämna den obetalda avgiften för indrivning enligt lagen (1993:891) om indrivning av statliga fordringar m.m.

Sanktionsavgiften tillfaller staten.

Paragrafen reglerar betalning och indrivning av sanktionsavgifter. Övervägandena finns i avsnitt 9.5.

Enligt *första stycket* ska avgiften betalas inom 30 dagar efter det att beslutet fått laga kraft. En möjlighet finns att förlänga tiden, t.ex. om det rör sig om en mindre aktör som behöver lite mer tid för att få fram medel att betala avgiften med.

Om avgiften inte betalas inom den angivna tiden ska enligt *andra stycket* den beslutande myndigheten lämna den obetalda avgiften för indrivning enligt lagen om indrivning av statliga fordringar m.m. Beslutet om sanktionsavgift utgör en exekutionstitel (3 kap. 1 § första stycket 6 utsökningsbalken). Det innebär att verkställighet enligt utsökningsbalken kan ske utan att det krävs något domstolsavgörande.

Av *tredje stycket* följer att avgiften tillfaller staten.

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

Paragrafen reglerar preskription av sanktionsavgifter. Övervägandena finns i avsnitt 9.5.

Bestämmelsen innebär att en sanktionsavgift preskriberas om verkställighet inte har skett inom fem år från det att beslutet fick laga kraft. Det som preskriberas är den del av avgiften som inte har drivits in när fem år har gått sedan beslutet fick laga kraft.

10 § Beslut om sanktionsavgift får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

I paragrafen regleras överklagande av beslut om sanktionsavgift. Övervägandena finns i avsnitt 9.5.

Första stycket anger att beslut om sanktionsavgift får överklagas till allmän förvaltningsdomstol. Endast den som beslutet angår får överklaga det och endast om det har gått honom eller henne emot (42 § förvaltningslagen).

Enligt *andra stycket* krävs prövningstillstånd vid överklagande till kammarrätten.

15.3 Förslaget till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål

1 kap.

7 a §

Denna lag gäller inte om lagen (2017:1000) om en europeisk utredningsorder är tillämplig.

Att lagen gäller vid skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter enligt artikel 29 i Europarådets konvention om it-relaterad brottslighet följer av 1 kap. 5 a § lagen (2017:1000) om en europeisk utredningsorder.

Paragrafen reglerar i vilken omfattning lagen om en europeisk utredningsorder ska tillämpas i stället för förevarande lag. Övervägandena finns i avsnitt 11.5.1.

I andra stycket, som är nytt, finns en upplysning om att det följer av 1 kap. 5 a § lagen om en europeisk utredningsorder att förevarande lag gäller vid skyndsamt säkrande av datorbehandlingsbara uppgifter enligt artikel 29 i Budapestkonventionen, se kommentaren till nämnda lagrum i avsnitt 15.5.

2 kap.

10 §

Ansökningar om rättslig hjälp *ska* behandlas skyndsamt. *Om det föreligger en omedelbar fara för liv, hälsa eller egendom, ska särskild hänsyn tas till kravet om skyndsambhet vid handläggningen av en ansökan.*

Om inte annat föreskrivs i denna lag tillämpas samma förfarande som när en motsvarande åtgärd vidtas vid en svensk förundersökning eller rättegång.

Domstol kan bestämma att handläggningen helt eller delvis ska ske på ett främmande språk, om det är lämpligt.

Paragrafen anger bl.a. krav på särskilt iakttagande av skyndsamhet i nödsituationer vid handläggning av en ansökan om rättslig hjälp. Övervägandena finns i avsnitt 12.7.4.

I *första stycket* görs ett tillägg med innebörden att det vid handläggningen av en ansökan ska särskild hänsyn tas till om det är fråga om en omedelbar fara för liv, hälsa eller egendom. Bestämmelsen ställer således ett krav på särskild skyndsamhet om en nödsituation är för handen. Exempel på en nödsituation som omfattas av paragrafen är en gisslansituation där det finns en trolig risk för omedelbar förlust av liv eller allvarlig skada för brottsoffret, pågående sexuella övergrepp mot barn, de omedelbara efterdyningarna av en terroristattack och hot mot säkerheten för kritisk infrastruktur där det finns en betydande och överhängande risk för en fysisk persons liv eller säkerhet. Andra exempel på en nödsituation är en ransomware-attack som riskerar att lamslå ett sjukhusssystem eller en kidnappningssituation där ett e-postkonto används av kidnappare för att ställa krav och kommunicera med offrets familj. Det är den handläggande myndigheten, dvs. åklagaren, som avgör om det föreligger en sådan nödsituation som avses i bestämmelsen.

Andra och tredje styckena motsvarar hittillsvarande andra respektive tredje meningen i paragrafen.

Övriga ändringar är endast av språklig karaktär.

3 kap.

1 §

Bestämmelserna i 2 kap. 4 § första och tredje styckena ska tillämpas vid ansökan om rättslig hjälp utomlands, om inte annat följer av en internationell överenskommelse som är bindande för Sverige eller av krav från den mottagande staten.

I 4 kap. 9, 10, 13, 24 b, 26, 26 c och 31 a §§ finns särskilda bestämmelser om vad en ansökan ytterligare ska innehålla vid vissa slag av åtgärder.

En order enligt artikel 8 i det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet om inhämtande av abonnemangs-

uppgifter och lagrade trafikuppgifter ska jämföras med en ansökan om rättslig hjälp.

Paragrafen innehåller regler om vad en ansökan om rättslig hjälp utomlands bör innehålla. Övervägandena finns i avsnitt 12.6.3.

I *tredje stycket*, som är nytt, anges att en order enligt artikel 8 i det andra tilläggsprotokollet till Budapestkonventionen ska jämföras med en ansökan om rättslig hjälp. Detta innebär att en svensk åklagare kan utfärda en order om inhämtning av uppgifter om abonnemang respektive lagrade trafikuppgifter som finns hos en tjänsteleverantör i en stat som har tillträtt det andra tilläggsprotokollet till Budapestkonventionen. Det är inte fråga om en traditionell ansökan om rättslig hjälp i brottmål, utan myndigheten ska i stället besluta om att uppgifterna ska lämnas ut, vilket beslut sedan verkställs av behöriga myndigheter i den andra staten.

Att en order ska jämföras med en ansökan om rättslig hjälp innebär att vad som sägs i lagen om ansökan även ska gälla för en order enligt artikel 8 i det andra tilläggsprotokollet till Budapestkonventionen. Av första stycket följer att 2 kap. 4 § första och tredje stycket ska tillämpas vid en ansökan om rättslig hjälp utomlands. Eftersom en order enligt artikel 8 ska jämföras med en sådan ansökan, gäller samma bestämmelser om orderns innehåll som för en ansökan om rättslig hjälp, dvs. ansökans innehåll ska anpassas till de krav som gäller enligt aktuell artikel i tilläggsprotokollet.

Om den andra staten kräver att en order om inhämtande av trafikuppgifter först ska prövas av domstol i Sverige får rätten enligt 4 kap. 26 § andra stycket på begäran av svensk åklagare pröva frågan om att tillåta den hemliga övervakningen.

Samma uppgifter som avses i artikel 8 kan alltså inhämtas genom en ansökan om rättslig hjälp i brottmål. Den andra staten som tar emot en order från en svensk åklagare kan vid sin prövning i huvudsak också tillämpa de förutsättningar som gäller för detta samarbete. Det är upp till åklagaren i det enskilda fallet att avgöra vilket förfarande – ansökan om rättslig hjälp eller en order enligt artikel 8 – som är att anse som mest effektivt för att inhämta uppgifter av aktuellt slag i förhållande till de stater som tillträtt det andra tilläggsprotokollet.

I förhållande till EU:s medlemsstater (utom Danmark och Irland) tillämpas EU-förordningen eller lagen om en europeisk utredningsorder för inhämtande av abonnemangsuppgifter eller lagrade trafikuppgifter.

15.4 Förslaget till lag om ändring i lagen (2003:1174) om vissa former av internationellt samarbete i brottmålsutredningar

1 §

Bestämmelserna i 2–9 §§ gäller för sådana gemensamma utredningsgrupper för brottsutredningar som inrättas mellanmyndigheter i Sverige och myndigheter i en eller flera stater med stöd av

1. rådets rambeslut 2002/465/RIF av den 13 juni 2002 om gemensamma utredningsgrupper,

2. konventionen av den 29 maj 2000 om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater,

3. avtalet av den 19 december 2003 mellan Europeiska unionen och Republiken Island och Konungariket Norge om tillämpningen av vissa bestämmelser i konventionen av den 29 maj 2000 om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater och 2001 års protokoll till denna,

4. det andra tilläggsprotokollet till den europeiska konventionen av den 20 april 1959 om ömsesidig rättslig hjälp i brottmål, *eller*

5. *det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet.*

I 10–14 §§ finns bestämmelser om internationellt samarbete med kontrollerade leveranser.

Bestämmelserna i 15–17 §§ gäller överenskommelser mellan myndigheter i Sverige och myndigheter i en annan stat om samarbete som avser åtgärder i en brottsutredning som utförs av tjänstemän med skyddsidentitet.

I 18–23 §§ finns bestämmelser om inhämtande av uppgifter om domännamnsregistrering och abonnemang.

Paragrafen innehåller regler om lagens tillämpningsområde. Övervägandena finns i avsnitt 12.8.3.

I *första stycket* görs en ändring som innebär att lagens tillämpningsområde utvidgas till att omfatta utredningsgrupper som inrättats med stöd av det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet.

Av fjärde stycket, som är nytt, följer att det i 18–23 §§ har tillkommit bestämmelser om inhämtande av uppgifter om domännamnsregistrering och abonnemang.

Inhämtande av uppgifter om domännamnsregistrering och abonnemang utomlands

18 §

Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott eller brottslig verksamhet får i en stat som har tillträtt det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet begära ut uppgifter från

1. en registreringsenhet för toppdomäner eller återförsäljare av domännamn för att identifiera eller kontakta innehavaren av ett domännamn, eller
2. en tjänsteleverantör om abonnemang.

En begäran får endast ske om uppgifterna rör brottslig verksamhet eller misstanke om brott.

Om en begäran enligt första stycket 2 inte har gjorts av en åklagare ska den godkännas av en åklagare om den andra staten kräver det.

Paragrafen, som är ny, reglerar förutsättningarna för inhämtning av uppgifter om innehavaren av ett domännamn samt uppgifter om abonnemang. Övervägandena finns i avsnitt 12.4.4 och 12.5.3.

Av första stycket punkt 1 följer att svenska brottsutredande myndigheter, dvs. Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott eller brottslig verksamhet, får begära uppgifter direkt från en registreringsenhet för toppdomäner eller återförsäljare av domännamn i en stat som har tillträtt det andra tilläggsprotokollet till Budapestkonventionen. Uppgifterna ska innehas eller kontrolleras av enheten. Uppgifter för att identifiera eller kontakta innehavaren av ett domännamn omfattar i huvudsak innehavarens namn, fysisk adress, e-postadress och telefonnummer.

Begreppet registreringsenhet för toppdomäner är att likställa med det nationella begreppet domänadministratör, som i 2 § lagen (2006:24) om nationella toppdomäner för Sverige på internet definieras som den som ansvarar för administration av en nationell toppdomän för Sverige.

Enligt *punkt 2* i samma stycke får de aktuella myndigheterna också inhämta uppgifter om abonnemang direkt från en tjänsteleverantör i en stat som har tillträtt det andra tilläggsprotokollet till Budapestkonventionen. Begreppet uppgift om abonnemang omfattar uppgifter om abonnentens nummer, namn, titel och adress, men även uppgifter om exempelvis avtal och fakturering. Vidare innefattas uppgift om vem som använt en fast eller dynamisk IP-adress samt IMSI-nummer (se vidare avsnitt 4.2.2 och 12.5.1–12.5.2). Begreppet tjänsteleverantör i det andra tilläggsprotokollet har samma innebörd som motsvarande begrepp i artikel 1 c i Budapestkonventionen. Det begreppet omfattar i huvudsak leverantörer som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst

Ett villkor för att de aktuella uppgifterna ska kunna hämtas in är enligt *andra stycket* att uppgifterna gäller brottslig verksamhet eller misstanke om brott, vilket motsvarar den reglering som finns i 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation. Uppgifterna kan alltså inhämtas även i de fall en förundersökning inte har inletts, t.ex. under en förutredning.

Har en begäran om uppgifter om abonnemang utfärdats av annan brottsbekämpande myndighet än åklagare följer det av *tredje stycket* att den ska godkännas av en åklagare, om den andra staten kräver det. Bestämmelsen avser det förhållande att den andra staten har avgett en förklaring enligt artikel 7.2 b i det andra tilläggsprotokollet, vilken Sverige är bunden av. Det bör enbart vara en åklagare inom det svenska åklagarväsendet som kan ge ett sådant godkännande som avses i bestämmelsen.

Om registreringsenheten, återförsäljaren eller tjänsteleverantören inte besvarar begäran är myndigheten som efterfrågat uppgiften hänvisad till att se till att en åklagare ansöker om rättslig hjälp enligt reglerna i lagen om internationell rättslig hjälp i brottmål eller utfärdar en europeisk utredningsorder om lagen om en europeisk utredningsorder i stället är tillämplig. Vidare kan uppgifterna begäras direkt från registreringsenheten, återförsäljaren eller tjänsteleverantören genom en europeisk utlämnandeorder avseende inhämtning av abonnentuppgifter och andra uppgifter som begärts med det enda syftet att identifiera användaren enligt EU-förordningen, om den förordningen är tillämplig.

Inhämtande av uppgifter om domännamnsregistrering och abonnemang i Sverige

19 §

En registreringsenhet för toppdomäner eller återförsäljare av domännamn som erbjuder tjänster för domännamnsregistrering i Sverige ska på begäran till en behörig myndighet i en annan stat som tillträtt det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet lämna ut uppgifter för att identifiera eller kontakta innehavaren av ett domännamn om uppgifterna rör brottslig verksamhet eller misstanke om brott.

Paragrafen, som är ny, reglerar skyldigheten för en registreringsenhet för toppdomäner eller återförsäljare av domännamn som erbjuder tjänster för domännamnsregistrering i Sverige att lämna ut uppgifter till behörig myndighet i en stat som tillträtt det andra tilläggsprotokollet till Budapestkonventionen. Övervägandena finns i avsnitt 12.4.5.

Enligt bestämmelsen ska en registreringsenhet för toppdomäner eller en återförsäljare av domännamn som erbjuder tjänster för domännamnsregistrering, på begäran lämna ut uppgifter var syfte är att identifiera eller kontakta innehavaren av ett domännamn till behörig myndighet i annan stat som tillträtt det andra tilläggsprotokollet till Budapestkonventionen. I Sverige är Internetstiftelsen domänadministratör enligt lagen om nationella toppdomäner för Sverige på internet och således registreringsenhet för toppdomäner.

Vad som utgör uppgifter för att identifiera eller kontakta innehavaren av ett domännamn behandlas i kommentaren till 18 §. Uppgifterna ska röra brottslig verksamhet eller misstanke om brott, se även här kommentaren till 18 §.

En begäran om uppgifter kan endast omfatta uppgifter som innehas vid tidpunkten för begäran. Bestämmelsen medför alltså inte någon skyldighet för de berörda enheterna att lagra informationen. Det kan dock i sammanhanget framhållas att det i lagen (2006:24) om nationella toppdomäner för Sverige på internet finns en skyldighet för domänadministratören, vilket begrepp motsvaras av registreringsenhet för toppdomän, att föra ett register som innehåller de aktuella uppgifterna.

20 §

En tjänsteleverantör som är skyldig att lämna ut uppgifter om abonnemang enligt 9 kap. 33 § första stycket 2 lagen (2022:482) om elektronisk kommunikation, ska på begäran av behörig myndighet i en stat som har tillträtt det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet lämna ut motsvarande uppgifter om uppgifterna rör brottslig verksamhet eller misstanke om brott.

Uppgifterna ska lämnas ut senast 30 dagar från mottagandet av begäran eller inom den tidsfrist som anges i begäran om fristen är längre än 30 dagar.

En begäran enligt första stycket ska vara beslutad av en åklagare eller annan rättslig myndighet eller på annat sätt vara utfärdad under oberoende tillsyn.

Paragrafen, som är ny, innehåller en skyldighet för tjänsteleverantörer att lämna ut uppgift om abonnemang till behörig myndighet i en stat som har tillträtt det andra tilläggsprotokollet till Budapestkonventionen. Övervägandena finns i avsnitt 12.5.4.

Enligt *första stycket* är de tjänsteleverantörer som omfattas av skyldigheten att lämna ut uppgifter om abonnemang enligt 9 kap. 33 § första stycket 2 lagen om elektronisk kommunikation till nationella brottsbekämpande myndigheter, skyldiga att lämna ut motsvarande uppgifter till en behörig myndighet i en stat som tillträtt det andra tilläggsprotokollet till Budapestkonventionen. Den krets av tjänsteleverantörer som omfattas av bestämmelsen är således de leverantörer som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst som inte är en Noik. För att uppgifterna ska kunna lämnas ut krävs att de rör brottslig verksamhet eller misstanke om brott. Bestämmelsen innebär inte något utökat krav på lagring av uppgifter om abonnemang. Någon ytterligare skyldighet att lagra uppgifter än vad som följer av lagen om elektronisk kommunikation gäller således inte för de berörda tjänsteleverantörerna.

I andra stycket anges inom vilka tidsfrister en begäran ska besvaras.

Av tredje stycket följer att en begäran enligt första stycket ska vara beslutad av en åklagare eller annan rättslig myndighet eller på annat sätt vara utfärdad under oberoende tillsyn. Detta följer av den förklaring Sverige lämnat enligt artikel 7.2 b i tilläggsprotokollet.

21 §

Uppgifterna som begärts enligt 19 och 20 §§ ska lämnas ut om inte begäran är så bristfällig att den inte utan väsentlig olägenhet kan läggas till grund för ett utlämnande. Om mottagaren inte följer begäran ska den ange skälen för detta.

En begäran enligt 19 och 20 §§ ska vara skriven på eller översatt till svenska eller engelska eller det språk som godtas av mottagaren.

Paragrafen, som är ny, innehåller bestämmelser om utlämnande av uppgifter och översättning. Övervägandena finns i avsnitt 12.4.5 och 12.5.4.

Enligt *första stycket* ska de uppgifter som begärts enligt 19 och 20 §§ lämnas ut om inte begäran är så bristfällig att den inte utan väsentlig olägenhet kan läggas till grund för ett utlämnande. En sådan brist kan vara att det inte framgår klart av begäran vilket domännamn eller abonnemang som avses. Ett annat exempel är att det av begäran inte följer att uppgifterna som begärs avser brottslig verksamhet eller misstanke om brott eller att det saknas uppgift om att begäran görs enligt det andra tilläggsprotokollet till Budapestkonventionen. Om det däremot står klart att uppgifterna har ett annat syfte är förevarande bestämmelse inte tillämplig, men då kan mottagaren direkt med stöd av 19 eller 20 § vägra att lämna ut uppgifterna. Bestämmelsen avser endast uppgifter som finns lagrade hos mottagaren vid tidpunkten för begäran och uppgifter som således inte är lagrade kan av det skälet inte heller lämnas ut.

Om en begäran inte efterföljs av mottagaren, dvs. registreringsenheten för toppdomäner, återförsäljaren av domännamn eller tjänsteleverantören, ska den ange skälen för detta.

Det följer inte några sanktioner för den aktör som inte efterkommer en begäran enligt 19 eller 20 §. Utgångspunkten är dock att uppgifterna ska lämnas ut. Om uppgifterna trots detta inte lämnas ut får den andra statens myndigheter i stället ansöka om rättslig hjälp enligt lagen om internationell rättslig hjälp i brottmål eller utfärda en europeisk utredningsorder enligt lagen om en europeisk utredningsorder, om det regelverket är tillämpligt. Mellan EU:s medlemsstater kan även EU-förordningen tillämpas, vilket innebär att uppgifterna kan begäras ut genom en europeisk utlämnandeorder avseende inhämtning av abonnentuppgifter eller andra uppgifter som begärts med enda syftet att identifiera användaren.

I *andra stycket* anges vilka språk en begäran ska vara skriven på eller översatt till. Om mottagaren accepterar ett annat språk än svenska eller engelska är det således möjligt att använda ett sådant annat språk.

22 §

Den underrättelse som den behöriga myndigheten i den andra staten ska lämna enligt artikel 7.5 a i det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet om att en begäran har gjorts enligt 20 § ska vara skriven på eller översatt till svenska, danska, norska eller engelska.

Paragrafen, som är ny, anger vilka språk som en underrättelse enligt artikel 7.5 a i det andra tilläggsprotokollet till Budapestkonventionen ska vara skrivet på eller översatt till. Övervägandena finns i avsnitt 12.5.4.

Enligt den förklaring som Sverige avser att lämna är Åklagarmyndigheten mottagande myndigheten i Sverige.

23 §

En tjänsteleverantör ska vid behov samråda med Åklagarmyndigheten innan de uppgifter som begärts enligt 20 § första stycket lämnas ut.

Åklagarmyndigheten får besluta att tjänsteleverantören inte får lämna ut uppgifterna om det finns skäl att anta att ett utlämnande kan skada en pågående utredning om brott eller om det finns förutsättningar att vägra att lämna ut motsvarande uppgifter om de hade begärts ut enligt lagen (2000:562) om internationell rättslig hjälp i brottmål.

Paragrafen, som är ny, innehåller bestämmelser om samråd och en möjlighet för Åklagarmyndigheten att besluta att begärda uppgifter enligt 20 § första stycket inte får lämnas ut. Övervägandena finns i avsnitt 12.5.4.

Av *första stycket* följer att en tjänsteleverantör vid behov ska samråda med Åklagarmyndigheten innan uppgifterna omfattas av begäran enligt 20 § första stycket lämnas ut. Skyldigheten är således inte absolut, utan samråd ska ske vid behov. Ett sådant behov kan exempelvis föreligga om det är tveksamt om uppgifterna begärs ut i ett sådant straffrättsligt förfarande som avses i 20 § första stycket eller om det är en behörig myndighet som har utfärdat ordern.

Det *andra stycket* reglerar Åklagarmyndighetens rätt att besluta att den begärda informationen enligt 20 § första stycket inte får lämnas ut. Ett sådant beslut kan fattas om det finns skäl att anta att ett utlämnande av uppgifterna kan skada en pågående utredning om brott. Utredning av brott kan även avse utredning i en annan stat, som t.ex. de brottsbekämpande myndigheterna i Sverige bidrar till i ett annat ärende. Ett annat skäl kan vara att det finns förutsättningar att vägra att lämna ut motsvarande uppgifter om de hade begärts ut enligt lagen om internationell rättslig hjälp i brottmål. I 2 kap. 14 § nämnda lag anges under vilka omständigheter en ansökan om rättslig hjälp ska respektive kan avslås. Åklagarmyndighetens beslut är bindande för tjänsteleverantören. Ett beslut kan meddelas oberoende av om tjänsteleverantören har samrätt med Åklagarmyndigheten.

15.5 Förslaget till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder

1 kap.

5 a §

Lagen gäller inte vid skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter enligt artikel 29 i Europarådets konvention om it-relaterad brottslighet. För sådant säkrande gäller i stället lagen (2000:562) om internationell rättslig hjälp i brottmål.

Paragrafen är ny och behandlar lagens tillämplighet i fråga om artikel 29 i Europarådets konvention om it-relaterad brottslighet. Övervägandena finns i avsnitt 11.5.1.

Av bestämmelsen följer att lagen inte är tillämplig vid skyndsamt säkrande av datorbehandlingsbara uppgifter enligt artikel 29 i Budapestkonventionen. I stället gäller för en sådan åtgärd bestämmelserna i lagen om internationell rättslig hjälp i brottmål. Paragrafen hindrar emellertid inte en utfärdande myndighet i en medlemsstat i EU att utfärda en europeisk utredningsorder för föreläggande om bevarande av lagrade uppgifter enligt 27 kap. 16 § rättegångsbalken. Ett sådant bevarande av uppgifter enligt en utfärdad utredningsorder sker däremot inte med stöd av artikel 29 i Budapestkonventionen.

3 kap.

23 §

En utredningsåtgärd ska verkställas skyndsamt och inom 90 dagar efter det att verkställbarhetsförklaringen meddelades enligt 19 §. Om det inte är praktiskt möjligt, får verkställigheten ske vid en senare tidpunkt. *Om det föreligger en omedelbar fara för liv, hälsa eller egendom, ska särskild hänsyn tas till kravet om skyndsambet vid verkställigheten av en utredningsåtgärd.*

Om en utredningsorder översänds enligt artikel 32 i Europaparlamentets och rådets direktiv 2014/41/EU, i den ursprungliga lydelsen, ska verkställighet om möjligt ske inom 24 timmar efter det att verkställbarhetsförklaringen meddelades enligt 19 §.

Paragrafen innehåller bestämmelser om tidsfrister för verkställigheten av en utredningsorder. Övervägandena finns i avsnitt 12.7.4.

I *första stycket* görs ett tillägg med innebörden att det vid verkställighet av en utredningsåtgärd ska särskild hänsyn tas till om det är fråga om en omedelbar fara för liv, hälsa eller egendom. Bestämmelsen ställer således ett krav på särskild skyndsambet om en nödsituation är för handen. För exempel på en nödsituation som omfattas av paragrafen, se kommentaren i avsnitt 15.3 till 2 kap. 10 § lagen om internationell rättslig hjälp i brottmål, som innehåller en motsvarande bestämmelse avseende handläggning av en ansökan om rättslig hjälp. Det är den handläggande myndigheten, dvs. åklagaren, som avgör om det föreligger en sådan nödsituation som avses i bestämmelsen.

15.6 Förslaget till lag om ändring i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder

1 §

Denna lag innehåller bestämmelser om *bevarande av vissa lagrade uppgifter i elektronisk form och om användning av hemliga tvångsmedel* för att lokalisera personer i syfte att möjliggöra verkställighet av frihetsberövande påföljder.

Paragrafen anger lagens huvudsakliga innehåll. I bestämmelsen har ett tillägg gjorts om att lagen även innehåller bestämmelser om be-

varande av vissa lagrade uppgifter i elektronisk form. Övervägandena finns i avsnitt 6.12.2.

4 a §

Den som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för att lokalisera en person för verkställighet av en frihetsberövande påföljd och som kan inhämtas med stöd av 3 § eller 9 kap. 33 § första stycket 1 lagen (2022:482) om elektronisk kommunikation får föreläggas att bevara uppgiften.

För ett föreläggande enligt första stycket tillämpas 27 kap. 16 § andra och tredje styckena och 16 a § rättegångsbalken.

Paragrafen, som är ny, gör det möjligt för brottsutredande myndigheter att skyndsamt säkra och bevara lagrade elektroniska uppgifter som kan antas ha betydelse för att lokalisera en person i verkställighetssyfte. Övervägandena finns i avsnitt 6.12.2.

Av första stycket följer att den som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för att lokalisera en person för verkställighet av en frihetsberövande påföljd och som kan inhämtas med stöd av 3 § eller 9 kap. 33 § första stycket 1 lagen (2022:482) om elektronisk kommunikation får föreläggas att bevara uppgiften. De uppgifter som kan inhämtas med stöd av paragrafen är således begränsade till trafikuppgifter respektive uppgifter om abonnemang. Detta är alltså en skillnad i förhållande till 27 kap. 16 § första stycket rättegångsbalken, som reglerar bevarande av lagrade uppgifter vid utredning av brott och som avser bevarande av alla typer av uppgifter i lagrad form.

Att uppgiften ska vara lagrad innebär – i likhet med vad som är fallet i fråga om bevarande av uppgifter i brottsutredande syfte enligt 27 kap. 16 § rättegångsbalken – att den ska finnas bevarad elektroniskt. Detta innebär att både sådana uppgifter som finns lagrade på grund av regler om datalagring och sådana som lagrats av annan anledning omfattas av bestämmelsen. Uppgifter som har lagrats av annan anledning kan t.ex. vara uppgifter som hos tillhandahållare av elektroniska kommunikationsnät eller kommunikationstjänster behandlats för fakturahantering eller liknande. Uppgiften måste finnas lagrad när föreläggandet meddelas och det är således inte möjligt att stöd av paragrafen förelägga någon att lagra eller spara eventuella framtida uppgifter.

Att föreläggandet ska avse en viss elektronisk uppgift innebär att det i föreläggandet måste anges vilken specifik elektronisk uppgift som ska bevaras, t.ex. uppgifter om ett visst abonnemang eller trafikuppgifter hänförliga till ett visst meddelande. Ett föreläggande kan alltså inte vara generellt och t.ex. utan närmare specificering endast ange att alla uppgifter som mottagits under en tid ska bevaras.

I likhet med vad som gäller för bevarande av uppgifter i brottsutredande syfte kan ett föreläggande kan rikta sig mot vem som helst som innehar en sådan lagrad uppgift som omfattas av bestämmelsen. Både fysiska och juridiska personer omfattas av bestämmelsen. Som gäller för ett bevarandeföreläggande enligt 27 kap. 16 § rättegångsbalken finns flera möjliga sätt att efterkomma ett föreläggande, t.ex. genom kopiering av uppgiften eller genom att vidta åtgärder för att uppgiften lämnas orubbad på sin ursprungliga plats. Den som har beslutat om föreläggandet får ge anvisningar om hur uppgiften ska bevaras i det enskilda fallet. Sådana anvisningar kan ges i samråd med den som föreläggandet riktar sig mot.

Att uppgiften skäligen kan antas ha betydelse för att lokalisera en person för verkställighet av en frihetsberövande påföljd innebär ett relativt lågt ställt krav på när ett föreläggande enligt paragrafen kan meddelas. Ett bevarandeföreläggande i verkställighetssyfte är – i likhet med sådant föreläggande i brottsutredande syfte enligt 27 kap. 16 § rättegångsbalken – att se som ett straffprocessuellt tvångsmedel. Åtgärden kan vidtas i ett förhållandevis tidigt skede i arbetet att lokalisera en person för verkställighet av en frihetsberövande påföljd.

De frihetsberövande påföljder som avses i paragrafen är fängelse, sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning.

Åtgärden är att se som ett straffprocessuellt tvångsmedel som omfattas av kravet på proportionalitet enligt 2 § i förevarande lag. Motsvarande krav gäller i fråga om ett bevarande vid misstanke om brott enligt 27 kap. 16 § rättegångsbalken. Åtgärden får således beviljas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.

Enligt *andra stycket* tillämpas för ett föreläggande i verkställighetssyfte bestämmelserna i 27 kap. 16 § andra och tredje styckena

och 16 a § rättegångsbalken. Hänvisningen till 27 kap. 16 § andra stycket rättegångsbalken innebär att det i föreläggandet ska anges hur länge uppgiften ska bevaras. Vidare följer av hänvisningen att tiden för bevarande aldrig får vara längre än vad som är nödvändigt i det enskilda fallet och att bevarandetiden som huvudregel inte får överstiga 90 dagar från dagen för beslutet.

Hänvisningen till 27 kap. 16 § tredje stycket rättegångsbalken innebär att tiden för bevarande får förlängas med upp till 90 dagar om det finns särskilda skäl. Särskilda skäl kan t.ex. vara att myndigheten som meddelat föreläggande måste vänta in uppgifter från eller åtgärder i utlandet för att kunna besluta om de bevarande uppgifterna ska begäras ut. Om informationen är krypterad eller skyddas på annat sätt kan det också ta tid att ta ställning till om de bevarade uppgifterna behövs. Inte heller vid förlängning ska tiden bestämmas till längre än nödvändigt. Tiden kan förlängas vid ett eller flera tillfällen så länge den maximala tiden för förlängning om 90 dagar inte överskrids.

Av hänvisningen till 27 kap. 16 a § rättegångsbalken följer att en undersökningsledare eller en åklagare får utfärda ett föreläggande enligt bestämmelsen. Mot bakgrund av att det rör sig om en lagakraftvunnen dom samt är fråga om ett straffprocessuellt tvångsmedel är det åklagare som meddelar ett föreläggande. Ett föreläggande om bevarande ska – likhet med vad som är fallet för ett bevarandeföreläggande enligt 27 kap. 16 § rättegångsbalken – som utgångspunkt vara skriftligt och omfattningen ska tydligt framgå av beslutet. Om det i brådskande fall inte är möjligt att ge ett skriftligt föreläggande finns det inte något hinder mot att föreläggandet ges muntligen och att den som har förelagts därefter informeras skriftligen om beslutet.

Vidare får det i föreläggandet anges att den som har förelagts att bevara en viss uppgift inte får uppenbara att åtgärden har vidtagits. Slutligen följer av hänvisningen till 27 kap. 16 a § rättegångsbalken att den förelagde får begära rättens prövning av föreläggandet. För rättens prövning gäller samma regler som för prövning av beslag enligt 27 kap. 6 § första stycket rättegångsbalken (se vidare kommentaren till 27 kap. 16 a rättegångsbalken, prop. 2020/21:72 s. 69–70).

Kommittédirektiv 2023:84

En effektivare gränsöverskridande åtkomst till elektroniska bevis för brottsbekämpande myndigheter

Beslut vid regeringssammanträde den 15 juni 2023

Sammanfattning

En särskild utredare får i uppdrag att se över regleringen om gränsöverskridande åtkomst till elektroniska bevis med anledning av nya internationella instrument. Tillgång till elektroniska uppgifter är ofta av avgörande betydelse i utredningar om allvarlig brottslighet. Inom Europarådet har det antagits ett tilläggsprotokoll till konventionen om it-relaterad brottslighet (Budapestkonventionen) och inom kort förväntas EU besluta en förordning om europeiska bevarande- och utlämnandeorder för elektroniska bevis samt ett till förordningen kompletterande direktiv. Tilläggsprotokollet och EU-rättsakterna innehåller bestämmelser om gränsöverskridande åtkomst till elektroniska bevis. Syftet med uppdraget är att säkerställa att svenska brottsbekämpande myndigheter på ett effektivt och rättssäkert sätt kan använda de gränsöverskridande verktyg som instrumenten erbjuder.

Utredaren ska bl.a.

- kartlägga vilka svenska bestämmelser som berörs av EU-förordningens bestämmelser om europeiska bevarande- och utlämnandeorder samt analysera om de svenska bestämmelserna bör ändras eller kompletteras,
- ta ställning till vilken eller vilka myndigheter som bör utses till behöriga myndigheter enligt EU-förordningen,

- analysera hur EU-direktivet om utsedda verksamhetsställen och rättsliga ombud bör genomföras i svensk rätt,
- kartlägga och analysera vilka sanktioner som bör aktualiseras vid överträdelse av EU-förordningen och relevanta nationella bestämmelser som genomför EU-direktivet,
- kartlägga vilka svenska bestämmelser som berörs av tilläggsprotokollet och analysera om de svenska bestämmelserna bör ändras eller kompletteras, och
- lämna nödvändiga författningsförslag.

Uppdraget ska redovisas senast den 13 december 2024.

Nya EU-rättsakter för gränsöverskridande åtkomst till elektroniska bevis

EU:s kommande förordning om europeiska utlämnandeorder och bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställande av annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden (här kallad EU-förordningen) träder i kraft tre år efter antagandet. Det kommande direktivet om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och utse rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden (här kallat EU-direktivet) ska genomföras senast två och ett halvt år efter antagandet. Syftet med de nya EU-reglerna är att medlemsstaterna i straffrättsliga förfaranden snabbare och effektivare ska kunna säkra och inhämta elektroniska bevis, samtidigt som skyddet för enskildas grundläggande fri- och rättigheter följs.

EU-förordningen innebär att en behörig myndighet i en medlemsstat kan vända sig till en tjänsteleverantör som är etablerad eller representerad i en annan medlemsstat, med ett beslut om att elektroniska bevis ska bevaras (bevarandeorder) eller lämnas ut (utlämnandeorder). Det spelar ingen roll i vilket land de elektroniska uppgifterna finns lagrade. Med elektroniska bevis avses abonnentuppgifter, trafikuppgifter och innehållsdata. Enligt EU-förordningen är medlemsstaterna skyldiga att utse en eller flera behöriga myndigheter som bland annat ska ha befogenhet att utfärda, sända,

erkänna och verkställa europeiska bevarande- och utlämnandeorder. EU-direktivet innehåller bestämmelser om att vissa tjänsteleverantörer är skyldiga att utse utsedda verksamhetsställen eller rättsliga ombud inom unionen. Det är de utsedda verksamhetsställen eller de rättsliga ombuden som ska ta emot europeiska bevarande- och utlämnandeorder för tjänsteleverantörernas räkning samt ansvara för att de fullföljs. Medlemsstaterna ska införa nationella bestämmelser om sanktioner vid överträdelse av vissa skyldigheter enligt EU-förordningen och relevanta nationella bestämmelser som genomför EU-direktivet.

För att Sverige ska uppfylla de skyldigheter som åläggs medlemsstaterna i förordningen och för att genomföra direktivet krävs ändringar och kompletteringar av svensk rätt. Myndigheter och domstolar som är behöriga att agera enligt förordningen och direktivet ska också utses. Det är angeläget att relevanta svenska brottsbekämpande myndigheter fullt ut kan använda systemet med europeiska bevarande- och utlämnandeorder för att på ett effektivt sätt kunna utreda och lagföra brott. Tillgång till elektroniska uppgifter är ofta av avgörande betydelse i utredningar om allvarlig brottslighet och i utredningar om brott som begås över internet. Elektroniska uppgifter lagras allt oftare på andra platser än hos användaren och inte sällan utomlands. Informationen kan ständigt förflyttas eller finnas på flera platser samtidigt, vilket många gånger gör det omöjligt att identifiera en specifik plats där informationen finns. Ett effektivt gränsöverskridande samarbete är därför av största vikt för att brottsbekämpande myndigheter ska kunna utreda och lagföra brott.

Uppdraget att möjliggöra en effektivare åtkomst till elektroniska bevis

Med en europeisk bevarandeorder avses enligt EU-förordningen ett beslut av en behörig myndighet i en medlemsstat enligt vilket en tjänsteleverantör i en annan medlemsstat ska bevara elektroniska bevis under en viss tid. Med en europeisk utlämnandeorder avses ett beslut av en behörig myndighet i en medlemsstat enligt vilket en tjänsteleverantör i en annan medlemsstat ska lämna ut elektroniska bevis till myndigheten. En europeisk bevarande- eller utlämnandeorder får utfärdas under förutsättning att en sådan åtgärd är möjlig

att vidta i ett jämförbart nationellt ärende. Europeiska bevarande- och utlämnandeorder som avser abonnentuppgifter eller trafikuppgifter som begärts med det enda syftet att identifiera användaren får utfärdas för utredning av alla brott. En order får också utfärdas för verkställande av ett fängelsestraff eller annan frihetsberövande åtgärd där strafftiden uppgår till minst fyra månader. För att få utfärda en europeisk utlämnandeorder som avser innehållsuppgifter eller trafikuppgifter som inte begärts med det enda syftet att identifiera användaren krävs att maximistraffet för det aktuella brottet ska vara minst tre års fängelse eller att det ingår i den lista över särskilda brott som anges i EU-förordningen.

Både traditionella tjänsteleverantörer och tjänsteleverantörer som tillhandahåller nummeroberoende interpersonella kommunikationstjänster (s.k. OTT-tjänster), till exempel Apple Imessage och Facetime, Facebook Messenger och Whatsapp, omfattas av EU-förordningen. Enligt EU-förordningen är tjänsteleverantörerna som utgångspunkt skyldiga att fullfölja en europeisk bevarande- eller utlämnandeorder. Om en tjänsteleverantör inte fullföljer en order får den utfärdande behöriga myndigheten skicka ordern till den behöriga myndigheten i den verkställande staten för verkställighet. Som utgångspunkt ska den verkställande myndigheten erkänna ordern och vidta de åtgärder som krävs för verkställighet. Det ska ske genom att den verkställande myndigheten informerar tjänsteleverantören om dennes skyldighet att fullfölja ordern, möjligheten att invända mot ordern och om tillämpliga sanktioner om skyldigheterna som följer av EU-förordningen inte följs. Den verkställande myndigheten ska även ange en tidpunkt för när tjänsteleverantören senast ska ha fullföljt ordern eller framställt en invändning mot den.

Svenska bestämmelser om bevarande av elektroniska uppgifter för utredning av brott finns i 27 kap. 16 och 16 a §§ rättegångsbalken. Både en fysisk och juridisk person, till exempel en tjänsteleverantör, kan föreläggas att bevara en viss uppgift som den innehar i elektronisk form om uppgiften skäligen kan antas ha betydelse för utredningen om ett brott. De uppgifter som avses kan vara av vilket slag som helst, till exempel en digitalt lagrad bild, innehåll i ett meddelande eller en uppgift om ett meddelandes ursprung eller adressat (se propositionen Sveriges tillträde till Europarådets konvention om it-relaterad brottslighet, prop. 2020/21:72 s. 23). I svensk rätt

finns även möjligheter för brottsutredande myndigheter att hämta in elektroniska uppgifter från traditionella tjänsteleverantörer. Traditionella tjänsteleverantörer är således under vissa förutsättningar skyldiga att lämna ut en uppgift om abonnemang, eller annan uppgift som angår ett specifikt elektroniskt meddelande när det gäller brottslig verksamhet eller vid misstanke om brott (9 kap. 33 § lagen [2022:486] om elektronisk kommunikation). Om en tjänsteleverantör inte uppfyller sina skyldigheter i fråga om att lämna ut vissa elektroniska uppgifter till brottsbekämpande myndigheter kan de påföras sanktionsavgift (12 kap. 1 § lagen om elektronisk kommunikation). Brottsutredande myndigheter kan dessutom få tillgång till uppgifter från tjänsteleverantörer genom hemliga tvångsmedel (27 kap. 18 och 19 §§ rättegångsbalken).

I propositionen Hemliga tvångsmedel – effektiva verktyg för att förhindra och utreda allvarliga brott (2022/23:126) föreslås flera ändringar i reglerna om hemliga tvångsmedel. I betänkandet Bättre möjligheter att verkställa frihetsberövanden (SOU 2022:50) föreslås bland annat att tjänsteleverantörer på begäran ska kunna lämna ut uppgifter om abonnemang till Polismyndigheten om uppgiften behövs för att lokalisera någon i syfte att möjliggöra verkställighet av frihetsberövande påföljder. Den 30 maj 2023 redovisades betänkandet Datalagring och åtkomst till elektronisk information (SOU 2023:22) som bland annat innehåller förslag om att OTT-tjänster ska omfattas av skyldigheterna att lagra och lämna ut uppgifter om elektronisk kommunikation.

Det är angeläget att säkerställa en effektiv och rättssäker hantering av europeiska bevarande- och utlämnandeorder och att svenska brottsbekämpande myndigheter fullt ut kan använda de möjligheter som EU-förordningen ger.

Utredaren ska därför

- kartlägga vilka svenska bestämmelser som berörs av EU-förordningens bestämmelser om europeiska bevarande- och utlämnandeorder,
- analysera om de svenska bestämmelserna bör ändras eller kompletteras, och
- lämna nödvändiga författningsförslag.

Uppdraget att föreslå behöriga och centrala myndigheter

Enligt EU-förordningen ska medlemsstaterna utse en eller flera myndigheter som bland annat ska vara behöriga att utfärda, sända och erkänna europeiska bevarande- och utlämnandeorder. I EU-förordningen ställs olika krav på vem eller vilken myndighet som har rätt att utfärda olika former av europeiska bevarande- eller utlämnandeorder. En behörig myndighet ska även kunna samråda med en annan medlemsstat innan en order utfärdas och i vissa fall ta emot anmälningar om utfärdade order. Vidare ska medlemsstaterna utse en eller flera myndigheter som ska vara behöriga att verkställa order på en annan medlemsstats vägnar. Utöver detta ska medlemsstaterna utse domstolar som ska pröva invändningar från en tjänsteleverantör om att ett tredjelands lag förhindrar ett utlämnande av de begärda elektroniska uppgifterna. Enligt EU-förordningen finns även en möjlighet för medlemsstaterna att inrätta en eller flera centrala myndigheter med administrativa uppgifter som rör europeiska bevarande- och utlämnandeorder. Medlemsstaterna ska även ange om framställningar enligt förordningen godtas på andra språk än deras egna officiella språk.

Utredaren ska därför

- ta ställning till vilken eller vilka myndigheter som bör utses till behöriga myndigheter enligt EU-förordningen,
- ta ställning till vilken eller vilka domstolar som bör kunna pröva invändningar om att ett tredjelands lag förhindrar ett utlämnande enligt EU-förordningen,
- analysera om det finns behov av att utse en central myndighet enligt EU-förordningen och i så fall ta ställning vilken myndighet som bör utses,
- analysera behovet av författningsändringar eller andra åtgärder som krävs för att de föreslagna myndigheterna och domstolarna ska kunna utföra sina skyldigheter enligt EU-förordningen på ett effektivt och rättssäkert sätt,
- ta ställning till om framställningar som skickas till Sverige ska godtas på andra språk än svenska, och
- lämna nödvändiga författningsförslag.

Uppdraget att genomföra EU-direktivet om att utse utsedda verksamhetsställen, rättsliga ombud och central myndighet

EU-direktivet utgör ett komplement till EU-förordningen och vissa andra rättsliga instrument som rör inhämtande av elektroniska bevis i straffrättsliga förfaranden, till exempel EU:s direktiv om en europeisk utredningsorder på det straffrättsliga området. I EU-direktivet finns bestämmelser om att vissa tjänsteleverantörer ska vara skyldiga att utse minst ett utsett verksamhetsställe eller ett rättsligt ombud i unionen, som medlemsstaterna ska kunna vända sig till med framställningar om insamling av bevis i straffrättsliga förfaranden. Uppdraget för de utsedda verksamhetsställena och rättsliga ombuden är att ta emot, följa och fullfölja förelägganden och beslut om insamling av bevis i straffrättsliga förfaranden från medlemsstater. Av EU-direktivet följer också att var och en av medlemsstaterna ska utse en eller flera centrala myndigheter med uppgift att samarbeta och samordna åtgärder med andra centrala myndigheter och kommissionen samt säkerställa tillämpningen av direktivet.

Utredaren ska därför

- analysera hur EU-direktivet om utsedda verksamhetsställen och rättsliga ombud bör genomföras i svensk rätt,
- föreslå vilken eller vilka myndigheter som bör utses till centrala myndigheter enligt EU-direktivet,
- analysera behovet av författningsändringar eller andra åtgärder som krävs för att den eller de föreslagna myndigheterna ska kunna utföra sina uppdrag enligt EU-direktivet på ett effektivt och rättssäkert sätt, och
- lämna nödvändiga författningsförslag.

Uppdraget att föreslå sanktioner och bedöma behovet av författningsändringar i övrigt

EU-förordningen innehåller bestämmelser om att medlemsstaterna ska fastställa regler om sanktioner vid tjänsteleverantörers överträdelse av skyldigheter enligt förordningen. Sanktionerna ska vara effektiva, proportionerliga och avskräckande. I EU-direktivet finns

liknande bestämmelser om sanktioner för överträdelser av de nationella bestämmelser som genomför vissa utpekade delar av direktivet.

Införandet av EU-förordningen och EU-direktivet kan även medföra behov av andra författningsändringar. Det kan bland annat gälla tjänsteleverantörers möjligheter att kräva ersättning av den utfärdande staten för kostnader som uppstår i samband med hanteringen av europeiska bevarande- och utlämnandeorder samt hur rätten till effektiva rättsmedel ska kunna utövas på ett ändamålsenligt sätt enligt vad som anges i EU-förordningen.

Utredaren ska därför

- kartlägga och analysera vilka sanktioner som bör aktualiseras vid överträdelser av EU-förordningen och relevanta nationella bestämmelser som genomför EU-direktivet, och
- analysera och vid behov lämna förslag om andra författningsändringar än sådana om sanktioner som bedöms nödvändiga med anledning av förordningen och direktivet.

Uppdraget att tillträda Budapestkonventionens andra tilläggsprotokoll

I november 2021 antog Europarådets ministerkommitté det andra tilläggsprotokollet till Europarådets konvention om it-relaterad brottslighet (Budapestkonventionen). Tilläggsprotokollet innehåller bestämmelser som syftar till att ge de brottsbekämpande myndigheterna nya och mer effektiva verktyg för gränsöverskridande åtkomst till elektroniska bevis. Det handlar om möjligheter för behöriga myndigheter i en stat att i brottsutredande syfte dels vända sig till privata aktörer i en annan stat för att få ut domän- och abonnemangsuppgifter, dels vända sig till behöriga myndigheter i den andra staten för verkställighet av en order om utlämnade av abonnemangs- och trafikuppgifter. Vidare finns bestämmelser som syftar till att stärka det rättsliga samarbetet mellan konventionsstaterna, bland annat genom rättslig hjälp i nödsituationer och utökat användande av Nätverket 24/7.

Bestämmelserna i tilläggsprotokollet faller inom ett område som i stor utsträckning omfattas av EU-gemensamma regler och därmed unionens exklusiva externa befogenhet. Unionen kan emellertid inte underteckna protokollet, eftersom endast stater kan bli

parter i det. Genom ett beslut av Europeiska unionens råd den 14 februari 2023 bemyndigades medlemsstaterna att i unionens intresse ratificera protokollet. Sverige undertecknade protokollet den 12 maj 2022.

Frågan om vilka ändringar av nationell rätt som kan krävas med anledning av tilläggsprotokollet bör lämpligtvis behandlas tillsammans med frågan om vilka ändringar som krävs med anledning av de nya EU-rättsakterna om åtkomst till elektroniska bevis. De ändringar som kan krävas i nationell rätt kan komma att påverkas av innehållet i rådets beslut när det gäller förbehåll, förklaringar, underrättelser, meddelanden och anvisningar.

Utredaren ska därför

- kartlägga vilka svenska bestämmelser som berörs av tilläggsprotokollet,
- analysera om de svenska bestämmelserna bör ändras eller kompletteras,
- föreslå de eventuella förbehåll och förklaringar som bör göras i samband med ett tillträde,
- ta ställning till vilken eller vilka myndigheter som bör utses till behöriga myndigheter för förfarandena i tilläggsprotokollet, och
- lämna nödvändiga författningsförslag.

Uppdraget att i övrigt se över regleringen om rättsligt samarbete vid frysning av elektroniska uppgifter

För att genomföra Budapestkonventionen i svensk rätt infördes den 1 maj 2021 bestämmelser om att den som innehar en viss lagrad elektronisk uppgift som behövs i en brottsutredning ska kunna föreläggas att bevara uppgiften, en form av s.k. frysning (27 kap. 16 § rättegångsbalken). När det gäller det gränsöverskridande rättsliga samarbetet omfattas ett föreläggande om bevarande av uppgifter av bestämmelserna om rättslig hjälp i lagen (2000:562) om internationell rättslig hjälp i brottmål. Ett sådant föreläggande anses också vara en sådan utredningsåtgärd som omfattas av lagen (2017:1000) om en europeisk utredningsorder. Lagen om inter-

nationell rättslig hjälp i brottmål gäller inte om lagen om en europeisk utredningsorder är tillämplig.

Den 13 december 2022 lämnade Åklagarmyndigheten in en framställan om förtydliganden i regleringen om gränsöverskridande hantering av förelägganden om bevarande av uppgifter (Ju2022/03650). I framställan anges bl.a. att andra EU-stater inte anser att en europeisk utredningsorder ska användas vid förelägganden om frysning och att det medför problem i det rättsliga samarbetet som kan behöva åtgärdas genom lagändringar.

Frågan om det med anledning av Åklagarmyndighetens framställan kan finnas skäl att ändra regleringen om gränsöverskridande hantering av förelägganden om bevarande av uppgifter bör lämpligtvis behandlas tillsammans med frågan om vilka ändringar som krävs med anledning av de nya EU-rättsakterna och det andra tilläggsprotokollet till Budapestkonventionen.

Utredaren ska därför

- analysera om det finns behov av att ändra eller komplettera
- bestämmelserna om gränsöverskridande hantering av förelägganden om bevarande av en viss lagrad uppgift, och
- lämna nödvändiga författningsförslag.

Arbetets genomförande, kontakter och redovisning av uppdraget

Under utförandet av uppdraget ska utredaren ha en dialog med och inhämta upplysningar från Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Domstolsverket och Sveriges advokatsamfund samt även med andra myndigheter och berörda aktörer, såsom civilsamhället och företag, i den utsträckning som utredaren finner lämpligt.

Utredaren ska hålla sig informerad om och beakta annat relevant arbete som pågår inom Regeringskansliet och utredningsväsendet samt inom EU och andra internationella forum. Förslagen som lämnas ska dessutom vara förenliga med Sveriges internationella åtaganden.

Utredaren ska vid sina överväganden noga beakta skyddet för grundläggande fri- och rättigheter, däribland yttrande- och infor-

mationsfriheten. Uppdraget bör ske med beaktande av brottsbekämpande myndigheternas redan existerande verktyg för åtkomst till elektroniska bevis och de befintliga lösningar som finns uppbyggda. Vid övervägandena om vilka myndigheter och domstolar som ska utses enligt EU-förordningen och EU-direktivet bör hänsyn tas till förfarandet vid liknande nationella förfarande och utredningsåtgärder. Förslagen ska utformas så att de kan genomföras på ett kostnadseffektivt sätt med minsta möjliga administrativa börda för berörda myndigheter och domstolar. Utredarens förslag ska vidare utformas så att företagens totala regelbörda och kostnader inte ökar mer än nödvändigt.

Utredaren får om det bedöms lämpligt ta upp andra frågor som har samband med de frågor som ska utredas eller som annars aktualiseras med anledning av EU-förordningens, EU-direktivets eller protokollets innehåll.

Uppdraget ska redovisas senast den 13 december 2024

(Justitiedepartementet)

Europaparlamentets och rådets förordning (EU) 2023/1543

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2023/1543

av den 12 juli 2023

om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 82.1,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ⁽¹⁾,i enlighet med det ordinarie lagstiftningsförfarandet ⁽²⁾, och

av följande skäl:

- (1) Unionen har satt som mål att bevara och utveckla ett område med frihet, säkerhet och rättvisa. I syfte att gradvis upprätta ett sådant område ska unionen besluta om åtgärder rörande straffrättsligt samarbete på grundval av principen om ömsesidigt erkännande av domar och rättsliga avgöranden, vilken sedan Europeiska rådets möte i Tammerfors den 15 och 16 oktober 1999 allmänt anses vara en hörnsten i det straffrättsliga samarbetet inom unionen.
- (2) Åtgärder för att inhämta och bevara elektroniska bevis är allt viktigare för brottsutredningar och åtal i hela unionen. Effektiva förfaranden för att inhämta elektroniska bevis är av yttersta vikt för att bekämpa brottslighet, och sådana förfaranden bör omfattas av villkor och skyddsåtgärder som säkerställer full efterlevnad av de grundläggande rättigheter och principer som erkänns i artikel 6 i fördraget om Europeiska unionen (EU-fördraget) och Europeiska unionens stadga om de grundläggande rättigheterna (*stadgan*), i synnerhet principerna om nödvändighet och proportionalitet, rättssäkerhet, integritetsskydd och skydd av personuppgifter samt konfidentialitet vid kommunikation.
- (3) I det gemensamma uttalandet av den 24 mars 2016 från EU:s ministrar med ansvar för rättsliga och inrikes frågor och företrädare för unionsinstitutionerna om terrorattacker i Bryssel poängterades behovet av att, som en prioritering, snabbare och effektivare säkra och inhämta digitala bevis samt fastställa konkreta åtgärder för att göra detta.
- (4) I rådets slutsatser av den 9 juni 2016 betonades den allt större betydelsen av elektroniska bevis i straffrättsliga förfaranden samt vikten av att skydda cyberrymden från oegentligheter och brottslig verksamhet, för våra ekonomiers och samhällens skull, och därmed behovet inom brottsbekämpande myndigheter och rättsliga myndigheter av effektiva verktyg för att utreda och lagföra it-relaterade brott.
- (5) I det gemensamma meddelandet från kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik till Europaparlamentet och rådet av den 13 september 2017 om resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU betonade kommissionen att en effektiv utredning och lagföring av cyberbrott är en viktig faktor för att avskräcka från cyberbrott, och att dagens förfaranden måste anpassas bättre till internetåldern. Cyberangreppen kan ibland överväldiga dagens förfaranden och därmed skapa särskilda behov av snabbt samarbete över gränserna.
- (6) I Europaparlamentets resolution av den 3 oktober 2017 om kampen mot it-brottslighet ⁽³⁾ underströks behovet av att finna sätt att snabbare säkra och inhämta elektroniska bevis samt betydelsen av ett nära samarbete mellan brottsbekämpande myndigheter, tredjeländer och tjänsteleverantörer som är verksamma på europeiskt territorium, i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 ⁽⁴⁾ och Europaparlamentets och rådets

⁽¹⁾ EUT C 367, 10.10.2018, s. 88.

⁽²⁾ Europaparlamentets ståndpunkt av den 13 juni 2023 (ännu ej offentliggjord i EUT) och rådets beslut av den 27 juni 2023.

⁽³⁾ EUT C 346, 27.9.2018, s. 29.

⁽⁴⁾ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

direktiv (EU) 2016/680⁽⁵⁾, och befintliga avtal om ömsesidig rättslig hjälp. I Europaparlamentets resolution betonades också att det befintliga fragmenterade regelverket kan skapa problem för tjänsteleverantörer som försöker svara på framställningar på brottsbekämpningsområdet, och kommissionen uppmanades att lägga fram ett förslag till en europeisk rättslig ram för elektroniska bevis, med lämpliga skyddsåtgärder för alla berörda parterers rättigheter och friheter, samtidigt som kommissionens pågående arbete välkomnades för att skapa en samarbetsplattform med en säker kommunikationskanal för digitalt utbyte av europeiska utredningsorder för elektroniska bevis och svar mellan rättsliga myndigheter i unionen.

- (7) Nätverksbaserade tjänster kan tillhandahållas från vilken plats som helst och kräver inte fysisk infrastruktur, lokaler eller personal i det land där den relevanta tjänsten erbjuds. Därför lagras relevanta elektroniska bevis ofta utanför den utredande staten eller av en tjänsteleverantör som har ett verksamhetsställe utanför den staten, vilket skapar utmaningar när det gäller insamling av elektroniska bevis i straffrättsliga förfaranden.
- (8) På grund av det sätt på vilket nätverksbaserade tjänster tillhandahålls riktas framställningar om rättsligt samarbete ofta till stater där många tjänsteleverantörer är etablerade. Dessutom har antalet framställningar ökat mångfaldigt på grund av att användningen av nätverksbaserade tjänster ökar. Europaparlamentets och rådets direktiv 2014/41/EU⁽⁶⁾ gör det möjligt att utfärda en europeisk utredningsorder för insamling av bevis i en annan medlemsstat. I den konvention som upprättats av rådet i enlighet med artikel 34 i fördraget om Europeiska unionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater⁽⁷⁾ (konventionen om ömsesidig rättslig hjälp i brottmål) föreskrivs också en möjlighet att begära bevis från en annan medlemsstat. De förfaranden och tidsfrister som föreskrivs i direktiv 2014/41/EU om en europeisk utredningsorder och i konventionen om ömsesidig rättslig hjälp i brottmål är inte alltid lämpliga för elektroniska bevis, som är mer flyktiga till sin natur och lättare och snabbare kan komma att raderas. Det tar ofta lång tid att inhämta elektroniska bevis genom kanaler för rättsligt samarbete, vilket leder till situationer där de ledtrådar bevisen kan ge kanske inte längre är tillgängliga. Dessutom finns ingen harmoniserad ram för samarbete med tjänsteleverantörer, samtidigt som vissa leverantörer i tredjeländer tar emot direkta framställningar om andra uppgifter än innehållsdata i enlighet med vad som tillåts enligt deras tillämpliga nationella rätt. Följaktligen förlitar sig medlemsstater i allt högre grad på kanaler för frivilligt direkt samarbete med tjänsteleverantörer när sådana finns, och de tillämpar olika nationella verktyg, villkor och förfaranden. Vissa medlemsstater har vidtagit ensidiga åtgärder för innehållsdata, medan andra fortfarande förlitar sig på rättsligt samarbete.
- (9) Det fragmenterade regelverket skapar problem för brottsbekämpande myndigheter och rättsliga myndigheter samt för tjänsteleverantörer som försöker svara på rättsliga framställningar om elektroniska bevis, eftersom de i allt större utsträckning ställs inför osäkerhet om rättsläget och, potentiellt, lagkonflikter. Därför finns det ett behov av att fastställa särskilda regler för gränsöverskridande rättsligt samarbete för bevarande och utlämnande av elektroniska bevis, som tar hänsyn till den särskilda karaktären hos elektroniska bevis. Sådana regler bör inbegripa en skyldighet för tjänsteleverantörer som omfattas av denna förordnings tillämpningsområde att svara direkt på framställningar från myndigheter i en annan medlemsstat. Denna förordning kommer därför att komplettera befintlig unionsrätt och klargöra de regler som är tillämpliga på brottsbekämpande myndigheter och rättsliga myndigheter samt på tjänsteleverantörer på området för elektroniska bevis, samtidigt som full efterlevnad av de grundläggande rättigheterna säkerställs.
- (10) Denna förordning är förenlig med de grundläggande rättigheter och de principer som erkänns i artikel 6 i EU-fördraget och i stadgan, i internationell rätt och i internationella avtal i vilka unionen eller samtliga medlemsstater är part, inbegripet Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande rättigheterna, samt i medlemsstaternas konstitutioner inom deras respektive tillämpningsområde. Sådana rättigheter och principer omfattar särskilt rätten till frihet och säkerhet, respekten för privatlivet och familjelivet, skyddet av personuppgifter, näringsfriheten, rätten till egendom, rätten till ett effektivt rättsmedel och till en opartisk domstol, presumptionen för oskuld och rätten till försvar, principerna om laglighet och proportionalitet samt rätten att i straffrättsliga förfaranden inte bli dömd eller straffad två gånger för samma brott.

⁽⁵⁾ 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 (EUT L 119, 4.5.2016, s. 89).

⁽⁶⁾ Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området (EUT L 130, 1.5.2014, s. 1).

⁽⁷⁾ Konvention, upprättad av rådet på grundval av artikel 34 i fördraget om Europeiska unionen, om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater (EGT C 197, 12.7.2000, s. 3).

- (11) Ingenting i denna förordning bör tolkas som ett förbud för en verkställande myndighet att vägra en europeisk utlämnandeorder om det på grundval av objektiva faktorer finns skäl att tro att den europeiska utlämnandeordern har utfärdats för att lagföra eller straffa en person på grund av dennes kön, ras eller etniska ursprung, religion, sexuella läggning eller könsidentitet, nationalitet, språk eller politiska uppfattning eller att den berörda personens ställning skulle kunna skadas av något av dessa skäl.
- (12) Förfarandet med en europeisk utlämnandeorder och en europeisk bevarandeorder för elektroniska bevis i straffrättsliga förfaranden bygger på principen om ömsesidigt förtroende mellan medlemsstaterna och en presumtion om att medlemsstaterna respekterar unionsrätten, rättsstatens principer och i synnerhet de grundläggande rättigheterna, som utgör avgörande delar av unionens område med frihet, säkerhet och rättvisa. Ett sådant förfarande gör det möjligt för nationella behöriga myndigheter att översända sådana order direkt till tjänsteleverantörer.
- (13) Respekten för privatlivet och familjelivet samt skyddet av fysiska personer när det gäller behandling av personuppgifter utgör grundläggande rättigheter. I enlighet med artiklarna 7 och 8.1 i stadgan har var och en rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer samt till skydd av de personuppgifter som rör honom eller henne.
- (14) Vid genomförandet av denna förordning bör medlemsstaterna säkerställa att personuppgifter skyddas och behandlas i enlighet med förordning (EU) 2016/679 och direktiv (EU) 2016/680 samt Europaparlamentets och rådets direktiv 2002/58/EG⁽⁸⁾, inbegripet vid ytterligare användning, överföring och vidarebefordran av de uppgifter som inhämtats.
- (15) Personuppgifter som inhämtas enligt denna förordning bör behandlas endast om det är nödvändigt och på ett sätt som är proportionellt i förhållande till ändamålen förebyggande, utredning, upptäckt och lagföring av brott eller verkställighet av straffrättsliga påföljder och utövande av rätten till försvar. Medlemsstaterna bör i synnerhet säkerställa att lämpliga strategier och åtgärder för dataskydd tillämpas på översändandet av personuppgifter från behöriga myndigheter till tjänsteleverantörer vid tillämpningen av denna förordning, inbegripet åtgärder för att säkerställa uppgifternas säkerhet. Tjänsteleverantörerna bör säkerställa att samma skyddsåtgärder tillämpas vid översändandet av personuppgifter till behöriga myndigheter. Endast behöriga personer bör ha tillgång till information som innehåller personuppgifter, vilket kan uppnås genom förfaranden för autentisering.
- (16) De processuella rättigheter i straffrättsliga förfaranden som fastställs i Europaparlamentets och rådets direktiv 2010/64/EU⁽⁹⁾, 2012/13/EU⁽¹⁰⁾, 2013/48/EU⁽¹¹⁾, (EU) 2016/343⁽¹²⁾, (EU) 2016/800⁽¹³⁾ och (EU) 2016/1919⁽¹⁴⁾ bör, inom dessa direktivs tillämpningsområden, tillämpas på straffrättsliga förfaranden som omfattas av denna förordning med avseende på de medlemsstater som är bundna av dessa direktiv. Rättssäkerhetsgarantierna enligt stadgan bör också tillämpas.
- (17) För att garantera full respekt för de grundläggande rättigheterna bör värdet av bevis som har samlats in vid tillämpningen av denna förordning bedömas av den behöriga rättsliga myndigheten vid en rättegång, i enlighet med nationell rätt och i framförallt i överensstämmelse med rätten till en opartisk domstol och rätten till försvar.

⁽⁸⁾ Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

⁽⁹⁾ Europaparlamentets och rådets direktiv 2010/64/EU av den 20 oktober 2010 om rätt till tolkning och översättning vid straffrättsliga förfaranden (EUT L 280, 26.10.2010, s. 1).

⁽¹⁰⁾ Europaparlamentets och rådets direktiv 2012/13/EU av den 22 maj 2012 om rätten till information vid straffrättsliga förfaranden (EUT L 142, 1.6.2012, s. 1).

⁽¹¹⁾ Europaparlamentets och rådets direktiv 2013/48/EU av den 22 oktober 2013 om rätt till tillgång till försvarare i straffrättsliga förfaranden och förfaranden i samband med en europeisk arresteringsorder samt om rätt att få en tredje part underrättad vid frihetsberövande och rätt att kontakta tredje parter och konsulära myndigheter under frihetsberövandet (EUT L 294, 6.11.2013, s. 1).

⁽¹²⁾ Europaparlamentets och rådets direktiv (EU) 2016/343 av den 9 mars 2016 om förstärkning av vissa aspekter av oskuldspresumtionen och av rätten att närvara vid rättegången i straffrättsliga förfaranden (EUT L 65, 11.3.2016, s. 1).

⁽¹³⁾ Europaparlamentets och rådets direktiv (EU) 2016/800 av den 11 maj 2016 om rättssäkerhetsgarantier för barn som är misstänkta eller tilltalade i straffrättsliga förfaranden (EUT L 132, 21.5.2016, s. 1).

⁽¹⁴⁾ Europaparlamentets och rådets direktiv (EU) 2016/1919 av den 26 oktober 2016 om rättshjälp för misstänkta och tilltalade i straffrättsliga förfaranden och för eftersökta personer i förfaranden i samband med en europeisk arresteringsorder (EUT L 297, 4.11.2016, s. 1).

- (18) I denna förordning fastställs regler enligt vilka en behörig rättslig myndighet i unionen, i straffrättsliga förfaranden eller för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden, inbegripet brottsutredningar, i enlighet med denna förordning, kan beordra en tjänsteleverantör som erbjuder tjänster i unionen att lämna ut eller bevara elektroniska bevis genom en europeisk utlämnandeorder eller en europeisk bevarandeorder. Denna förordning bör tillämpas i samtliga gränsöverskridande fall när en tjänsteleverantör har sitt utsedda verksamhetsställe eller rättsliga ombud i en annan medlemsstat. Denna förordning påverkar inte de nationella myndigheternas befogenheter att rikta framställningar till tjänsteleverantörer som har ett verksamhetsställe eller är representerade på deras territorium i syfte att säkerställa att dessa följer liknande nationella bestämmelser.
- (19) Denna förordning bör endast reglera insamling av uppgifter som lagras av en tjänsteleverantör vid den tidpunkt då en europeisk utlämnandeorder eller en europeisk bevarandeorder tas emot. Den bör inte föreskriva någon allmän datalagringskyldighet för tjänsteleverantörer och bör inte leda till någon allmän och odifferentierad lagring av data. Denna förordning bör inte heller ge rätt till dataavlysning eller inhämtande av uppgifter som har lagrats efter mottagandet av en europeisk utlämnandeorder eller en europeisk bevarandeorder.
- (20) Tillämpningen av denna förordning bör inte påverka tjänsteleverantörernas eller deras användares användning av kryptering. Uppgifter som begärs genom en europeisk utlämnandeorder eller en europeisk bevarandeorder bör tillhandahållas eller bevaras oavsett om de är krypterade eller inte. Denna förordning bör dock inte föreskriva någon skyldighet för tjänsteleverantörer att dekryptera uppgifter.
- (21) I många fall lagras uppgifter, eller behandlas på annat sätt, inte längre i användarens utrustning, utan via en molnbaserad infrastruktur som är tillgänglig var som helst. För att driva sådana tjänster måste tjänsteleverantörer inte ha ett verksamhetsställe eller serverar i en viss jurisdiktion. Därför bör tillämpningen av denna förordning inte vara beroende av den faktiska platsen för tjänsteleverantörens verksamhet eller den lokal där uppgifterna behandlas eller lagras.
- (22) Denna förordning påverkar inte myndigheternas utredningsbefogenheter i civilrättsliga eller administrativa förfaranden, inte heller då sådana förfaranden kan leda till sanktioner.
- (23) Eftersom förfaranden för ömsesidig rättslig hjälp kan betraktas som straffrättsliga förfaranden i enlighet med tillämplig nationell rätt i medlemsstaterna bör det tydliggöras att en europeisk utlämnandeorder eller en europeisk bevarandeorder inte bör utfärdas för tillhandahållande av ömsesidig rättslig hjälp till en annan medlemsstat eller ett tredjeland. I sådana fall bör framställningar om ömsesidig rättslig hjälp ställas till den medlemsstat eller det tredjeland som kan tillhandahålla ömsesidig rättslig hjälp enligt nationell rätt.
- (24) Inom ramen för straffrättsliga förfaranden bör en europeisk utlämnandeorder och en europeisk bevarandeorder endast utfärdas för specifika straffrättsliga förfaranden rörande ett specifikt brott som redan har ägt rum, efter en individuell bedömning av nödvändigheten och proportionaliteten av en sådan order i varje enskilt fall, med beaktande av den misstänkte eller tilltalade personens rättigheter.
- (25) Denna förordning bör också tillämpas på förfaranden som inleds av en utfärdande myndighet för att lokalisera en dömd person som har undandragit sig lagföring, i syfte att verkställa fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden. Om fängelsestraffet eller den andra frihetsberövande åtgärden beslutats genom en dom där personen inte var personligen närvarande vid förhandlingen bör det emellertid inte vara möjligt att utfärda en europeisk utlämnandeorder eller en europeisk bevarandeorder eftersom medlemsstaternas nationella rätt avseende sådana domar varierar avsevärt inom unionen.
- (26) Denna förordning bör tillämpas på tjänsteleverantörer som erbjuder tjänster i unionen, och det bör vara möjligt att utfärda de order som föreskrivs i denna förordning endast för uppgifter som hänför sig till tjänster som erbjuds i unionen. Tjänster som erbjuds uteslutande utanför unionen bör inte omfattas av denna förordnings tillämpningsområde, även om tjänsteleverantören har ett verksamhetsställe i unionen. Därför bör denna förordning inte tillåta åtkomst till andra uppgifter än uppgifter som rör de tjänster som erbjuds användaren i unionen av dessa tjänsteleverantörer.
- (27) De tjänsteleverantörer som är mest relevanta när det gäller insamling av bevis i straffrättsliga förfaranden är leverantörer av elektroniska kommunikationstjänster och specifika leverantörer av sådana informationssamhällets tjänster som underlättar interaktion mellan användare. Båda grupperna bör därför omfattas av denna förordning. Elektroniska kommunikationstjänster definieras i Europaparlamentets och rådets direktiv (EU) 2018/1972⁽¹⁵⁾, och omfattar interpersonella kommunikationstjänster såsom VoIP, meddelandetjänster och e-posttjänster. Denna

⁽¹⁵⁾ 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).

förordning bör också vara tillämplig på leverantörer av informationssamhällets tjänster i den mening som avses i Europaparlamentets och rådets direktiv (EU) 2015/1535⁽¹⁶⁾ som inte kan klassas som leverantörer av elektroniska kommunikationstjänster, men som erbjuder sina användare möjligheten att kommunicera med varandra eller erbjuder sina användare tjänster som kan användas för att lagra eller på annat sätt behandla uppgifter för deras räkning. Detta skulle vara i linje med de termer som används i Europarådets konvention om it-brottslighet (ETS nr 185) (*Budapestkonventionen*), upprättad i Budapest den 23 november 2001. Uppgiftsbehandling bör förstås i teknisk mening, alltså som skapande eller manipulation av uppgifter, dvs. teknisk bearbetning för att framställa eller ändra uppgifter med hjälp av datorernas bearbetningskapacitet. De kategorier av tjänsteleverantörer som omfattas av denna förordning bör exempelvis inkludera marknadsplatser online som ger konsumenter och företag möjlighet att kommunicera med varandra och andra värdtjänster, även när tjänsten tillhandahålls via molntjänster, liksom plattformar för onlinespel. Om en leverantör av informationssamhällets tjänster inte ger sina användare möjlighet att kommunicera med varandra utan endast med tjänsteleverantören, eller inte ger en möjlighet att lagra eller på annat sätt behandla uppgifter, eller om lagringen av uppgifter inte är en avgörande komponent, det vill säga en väsentlig del, av den tjänst som tillhandahålls användarna, såsom rättsliga tjänster, dataarkitektur tjänster och bokföringstjänster som tillhandahålls online på distans, bör den inte omfattas av definitionen av *tjänsteleverantör* i denna förordning, även om de tjänster som tillhandahålls av den tjänsteleverantören är informationssamhällets tjänster i den mening som avses i direktiv (EU) 2015/1535.

- (28) Leverantörer av infrastrukturtjänster som rör tilldelning av namn och nummer, såsom domännamnregister och domännamnregistratorer samt leverantörer av integritetstjänster och proxytjänster eller regionala internetregister för IP-adresser, är särskilt relevanta när det gäller att identifiera aktörer bakom skadliga eller komprometterade webbplatser. De inehar uppgifter som skulle kunna göra det möjligt att identifiera en person eller enhet som ligger bakom en webbplats som används för brottslig verksamhet, eller offret för en brottslig verksamhet.
- (29) För att fastställa om en tjänsteleverantör erbjuder tjänster i unionen krävs en bedömning av huruvida tjänsteleverantören gör det möjligt för fysiska eller juridiska personer i en eller flera medlemsstater att använda dess tjänster. Enbart det faktum att ett onlinegränssnitt är tillgängligt i unionen, till exempel genom en tjänsteleverantörs eller en mellanhands webbplats eller en e-postadress eller andra kontaktuppgifter, bör dock inte i sig anses vara tillräckligt för att fastställa att en tjänsteleverantör erbjuder tjänster i unionen i den mening som avses i denna förordning.
- (30) En betydande anknytning till unionen bör också vara relevant för att fastställa huruvida en tjänsteleverantör erbjuder tjänster i unionen. En sådan betydande anknytning till unionen bör anses föreligga om tjänsteleverantören har ett verksamhetsställe i unionen. I avsaknad av ett sådant verksamhetsställe bör kriteriet avseende en betydande anknytning baseras på specifika faktiska kriterier som att det finns ett betydande antal användare i en eller flera medlemsstater, eller att verksamheten är inriktad på en eller flera medlemsstater. Huruvida verksamheten är inriktad på en eller flera medlemsstater bör fastställas på grundval av alla relevanta omständigheter, inbegripet faktorer som användningen av ett språk eller en valuta som allmänt används i den medlemsstaten, eller möjligheten att beställa varor eller tjänster. Att verksamheten är inriktad på en medlemsstat skulle också kunna härledas från det faktum att det finns en app i den berörda nationella appbutiken, att lokal marknadsföring eller reklam görs på det språk som allmänt används i den medlemsstaten eller att kundkontakter, till exempel kundtjänst, sköts på det språk som allmänt används i den medlemsstaten. En betydande anknytning bör också anses föreligga när en tjänsteleverantör riktar sin verksamhet mot en eller flera medlemsstater enligt Europaparlamentets och rådets förordning (EU) nr 1215/2012⁽¹⁷⁾. Däremot bör tillhandahållande av en tjänst enbart i syfte att efterleva det förbud mot diskriminering som fastställs i Europaparlamentets och rådets förordning (EU) 2018/302⁽¹⁸⁾ inte utan ytterligare skäl anses innebära att verksamheten är inriktad på ett visst territorium inom unionen. Samma överväganden bör tillämpas för att fastställa huruvida en tjänsteleverantör erbjuder tjänster i en medlemsstat.

⁽¹⁶⁾ 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).

⁽¹⁷⁾ Europaparlamentets och rådets förordning (EU) nr 1215/2012 av den 12 december 2012 om domstols behörighet och om erkännande och verkställighet av domar på privaträttsens område (EUT L 351, 20.12.2012, s. 1).

⁽¹⁸⁾ Europaparlamentets och rådets förordning (EU) 2018/302 av den 28 februari 2018 om åtgärder mot omutiverad geoblocking och andra former av diskriminering på grund av kunders nationalitet, bostättsort eller etableringsort på den inre marknaden och om ändring av förordningarna (EG) nr 2006/2004 och (EU) 2017/2394 samt direktiv 2009/22/EG (EUT L 60 I, 2.3.2018, s. 1).

- (31) Denna förordning bör omfatta uppgiftskategorierna abonnentuppgifter, trafikuppgifter och innehållsdata. Sådana kategoriseringar är i linje med många medlemsstaters rätt och unionsrätten, såsom direktiv 2002/58/EG och domstolens rättspraxis samt internationell rätt, särskilt Budapestkonventionen.
- (32) IP-adresser samt åtkomstnummer och relaterad information kan utgöra en avgörande utgångspunkt för brottsutredningar där en misstänkt persons identitet inte är känd. De registreras vanligen som en del av registreringen av en händelse, också kallat en serverlogg, som anger när en användares åtkomst till en tjänst inleds och avslutas. De utgörs ofta av en enskild IP-adress, antingen statisk eller dynamisk, eller annan identifierare som utpekar det nätverksgränssnitt som använts under åtkomstsessionen. Relaterad information om när användares åtkomst till en tjänst såsom källportar och tidsstämpel inleds och avslutas behövs eftersom IP-adresser ofta delas mellan användarna, till exempel när det finns Carrier Grade Network Address Translation (CGN) eller tekniska motsvarigheter. I enlighet med unionens regelverk ska IP-adresser dock betraktas som personuppgifter och åtnjuta fullständigt skydd enligt unionens dataskyddsregelverk. Dessutom kan IP-adresser under vissa omständigheter betraktas som trafikuppgifter. Åtkomstnummer och relaterad information betraktas också som trafikuppgifter i vissa medlemsstater. I samband med en viss brottsutredning kan dock brottsbekämpande myndigheter tvingas begära en IP-adress samt åtkomstnummer och relaterad information med det enda syftet att identifiera användaren innan abonnentuppgifter avseende den identifieraren kan begäras från tjänsteleverantören. I sådana fall är det lämpligt att tillämpa samma ordning som för abonnentuppgifter enligt definitionen i denna förordning.
- (33) När IP-adresser, åtkomstnummer och relaterad information inte begärs med det enda syftet att identifiera användaren i en specifik brottsutredning, begärs de i allmänhet för inhämtande av information som i högre grad inkräktar på den personliga integriteten, såsom användarens kontakter och vistelseort. De skulle därmed kunna användas för att fastställa en omfattande profil för en berörd person, men kan samtidigt behandlas och analyseras lättare än innehållsdata eftersom de presenteras i ett strukturerat och standardiserat format. I sådana situationer är det därför viktigt att IP-adresser, åtkomstnummer och relaterad information som inte begärs med det enda syftet att identifiera användaren i en specifik brottsutredning behandlas som trafikuppgifter och begärs enligt samma ordning som för innehållsdata, enligt definitionen i denna förordning.
- (34) Alla uppgiftskategorier innehåller personuppgifter och omfattas därmed av skyddsåtgärder enligt unionens dataskyddsregelverk. Graden av inverkan på de grundläggande rättigheterna varierar dock mellan kategorierna, i synnerhet mellan abonnentuppgifter och uppgifter som begärs med det enda syftet att identifiera användaren, enligt definitionen i denna förordning, å ena sidan, och trafikuppgifter, med undantag för uppgifter som begärs med det enda syftet att identifiera användaren, enligt definitionen i denna förordning, å andra sidan. Abonnentuppgifter och IP-adresser, åtkomstnummer och relaterad information, om de begärs med det enda syftet att identifiera användaren, kan vara användbara för att vid en utredning få de första ledtrådarna om en misstänkt persons identitet, men trafikuppgifter, med undantag för uppgifter som begärs med det enda syftet att identifiera användaren, enligt definitionen i denna förordning, och innehållsdata är i många fall mer relevanta som bevismaterial. Det är därför viktigt att alla dessa uppgiftskategorier omfattas av denna förordning. På grund av den varierande graden av ingrepp i de grundläggande rättigheterna bör det införas lämpliga skyddsåtgärder och villkor för inhämtande av sådana uppgifter.
- (35) Situationer där det föreligger ett överhängande hot mot en persons liv, fysiska integritet eller säkerhet bör behandlas som nödsituationer och medge kortare tidsfrister för tjänsteleverantören och den verkställande myndigheten. Om en driftsstörning vid eller en förstörelse av kritisk infrastruktur enligt definitionen i rådets direktiv 2008/114/EG⁽¹⁹⁾ skulle innebära ett sådant hot, inbegripet genom allvarlig skada på tillhandahållandet av basförnödenheter till befolkningen eller på utövanheten av statens kärnfunktioner, bör en sådan situation också behandlas som en nödsituation, i enlighet med unionsrätten.
- (36) När en europeisk utlämnandeorder eller en europeisk bevarandeorder utfärdas bör en rättslig myndighet alltid delta i antingen utfärdandet eller godkännandet av ordern. Med tanke på den mer känsliga karaktären hos trafikuppgifter, med undantag för uppgifter som begärs med det enda syftet att identifiera användaren, enligt definitionen i denna förordning, och hos innehållsdata, kräver utfärdande eller godkännande av en europeisk utlämnandeorder för att inhämta dessa uppgiftskategorier prövning av en domare. Eftersom abonnentuppgifter och uppgifter som begärs med det enda syftet att identifiera användaren, enligt definitionen i denna förordning, är mindre känsliga, kan en europeisk utlämnandeorder för att inhämta sådana uppgifter dessutom utfärdas eller

⁽¹⁹⁾ Rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna (EUT L 345, 23.12.2008, s. 75).

godkännas av en behörig allmän åklagare. I enlighet med rätten till en opartisk domstol, som skyddas av stadgan och Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, ska allmänna åklagare utöva sitt ansvar på ett objektivt sätt och fatta beslut om utfärdande eller godkännande av en europeiska utlämnandeorder eller en europeisk bevarandeorder enbart på grundval av de faktiska omständigheterna i ärendet och med beaktande av all bevisning som talar till den berörda personens för- och nackdel.

- (37) För att säkerställa att de grundläggande rättigheterna fullt ut skyddas bör rättsliga myndigheters godkännanden av europeiska utlämnandeorder eller europeiska bevarandeorder i princip erhållas innan den berörda ordern utfärdas. Undantag från den principen bör göras endast i vederbörligen motiverade nödsituationer när det gäller utlämnande av abonnentuppgifter eller uppgifter som begärts med det enda syftet att identifiera användaren, enligt definitionen i denna förordning, eller för bevarande av uppgifter, om det inte är möjligt att erhålla förhandsgodkännande från den rättsliga myndigheten i tid, särskilt om anledningen är att den godkännande myndigheten inte kan nås för att lämna ett godkännande och hotet är så överhängande att omedelbara åtgärder måste vidtas. Sådana undantag bör dock göras endast om den myndighet som utfärdar den berörda ordern skulle kunna utfärda en order i ett liknande inhemskt ärende enligt nationell rätt utan förhandsgodkännande.
- (38) En europeisk utlämnandeorder bör utfärdas endast om det är nödvändigt, proportionellt, lämpligt och relevant i det berörda fallet. Den utfärdande myndigheten bör beakta den misstänktes eller tilltalades rättigheter i förfaranden som rör ett brott och bör utfärda en europeisk utlämnandeorder endast om en sådan order skulle ha kunnat utfärdas på samma villkor i ett liknande inhemskt ärende. Vid bedömningen av huruvida en europeisk utlämnandeorder ska utfärdas bör hänsyn tas till om ordern är begränsad till vad som är strikt nödvändigt för att uppnå det legitima målet att inhämta de uppgifter som är relevanta och nödvändiga som bevis i det enskilda fallet.
- (39) Om en europeisk utlämnandeorder utfärdas för inhämtande av olika uppgiftskategorier bör den utfärdande myndigheten säkerställa att villkor och förfaranden, såsom anmälan till den verkställande myndigheten, iaktas för var och en av dessa uppgiftskategorier.
- (40) Med tanke på den mer känsliga karaktären hos trafikuppgifter, med undantag för uppgifter som begärts med det enda syftet att identifiera användaren, enligt definitionen i denna förordning, och innehållsdata, bör en avgränsning göras avseende det materiella tillämpningsområdet för denna förordning. Det bör vara möjligt att utfärda en europeisk utlämnandeorder för att inhämta abonnentuppgifter eller uppgifter som begärts med det enda syftet att identifiera användaren, enligt definitionen i denna förordning, för alla brott; en europeisk utlämnandeorder för att inhämta trafikuppgifter, med undantag för uppgifter som begärts med det enda syftet att identifiera användaren, enligt definitionen i denna förordning, eller för att inhämta innehållsdata bör vara föremål för striktare krav med tanke på att dessa uppgifter är känsligare. Denna förordning bör föreskriva ett tröskelvärde med avseende på dess tillämpningsområde, för att möjliggöra en mer proportionell ansats, tillsammans med ett antal andra förhands- och efterhandsvillkor och skyddsåtgärder för att säkerställa respekt för proportionalitetsprincipen och de berörda personernas rättigheter. Samtidigt bör ett sådant tröskelvärde inte begränsa denna förordnings effektivitet och tillämpningsområde användning av den. Genom att tillåta utfärdande av europeiska utlämnandeorder i straffrättsliga förfaranden endast för brott med maximistraff på minst tre års fängelse eller annan frihetsberövande åtgärd begränsas denna förordnings tillämpningsområde till allvarigare brott, utan att i alltför hög grad påverka aktörernas möjligheter att använda den. Den begränsningen skulle utesluta ett betydande antal brott som medlemsstaterna anser vara mindre allvariga från tillämpningsområdet för denna förordning, vilket uttrycks genom kortare maximistraff. Den begränsningen har också fördelen att den är lätt att tillämpa i praktiken.
- (41) Vid vissa typer av brott finns bevisen vanligen tillgängliga endast i elektronisk form, vilket innebär att de till sin natur är flyktiga. Detta är fallet när det gäller it-relaterade brott – även sådana som inte kan betraktas som allvarliga i sig, men som skulle kunna orsaka omfattande eller betydande skador, särskilt brott med liten enskild inverkan men stor volym och total skadeverkan. I de flesta fall där brottet har begåtts med hjälp av ett informationssystem skulle en tillämpning av samma tröskelvärde som för andra typer av brott i stor utsträckning leda till straffrihet. Detta motiverar att denna förordning tillämpas på sådana brott även om maximistraffet är fängelse eller annan frihetsberövande åtgärd på mindre än tre års fängelse. Terrorismrelaterade brott i den mening som avses i Europaparlamentets och rådets direktiv (EU) 2017/541⁽²⁰⁾ och brott i fråga om sexuella övergrepp mot

⁽²⁰⁾ Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF (EUT L 88, 31.3.2017, s. 6).

och sexuell exploatering av barn i den mening som avses i Europaparlamentets och rådets direktiv 2011/93/EU⁽¹⁾ bör inte kräva att det lägsta maximistraffet är fängelse eller annan frihetsberövande åtgärd i tre år.

- (42) Som utgångspunkt bör en europeisk utlämnandeorder ställas till tjänsteleverantörer som agerar som personuppgiftsansvariga. Under vissa omständigheter kan det dock vara särskilt svårt att avgöra om en tjänsteleverantör har rollen som personuppgiftsansvarig eller personuppgiftsbiträde, särskilt när flera tjänsteleverantörer är involverade i behandlingen av uppgifter eller när tjänsteleverantörer behandlar uppgifterna på en fysisk persons vägnar. För att skilja mellan den personuppgiftsansvariges och personuppgiftsbitrådets roller när det gäller en viss uppsättning uppgifter krävs inte bara specialkunskaper om det rättsliga sammanhanget, utan det kan också kräva en tolkning av i många fall mycket komplexa avtalsramar som i ett specifikt fall ger olika tjänsteleverantörer olika uppgifter och roller med avseende på en viss uppsättning uppgifter. När tjänsteleverantörer behandlar uppgifter på en fysisk persons vägnar kan det i vissa fall vara svårt att fastställa vem som är personuppgiftsansvarig, även om bara en tjänsteleverantör är involverad. Om de berörda uppgifterna lagras eller på annat sätt behandlas av en tjänsteleverantör och det trots rimliga ansträngningar från den utfärdande myndighetens sida inte råder klarhet om vem som är personuppgiftsansvarig, bör det därför vara möjligt att ställa en europeisk utlämnandeorder direkt till den tjänsteleverantören. I vissa fall skulle det dessutom kunna vara till skada för utredningen i det berörda fallet att rikta sig till den personuppgiftsansvarige, till exempel på grund av att den personuppgiftsansvarige är en misstänkt, tilltalad eller dömd person eller att det finns tecken på att den personuppgiftsansvarige skulle kunna agera i den persons intresse som är föremål för utredningen. Även i dessa fall bör det vara möjligt att ställa en europeisk utlämnandeorder direkt till den tjänsteleverantör som behandlar uppgifterna på den personuppgiftsansvariges vägnar. Detta bör inte påverka den utfärdande myndighetens rätt att beordra tjänsteleverantören att bevara uppgifterna.
- (43) I enlighet med förordning (EU) 2016/679 bör det personuppgiftsbiträde som lagrar eller på annat sätt behandlar uppgifterna på den personuppgiftsansvariges vägnar informera den personuppgiftsansvarige om utlämnandet av uppgifterna, såvida inte den utfärdande myndigheten har begärt att tjänsteleverantören ska avstå från att informera den personuppgiftsansvarige, under så lång tid som det är nödvändigt och proportionellt, för att inte hindra de relevanta straffrättsliga förfarandena. I det fallet bör den utfärdande myndigheten i ärendet ange skälen till fördröjningen med att informera den personuppgiftsansvarige, och en kort motivering bör också läggas till i det åtföljande intyg som översänds till mottagaren.
- (44) Om uppgifterna lagras eller på annat sätt behandlas som en del av en infrastruktur som en tjänsteleverantör tillhandahåller en offentlig myndighet bör det vara möjligt att utfärda en europeisk utlämnandeorder eller en europeisk bevarandeorder endast om den offentliga myndighet för vilken uppgifterna lagras eller på annat sätt behandlas är belägen i den utfärdande staten.
- (45) I fall där uppgifter som omfattas av sekretess eller tystnadsplikt enligt den utfärdande statens rätt lagras eller på annat sätt behandlas av en tjänsteleverantör som en del av en infrastruktur som tillhandahålls yrkesutövare som omfattas av sekretess eller tystnadsplikt inom ramen för deras verksamhet, bör det vara möjligt att utfärda en europeisk utlämnandeorder endast för att inhämta trafikuppgifter, med undantag för uppgifter som begärs med det enda syftet att identifiera användaren, enligt definitionen i denna förordning, eller för att inhämta innehållsdata om den yrkesutövare som omfattas av sekretess eller tystnadsplikt är bosatt i den utfärdande staten, om det skulle kunna vara till skada för utredningen att rikta sig till den yrkesutövare som omfattas av sekretesskydd eller om undantag gjorts från sekretessen eller tystnadsplikten i enlighet med tillämplig rätt.
- (46) Principen *ne bis in idem* är en grundläggande rättsprincip i unionen som erkänns i stadgan och vidareutvecklas i Europeiska unionens domstols rättspraxis. Om den utfärdande myndigheten har skäl att anta att parallella straffrättsliga förfaranden kan pågå i en annan medlemsstat bör den samråda med myndigheterna i den medlemsstaten i enlighet med rådets rambeslut 2009/948/RIF⁽²⁾. Under alla omständigheter ska en europeisk utlämnandeorder eller en europeisk bevarandeorder inte utfärdas om den utfärdande myndigheten har skäl att anta att detta skulle strida mot principen *ne bis in idem*.
- (47) I andra instrument för ömsesidigt erkännande, såsom direktiv 2014/41/EU om en europeisk utredningsorder, hänvisas det till immunitet och privilegier, som kan avse kategorier av personer, till exempel diplomater, eller särskilt skyddade förhållanden, till exempel rätten till förtrolig kommunikation mellan advokat och klient eller journalisters rätt att inte röja sina källor. Omfattningen och effekterna av immunitet och privilegier varierar beroende på den tillämpliga nationella rätt som bör beaktas vid tidpunkten för utfärdandet av en europeisk utlämnandeorder eller en europeisk bevarandeorder, eftersom den utfärdande myndigheten bör kunna utfärda orden endast om den skulle ha kunnat utfärdas på samma villkor i ett liknande inhemskt fall. Det finns ingen

⁽¹⁾ 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).

⁽²⁾ Rådets rambeslut 2009/948/RIF av den 30 november 2009 om förebyggande och lösning av tvister om utövande av jurisdiktion i straffrättsliga förfaranden (EUT L 328, 15.12.2009, s. 42).

gemensam definition av vad som utgör immunitet eller privilegier i unionsrätten. Den exakta definitionen av dessa begrepp överläts därför till nationell rätt, och definitionen kan omfatta skydd som är tillämpligt på exempelvis medicinska och juridiska yrken, även när specialiserade plattformar används inom dessa yrken. Den exakta definitionen av immunitet och privilegier kan också omfatta regler om fastställande och begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet och yttrandefrihet i andra medier.

- (48) Om den utfärdande myndigheten försöker inhämta trafikuppgifter, med undantag för uppgifter som begärts med det enda syftet att identifiera användaren, enligt definitionen i denna förordning, eller för att inhämta innehållsdata, genom att utfärda en europeisk utlämnandeorder och har rimliga skäl att anta att de begärda uppgifterna skyddas av immunitet eller privilegier som beviljas enligt den verkställande statens rätt, eller att dessa uppgifter i den staten omfattas av regler om fastställande och begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet och yttrandefrihet i andra medier, bör den utfärdande myndigheten kunna begära klagoranden innan den europeiska utlämnandeordern utfärdas, inbegripet genom samråd med de behöriga myndigheterna i den verkställande staten, antingen direkt eller via Eurojust eller det europeiska rättsliga nätverket.
- (49) Det bör vara möjligt att utfärda en europeisk bevarandeorder för alla brott. Den utfärdande myndigheten bör beakta den misstänktes eller tilltalades rättigheter i förfaranden som rör ett brott och bör utfärda en europeisk bevarandeorder endast om en sådan order skulle ha kunnat utfärdas på samma villkor i ett liknande inhemskt fall och om det är nödvändigt, proportionellt, lämpligt och relevant i det berörda fallet. Vid bedömningen av huruvida en europeisk bevarandeorder ska utfärdas bör hänsyn tas till om ordern är begränsad till vad som är strikt nödvändigt för att uppnå det legitima syftet att förhindra avlägsnande, radering eller ändring av uppgifter som är relevanta och nödvändiga som bevis i ett enskilt fall i situationer där utlämnandet av dessa uppgifter skulle kunna ta längre tid.
- (50) Europeiska utlämnandeorder och europeiska bevarandeorder bör ställas direkt till det utsedda verksamhetsstället eller till det rättsliga ombud som utsetts av tjänsteleverantören enligt Europaparlamentets och rådets direktiv (EU) 2023/1544⁽²³⁾. I nödsituationer enligt definitionen i denna förordning, där en tjänsteleverantörs utsedda verksamhetsställe eller rättsliga ombud inte reagerar på det åtföljande intyget om en europeisk utlämnandeorder eller intyget om en europeisk bevarandeorder inom tidsfristerna eller inte har utsetts inom de tidsfrister som anges i direktiv (EU) 2023/1544, bör det undantagsvis vara möjligt att ställa intyget om en europeisk utlämnandeorder eller intyget om en europeisk bevarandeorder till något annat av tjänsteleverantörens verksamhetsställen eller rättsliga ombud i unionen samtidigt som eller i stället för att begära fullföljande av den ursprungliga ordern i enlighet med denna förordning. Med hänsyn till dessa olika möjliga scenarier används den allmänna termen *mottagare* i bestämmelserna i denna förordning.
- (51) Med tanke på den mer känsliga karaktären hos en europeisk utlämnandeorder för att inhämta trafikuppgifter, med undantag för uppgifter som begärts med det enda syftet att identifiera användaren, enligt definitionen i denna förordning, eller för att inhämta innehållsdata, är det lämpligt att införa ett anmälningsförfarande för europeiska utlämnandeorder för att inhämta dessa uppgiftskategorier. Det anmälningsförfarandet bör involvera en verkställande myndighet och utgöras av översändandet av intyget om en europeisk utlämnandeorder till den myndigheten samtidigt som intyget om en europeisk utlämnandeorder översänds till mottagaren. Om en europeisk utlämnandeorder utfärdas för att inhämta elektroniska bevis i straffrättsliga förfaranden med betydande och starka kopplingar till den utfärdande staten bör det dock inte krävas någon anmälan till den verkställande myndigheten. Sådana kopplingar bör antas föreligga om den utfärdande myndigheten vid tidpunkten för utfärdandet av den europeiska utlämnandeordern har rimliga skäl att anta att brottet har begåtts, är på väg att begås eller sannolikt kommer att begås i den utfärdande staten, och om den person vars uppgifter begärs är bosatt i den utfärdande staten.
- (52) Vid tillämpningen av denna förordning bör ett brott anses ha begåtts, vara på väg att begås eller sannolikt komma att begås i den utfärdande staten om detta anses vara fallet i enlighet med den utfärdande statens nationella rätt. I vissa fall, särskilt när det gäller it-brottslighet, är vissa faktiska omständigheter, såsom brottsoffrets bosättningsort, vanligtvis viktiga indikationer att beakta vid fastställandet av var brottet har begåtts. Till exempel kan brott som begås med utpressningsprogram (ransomware) ofta anses ha begåtts där offret för ett sådant brott är bosatt, även om det är osäkert exakt var brottet som begås med utpressningsprogrammet har inletts. Fastställandet av den plats där brottet begicks bör inte påverka tillämpningen av bestämmelserna om behörighet för de relevanta brotten enligt tillämplig nationell rätt.

⁽²³⁾ Europaparlamentets och rådets direktiv (EU) 2023/1544 av den 12 juli 2023 om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden (se sidan 181 i detta nummer av EUT).

- (53) Det är den utfärdande myndigheten som, vid tidpunkten för utfärdandet av den europeiska utlämnandeordern för att inhämta trafikuppgifter, med undantag för uppgifter som begärs med det enda syftet att identifiera användaren, enligt definitionen i denna förordning, eller för att inhämta innehållsdata, och på grundval av det material som den har tillgång till, ska bedöma om det finns rimliga skäl att anta att den person vars uppgifter begärs är bosatt i den utfärdande staten. I detta avseende kan olika objektiva omständigheter som kan tyda på att den berörda personen har etablerat eller har för avsikt att etablera sina huvudsakliga intressen i en viss medlemsstat vara relevanta. Det följer av behovet av en enhetlig tillämpning av unionsrätten och av principen om likabehandling att begreppet *bosättning* i detta särskilda sammanhang bör ges en enhetlig tolkning i hela unionen. Det kan finnas rimliga skäl att anta att en person är bosatt i en utfärdande stat, särskilt om en person är registrerad som bosatt i en utfärdande stat, vilket framgår genom innehav av ett identitetskort eller ett uppehållstillstånd eller av en registrering i ett officiellt bosättningsregister. I avsaknad av registrering i den utfärdande staten skulle bosättningsorten kunna indikeras av att en person har uttryckt sin avsikt att bosätta sig i den medlemsstaten eller, efter en stadig vistelse under en viss tid i den medlemsstaten, har fått en sådan anknytning till denna medlemsstat som kan jämföras med sådan anknytning som följer av att personen är formellt bosatt i den medlemsstaten. För att avgöra huruvida det i en specifik situation föreligger tillräcklig anknytning mellan den berörda personen och den utfärdande staten som ger upphov till rimliga skäl att anta att den berörda personen är bosatt i den staten, kan olika objektiva omständigheter som kännetecknar denna persons situation beaktas, särskilt inbegripet varaktigheten för, arten av och villkoren för personens vistelse i den utfärdande staten eller de familjeband eller ekonomiska band som personen har till denna medlemsstat. Ett registrerat fordon, ett bankkonto, det faktum att personens vistelse i den utfärdande staten har varit oavbruten eller andra objektiva faktorer kan vara av betydelse för att fastställa att det finns rimliga skäl att anta att den berörda personen är bosatt i den utfärdande staten. Ett kort besök, en semestervistelse, även i en semesterbostad, eller en liknande vistelse i den utfärdande staten utan ytterligare betydande anknytning är inte tillräckligt för ett antagande om bosättning i den medlemsstaten. I fall där den utfärdande myndigheten vid tidpunkten för utfärdandet av den europeiska utlämnandeordern för att inhämta trafikuppgifter, med undantag för uppgifter som begärs med det enda syftet att identifiera användaren, enligt definitionen i denna förordning, eller för att inhämta innehållsdata, inte har rimliga skäl att anta att den person vars uppgifter begärs är bosatt i den utfärdande staten, bör den utfärdande myndigheten anmäla detta till den verkställande myndigheten.
- (54) För att påskynda förfarandet bör bedömningen av huruvida det finns ett behov av anmälan till den verkställande myndigheten ske vid tidpunkten för utfärdandet av den europeiska utlämnandeordern. Eventuella senare ändringar av bosättning bör inte påverka förfarandet. Den berörda personen bör kunna åberopa sina rättigheter samt reglerna om fastställande och begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet och yttrandefrihet i andra medier under hela det straffrättsliga förfarandet, och den verkställande myndigheten bör kunna åberopa en vägransgrund om det i undantagsfall, på grundval av specifika och objektiva uppgifter, finns goda skäl att anta att ett fullföljande av ordern, mot bakgrund av de särskilda omständigheterna i ärendet, skulle innebära ett uppenbart åsidosättande av en relevant grundläggande rättighet enligt artikel 6 i EU-fördraget och stadgan. Dessutom bör det vara möjligt att åberopa dessa grunder under verkställighetsförfarandet.
- (55) En europeisk utlämnandeorder bör översändas genom ett intyg om en europeisk utlämnandeorder, och en europeisk bevarandeorder bör översändas genom ett intyg om en europeisk bevarandeorder. Om det behövs bör intyget om en europeisk utlämnandeorder eller intyget om en europeisk bevarandeorder översättas till ett av unionens officiella språk som godtas av mottagaren. Om tjänsteleverantören inte har angett något språk bör intyget om en europeisk utlämnandeorder eller intyget om en europeisk bevarandeorder översättas till ett officiellt språk i den medlemsstat där det utsedda verksamhetsstället eller tjänsteleverantörens rättsliga ombud befinner sig, eller till ett annat officiellt språk som det utsedda verksamhetsstället eller tjänsteleverantörens rättsliga ombud har uppgett att det godtar. Om en anmälan till den verkställande myndigheten krävs enligt denna förordning bör det intyg om en europeisk utlämnandeorder som ska översändas till den myndigheten översättas till ett officiellt språk i den verkställande staten eller till ett annat av unionens officiella språk som godtas av den staten. I detta avseende bör varje medlemsstat uppmuntras att när som helst i en skriftlig förklaring till kommissionen ange om och på vilket eller vilka av unionens officiella språk utöver det eller de officiella språken i den egna medlemsstaten som de godtar översättningar av intyg om en europeisk utlämnandeorder och intyg om en europeisk bevarandeorder. Kommissionen bör göra sådana förklaringar tillgängliga för samtliga medlemsstater och för det europeiska rättsliga nätverket.
- (56) Om ett intyg om en europeisk utlämnandeorder har utfärdats och en anmälan till den verkställande myndigheten inte krävs enligt denna förordning bör mottagaren vid mottagandet av intyget säkerställa att de begärda uppgifterna översänds direkt till den utfärdande myndigheten eller de i intyget angivna brottsbekämpande myndigheterna senast tio dagar efter mottagandet av intyget. Om det enligt denna förordning krävs en anmälan till den verkställande myndigheten vid mottagandet av intyget om en europeisk utlämnandeorder bör tjänsteleverantören agera skyndsamt för att bevara uppgifterna. Om den verkställande myndigheten inte har åberopat några vägransgrunder enligt denna förordning inom tio dagar efter mottagandet av intyget om en europeisk utlämnandeorder bör mottagaren säkerställa att de begärda uppgifterna direkt översänds till den utfärdande myndigheten eller de i intyget angivna brottsbekämpande myndigheterna vid utgången av den tiodagarsperioden. Om den verkställande myndigheten, redan före utgången av tiodagarsperioden, bekräftar för den utfärdande myndigheten och

mottagaren att den inte kommer att återropa någon vägransgrund bör mottagaren agera så snart som möjligt efter en sådan bekräftelse och senast vid utgången av denna tiodagarsperiod. De kortare tidsfrister som är tillämpliga i nödsituationer enligt definitionen i denna förordning bör respekteras av mottagaren och, i tillämpliga fall, av den verkställande myndigheten. Mottagaren och, i tillämpliga fall, den verkställande myndigheten bör fullfölja intyget om en europeisk utlämnandeorder så snart som möjligt, inom de tidsfrister som fastställs i denna förordning, med största möjliga beaktande av de processuella tidsfrister och andra tidsfrister som anges av den utfärdande staten.

- (57) Om mottagaren, enbart på grundval av informationen i intyget om en europeisk utlämnandeorder eller i intyget om en europeisk bevarandeorder, anser att fullföljandet av intyget om en europeisk utlämnandeorder eller intyget om en europeisk bevarandeorder skulle kunna inkräkta på immunitet eller privilegier, eller på regler om fastställande eller begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet eller yttrandefrihet i andra medier, enligt rätten i den verkställande staten, bör mottagaren informera den utfärdande myndigheten och den verkställande myndigheten. När det gäller intyg om en europeisk utlämnandeorder bör den utfärdande myndigheten, om ingen anmälan till den verkställande myndigheten har skett enligt denna förordning, beakta den information som mottagits från mottagaren och, på eget initiativ eller på begäran av den verkställande myndigheten, besluta huruvida den europeiska utlämnandeordern ska återkallas, anpassas eller upprätthållas. Om en anmälan till den verkställande myndigheten har skett enligt denna förordning bör den utfärdande myndigheten beakta den information som mottagits från mottagaren och besluta huruvida den europeiska utlämnandeordern ska återkallas, anpassas eller upprätthållas. Det bör också vara möjligt för den verkställande myndigheten att återropa de vägransgrunder som anges i denna förordning.
- (58) För att göra det möjligt för mottagaren att hantera formella problem med ett intyg om en europeisk utlämnandeorder eller ett intyg om en europeisk bevarandeorder är det nödvändigt att upprätta ett kommunikationsförfarande mellan mottagaren och den utfärdande myndigheten samt, om en anmälan till den verkställande myndigheten har gjorts enligt denna förordning, mellan mottagaren och den verkställande myndigheten, i de fall där intyget om en europeisk utlämnandeorder eller intyget om en europeisk bevarandeorder är ofullständigt, innehåller uppenbara fel eller inte innehåller tillräcklig information för att fullfölja den berörda ordern. Om mottagaren av andra skäl inte tillhandahåller informationen på ett uttömmande sätt eller inom angiven tid, till exempel eftersom den anser att det strider mot en skyldighet enligt rätten i ett tredjeland eller eftersom den anser att den europeiska utlämnandeordern eller den europeiska bevarandeordern inte har utfärdats i enlighet med de villkor som fastställs i denna förordning, bör den informera den utfärdande myndigheten samt, om en anmälan till den verkställande myndigheten gjorts, den verkställande myndigheten och tillhandahålla motiveringar till att intyget om den europeiska utlämnandeordern eller intyget om den europeiska bevarandeordern inte fullföljts inom angiven tid. Kommunikationsförfarandet bör alltså göra det möjligt för den utfärdande myndigheten att korrigera eller ompröva den europeiska utlämnandeordern eller den europeiska bevarandeordern i ett tidigt skede. För att garantera att de begärda uppgifterna finns tillgängliga bör mottagaren bevara dessa uppgifter om den mottagaren kan identifiera dessa uppgifter.
- (59) Mottagaren bör inte vara skyldig att efterleva den europeiska utlämnandeordern eller den europeiska bevarandeordern om det föreligger en faktisk omöjlighet till följd av omständigheter som inte beror på mottagaren eller, om den inte är densamme, tjänsteleverantören vid den tidpunkt då den europeiska utlämnandeordern eller den europeiska bevarandeordern mottogs. En faktisk omöjlighet ska anses föreligga om den person vars uppgifter begärs inte är kund hos tjänsteleverantören eller inte kan identifieras som kund ens efter en framställan om ytterligare information till den utfärdande myndigheten, eller om uppgifterna lagenligt raderades innan ordern mottogs.
- (60) Vid mottagande av ett intyg om en europeisk bevarandeorder bör mottagaren bevara de begärda uppgifterna i högst 60 dagar, såvida inte den utfärdande myndigheten bekräftar att en efterföljande framställan om utlämnande har utfärdats, varvid bevarandet bör fortsätta. Den utfärdande myndigheten bör kunna förlänga bevarandeperioden med ytterligare 30 dagar om det är nödvändigt för att göra det möjligt att utfärda en efterföljande framställan om utlämnande, med hjälp av det formulär som anges i denna förordning. Om den utfärdande myndigheten under tidsperioden för bevarande bekräftar att en efterföljande framställan om utlämnande har utfärdats bör mottagaren bevara uppgifterna så länge som det krävs för att lämna ut uppgifterna när den efterföljande framställan om utlämnande har mottagits. En sådan bekräftelse bör sändas till mottagaren inom den relevanta tidsfristen, på ett av den verkställande statens officiella språk eller på något annat språk som godtas av mottagaren, med hjälp av det formulär som anges i denna förordning. För att förhindra att bevarandet upphör bör det vara tillräckligt att den efterföljande framställan om utlämnande har utfärdats och att bekräftelsen har skickats av den utfärdande myndigheten. Det bör inte vara nödvändigt att fullgöra ytterligare formaliteter som krävs för översändandet, såsom översättning av handlingar, vid den tidpunkten. Om det inte längre är nödvändigt att bevara uppgifterna bör den utfärdande myndigheten informera mottagaren utan onödigt dröjsmål, varvid bevarandeskyldigheten på grundval av den europeiska bevarandeorderns bör upphöra.

- (61) Utan hinder av principen om ömsesidigt förtroende bör det vara möjligt för den verkställande myndigheten att åberopa skäl för att vägra en europeisk utlämnandeorder, om en anmälan till den verkställande myndigheten har skett enligt denna förordning, på grundval av den förteckning över vägransgrunder som föreskrivs i denna förordning. Om en anmälan till den verkställande myndigheten, eller verkställigheten, sker i enlighet med denna förordning, kan den verkställande staten föreskriva i nationell rätt att verkställigheten av en europeisk utlämnandeorder skulle kunna kräva att en domstol involveras i förfarandet i den verkställande staten.
- (62) Om den verkställande myndigheten mottar en anmälan om en europeisk utlämnandeorder för att inhämta trafikuppgifter, med undantag för uppgifter som begärs med det enda syftet att identifiera användaren, enligt definitionen i denna förordning, eller för att inhämta innehållsdata, bör den ha rätt att bedöma den information som anges i ordern och, i förekommande fall, vägra ordern om den, på grundval av en obligatorisk och vederbörlig analys av informationen i den ordern och i enlighet med tillämpliga regler i unionens primärrätt, särskilt stadgan, bedömer att en eller flera av de vägransgrunder som föreskrivs i denna förordning kan åberopas. Nödvändigheten av att respektera de rättsliga myndigheternas oberoende kräver att dessa myndigheter ges ett visst utrymme för skönsmässig bedömning när de fattar beslut om vägransgrunderna.
- (63) Det bör vara möjligt för den verkställande myndigheten, om den mottar en anmälan enligt denna förordning, att vägra en europeisk utlämnandeorder om de uppgifter som begärs skyddas av immunitet eller privilegier som beviljas enligt den verkställande statens rätt och som förhindrar att den europeiska utlämnandeordern fullföljs eller verkställs, eller de begärda uppgifterna omfattas av reglerna för fastställande eller begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet eller yttrandefrihet i andra medier och som förhindrar att den europeiska utlämnandeordern fullföljs eller verkställs.
- (64) Det bör i undantagsfall vara möjligt för den verkställande myndigheten att vägra en order, om det finns goda skäl att anta, på grundval av precisa och objektiva uppgifter, att fullföljandet av den europeiska utlämnandeordern, mot bakgrund av de särskilda omständigheterna i ärendet, skulle innebära ett uppenbart åsidosättande av en relevant grundläggande rättighet enligt artikel 6 i EU-fördraget och stadgan. Vid bedömningen av denna vägransgrund, om den verkställande myndigheten förfogar över bevis eller uppgifter, till exempel uppgifter som återfinns i ett motiverat förslag från en tredjedel av medlemsstaterna, Europaparlamentet eller kommissionen som antagits enligt artikel 7.1 i EU-fördraget, som visar att det finns en verklig risk, om ordern fullföljs, för ett allvarligt åsidosättande av den grundläggande rätten till ett effektivt rättsmedel och till en opartisk domstol enligt artikel 47 i stadgan, på grund av systematiska eller allmänna brister i fråga om domstolsväsendets oavhängighet i den utfärdande staten, bör den verkställande myndigheten i synnerhet göra en konkret, precis prövning av om det med hänsyn till den berörda personens personliga situation samt arten av det brott för vilket det straffrättsliga förfarandet genomförs och de faktiska förhållanden som ligger till grund för ordern, och mot bakgrund av de uppgifter som lämnats av den utfärdande myndigheten, finns välgrundade skäl att anta att det föreligger en verklig risk att en persons rätt till en opartisk domstol åsidosätts.
- (65) Det bör vara möjligt för den verkställande myndigheten att vägra en order ifall fullföljandet av en sådan order skulle strida mot principen *ne bis in idem*.
- (66) Det bör vara möjligt för den verkställande myndigheten, om den mottar en anmälan enligt denna förordning, att vägra en europeisk utlämnandeorder om den gärning för vilken ordern har utfärdats inte utgör ett brott enligt den verkställande statens rätt, såvida det inte gäller ett brott som förtecknas i de brottskategorier som anges i en bilaga till denna förordning, enligt uppgift från den utfärdande myndigheten i intyget om en europeisk utlämnandeorder, om maximistraffet för gärningen i fråga i den utfärdande staten är fängelse eller annan frihetsberövande åtgärd i minst tre år.
- (67) Eftersom information till den person vars uppgifter begärs är en nödvändig förutsättning när det gäller att upprätthålla rätten till skydd av personuppgifter och rätten till försvar, för att få till stånd effektiv granskning och rättslig prövning, i enlighet med artikel 6 i EU-fördraget och stadgan, bör den utfärdande myndigheten utan onödigt dröjsmål informera den person vars uppgifter begärs om utlämnandet av uppgifter på grundval av en europeisk utlämnandeorder. Den utfärdande myndigheten bör dock, i enlighet med nationell rätt, kunna skjuta upp eller begränsa informationen eller underlåta att informera den person vars uppgifter begärs, i den mån och så länge som villkoren i direktiv (EU) 2016/680 är uppfyllda, i vilket fall den utfärdande myndigheten i ärendet bör ange skälen till uppskjutandet, begränsningen eller underlåtelserna och lägga till en kort motivering i intyget om en europeisk utlämnandeorder. Mottagarna och, om de inte är desamma, tjänsteleverantörerna bör vidta de senaste operativa och tekniska åtgärder som krävs för att säkerställa konfidentialiteten, sekretessen och integriteten för intyget om en europeisk utlämnandeorder eller intyget om en europeisk bevarandeorder och för de uppgifter som lämnas ut eller bevaras.

- (68) Det bör vara möjligt för en tjänsteleverantör att begära ersättning för sina kostnader för att svara på en europeisk utlämnandeorder eller en europeisk bevarandeorder från den utfärdande staten, om denna möjlighet föreskrivs i den utfärdande statens nationella rätt för inhemska förelägganden i liknande situationer, i enlighet med den statens nationella rätt. Medlemsstaterna bör informera kommissionen om sina nationella regler för ersättning, och kommissionen bör offentliggöra dem. I denna förordning föreskrivs särskilda regler för ersättning av kostnader i samband med det decentraliserade it-systemet.
- (69) Utan att det påverkar tillämpningen av nationell rätt som föreskriver straffrättsliga påföljder bör medlemsstaterna fastställa regler om sanktionsavgifter som är tillämpliga på överträdelse av denna förordning och vidta alla nödvändiga åtgärder för att säkerställa att de genomförs. Medlemsstaterna bör säkerställa att sanktionsavgifter enligt deras nationella rätt är effektiva, proportionella och avskräckande. Medlemsstaterna bör utan dröjsmål meddela kommissionen dessa regler och åtgärder och utan dröjsmål informera den om eventuella ändringar som berör dem.
- (70) Vid bedömningen av lämpliga sanktionsavgifter i ett enskilt fall bör den behöriga myndigheten beakta alla relevanta omständigheter, såsom överträdelsens art, allvarlighetsgrad och varaktighet, huruvida den begicks uppsätligen eller genom försummelse, huruvida tjänsteleverantören har hållits ansvarig för liknande tidigare överträdelse och den finansiella styrkan hos den tjänsteleverantör som hålls ansvarig. I undantagsfall kan den bedömningen leda till att den verkställande myndigheten beslutar att avstå från att ålägga sanktionsavgifter. I detta avseende ska särskild hänsyn tas till mikroföretag som underlåter att efterleva en europeisk utlämnandeorder eller en europeisk bevarandeorder i en nödsituation på grund av bristande personalresurser utanför kontorstid, om uppgifterna överförs utan onödigt dröjsmål.
- (71) Utan att det påverkar deras dataskyddsskyldigheter bör tjänsteleverantörer inte hållas ansvariga i medlemsstaterna för olägenheter som orsakas deras användare eller tredje parter uteslutande till följd av att de i god tro efterlever ett intyg om en europeisk utlämnandeorder eller ett intyg om en europeisk bevarandeorder. Ansvaret för att säkerställa att den berörda ordern är laglig, särskilt att den är nödvändig och proportionell, bör ligga hos den utfärdande myndigheten.
- (72) Om mottagaren inte efterlever intyget om en europeisk utlämnandeorder inom tidsfristen eller intyget om en europeisk bevarandeorder utan att ange orsaker som godtas av den utfärdande myndigheten, och, i tillämpliga fall, om den verkställande myndigheten inte har åberopat någon av vägransgrunderna enligt denna förordning, bör det vara möjligt för den utfärdande myndigheten att begära att den verkställande myndigheten verkställer den europeiska utlämnandeordern eller den europeiska bevarandeordern. I detta syfte bör den utfärdande myndigheten översända den berörda ordern, den relevanta formulär som föreskrivs i denna förordning ifyllt av mottagaren och alla relevanta handlingar till den verkställande myndigheten. Den utfärdande myndigheten bör översända den berörda ordern och alla handlingar som ska översändas till ett av de språk som godtas av den verkställande staten och bör informera mottagaren om översändandet. Den staten bör verkställa den berörda ordern i enlighet med sin nationella rätt.
- (73) Verkställighetsförfarandet bör göra det möjligt för mottagaren att åberopa skäl mot verkställigheten på grundval av en förteckning över särskilda grunder som anges i denna förordning, inbegripet att den berörda ordern inte har utfärdats eller godkänts av en behörig myndighet enligt denna förordning, eller om ordern inte avser uppgifter som lagrats av tjänsteleverantören eller på dennes vägnar vid tidpunkten för mottagandet av det relevanta intyget. Den verkställande myndigheten bör kunna vägra att erkänna och verkställa en europeisk utlämnandeorder eller en europeisk bevarandeorder på samma grunder och även, i undantagsfall, på grund av ett uppenbart åsidosättande av en relevant grundläggande rättighet enligt artikel 6 i EU-fördraget och stadgan. Den verkställande myndigheten bör samråda med den utfärdande myndigheten innan den beslutar att inte erkänna eller inte verkställa ordern på dessa grunder. Om mottagaren inte fullgör sina skyldigheter enligt en erkänd europeisk utlämnandeorder eller europeisk bevarandeorder vars verkställbarhet har bekräftats av den verkställande myndigheten, bör den myndigheten ålägga en sanktionsavgift. Sanktionsavgiften bör vara proportionella, i synnerhet med tanke på särskilda omständigheter såsom upprepad eller systematisk bristande efterlevnad.
- (74) Efterlevnad av en europeisk utlämnandeorder skulle kunna strida mot en skyldighet enligt ett tredjelands tillämpliga rätt. För att säkerställa samförstånd i fråga om tredjeländers suveräna intressen, skydda den berörda personen och hantera tjänsteleverantörers motstridiga skyldigheter, föreskriver denna förordning en särskild mekanism för rättslig prövning om efterlevnad av en europeisk utlämnandeorder skulle hindra en tjänsteleverantör från att fullgöra rättsliga skyldigheter enligt rätten i ett tredjeland.

- (75) Om en mottagare som anser att en europeisk utlämnandeorder i ett visst fall skulle medföra en överträdelse av en rättslig skyldighet enligt rätten i ett tredjeland bör den informera den utfärdande myndigheten och den verkställande myndigheten om grunderna till att inte fullfölja ordern genom en motiverad invändning med hjälp av det formulär som tillhandahålls i denna förordning. Den utfärdande myndigheten bör ompröva den europeiska utlämnandeordern mot bakgrund av den motiverade invändningen och eventuella synpunkter från den verkställande staten, med beaktande av samma kriterier som behörig domstol i den utfärdande staten skulle tvingas följa. Om den utfärdande myndigheten har för avsikt att upprätthålla ordern bör den begära granskning av behörig domstol i den utfärdande staten, enligt den berörda medlemsstatens anmälan, som bör granska ordern.
- (76) När den behöriga domstolen avgör om det föreligger en motstridig skyldighet i de särskilda omständigheterna i det aktuella ärendet kan den förlita sig på lämplig extern sakkunskap när så behövs, till exempel om tolkningen av rätten i det berörda tredjelandet. I detta syfte skulle den behöriga domstolen till exempel kunna samråda med centralmyndigheten i tredjelandet, med beaktande av direktiv (EU) 2016/680. Den utfärdande staten bör särskilt begära information från den behöriga myndigheten i tredjelandet om konflikten rör grundläggande rättigheter eller andra grundläggande intressen i tredjelandet som rör nationell säkerhet och försvar.
- (77) Sakkunskap om tolkning skulle också kunna tillhandahållas genom expertutlåtanden, om sådana finns tillgängliga. Information och rättspraxis avseende tolkningen av ett tredjelandets rätt och om förfaranden för lagvalskonflikter i medlemsstaterna bör göras tillgänglig på en central plattform såsom Sirius-projektet eller det europeiska rättsliga nätverket, för att göra det möjligt att dra nytta av erfarenheter och sakkunskap som samlats in om samma eller liknande frågor. Tillgången till sådan information på en central plattform bör inte förhindra ett förnyat samråd med tredjelandet i tillämpliga fall.
- (78) Vid bedömningen av huruvida motstridiga skyldigheter föreligger bör den behöriga domstolen avgöra om tredjelandets rätt är tillämplig och, om så är fallet, om tredjelandets rätt förhindrar röjande av de berörda uppgifterna. Om den behöriga domstolen anser att tredjelandets rätt förhindrar röjande av de berörda uppgifterna bör den domstolen bedöma huruvida den europeiska utlämnandeordern ska upprätthållas eller upphävas, genom att väga ett antal element som är avsedda att avgöra hur stark anknytningen till endera av de två berörda jurisdiktionerna, intressena av att inhämta respektive förhindra röjandet av uppgifterna samt möjliga konsekvenser för mottagaren eller för tjänsteleverantören om den rättar sig efter ordern. Det bör läggas särskild betydelse och vikt vid skyddet av de grundläggande rättigheterna enligt tredjelandets relevanta rätt och andra grundläggande intressen, såsom tredjelandets nationella säkerhetsintressen och graden av anknytning mellan brottmålet och endera av de två jurisdiktionerna när bedömningen genomförs. Om domstolen beslutar att upphäva ordern bör den informera den utfärdande myndigheten och mottagaren. Om den behöriga myndigheten beslutar att ordern ska upprätthållas bör den informera den utfärdande myndigheten och mottagaren, och den mottagaren bör fullfölja ordern i fråga. Den utfärdande myndigheten bör informera den verkställande myndigheten om resultatet av prövningsförfarandet.
- (79) De villkor som anges i denna förordning för fullföljande av ett intyg om en europeisk utlämnandeorder bör även tillämpas i händelse av motstridiga skyldigheter som följer av ett tredjelandets rätt. Under den rättsliga prövningen, i fall där efterlevnaden av en europeisk utlämnandeorder skulle hindra tjänsteleverantörer från att fullgöra en rättslig skyldighet som följer av ett tredjelandets rätt, bör därför de uppgifter som begärs i den ordern bevaras. Om den behöriga domstolen efter en rättslig prövning beslutar att upphäva en europeisk utlämnandeorder bör det vara möjligt att utfärda en europeisk bevarandeorder för att göra det möjligt för den utfärdande myndigheten att begära utlämnande av uppgifterna via andra kanaler, såsom ömsesidig rättslig hjälp.
- (80) Det är viktigt att alla personer vars uppgifter begärs inom ramen för brottsutredningar eller straffrättsliga förfaranden har tillgång till ett effektivt rättsmedel i enlighet med artikel 47 i stadgan. I linje med det kravet och utan att det påverkar andra rättsmedel som finns att tillgå enligt nationell rätt bör varje person vars uppgifter har begärts genom en europeisk utlämnandeorder ha rätt till effektiva rättsmedel mot den ordern. Om personen i fråga är en misstänkt eller tilltalad bör vederbörande ha rätt till effektiva rättsmedel under det straffrättsliga förfarande i vilket uppgifterna används som bevis. Rätten till effektiva rättsmedel bör utövas vid en domstol i den utfärdande staten i enlighet med dess nationella rätt och bör inbegripa möjligheten att ifrågasätta åtgärdens lagenlighet, inklusive dess nödvändighet och proportionalitet, utan att det påverkar garantierna för de grundläggande rättigheterna i den verkställande staten, eller andra rättsmedel i enlighet med nationell rätt. Denna förordning bör inte begränsa de möjliga skälen att ifrågasätta lagenligheten av en order. Den rätt till effektiva rättsmedel som föreskrivs i denna förordning bör inte påverka rätten att söka rättsmedel enligt förordning (EU) 2016/679 och direktiv (EU) 2016/680. Information bör ges i god tid om möjligheterna enligt nationell rätt att söka rättsmedel, och det bör säkerställas att de kan utövas på ett effektivt sätt.

- (81) Lämpliga kanaler bör utvecklas för att säkerställa att alla parter på ett effektivt sätt kan samarbeta digitalt genom ett decentraliserat it-system som möjliggör ett snabbt, direkt, interoperabelt, hållbart, tillförlitligt och säkert gränsöverskridande elektroniskt utbyte av ärendelaterade formulär, uppgifter och tillhörande information.
- (82) För att möjliggöra effektiv och säker skriftlig kommunikation mellan behöriga myndigheter och utsedda verksamhetsställen eller tjänsteleverantörers rättsliga ombud enligt denna förordning bör dessa utsedda verksamhetsställen respektive rättsliga ombud förses med elektroniska medel för åtkomst till de nationella it-system som ingår i det decentraliserade it-systemet och som drivs av medlemsstaterna.
- (83) Det decentraliserade it-systemet bör omfatta medlemsstaternas samt unionsbyråernas och unionsorganens it-system, och interoperabla åtkomstpunkter som dessa it-system är sammankopplade genom. Åtkomstpunkterna i det decentraliserade it-systemet bör baseras på e-Codex-systemet, som inrättades genom Europaparlamentets och rådets förordning (EU) 2022/850 ⁽²⁴⁾.
- (84) Tjänsteleverantörer som använder skräddarsydda it-lösningar för utbyte av information och uppgifter som rör framställningar om elektroniska bevis bör förses med automatiserade medel för åtkomst till de decentraliserade it-systemen med hjälp av en gemensam standard för utbyte av uppgifter.
- (85) Som regel bör all skriftlig kommunikation mellan behöriga myndigheter eller mellan behöriga myndigheter och utsedda verksamhetsställen eller rättsliga ombud ske via det decentraliserade it-systemet. Det bör vara möjligt att använda alternativa medel endast om det inte är möjligt att använda det decentraliserade it-systemet, till exempel på grund av särskilda kriminaltekniska krav, på grund av att den mängd uppgifter som ska överföras hämmas av begränsningar av den tekniska kapaciteten eller på grund av att ett annat verksamhetsställe, som inte är anslutet till det decentraliserade it-systemet, måste ingå bland mottagarna i en nödsituation. I sådana fall bör överföringen ske på lämpligast möjliga alternativa sätt, med beaktande av behovet att säkerställa ett snabbt, säkert och tillförlitligt informationsutbyte.
- (86) För att säkerställa att det decentraliserade it-systemet innehåller en fullständig förteckning över skriftlig kommunikation enligt denna förordning bör all överföring som sker på alternativa sätt registreras i det decentraliserade it-systemet utan onödigt dröjsmål.
- (87) Användning av mekanismer för att säkerställa äkthet – som föreskrivs i Europaparlamentets och rådets förordning (EU) nr 910/2014 ⁽²⁵⁾ – bör övervägas.
- (88) Tjänsteleverantörer, särskilt små och medelstora företag, bör inte belastas med oproportionerliga kostnader i förhållande till inrättandet och driften av det decentraliserade it-systemet. Som en del av skapandet, underhållet och utvecklingen av referensprogramvaran bör kommissionen därför också tillhandahålla ett webbaserat gränssnitt som gör det möjligt för tjänsteleverantörer att kommunicera säkert med myndigheterna utan att behöva inrätta en egen särskild infrastruktur för att få åtkomst till det decentraliserade it-systemet.
- (89) Det bör vara möjligt för medlemsstaterna att använda den programvara som utvecklats av kommissionen, närmare bestämt referensprogramvaran, i stället för ett nationellt it-system. Den referensprogramvaran bör baseras på en modulstruktur, vilket innebär att programvaran paketeras och levereras separat från de e-Codex-komponenter som behövs för att ansluta den till det decentraliserade it-systemet. Denna struktur bör göra det möjligt för medlemsstaterna att återanvända eller förbättra respektive befintliga nationella infrastruktur för rättslig kommunikation för gränsöverskridande användning.
- (90) Kommissionen bör ansvara för att skapa, underhålla och utveckla referensprogramvaran. Kommissionen bör utforma, utveckla och underhålla referensprogramvaran i enlighet med de krav och principer för dataskydd som fastställs i Europaparlamentets och rådets förordning (EU) 2018/1725 ⁽²⁶⁾, förordning (EU) 2016/679 och direktiv (EU) 2016/680, särskilt principerna om inbyggt dataskydd och dataskydd som standard samt en hög cybersäkerhetsnivå. Det är viktigt att referensprogramvaran även innehåller lämpliga tekniska åtgärder för – och gör det möjligt – att vidta de organisatoriska åtgärder som krävs för att säkerställa en adekvat nivå av säkerhet och interoperabilitet.

⁽²⁴⁾ Europaparlamentets och rådets förordning (EU) 2022/850 av den 30 maj 2022 om ett datoriserat system för gränsöverskridande elektroniskt utbyte av uppgifter på området civil- och straffrättsligt samarbete (e-Codex-systemet) och om ändring av förordning (EU) 2018/1726 (EUT L 150, 1.6.2022, s. 1).

⁽²⁵⁾ 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).

⁽²⁶⁾ 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).

- (91) För att säkerställa enhetliga villkor för genomförandet av denna förordning bör kommissionen tilldelas genomförandebefogenheter. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011⁽²⁷⁾.
- (92) För utbyte av uppgifter som utförs via det decentraliserade it-systemet eller registreras i det decentraliserade it-systemet bör medlemsstaterna kunna samla in statistik för att fullgöra sina övervaknings- och rapporterings-skyldigheter enligt denna förordning via sina nationella portaler.
- (93) För att övervaka denna förordnings utfall, resultat och effekter bör kommissionen offentliggöra en årsrapport om det föregående kalenderåret på grundval av uppgifter som erhållits från medlemsstaterna. För detta ändamål bör medlemsstaterna samla in och förse kommissionen med omfattande statistik om olika aspekter av denna förordning, per typ av uppgifter som begärs, mottagare och huruvida det var en nödsituation eller inte.
- (94) Användningen av redan översatta och standardiserade formulär skulle underlätta samarbetet och informationsutbytet enligt denna förordning och därigenom möjliggöra snabbare och effektivare kommunikation på ett användarvänligt sätt. Sådana formulär skulle minska översättningskostnaderna och bidra till en hög kvalitetsstandard för kommunikation. Svarsformulär skulle likaledes möjliggöra ett standardiserat informationsutbyte, i synnerhet i de fall där tjänsteleverantörerna inte kan tillmötesgå framställan eftersom användarkontot inte existerar eller det inte finns några tillgängliga uppgifter. De formulär som föreskrivs i denna förordning skulle också underlätta insamlingen av statistik.
- (95) I syfte att effektivt hantera eventuella behov av förbättringar när det gäller innehållet i intyg om en europeisk utlämnandeorder och intyg om en europeisk bevarandeorder och de formulär som ska användas för att meddela att det inte är möjligt att fullfölja ett intyg om en europeisk utlämnandeorder eller ett intyg om en europeisk bevarandeorder, i syfte att bekräfta utfärdandet av en framställan om utlämnande till följd av en europeisk bevarandeorder och i syfte att förlänga bevarandet av elektroniska bevis, bör befogenheten att anta akter i enlighet med artikel 290 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) delegeras till kommissionen med avseende på ändringar av de formulär som föreskrivs i denna förordning. 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⁽²⁸⁾. 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.
- (96) Denna förordning bör inte påverka unionens eller andra internationella instrument, avtal och överenskommelser avseende bevisinhämtning som omfattas av denna förordnings tillämpningsområde. Medlemsstaternas myndigheter bör välja det verktyg som är bäst lämpat för det aktuella ärendet. I vissa fall kan de föredra att använda unionens och andra internationella instrument, avtal och överenskommelser när de begär flera olika typer av utredningsåtgärder som inte är begränsade till utlämnande av elektroniska bevis från en annan medlemsstat. Medlemsstaterna bör meddela kommissionen senast tre år efter denna förordnings ikraftträdande om de befintliga instrument, avtal och överenskommelser som avses i denna förordning och som de fortsatt kommer att tillämpa. Medlemsstaterna bör också inom tre månader efter att de har undertecknat nya avtal eller överenskommelser som avses i denna förordning meddela kommissionen om detta.
- (97) Med tanke på den tekniska utvecklingen skulle nya former av kommunikationsverktyg kunna användas om några år, eller så skulle det kunna uppstå luckor i tillämpningen av denna förordning. Det är därför viktigt att föreskriva en utvärdering av dess tillämpning.
- (98) Kommissionen bör göra en utvärdering av denna förordning som bör grunda sig på de fem kriterierna effektivitet, ändamålsenlighet, relevans, enhetlighet och mervärde för EU, och den utvärderingen bör ligga till grund för konsekvensbedömningar av eventuella ytterligare åtgärder. Utvärderingsrapporten bör innehålla en bedömning av tillämpningen av denna förordning och av de resultat som har uppnåtts med avseende på dess mål samt en bedömning av denna förordnings inverkan på de grundläggande rättigheterna. Kommissionen bör regelbundet samla in information för utvärderingen av denna förordning.

⁽²⁷⁾ 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).

⁽²⁸⁾ EUT L 123, 12.5.2016, s. 1.

- (99) Eftersom målet för denna förordning, nämligen att förbättra säkrande och inhämtande av elektroniska bevis över gränserna, på grund av dess gränsoverskridande karaktär inte i tillräcklig utsträckning kan uppnås av medlemsstaterna, utan snarare kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i EU-fördraget. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.
- (100) I enlighet med artikel 3 i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till EU-fördraget och EUF-fördraget, har Irland meddelat att det önskar delta i antagandet och tillämpningen av denna förordning.
- (101) I enlighet med artiklarna 1 och 2 i protokoll nr 22 om Danmarks ställning, fogat till EU-fördraget och EUF-fördraget, deltar Danmark inte i antagandet av denna förordning, som inte är bindande för eller tillämplig på Danmark.
- (102) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i förordning (EU) 2018/1725 och avgav ett yttrande den 6 november 2019 ⁽²⁹⁾.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

INNEHÅLL, TILLÄMPNINGSOMRÅDE OCH DEFINITIONER

Artikel 1

Innehåll

1. I denna förordning fastställs regler enligt vilka en myndighet i en medlemsstat i straffrättsliga förfaranden får utfärda en europeisk utlämnandeorder eller en europeisk bevarandeorder och därigenom beordra en tjänsteleverantör som erbjuder tjänster i unionen och som har ett verksamhetsställe i en annan medlemsstat, eller, om den inte har något verksamhetsställe, är representerad av ett rättsligt ombud i en annan medlemsstat, att lämna ut eller att bevara elektroniska bevis, oavsett var uppgifterna finns.

Denna förordning påverkar inte de nationella myndigheternas befogenheter att rikta sig till tjänsteleverantörer som har ett verksamhetsställe eller är representerade på deras territorium i syfte att säkerställa att dessa följer nationella åtgärder liknande dem som avses i första stycket.

2. Utfärdande av en europeisk utlämnandeorder eller en europeisk bevarandeorder får också begäras av en misstänkt eller en tilltalad, eller av en försvarare för denna persons räkning, inom ramen för de rättigheter som är tillämpliga på försvaret och i överensstämmelse med nationell straffprocessrätt.

3. Denna förordning får inte medföra någon ändring av skyldigheten att respektera de grundläggande rättigheter och rättsprinciper som återges i stadgan och i artikel 6 i EU-fördraget, och alla skyldigheter som är tillämpliga på brottsbekämpande myndigheter eller rättsliga myndigheter i detta avseende ska kvarstå opåverkade. Denna förordning ska tillämpas utan att det påverkar tillämpningen av grundläggande principer, särskilt yttrande- och informationsfriheten, inbegripet mediernas frihet och mångfald, respekten för privatlivet och familjelivet, skyddet av personuppgifter och rätten till ett effektivt rättsligt skydd.

Artikel 2

Tillämpningsområde

1. Denna förordning är tillämplig på tjänsteleverantörer som erbjuder tjänster i unionen.

2. Europeiska utlämnandeorder och europeiska bevarandeorder får utfärdas endast inom ramen för, och för tillämpning i, straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd i minst fyra månader – till följd av straffrättsliga förfaranden – som inte beslutats genom en dom där personen inte var personligen närvarande vid förhandlingen, i fall där den dömda personen undandragit sig lagföring. Sådana order får också utfärdas i förfaranden som rör brott för vilka en juridisk person skulle kunna ställas till ansvar eller bestraffas i den utfärdande staten.

3. Europeiska utlämnandeorder och europeiska bevarandeorder får utfärdas endast för uppgifter som hänför sig till de tjänster som avses i artikel 3.3 och som erbjuds i unionen.

4. Denna förordning är inte tillämplig på förfaranden som inletts i syfte att ge en annan medlemsstat eller ett tredjeland ömsesidig rättslig hjälp.

⁽²⁹⁾ EUT C 32, 31.1.2020, s. 11.

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

1. *europensk utlämnandeorder*: ett beslut som förelägger utlämnande av elektroniska bevis vilket utfärdats eller godkänts av en rättslig myndighet i en medlemsstat i enlighet med artikel 4.1, 4.2, 4.4 och 4.5 och riktas till ett utsett verksamhetsställe eller ett rättsligt ombud för en tjänsteleverantör som erbjuder tjänster i unionen, om det utsedda verksamhetsstället eller det rättsliga ombudet befinner sig i en annan medlemsstat som är bunden av denna förordning.
2. *europensk bevarandeorder*: ett beslut som förelägger bevarande av elektroniska bevis i avvaktan på en efterföljande framställan om utlämnande, som utfärdas eller godkänns av en rättslig myndighet i en medlemsstat i enlighet med artikel 4.3, 4.4 och 4.5 och riktas till ett utsett verksamhetsställe eller ett rättsligt ombud för en tjänsteleverantör som erbjuder tjänster i unionen, om det utsedda verksamhetsstället eller det rättsliga ombudet befinner sig i en annan medlemsstat som är bunden av denna förordning.
3. *tjänsteleverantör*: en fysisk eller juridisk person som tillhandahåller en eller flera av följande kategorier av tjänster, med undantag för finansiella tjänster som avses i artikel 2.2 b i Europaparlamentets och rådets direktiv 2006/123/EG⁽³⁰⁾:
 - a) Elektroniska kommunikationstjänster enligt definitionen i artikel 2.4 i direktiv (EU) 2018/1972.
 - b) Tjänster för internetdomännamn och IP-numrering, såsom tjänster för tilldelning av IP-adresser, tjänster för domännamnsregister, tjänster för domännamnsregistratorer och domännamnsrelaterade integritets- och proxytjänster.
 - c) Andra av informationssamhällets tjänster enligt artikel 1.1 b i direktiv (EU) 2015/1535 som
 - i) gör det möjligt för användarna att kommunicera med varandra, eller
 - ii) gör det möjligt att lagra eller på annat sätt behandla uppgifter på uppdrag av de användare till vilka tjänsten tillhandahålls, förutsatt att datalagringen är en väsentlig del av den tjänst som tillhandahålls användaren.
4. *erbjuda tjänster i unionen*:
 - a) att göra det möjligt för fysiska eller juridiska personer i en medlemsstat att använda de tjänster som i punkt 3, och
 - b) att ha en betydande anknytning baserad på specifika faktiska kriterier till den medlemsstat som avses i led a; en sådan betydande anknytning ska anses föreligga om tjänsteleverantören har ett verksamhetsställe i en medlemsstat eller, i avsaknad av ett sådant verksamhetsställe, om det finns ett betydande antal användare i en eller flera medlemsstater eller om verksamheten är inriktad på en eller flera medlemsstater.
5. *verksamhetsställe*: en enhet som de facto utövar en ekonomisk verksamhet under en obegränsad tid genom en stabil infrastruktur varifrån tillhandahållandet av tjänster genomförs eller verksamheten förvaltas.
6. *utsett verksamhetsställe*: ett verksamhetsställe med ställning som juridisk person vilket skriftligen utsetts av en tjänsteleverantör som är etablerad i en medlemsstat, och vilket deltar i ett rättsligt instrument som avses i artikel 1.2 i direktiv (EU) 2023/1544, för de ändamål som avses i artiklarna 1.1 och 3.1 i det direktivet.
7. *rättsligt ombud*: en fysisk eller juridisk person som skriftligen utsetts av en tjänsteleverantör som inte är etablerad i en medlemsstat, och som deltar i ett rättsligt instrument som avses i artikel 1.2 i direktiv (EU) 2023/1544, för de ändamål som avses i artiklarna 1.1 och 3.1 i det direktivet.
8. *elektroniska bevis*: abonnentuppgifter, trafikuppgifter eller innehållsdata som lagras i elektronisk form av en tjänsteleverantör eller på en tjänsteleverantörs vägnar vid tidpunkten för mottagandet av ett intyg om en europeisk utlämnandeorder eller av ett intyg om en europeisk bevarandeorder.

⁽³⁰⁾ Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden (EUT L 376, 27.12.2006, s. 36).

9. *abonnentuppgifter*: alla uppgifter som innehas av en tjänsteleverantör och som rör abonnemang på dennes tjänster, och som avser
 - a) en abonnents eller kunds identitet, såsom angivet namn, födelsedatum, postadress eller geografisk adress, fakturerings- och betalningsuppgifter, telefonnummer eller e-postadress,
 - b) typen av tjänst och dess varaktighet, inbegripet tekniska data och uppgifter om relaterade tekniska åtgärder eller gränssnitt som använts av eller tillhandahållits abonnenten eller kunden vid tidpunkten för den ursprungliga registreringen eller aktiveringen, samt uppgifter som rör valideringen av tjänsteanvändningen, förutom lösenord eller andra autentiseringsmetoder som används i stället för ett lösenord och som tillhandahålls av användaren eller skapas på dennes begäran.
10. *uppgifter som begärs med det enda syftet att identifiera användaren*: IP-adresser och, vid behov, relevanta källportar och tidsstämpel, dvs. datum och tid, eller tekniska motsvarigheter till dessa identifierare och relaterad information, när brottsbekämpande myndigheter eller rättsliga myndigheter begärt detta med det enda syftet att identifiera användaren i en specifik brottsutredning.
11. *trafikuppgifter*: uppgifter som rör tillhandahållandet av en tjänst som erbjuds av en tjänsteleverantör och vilka tjänar till att ge kontext eller ytterligare information om tjänsten samt som genereras eller behandlas av tjänsteleverantörens informationssystem, till exempel källan till eller destinationen för ett meddelande eller en annan typ av interaktion, var utrustningen är belägen, datum, tid, varaktighet, storlek, rutt, format, vilket protokoll som använts och typen av komprimering samt andra metadata från elektronisk kommunikation och uppgifter, med undantag för abonnentuppgifter, som rör inledande och avslutande av en användares åtkomst till en tjänst, såsom datum och tid för användningen, eller inloggning i och utloggning från tjänsten.
12. *innehållsdata*: alla uppgifter i digital form, till exempel text, röst, video, bilder och ljud, med undantag för abonnentuppgifter och trafikuppgifter.
13. *informationssystem*: informationssystem enligt definitionen i artikel 2 a i Europaparlamentets och rådets direktiv 2013/40/EU ⁽³¹⁾.
14. *utfärdande stat*: den medlemsstat i vilken den europeiska utlämnandeordern eller den europeiska bevarandeordern utfärdas.
15. *utfärdande myndighet*: den behöriga myndighet i den utfärdande staten som i enlighet med artikel 4 kan utfärda en europeisk utlämnandeorder eller en europeisk bevarandeorder.
16. *verkställande stat*: den medlemsstat i vilken det utsedda verksamhetsstället är etablerat eller det rättsliga ombudet har sin hemvist och till vilken en europeisk utlämnandeorder och ett intyg om en europeisk utlämnandeorder eller en europeisk bevarandeorder och ett intyg om en europeisk bevarandeorder översänds av den utfärdande myndigheten för anmälan eller för verkställighet i enlighet med denna förordning.
17. *verkställande myndighet*: den myndighet i den verkställande staten som i enlighet med den statens nationella rätt är behörig att ta emot en europeisk utlämnandeorder och ett intyg om en europeisk utlämnandeorder eller en europeisk bevarandeorder och ett intyg om en europeisk bevarandeorder som översänds av den utfärdande myndigheten för anmälan eller för verkställighet i enlighet med denna förordning.
18. *nödsituation*: en situation där det råder ett överhängande hot mot en persons liv, fysiska integritet eller säkerhet eller mot en kritisk infrastruktur enligt definitionen i artikel 2 a i direktiv 2008/114/EG, om en driftsstörning vid eller en förstörelse av sådan kritisk infrastruktur skulle leda till en omedelbar fara för en persons liv, fysiska integritet eller säkerhet, inbegripet genom allvarlig skada på tillhandahållandet av basförmåigheter till befolkningen eller på utövandet av statens kärnfunktioner.
19. *personuppgiftsansvarig*: personuppgiftsansvarig enligt definitionen i artikel 4.7 i förordning (EU) 2016/679.
20. *personuppgiftsbiträde*: personuppgiftsbiträde enligt definitionen i artikel 4.8 i förordning (EU) 2016/679.

⁽³¹⁾ 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).

21. *decentraliserat it-system*: ett nätverk av it-system och interoperabla åtkomstpunkter som drivs under varje medlemsstats, unionsbyrås eller unionsorgans individuella ansvar och förvaltning och möjliggör ett gränsöverskridande utbyte av uppgifter under säkra och tillförlitliga former.

KAPITEL II

EUROPEISK UTLÄMNANDEORDER, EUROPEISK BEVARANDEORDER OCH INTYG

Artikel 4

Utfärdande myndighet

1. En europeisk utlämnandeorder för att inhämta abonnentuppgifter eller inhämta uppgifter som begärts med det enda syftet att identifiera användaren, enligt definitionen i artikel 3.10, får endast utfärdas av
- a) en domare, en domstol, en undersökningsdomare eller en allmän åklagare som är behörig i det berörda ärendet, eller
 - b) en annan behörig myndighet, enligt den utfärdande statens definition, som i det berörda ärendet agerar i egenskap av utredande myndighet i straffrättsliga förfaranden, med behörighet att besluta om bevisinhämtning i enlighet med nationell rätt; i ett sådant ärende ska den europeiska utlämnandeordern, efter granskning av dess överensstämmelse med villkoren för utfärdande av en europeisk utlämnandeorder enligt denna förordning, godkännas av en domare, domstol, undersökningsdomare eller allmän åklagare i den utfärdande staten.
2. En europeisk utlämnandeorder för att inhämta trafikuppgifter, med undantag för uppgifter som begärts med det enda syftet att identifiera användaren enligt definitionen i artikel 3.10, eller inhämta innehållsdata får endast utfärdas av
- a) en domare, en domstol eller en undersökningsdomare som är behörig i det berörda ärendet, eller
 - b) en annan behörig myndighet, enligt den utfärdande statens definition, som i det berörda ärendet agerar i egenskap av utredande myndighet i straffrättsliga förfaranden, med behörighet att besluta om bevisinhämtning i enlighet med nationell rätt; i ett sådant ärende ska den europeiska utlämnandeordern, efter granskning av dess överensstämmelse med villkoren för utfärdande av en europeisk utlämnandeorder enligt denna förordning, godkännas av en domare, en domstol eller en undersökningsdomare i den utfärdande staten.
3. En europeisk bevarandeorder avseende alla slags uppgiftskategorier får endast utfärdas av
- a) en domare, en domstol, en undersökningsdomare eller en allmän åklagare som är behörig i det berörda ärendet, eller
 - b) en annan behörig myndighet, enligt den utfärdande statens definition, som i det berörda ärendet agerar i egenskap av utredande myndighet i straffrättsliga förfaranden, med behörighet att besluta om bevisinhämtning i enlighet med nationell rätt; i ett sådant ärende ska den europeiska bevarandeordern, efter granskning av dess överensstämmelse med villkoren för utfärdande av en europeisk bevarandeorder enligt denna förordning, godkännas av en domare, domstol, undersökningsdomare eller allmän åklagare i den utfärdande staten.
4. Om en europeisk utlämnandeorder eller en europeisk bevarandeorder har godkänts av en rättslig myndighet enligt punkt 1 b, 2 b eller 3 b får den myndigheten också betraktas som en utfärdande myndighet för översändandet av intyget om en europeisk utlämnandeorder och intyget om en europeisk bevarandeorder.
5. I en vederbörligen fastställd nödsituation enligt definitionen i artikel 3.18 får de behöriga myndigheter som avses i punkterna 1 b och 3 b i den här artikeln undantagsvis utfärda en europeisk utlämnandeorder för abonnentuppgifter eller för uppgifter som begärts med det enda syftet att identifiera användaren enligt definitionen i artikel 3.10, eller en europeisk bevarandeorder, utan förhandsgodkännande av den berörda ordern, om godkännandet inte kan erhållas i tid och om dessa myndigheter skulle kunna utfärda en order i ett liknande inhemskt ärende utan förhandsgodkännande. Den utfärdande myndigheten ska utan onödigt dröjsmål, inom 48 timmar, begära efterhandsgodkännande av ordern i fråga. Om ett sådant efterhandsgodkännande av den berörda ordern inte ges ska den utfärdande myndigheten omedelbart återkalla ordern och radera eller på annat sätt begränsa användningen av alla uppgifter som inhämtats.
6. Varje medlemsstat får utse en eller flera centralmyndigheter som ska ansvara för det administrativa översändandet av intyg om europeiska utlämnandeorder och intyg om europeiska bevarandeorder, europeiska utlämnandeorder och europeiska bevarandeorder, för mottagande av uppgifter och anmälningar samt för översändande av annan officiell kommunikation avseende sådana intyg eller order.

Artikel 5

Villkor för utfärdande av en europeisk utlämnandeorder

1. En utfärdande myndighet får utfärda en europeisk utlämnandeorder endast om de villkor som anges i denna artikel är uppfyllda.
2. En europeisk utlämnandeorder ska vara nödvändig och proportionell med avseende på de förfaranden som avses i artikel 2.3, med beaktande av den misstänktes eller tilltalades rättigheter, och får utfärdas endast om en liknande order skulle ha kunnat utfärdas på samma villkor i ett liknande inhemskt ärende.
3. En europeisk utlämnandeorder för att inhämta abonnentuppgifter eller för att inhämta uppgifter som begärts med det enda syftet att identifiera användaren enligt definitionen i artikel 3.10 får utfärdas för alla brott och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd i minst fyra månader – till följd av straffrättsliga förfaranden – som inte beslutats genom en dom där personen inte var personligen närvarande vid förhandlingen, i fall där den dömda personen undandragit sig lagföring.
4. En europeisk utlämnandeorder för att inhämta trafikuppgifter, med undantag för uppgifter som begärts med det enda syftet att identifiera användaren enligt definitionen i artikel 3.10 i denna förordning, eller inhämta innehållsdata får utfärdas endast
 - a) för brott för vilka maximistraffet i den utfärdande staten är fängelse eller annan frihetsberövande åtgärd i minst tre år, eller
 - b) för följande brott, om de helt eller delvis begås med hjälp av ett informationssystem:
 - i) brott enligt definitionerna i artiklarna 3–8 i Europaparlamentets och rådets direktiv (EU) 2019/713 ⁽³²⁾,
 - ii) brott enligt definitionerna i artiklarna 3–7 i direktiv 2011/93/EU,
 - iii) brott enligt definitionerna i artiklarna 3–8 i direktiv 2013/40/EU,
 - c) för brott enligt definitionerna i artiklarna 3–12 och 14 i direktiv (EU) 2017/541,
 - d) för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd i minst fyra månader – till följd av straffrättsliga förfaranden – som inte beslutats genom en dom där personen inte var personligen närvarande vid förhandlingen, i fall där den dömda personen undandragit sig lagföring, för brott som avses i leden a, b och c i denna punkt.
5. En europeisk utlämnandeorder ska innehålla följande information:
 - a) Den utfärdande myndigheten och i förekommande fall den godkännande myndigheten.
 - b) Den europeiska utlämnandeorderns mottagare i den mening som avses i artikel 7.
 - c) Användaren, förutom när det enda syftet med ordern är att identifiera användaren, eller någon annan unik identifierare såsom användarnamn, inloggnings-ID eller kontobeteckning för att fastställa de uppgifter som begärs.
 - d) Kategorin för de uppgifter som begärs enligt definitionerna i artikel 3.9–3.12.
 - e) Om tillämpligt, tidsintervallet för de uppgifter för vilka utlämnande begärs.
 - f) De tillämpliga bestämmelserna i den utfärdande statens straffrätt.
 - g) I nödsituationer enligt definitionen i artikel 3.18, vederbörligen motiverade orsaker till respektive nödfall.
 - h) I ärenden där den europeiska utlämnandeordern är direkt riktad till den tjänsteleverantör som lagrar eller på annat sätt behandlar uppgifterna på den personuppgiftsansvariges vägnar, en bekräftelse på att villkoren i punkt 6 i denna artikel är uppfyllda.
 - i) Skälen till att fastställa att den europeiska utlämnandeordern uppfyller villkoren för att vara nödvändig och proportionell enligt punkt 2 i denna artikel.
 - j) En kortfattad beskrivning av ärendet.

⁽³²⁾ Europaparlamentets och rådets direktiv (EU) 2019/713 av den 17 april 2019 om bekämpande av bedrägeri och förfälskning som rör andra betalningsmedel än kontanter och om ersättande av rådets rambeslut 2001/413/RIF (EUT L 123, 10.5.2019, s. 18).

6. En europeisk utlämnandeorder ska riktas till den tjänsteleverantör som agerar som personuppgiftsansvarig i enlighet med förordning (EU) 2016/679.

Undantagsvis får den europeiska utlämnandeordern riktas direkt till den tjänsteleverantör som lagrar eller på annat sätt behandlar uppgifterna på den personuppgiftsansvariges vägnar, om

- a) den personuppgiftsansvarige inte kan identifieras trots att rimliga ansträngningar gjorts från den utfärdande myndighetens sida, eller
- b) det kan vara till skada för utredningen att rikta sig till den personuppgiftsansvarige.

7. I enlighet med förordning (EU) 2016/679 ska det personuppgiftsbiträde som lagrar eller på annat sätt behandlar uppgifterna på den personuppgiftsansvariges vägnar informera den personuppgiftsansvarige om utlämnandet av uppgifterna, såvida inte den utfärdande myndigheten har begärt att tjänsteleverantören ska avstå från att informera den personuppgiftsansvarige, under så lång tid som det är nödvändigt och proportionellt, för att inte hindra de straffrättsliga förfarandena i fråga. I sådant fall ska den utfärdande myndigheten i ärendet ange skälen till fördröjningen med att informera den personuppgiftsansvarige. En kort motivering ska också läggas till i intyget om en europeisk utlämnandeorder.

8. Om uppgifterna lagras eller på annat sätt behandlas som en del av en infrastruktur som en tjänsteleverantör tillhandahåller en offentlig myndighet får en europeisk utlämnandeorder utfärdas endast om den offentliga myndighet för vilken uppgifterna lagras eller på annat sätt behandlas är belägen i den utfärdande staten.

9. I fall där uppgifter som omfattas av sekretess eller tystnadsplikt enligt den utfärdande statens rätt lagras eller på annat sätt behandlas av en tjänsteleverantör som en del av en infrastruktur som tillhandahålls yrkesutövare som omfattas av sekretess eller tystnadsplikt inom ramen för deras verksamhet, får en europeisk utlämnandeorder för att inhämta trafikuppgifter, med undantag för uppgifter som begärts med det enda syftet att identifiera användaren enligt definitionen i artikel 3.10, eller för att inhämta innehållsdata utfärdas endast

- a) om den yrkesutövare som omfattas av sekretess eller tystnadsplikt är bosatt i den utfärdande staten,
- b) om det kan vara till skada för utredningen att rikta sig till den yrkesutövare som omfattas av sekretess eller tystnadsplikt, eller
- c) om undantag gjorts från sekretessen eller tystnadsplikten i enlighet med tillämplig rätt.

10. Om den utfärdande myndigheten har skäl att anta att de trafikuppgifter, med undantag för uppgifter som begärts med det enda syftet att identifiera användaren enligt definitionen i artikel 3.10, eller de innehållsdata som begärts genom den europeiska utlämnandeordern skyddas av immunitet eller privilegier som beviljas enligt den verkställande statens rätt, eller att dessa uppgifter omfattas av den statens regler om fastställande och begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet eller yttrandefrihet i andra medier, får den utfärdande myndigheten söka klagöranden före utfärdandet av den europeiska utlämnandeordern, inbegripet genom att samråda med de behöriga myndigheterna i den verkställande staten, antingen direkt eller via Eurojust eller det europeiska rättsliga nätverket.

Den utfärdande myndigheten får inte utfärda en europeisk utlämnandeorder om den anser att de begärda trafikuppgifterna, med undantag för uppgifter som begärts med det enda syftet att identifiera användaren enligt definitionen i artikel 3.10, eller innehållsdata skyddas av immunitet eller privilegier som beviljas enligt den verkställande statens rätt, eller att dessa uppgifter omfattas av den statens regler om fastställande och begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet eller yttrandefrihet i andra medier.

Artikel 6

Villkor för utfärdande av en europeisk bevarandeorder

1. En utfärdande myndighet får utfärda en europeisk bevarandeorder endast om de villkor som anges i denna artikel är uppfyllda. Artikel 5.8 ska gälla i tillämpliga delar.

2. En europeisk bevarandeorder ska vara nödvändig och proportionell för ändamålet att förhindra avlägsnande, radering eller ändring av uppgifter i avvaktan på en efterföljande framställan om utlämnande av dessa uppgifter via ömsesidig rättslig hjälp, en europeisk utredningsorder eller en europeisk utlämnandeorder, med beaktande av den misstänkta eller tilltalade personens rättigheter.

3. En europeisk bevarandeorder får utfärdas för alla brott, om den skulle kunna ha utfärdats på samma villkor i ett liknande inhemskt ärende, och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd i minst fyra månader – till följd av straffrättsliga förfaranden – som inte beslutats genom en dom där personen inte var personligen närvarande vid förhandlingen, i fall där den dömda personen undandragit sig lagföring.

4. En europeisk bevarandeorder ska innehålla följande information:
- Den utfärdande myndigheten och i förekommande fall den godkännande myndigheten.
 - Den europeiska bevarandeorderns mottagare i den mening som avses i artikel 7.
 - Användaren, förutom när det enda syftet med ordern är att identifiera användaren, eller någon annan unik identifierare såsom användarnamn, inloggnings-ID eller kontobeteckning för att fastställa de uppgifter för vilka bevarande begärs.
 - Kategorin för de uppgifter som begärs enligt definitionerna i artikel 3.9–3.12.
 - Om tillämpligt, tidsintervallet för de uppgifter för vilka bevarande begärs.
 - De tillämpliga bestämmelserna i den utfärdande statens straffrätt.
 - Skälen till att fastställa att den europeiska bevarandeordern uppfyller villkoren för att vara nödvändig och proportionell enligt punkt 2 i denna artikel.

Artikel 7

Mottagare av europeiska utlämnandeorder och europeiska bevarandeorder

- Europeiska utlämnandeorder och europeiska bevarandeorder ska ställas direkt till ett utsett verksamhetsställe eller till ett rättsligt ombud för den berörda tjänsteleverantören.
- I nödsituationer enligt definitionen i artikel 3.18, där det utsedda verksamhetsstället eller det rättsliga ombudet för en tjänsteleverantör inte reagerar på ett intyg om en europeisk utlämnandeorder eller ett intyg om en europeisk bevarandeorder inom tidsfristerna, får intyget om en europeisk utlämnandeorder respektive intyget om en europeisk bevarandeorder undantagsvis ställas till något annat av tjänsteleverantörens verksamhetsställen eller rättsliga ombud i unionen.

Artikel 8

Anmälan till den verkställande myndigheten

- Om en europeisk utlämnandeorder utfärdas i syfte att inhämta trafikuppgifter, med undantag för uppgifter som begärts med det enda syftet att identifiera användaren enligt definitionen i artikel 3.10, eller i syfte att inhämta innehållsdata, ska den utfärdande myndigheten anmäla detta till den verkställande myndigheten genom att översända intyget om en europeisk utlämnandeorder till den myndigheten samtidigt som den översänder intyget om en europeisk utlämnandeorder till mottagaren i enlighet med artikel 9.1 och 9.2.
- Punkt 1 ska inte tillämpas om den utfärdande myndigheten vid tidpunkten för utfärdandet av ordern har rimliga skäl att anta att
 - brottet har begåtts, är på väg att begås eller sannolikt kommer att begås i den utfärdande staten, och
 - den person vars uppgifter begärs är bosatt i den utfärdande staten.
- När den utfärdande myndigheten översänder intyget om en europeisk utlämnandeorder enligt punkt 1 i denna artikel till den verkställande myndigheten ska den, när så är lämpligt, inkludera all ytterligare information som kan behövas för att bedöma möjligheten att återopa en vägransgrund i enlighet med artikel 12.
- Den anmälan till den verkställande myndigheten som avses i punkt 1 i denna artikel ska ha suspensiv verkan på mottagarens skyldigheter enligt artikel 10.2, utom i nödsituationer enligt definitionen i artikel 3.18.

Artikel 9

Intyg om en europeisk utlämnandeorder och intyg om en europeisk bevarandeorder

- En europeisk utlämnandeorder eller en europeisk bevarandeorder ska översändas till mottagaren i enlighet med artikel 7, genom ett intyg om en europeisk utlämnandeorder eller genom ett intyg om en europeisk bevarandeorder.

Den utfärdande myndigheten eller i tillämpliga fall, den godkännande myndigheten ska fylla i intyget i bilaga I eller intyget i bilaga II, underteckna det och intyga att dess innehåll är riktigt och korrekt.

2. Ett intyg om en europeisk utlämnandeorder ska innehålla den information som anges i artikel 5.5 a–h, inklusive tillräcklig information för att göra det möjligt för mottagaren att identifiera och vid behov kontakta den utfärdande myndigheten och den verkställande myndigheten.

Om en anmälan till den verkställande myndigheten krävs enligt artikel 8 ska det intyg om en europeisk utlämnandeorder som översänts till den myndigheten innehålla den information som anges i artikel 5.5 a–j.

3. Ett intyg om en europeisk bevarandeorder ska innehålla den information som anges i artikel 6.4 a–f, inklusive tillräcklig information för att göra det möjligt för mottagaren att identifiera och kontakta den utfärdande myndigheten.

4. Om det behövs ska intyget om en europeisk utlämnandeorder eller intyget om en europeisk bevarandeorder översättas till ett av unionens officiella språk som godtas av mottagaren enligt vad som föreskrivs i artikel 4 i direktiv (EU) 2023/1544. Om inget språk har angetts av tjänsteleverantören ska intyget om en europeisk utlämnandeorder eller intyget om en europeisk bevarandeorder översättas till ett officiellt språk i den medlemsstat där det utsedda verksamhetsstället eller det rättsliga ombudet för tjänsteleverantören befinner sig.

Om en anmälan till den verkställande myndigheten krävs enligt artikel 8 ska det intyg om en europeisk utlämnandeorder som ska översändas till den myndigheten översättas till ett officiellt språk i den verkställande staten eller till ett annat av unionens officiella språk som godtas av den staten.

Artikel 10

Fullföljande av ett intyg om en europeisk utlämnandeorder

1. Vid mottagande av ett intyg om en europeisk utlämnandeorder ska mottagaren agera skyndsamt för att bevara de uppgifter som begärs i intyget om en europeisk utlämnandeorder.

2. Om en anmälan till den verkställande myndigheten krävs enligt artikel 8 och den myndigheten inte har åberopat någon vägransgrund i enlighet med artikel 12 inom tio dagar efter mottagandet av intyget om en europeisk utlämnandeorder, ska mottagaren säkerställa att de begärda uppgifterna översänds direkt till den utfärdande myndigheten eller de i intyget angivna brottsbekämpande myndigheterna vid utgången av den tiodagarsperioden. Om den verkställande myndigheten redan före utgången av tiodagarsperioden bekräftar för den utfärdande myndigheten och mottagaren att den inte kommer att åberopa någon vägransgrund, ska mottagaren agera så snart som möjligt efter att ha mottagit en sådan bekräftelse och senast vid utgången av tiodagarsperioden.

3. Om en anmälan till den verkställande myndigheten inte krävs enligt artikel 8 ska mottagaren vid mottagandet av intyget om en europeisk utlämnandeorder säkerställa att de begärda uppgifterna översänds direkt till den utfärdande myndigheten eller de i intyget angivna brottsbekämpande myndigheterna om en europeisk utlämnandeorder senast tio dagar efter mottagandet av intyget.

4. I nödsituationer ska mottagaren översända de begärda uppgifterna utan onödigt dröjsmål, inom åtta timmar efter mottagandet av intyget om en europeisk utlämnandeorder. Om en anmälan till den verkställande myndigheten krävs enligt artikel 8 får den verkställande myndigheten, om den beslutar att åberopa en vägransgrund i enlighet med artikel 12.1, utan dröjsmål och inom 96 timmar efter mottagandet av anmälan, meddela den utfärdande myndigheten och mottagaren om att den invänder mot användningen av uppgifterna eller att uppgifterna får användas endast på villkor som den ska ange. Om en vägransgrund åberopas av den verkställande myndigheten, och om uppgifterna redan har översänts av mottagaren till den utfärdande myndigheten, ska den utfärdande myndigheten radera eller på annat sätt begränsa användningen av uppgifterna, eller – om den verkställande myndigheten har angett villkor – ska den utfärdande myndigheten uppfylla villkoren i fråga vid användningen av uppgifterna.

5. Om mottagaren, enbart på grundval av informationen i intyget om en europeisk utlämnandeorder, anser att fullföljandet av intyget om en europeisk utlämnandeorder skulle kunna inkräkta på immunitet eller privilegier, eller på regler om fastställande eller begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet eller yttrandefrihet i andra medier enligt den verkställande statens rätt, ska mottagaren informera den utfärdande myndigheten och den verkställande myndigheten med hjälp av formuläret i bilaga III.

Om ingen anmälan till den verkställande myndigheten har skett enligt artikel 8 ska den utfärdande myndigheten beakta den information som avses i första stycket i denna punkt och ska, på eget initiativ eller på begäran av den verkställande myndigheten, besluta huruvida den europeiska utlämnandeordern ska återkallas, anpassas eller upprätthållas.

Om en anmälan till den verkställande myndigheten har skett enligt artikel 8 ska den utfärdande myndigheten beakta den information som avses i första stycket i denna punkt och besluta huruvida den europeiska utlämnandeordern ska återkallas, anpassas eller upprätthållas. Den verkställande myndigheten får besluta att åberopa de vägransgrunder som anges i artikel 12.

6. Om mottagaren inte kan fullgöra sin skyldighet att lämna ut de begärda uppgifterna eftersom intyget om en europeisk utlämnandeorder är ofullständigt, innehåller uppenbara fel eller saknar information som krävs för att verkställa intyget, ska mottagaren utan onödigt dröjsmål informera den utfärdande myndigheten och, om en anmälan till den verkställande myndigheten har skett enligt artikel 8, den verkställande myndighet som anges i intyget och be om förtydligande, med hjälp av formuläret i bilaga III. Samtidigt ska mottagaren informera den utfärdande myndigheten om huruvida det var möjligt att identifiera de begärda uppgifterna och bevara dessa uppgifter enligt punkt 9 i den här artikeln.

Den utfärdande myndigheten ska reagera skyndsamt och senast fem dagar efter mottagandet av formuläret. Mottagaren ska säkerställa att den kan få de förtydliganden eller rättelser från den utfärdande myndigheten som behövs för att mottagaren ska kunna fullgöra sina skyldigheter enligt punkterna 1–4. De skyldigheter som anges i punkterna 1–4 ska inte tillämpas förrän den utfärdande myndigheten eller den verkställande myndigheten tillhandahåller ett sådant förtydligande eller en sådan rätelse.

7. Om mottagaren inte kan fullgöra sin skyldighet att lämna ut de begärda uppgifterna på grund av en faktisk omöjlighet till följd av omständigheter som inte beror på mottagaren, ska mottagaren utan onödigt dröjsmål informera den utfärdande myndigheten och, om en anmälan till den verkställande myndigheten har skett enligt artikel 8, den verkställande myndighet som anges i intyget, med en förklaring av orsakerna till den faktiska omöjligheten, med hjälp av formuläret i bilaga III. Om den utfärdande myndigheten bedömer att en sådan faktisk omöjlighet föreligger ska den informera mottagaren och, om en anmälan till den verkställande myndigheten har skett enligt artikel 8, den verkställande myndigheten om att intyget inte längre behöver fullföljas.

8. I samtliga fall där mottagaren inte tillhandahåller de begärda uppgifterna, inte tillhandahåller de begärda uppgifterna i deras helhet eller inte tillhandahåller de begärda uppgifterna inom den angivna tidsfristen, av andra orsaker än de som avses i punkterna 5, 6 och 7 i denna artikel, ska mottagaren, utan onödigt dröjsmål och inom de tidsfrister som anges i punkterna 2, 3 och 4 i denna artikel, informera den utfärdande myndigheten och, om en anmälan till den verkställande myndigheten har skett enligt artikel 8, den verkställande myndighet som anges i intyget om dessa orsaker, med hjälp av formuläret i bilaga III. Den utfärdande myndigheten ska ompröva den europeiska utlämnandeordern mot bakgrund av den information som mottagaren har tillhandahållit och, vid behov, ange en ny tidsfrist inom vilken mottagaren ska lämna ut uppgifterna.

9. Uppgifterna ska i möjligaste mån bevaras tills de lämnas ut, oavsett om utlämnandet i slutändan begärs på grundval av en förtydligad europeisk utlämnandeorder och dess intyg eller via andra kanaler, såsom ömsesidig rättslig hjälp, eller tills den europeiska utlämnandeordern återkallas.

Om utlämnandet av uppgifter och deras bevarande inte längre är nödvändigt ska den utfärdande myndigheten och, i tillämpliga fall enligt artikel 16.8, den verkställande myndigheten informera mottagaren utan onödigt dröjsmål.

Artikel 11

Fullföljande av ett intyg om en europeisk bevarandeorder

1. Vid mottagande av ett intyg om en europeisk bevarandeorder ska mottagaren utan onödigt dröjsmål bevara de begärda uppgifterna. Skyldigheten att bevara uppgifterna ska upphöra efter 60 dagar, såvida inte den utfärdande myndigheten, med hjälp av formuläret i bilaga V, bekräftar att en efterföljande framställan om utlämnande har utfärdats. Under denna 60-dagarsperiod får den utfärdande myndigheten, med hjälp av formuläret i bilaga VI, förlänga varaktigheten för skyldigheten att bevara uppgifterna med ytterligare 30 dagar, om det är nödvändigt för att en efterföljande framställan om utlämnande ska kunna utfärdas.

2. Om den utfärdande myndigheten under den tidsperiod för bevarande som fastställs i punkt 1 bekräftar att en efterföljande framställan om utlämnande har utfärdats ska mottagaren bevara uppgifterna så länge som krävs för att lämna ut uppgifterna när framställan om utlämnande mottas.

3. Om det inte längre är nödvändigt att bevara uppgifterna ska den utfärdande myndigheten informera mottagaren utan onödigt dröjsmål, varvid bevarandeskyldigheten på grundval av den europeiska bevarandeordern i fråga ska upphöra.

4. Om mottagaren, enbart på grundval av informationen i intyget om en europeisk bevarandeorder, anser att fullföljandet av intyget om en europeisk bevarandeorder skulle kunna inkräkta på immunitet eller privilegier, eller på regler om fastställande eller begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet eller yttrandefrihet i andra medier enligt den verkställande statens rätt, ska mottagaren informera den utfärdande myndigheten och den verkställande myndigheten med hjälp av formuläret i bilaga III.

Den utfärdande myndigheten ska beakta den information som avses i första stycket och ska, på eget initiativ eller på begäran av den verkställande myndigheten, besluta huruvida den europeiska bevarandeordern ska återkallas, anpassas eller upprätthållas.

5. Om mottagaren inte kan fullgöra sin skyldighet att bevara de begärda uppgifterna eftersom intyget om en europeisk bevarandeorder är ofullständigt, innehåller uppenbara fel eller saknar information som krävs för att fullfölja intyget, ska mottagaren utan onödigt dröjsmål informera den utfärdande myndighet som anges i intyget och be om förtydligande, med hjälp av formuläret i bilaga III.

Den utfärdande myndigheten ska reagera skyndsamt och senast fem dagar efter mottagandet av formuläret. Mottagaren ska säkerställa att den kan få de förtydliganden eller rättelser från den utfärdande myndigheten som behövs för att mottagaren ska kunna fullgöra sina skyldigheter enligt punkterna 1, 2, och 3. Om den utfärdande myndigheten inte reagerar inom femdagsperioden ska tjänsteleverantören undantas från skyldigheterna enligt punkterna 1 och 2.

6. Om mottagaren inte kan fullgöra sin skyldighet att bevara de begärda uppgifterna på grund av en faktisk omöjlighet till följd av omständigheter som inte beror på mottagaren, ska mottagaren utan onödigt dröjsmål informera den utfärdande myndighet som anges i intyget, med en förklaring av orsakerna till den faktiska omöjligheten, med hjälp av formuläret i bilaga III. Om den utfärdande myndigheten bedömer att en sådan omöjlighet föreligger ska den informera mottagaren om att intyget inte längre behöver fullföljas.

7. I samtliga fall där mottagaren inte bevarar de begärda uppgifterna av andra orsaker än de som avses i punkterna 4, 5 och 6 ska mottagaren utan onödigt dröjsmål informera den utfärdande myndigheten om dessa orsaker, med hjälp av formuläret i bilaga III. Den utfärdande myndigheten ska ompröva den europeiska bevarandeordern mot bakgrund av de motiveringar som mottagaren har tillhandahållit.

Artikel 12

Vägransgrunder för europeiska utlämnandeorder

1. Om den utfärdande myndigheten har gjort en anmälan till den verkställande myndigheten enligt artikel 8, och utan att det påverkar tillämpningen av artikel 1.3, ska den verkställande myndigheten så snart som möjligt och senast tio dagar efter mottagandet av anmälan eller, i nödsituationer, senast 96 timmar efter mottagandet, bedöma den information som anges i ordern och vid behov åberopa en eller flera av följande vägransgrunder:

- a) De begärda uppgifterna skyddas av immunitet eller privilegier som beviljas enligt den verkställande statens rätt och som hindrar ordern från att fullföljas eller verkställas, eller de begärda uppgifterna omfattas av regler om fastställande eller begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet eller yttrandefrihet i andra medier och som hindrar ordern från att fullföljas eller verkställas.
- b) Det finns, i undantagsfall och på grundval av precisa och objektiva uppgifter, grundad anledning att anta att fullföljandet av ordern, mot bakgrund av de särskilda omständigheterna i ärendet, skulle innebära ett uppenbart åsidosättande av en relevant grundläggande rättighet enligt artikel 6 i EU-fördraget och stadgan.
- c) Fullföljandet av ordern skulle strida mot principen *ne bis in idem*.
- d) Det handlande för vilken ordern har utfärdats utgör inte ett brott enligt den verkställande statens rätt, såvida det inte gäller ett brott som förtecknas i de brottskategorier som anges i bilaga IV, enligt uppgift från den utfärdande myndigheten i intyget om en europeisk utlämnandeorder, om maximistraffet för brottet i fråga i den utfärdande staten är fängelsestraff eller annan frihetsberövande åtgärd i minst tre år.

2. Om den verkställande myndigheten åberopar en vägransgrund enligt punkt 1 ska den informera mottagaren och den utfärdande myndigheten. Mottagaren ska stoppa fullföljandet av den europeiska utlämnandeordern och inte överföra uppgifterna, och den utfärdande myndigheten ska återkalla ordern.

3. Innan beslut fattas om att åberopa en vägransgrund ska den verkställande myndighet som mottagit anmälan enligt artikel 8 på lämpligt sätt kontakta den utfärdande myndigheten för att diskutera lämpliga åtgärder. På grundval av detta får den utfärdande myndigheten besluta att anpassa eller återkalla den europeiska utlämnandeordern. Om ingen lösning nås efter sådana diskussioner får den verkställande myndighet som mottagit anmälan enligt artikel 8 besluta att åberopa vägransgrunder av den europeiska utlämnandeordern och informera den utfärdande myndigheten och mottagaren om detta.

4. Om den verkställande myndigheten beslutar att åberopa vägransgrunder enligt punkt 1 får den ange om den motsätter sig överföring av samtliga uppgifter som begärs i den europeiska utlämnandeordern eller om uppgifterna bara delvis får överföras eller användas på villkor som anges av den verkställande myndigheten.

5. Om en myndighet i den verkställande staten har behörighet att upphäva immunitet eller privilegier enligt punkt 1 a i denna artikel får den utfärdande myndigheten begära att den verkställande myndighet som mottagit anmälan enligt artikel 8 kontaktar den myndigheten i den verkställande staten och begär att den utan dröjsmål utövar den behörigheten. Om en myndighet i en annan medlemsstat eller ett tredjeland eller en internationell organisation har behörighet att upphäva immuniteten eller privilegierna i fråga får den utfärdande myndigheten begära att den berörda myndigheten utövar den behörigheten.

Artikel 13

Användarinformation och sekretess

1. Den utfärdande myndigheten ska utan onödigt dröjsmål informera den person vars uppgifter begärs genom en europeisk utlämnandeorder om utlämnandet av uppgifter.
2. Den utfärdande myndigheten får i enlighet med den utfärdande statens nationella rätt skjuta upp, eller begränsa informationen till, eller underlåta att informera, den person vars uppgifter begärs, i den mån och så länge som villkoren i artikel 13.3 i direktiv (EU) 2016/680 är uppfyllda, i vilket fall den utfärdande myndigheten i ärendet ska ange skälen till uppskjutandet, begränsningen eller underlåtelser. En kort motivering ska också läggas till i intyget om en europeisk utlämnandeorder.
3. När den utfärdande myndigheten informerar den person vars uppgifter begärs enligt punkt 1 i denna artikel ska den inkludera information om tillgängliga rättsmedel enligt artikel 18.
4. Mottagarna och, om de inte är desamma, tjänsteleverantörerna ska vidta de senaste operativa och tekniska åtgärder som krävs för att säkerställa konfidentialiteten, sekretessen och integriteten för intyget om en europeisk utlämnandeorder eller intyget om en europeisk bevarandeorder och för de uppgifter som lämnas ut eller bevaras.

Artikel 14

Ersättning för kostnader

1. Tjänsteleverantören får kräva ersättning för sina kostnader från den utfärdande staten, om denna möjlighet föreskrivs i den utfärdande statens nationella rätt för inhemska förelägganden i liknande situationer, i enlighet med den statens nationella rätt. Medlemsstaterna ska informera kommissionen om sina nationella regler för ersättning, och kommissionen ska offentliggöra dessa.
2. Denna artikel är inte tillämplig på ersättning av kostnader för det decentraliserade it-system som avses i artikel 25.

KAPITEL III

SANKTIONER OCH VERKSTÄLLIGHET

Artikel 15

Sanktioner

1. Utan att det påverkar tillämpningen av nationell rätt som föreskriver straffrättsliga påföljder ska medlemsstaterna fastställa regler om sanktionsavgifter som är tillämpliga på överträdelser av artiklarna 10, 11 och 13.4, i enlighet med artikel 16.10, och ska vidta alla nödvändiga åtgärder för att säkerställa att de genomförs. Sanktionsavgifterna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska säkerställa att sanktionsavgifter på upp till 2 % av tjänsteleverantörens totala globala årsomsättning föregående räkenskapsår kan åläggas. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder utan dröjsmål samt utan dröjsmål eventuella ändringar som berör dem.
2. Utan att det påverkar deras dataskyddsskyldigheter ska tjänsteleverantörer inte hållas ansvariga i medlemsstaterna för olägenheter som orsakas deras användare eller tredje parter uteslutande till följd av att de i god tro rättar sig efter ett intyg om en europeisk utlämnandeorder eller ett intyg om en europeisk bevarandeorder.

Artikel 16

Verkställighetsförfarande

1. Om mottagaren inte efterlever intyget om en europeisk utlämnandeorder inom tidsfristen eller intyget om en europeisk bevarandeorder, utan att ange orsaker som godtas av den utfärdande myndigheten, och, i tillämpliga fall, om den verkställande myndigheten inte har åberopat någon av vägransgrunderna enligt artikel 12, får den utfärdande myndigheten begära att den verkställande myndigheten verkställer den europeiska utlämnandeordern eller den europeiska bevarandeordern.

För verkställighet enligt första stycket ska den utfärdande myndigheten översända den berörda ordern, det formulär som återges i bilaga III, ifyllt av mottagaren, och alla relevanta handlingar i enlighet med artikel 19. Den utfärdande myndigheten ska översätta den berörda ordern och alla handlingar som ska översändas till ett av de språk som godtas av den verkställande staten och ska informera mottagaren om översändandet.

2. Vid mottagandet ska den verkställande myndigheten utan vidare formaliteter erkänna och vidta de åtgärder som krävs för att verkställa:

- a) en europeisk utlämnandeorder, såvida inte den verkställande myndigheten anser att ett av de skäl som anges i punkt 4 är tillämpligt, eller
- b) en europeisk bevarandeorder, såvida inte den verkställande myndigheten anser att ett av de skäl som anges i punkt 5 är tillämpligt.

Den verkställande myndigheten ska fatta beslut om ett erkännande av den berörda ordern utan onödigt dröjsmål och senast fem arbetsdagar efter mottagandet av den ordern.

3. Den verkställande myndigheten ska formellt kräva att mottagaren fullgör sina motsvarande skyldigheter och ska informera mottagaren om följande:

- a) möjligheten att invända mot fullföljandet av den berörda ordern genom att hänvisa till ett eller flera av de skäl som anges i punkt 4 a–f eller i punkt 5 a–c,
- b) de tillämpliga sanktionerna vid bristande efterlevnad, samt
- c) tidsfristen för efterlevnad eller invändningar.

4. Verkställighet av den europeiska utlämnandeordern får nekas endast av ett eller flera av följande skäl:

- a) Den europeiska utlämnandeordern har inte utfärdats eller godkänts av en utfärdande myndighet som anges i artikel 4.
- b) Den europeiska utlämnandeordern har inte utfärdats för ett brott som anges i artikel 5.4.
- c) Mottagaren kunde inte efterleva intyget om en europeisk utlämnandeorder på grund av en faktisk omöjlighet till följd av omständigheter som inte beror på mottagaren, eller på grund av att intyget innehåller uppenbara fel.
- d) Den europeiska utlämnandeordern gäller inte uppgifter som lagras av eller på uppdrag av tjänsteleverantören vid den tidpunkt då intyget om den europeiska utlämnandeordern mottas.
- e) Tjänsten omfattas inte av denna förordning.
- f) De begärda uppgifterna skyddas av immunitet eller privilegier som beviljas enligt den verkställande statens rätt, eller de begärda uppgifterna omfattas av reglerna för fastställande eller begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet eller yttrandefrihet i andra medier och som hindrar den europeiska utlämnandeordern från att fullföljas eller verkställas.
- g) Det är i undantagsfall, enbart baserat på den information som ingår i intyget om en europeisk utlämnandeorder, uppenbart att det finns grundad anledning att anta, på grundval av precisa och objektiva uppgifter, att verkställigheten av den europeiska utlämnandeordern, mot bakgrund av de särskilda omständigheterna i ärendet, skulle innebära ett uppenbart åsidosättande av en relevant grundläggande rättighet enligt artikel 6 i EU-fördraget och stadgan.

5. Verkställighet av den europeiska bevarandeordern får nekas endast av ett eller flera av följande skäl:

- a) Den europeiska bevarandeordern har inte utfärdats eller godkänts av en utfärdande myndighet som anges i artikel 4.
- b) Mottagaren kunde inte efterleva intyget om en europeisk bevarandeorder på grund av en faktisk omöjlighet till följd av omständigheter som inte beror på mottagaren, eller på grund av att intyget innehåller uppenbara fel.
- c) Den europeiska bevarandeordern gäller inte uppgifter som lagras av eller på uppdrag av tjänsteleverantören vid den tidpunkt då intyget om den europeiska bevarandeordern mottas.
- d) Tjänsten omfattas inte av denna förordnings tillämpningsområde.

- e) De begärda uppgifterna skyddas av immunitet eller privilegier som beviljas enligt den verkställande statens rätt, eller de begärda uppgifterna omfattas av reglerna för fastställande eller begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet eller yttrandefrihet i andra medier och som hindrar den europeiska bevarandeordern från att fullföljas eller verkställas.
- f) I undantagsfall, enbart baserat på den information som ingår i intyget om en europeisk bevarandeorder, är det uppenbart att det finns goda skäl att anta, på grundval av precisa och objektiva uppgifter, att fullföljandet av den europeiska bevarandeordern, mot bakgrund av de särskilda omständigheterna i ärendet, skulle innebära ett uppenbart åsidosättande av en relevant grundläggande rättighet enligt artikel 6 i EU-fördraget och stadgan.
6. Om mottagaren invänder enligt punkt 3 a ska den verkställande myndigheten besluta huruvida den europeiska utlämnandeordern eller den europeiska bevarandeordern ska verkställas eller inte på grundval av information som lämnats av mottagaren och, vid behov, kompletterande information från den utfärdande myndigheten i enlighet med punkt 7.
7. Innan den verkställande myndigheten beslutar att inte erkänna eller att inte verkställa den europeiska utlämnandeordern eller den europeiska bevarandeordern i enlighet med punkt 2 respektive punkt 6 ska den samråda med den utfärdande myndigheten på lämpligt sätt. Om det är lämpligt ska den begära ytterligare information från den utfärdande myndigheten. Den utfärdande myndigheten ska svara på en sådan begäran inom fem arbetsdagar.
8. Den verkställande myndigheten ska omedelbart meddela den utfärdande myndigheten och mottagaren om alla sina beslut.
9. Om den verkställande myndigheten inhämtar de uppgifter som begärs genom en europeisk utlämnandeorder från mottagaren ska den översända dessa uppgifter till den utfärdande myndigheten utan onödigt dröjsmål.
10. Om mottagaren inte fullgör sina skyldigheter enligt en erkänd europeisk utlämnandeorder eller europeisk bevarandeorder vars verkställbarhet har bekräftats av den verkställande myndigheten, ska den myndigheten ålägga en sanktionsavgift i enlighet med artikel 15. Ett effektivt rättsmedel ska finnas tillgängligt mot ett beslut att ålägga en sanktionsavgift.

KAPITEL IV

LAGKONFLIKTER OCH RÄTTSMEDEL

Artikel 17

Prövning i händelse av motstridiga skyldigheter

1. Om en mottagare anser att efterlevnaden av en europeisk utlämnandeorder skulle stå i strid med en skyldighet enligt ett tredjelands tillämpliga rätt, ska den informera den utfärdande myndigheten och den verkställande myndigheten om sina skäl till att inte fullfölja den europeiska utlämnandeordern, i enlighet med det förfarande som fastställs i artikel 10.8 och 10.9, med hjälp av formuläret i bilaga III (*en motiverad invändning*).

2. En motiverad invändning ska innehålla alla relevanta uppgifter om tredjelands rätt, dess tillämpning i det aktuella fallet och arten av den motstridiga skyldigheten. En motiverad invändning får inte grundas på

- a) att liknande bestämmelser om villkor, formaliteter och förfaranden för utfärdande av en order om utlämnande inte existerar i tredjelands tillämpliga rätt, eller
- b) endast det faktum att uppgifterna lagras i ett tredjeland.

En motiverad invändning ska inges senast tio dagar efter det datum då mottagaren mottog intyget om en europeisk utlämnandeorder.

3. Den utfärdande myndigheten ska ompröva den europeiska utlämnandeordern på grundval av den motiverade invändningen och eventuella synpunkter från den verkställande staten. Om den utfärdande myndigheten har för avsikt att upprätthålla den europeiska utlämnandeordern ska den begära en prövning av den behöriga domstolen i den utfärdande staten. Fullföljandet av den europeiska utlämnandeordern ska avbrytas i avvaktan på att prövningsförfarandet avslutas.

4. Den behöriga domstolen ska först bedöma om en motstridig skyldighet föreligger, på grundval av en granskning av om

- a) tredjelands rätt är tillämplig utifrån de särskilda omständigheterna i ärendet i fråga, och
- b) tredjelands rätt, om den är tillämplig enligt led a, förbjuder röjande av de berörda uppgifterna när den tillämpas på de särskilda omständigheterna i ärendet i fråga.

5. Om den behöriga domstolen anser att det inte föreligger några motstridiga skyldigheter i den mening som avses i punkterna 1 och 4, ska den upprätthålla den europeiska utlämnandeordern.
6. Om den behöriga domstolen, på grundval av granskningen enligt punkt 4 b, fastställer att tredjelandets rätt förbjuder röjande av de berörda uppgifterna, ska den behöriga domstolen avgöra huruvida den europeiska utlämnandeordern ska upprätthållas eller upphävas. Denna bedömning ska i synnerhet baseras på följande faktorer, samtidigt som särskild vikt ges till de faktorer som avses i leden a och b:
- a) Det intresse som skyddas genom tredjelandets relevanta rätt, inklusive grundläggande rättigheter samt andra grundläggande intressen som förhindrar röjande av uppgifterna, framför allt tredjelandets nationella säkerhetsintressen.
 - b) Grad av anknytning mellan det brottmål för vilket den europeiska utlämnandeordern utfärdades och endera av de två jurisdiktionerna, vilken bland annat kan framgå av
 - i) plats, medborgarskap och boställningsort för den person vars uppgifter begärs eller för offret eller offren för brottet i fråga,
 - ii) platsen där brottet i fråga begicks,
 - c) graden av anknytning mellan tjänsteleverantören och tredjelandet i fråga; i detta sammanhang ska inte enbart platsen för lagring av uppgifterna räcka för att fastställa en betydande grad av anknytning,
 - d) den utredande statens intresse av att inhämta de aktuella bevisen, utifrån en bedömning av brottets svårhetsgrad och vikten av att inhämta bevis på ett snabbt sätt,
 - e) möjliga konsekvenser för mottagaren eller för tjänsteleverantören av att efterleva den europeiska utlämnandeordern, inklusive eventuella sanktioner.
7. Den behöriga domstolen får begära information från tredjelandets behöriga myndighet med beaktande av direktiv (EU) 2016/680, särskilt kapitel V, och i den mån en sådan begäran inte hindrar det berörda straffrättsliga förfarandet. Den utfärdande staten ska framför allt begära information från den behöriga myndigheten i tredjelandet om den motstridiga skyldigheten rör grundläggande rättigheter eller andra grundläggande intressen i tredjelandet avseende nationell säkerhet och försvar.
8. Om den behöriga domstolen beslutar att upphäva den europeiska utlämnandeordern ska den informera den utfärdande myndigheten och mottagaren. Om den behöriga myndigheten beslutar att den europeiska utlämnandeordern ska upprätthållas ska den informera den utfärdande myndigheten och mottagaren, och den mottagaren ska fullfölja den europeiska utlämnandeordern.
9. Vid tillämpning av förfarandena enligt denna artikel ska tidsfristerna beräknas i enlighet med den utfärdande myndighetens nationella rätt.
10. Den utfärdande myndigheten ska informera den verkställande myndigheten om resultatet av prövningsförfarandet.

Artikel 18

Effektiva rättsmedel

1. Utan att det påverkar andra rättsmedel som finns att tillgå enligt nationell rätt ska varje person vars uppgifter har begärts genom en europeisk utlämnandeorder ha rätt till effektiva rättsmedel mot den ordern. Om den personen är en misstänkt eller en tilltalad, ska personen ha rätt till effektiva rättsmedel under det straffrättsliga förfarande där uppgifterna användes. Den rätt till effektiva rättsmedel som avses i denna punkt ska inte påverka rätten att söka rättsmedel enligt förordning (EU) 2016/679 och direktiv (EU) 2016/680.
2. Rätten till effektiva rättsmedel ska utövas vid en domstol i den utfärdande staten i enlighet med dess nationella rätt och ska inbegripa möjligheten att bestrida åtgärdens lagenlighet, inklusive dess nödvändighet och proportionalitet, utan att det påverkar garantierna för de grundläggande rättigheterna i den verkställande staten.
3. Vid tillämpningen av artikel 13.1 ska information ges i god tid om möjligheterna enligt nationell rätt att utnyttja rättsmedel, och det ska säkerställas att de kan utövas på ett effektivt sätt.

4. Samma tidsfrister eller andra villkor för att utnyttja rättsmedel ska gälla vid tillämpning av denna förordning som i liknande inhemska ärenden och på ett sätt som garanterar att de berörda personerna kan utöva sin rätt till dessa rättsmedel på ett effektivt sätt.

5. Utan att det påverkar nationella förfaranderegler ska den utfärdande staten och varje annan medlemsstat till vilken elektroniska bevis har överförts enligt denna förordning säkerställa att rätten till försvar och ett rättvist förfarande vid bedömningen av de bevis som inhämtats genom den europeiska utlämnandeordern respekteras.

KAPITEL V

DECENTRALISERAT IT-SYSTEM

Artikel 19

Säker digital kommunikation och säkert utbyte av uppgifter mellan behöriga myndigheter och tjänsteleverantörer samt mellan behöriga myndigheter

1. Skriftlig kommunikation mellan behöriga myndigheter och utsedda verksamhetsställen eller rättsliga ombud enligt denna förordning, inbegripet utbyte av de formulär som föreskrivs i denna förordning och de uppgifter som begärs genom en europeisk utlämnandeorder eller en europeisk bevarandeorder, ska ske genom ett säkert och tillförlitligt decentraliserat it-system (*det decentraliserade it-systemet*).

2. Varje medlemsstat ska säkerställa att de utsedda verksamhetsställena eller tjänsteleverantörernas rättsliga ombud i den medlemsstaten ges åtkomst till det decentraliserade it-systemet via sina respektive nationella it-system.

3. Tjänsteleverantörer ska säkerställa att deras utsedda verksamhetsställen eller rättsliga ombud kan använda det decentraliserade it-systemet via respektive nationella it-system för att ta emot intyg om en europeisk utlämnandeorder och intyg om en europeisk bevarandeorder, skicka de begärda uppgifterna till den utfärdande myndigheten och på annat sätt kommunicera med den utfärdande myndigheten och den verkställande myndigheten, enligt denna förordning.

4. Skriftlig kommunikation mellan behöriga myndigheter enligt denna förordning, inbegripet utbyte av de formulär som föreskrivs i denna förordning, och av begärda uppgifter inom ramen för verkställighetsförfarandet enligt artikel 16, samt skriftlig kommunikation med behöriga unionsbyråer eller unionsorgan, ska ske via det decentraliserade it-systemet.

5. Om kommunikation via det decentraliserade it-systemet i enlighet med punkt 1 eller 4 inte är möjlig på grund av exempelvis störningar i det decentraliserade it-systemet, det överförda materialets art, tekniska begränsningar, såsom uppgifternas storlek, rättsliga begränsningar som rör de begärda uppgifternas godtagbarhet som bevis eller de kriminaltekniska krav som är tillämpliga på de begärda uppgifterna, eller exceptionella omständigheter, ska överföringen ske på lämpligaste alternativa sätt, med beaktande av behovet av att säkerställa ett informationsutbyte som är snabbt, säkert och tillförlitligt och som gör det möjligt för mottagaren att fastställa äktheten.

6. Om en överföring sker på ett alternativt sätt enligt vad som föreskrivs i punkt 5 ska den som utför överföringen utan onödigt dröjsmål registrera överföringen, inbegripet, i förekommande fall, dag och tidpunkt för överföringen, avsändare och mottagare samt filens namn och storlek, i det decentraliserade it-systemet.

Artikel 20

Rättslig verkan av elektroniska dokument

Dokument som överförs som ett led i elektronisk kommunikation får inte nekas rättslig verkan eller betraktas som icke godtagbara i gränsöverskridande rättsliga förfaranden enligt denna förordning enbart för att de är i elektronisk form.

Artikel 21

Elektroniska underskrifter och stämplar

1. Den allmänna rättsliga ramen för användningen av betrodda tjänster som anges i förordning (EU) nr 910/2014 ska tillämpas på elektronisk kommunikation enligt den här förordningen.

2. Om ett dokument som överförs som ett led i elektronisk kommunikation enligt artikel 19.1 eller 19.4 i denna förordning kräver en stämpel eller underskrift i enlighet med denna förordning, ska dokumentet innehålla en kvalificerad elektronisk stämpel eller en kvalificerad elektronisk underskrift enligt definitionerna i förordning (EU) nr 910/2014.

Artikel 22

Referensprogramvara

1. Kommissionen ska ansvara för skapandet, underhållet och utvecklingen av en referensprogramvara som medlemsstaterna får välja att använda som sitt backend-system i stället för ett nationellt it-system. Skapandet, underhållet och utvecklingen av referensprogramvaran ska finansieras genom unionens allmänna budget.
2. Kommissionen ska tillhandahålla, underhålla och stödja referensprogramvaran kostnadsfritt.

Artikel 23

Kostnaderna för det decentraliserade it-systemet

1. Varje medlemsstat ska bära kostnaderna för installation, drift och underhåll av de åtkomstpunkter i det decentraliserade it-systemet som den medlemsstaten har ansvar för.
2. Varje medlemsstat ska bära kostnaderna för att upprätta och anpassa sina relevanta nationella it-system i syfte att göra dem interoperabla med åtkomstpunkterna, och ska stå för kostnaderna för att administrera, driva och underhålla dessa system.
3. Unionens byråer och organ ska bära kostnaderna för installation, drift och underhåll av de komponenter i det decentraliserade it-system som de har ansvar för.
4. Unionens byråer och organ ska bära kostnaderna för att upprätta och anpassa sina ärendehanteringssystem i syfte att göra dem interoperabla med åtkomstpunkterna och ska bära kostnaderna för att administrera, driva och underhålla dessa system.
5. Tjänsteleverantörerna ska bära alla kostnader som är nödvändiga för att de framgångsrikt ska kunna integrera eller på annat sätt interagera med det decentraliserade it-systemet.

Artikel 24

Övergångsperiod

Innan den skyldighet att använda skriftlig kommunikation genom det decentraliserade it-system som avses i artikel 19 blir tillämplig (*övergångsperiod*) ska den skriftliga kommunikationen mellan behöriga myndigheter och utsedda verksamhetsställen eller rättsliga ombud enligt denna förordning ske på lämpligaste alternativa sätt, med beaktande av behovet av att säkerställa ett snabbt, säkert och tillförlitligt informationsutbyte. Om tjänsteleverantörer, medlemsstater eller unionsbyråer eller unionsorgan har inrättat särskilda plattformar eller andra säkra kanaler för hantering av framställningar om uppgifter från brottsbekämpande myndigheter och rättsliga myndigheter, får utfärdande myndigheter också välja att översända ett intyg om en europeisk utlämnandeorder eller ett intyg om en europeisk bevarandeorder under övergångsperioden.

Artikel 25

Genomförandeakter

1. Kommissionen ska anta genomförandeakter som är nödvändiga för inrättandet och användningen av det decentraliserade it-systemet vid tillämpning av denna förordning och fastställa följande:
 - a) De tekniska specifikationer som fastställer de elektroniska kommunikationsmetoderna för det decentraliserade it-systemet.
 - b) De tekniska specifikationerna för kommunikationsprotokoll.
 - c) Målen för informationssäkerhet och relevanta tekniska åtgärder som säkerställer minimistandarder för informationssäkerhet och en hög cybersäkerhetsnivå för behandlingen och överföringen av information inom det decentraliserade it-systemet.
 - d) Minimimålen för tillgänglighet och eventuella därtill relaterade tekniska krav för de tjänster som tillhandahålls genom det decentraliserade it-systemet.

2. De genomförandeakter som avses i punkt 1 i denna artikel ska antas i enlighet med det granskningsförfarande som avses i artikel 26.
3. De genomförandeakter som avses i punkt 1 ska antas senast den 18 August 2025.

Artikel 26

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.

KAPITEL VI

SLUTBESTÄMMELSER

Artikel 27

Språk

Varje medlemsstat får när som helst besluta att den kommer att godta översättningar av intyg om en europeisk utlämnandeorder och av intyg om en europeisk bevarandeorder till ett eller flera av unionens officiella språk utöver deras officiella språk, och ska ange ett sådant beslut i en skriftlig förklaring som lämnas till kommissionen. Kommissionen ska göra förklaringarna tillgängliga för samtliga medlemsstater och för det europeiska rättsliga nätverket.

Artikel 28

Övervakning och rapportering

1. Senast den 18 August 2026 ska kommissionen upprätta ett detaljerat program för övervakning av resultaten och effekterna av denna förordning. Övervakningsprogrammet ska ange vilka metoder som kommer att användas för att samla in uppgifter och med vilka intervaller detta kommer att ske. Det ska närmare ange vilka åtgärder som kommissionen respektive medlemsstaterna ska vidta när det gäller att samla in och analysera uppgifterna.
2. I alla händelser ska medlemsstaterna från och med den 18 August 2026 samla in heltäckande statistik från de relevanta myndigheterna och föra denna statistik. De insamlade uppgifterna för det föregående kalenderåret ska sändas till kommissionen senast den 31 mars varje år, och ska omfatta följande:
 - a) Antalet intyg om en europeisk utlämnandeorder och intyg om en europeisk bevarandeorder som utfärdats, indelat efter typen av uppgifter som begärts, mottagarna och situationen (nödsituation eller inte).
 - b) Antalet intyg om en europeisk utlämnandeorder som utfärdats enligt det undantagsförfarande som gäller i en nödsituation.
 - c) Antalet fullföljda respektive icke fullföljda intyg om en europeisk utlämnandeorder och intyg om en europeisk bevarandeorder, indelat efter typen av uppgifter som begärts, mottagarna och situationen (nödsituation eller inte).
 - d) Antalet anmälningar till verkställande myndigheter enligt artikel 8, och antalet intyg om en europeisk utlämnandeorder som vägrats, indelat efter typen av uppgifter som begärts, mottagarna och situationen (nödsituation eller inte) samt de återopade vägransgrundarna.
 - e) För fullföljda intyg om en europeisk utlämnandeorder, den genomsnittliga perioden mellan den tidpunkt då intyget utfärdades och den tidpunkt då de begärda uppgifterna erhöles, indelat efter typen av uppgifter som begärts, mottagarna och situationen (nödsituation eller inte).
 - f) För fullföljda intyg om en europeisk bevarandeorder, den genomsnittliga perioden mellan den tidpunkt då intyget om en europeisk bevarandeorder utfärdades och den tidpunkt då den efterföljande framställan om utlämnande utfärdades, indelat efter typen av uppgifter som begärts och mottagarna.
 - g) Antalet europeiska utlämnandeorder eller europeiska bevarandeorder som översänts till och mottagits av en verkställande stat för verkställighet, indelat efter typen av uppgifter som begärts, mottagarna och situationen (nödsituation eller inte) samt antalet sådana order som verkställdes.
 - h) Antalet rättsmedel som använts mot europeiska utlämnandeorder i den utfärdande staten och i den verkställande staten, indelat efter typen av uppgifter som begärts.

- i) Antalet fall där efterhandsgodkännande, i enlighet med artikel 4.5, inte beviljades.
- j) En översikt över de kostnader som tjänsteleverantörer har begärt ersättning för fullföljande av intyg om en europeisk utlämnandeorder eller intyg om en europeisk bevarandeorder samt de kostnader som de utfärdande myndigheterna gett ersättning för.
3. Från och med den 18 August 2026 får den statistik som avses i punkt 2 i denna artikel samlas in automatiskt av nationella portaler när det gäller de utbyten av uppgifter som skett via det decentraliserade it-systemet enligt artikel 19.1. Den referensprogramvara som avses i artikel 22 ska vara tekniskt utrustad för att tillhandahålla sådana funktioner.
4. Tjänsteleverantörer får samla in, föra och offentliggöra statistik i enlighet med befintliga dataskyddsprinciper. Om sådan statistik samlas in för det föregående kalenderåret får den sändas till kommissionen senast den 31 mars och får i möjligaste mån omfatta följande:
- a) Antalet intyg om en europeisk utlämnandeorder och intyg om en europeisk bevarandeorder som mottagits, indelat efter typen av uppgifter som begärts, utfärdande stat och situation (nödsituation eller inte).
- b) Antalet fullföljda respektive icke fullföljda intyg om en europeisk utlämnandeorder och intyg om en europeisk bevarandeorder, indelat efter typen av uppgifter som begärts, utfärdande stat och situation (nödsituation eller inte).
- c) För fullföljda intyg om en europeisk utlämnandeorder, den genomsnittliga period som krävdes för att tillhandahålla de begärda uppgifterna från den tidpunkt då intyget om en europeisk utlämnandeorder mottogs till den tidpunkt då uppgifterna tillhandahölls, indelat efter typen av uppgifter som begärts, utfärdande stat och situation (nödsituation eller inte).
- d) För fullföljda intyg om en europeisk bevarandeorder, den genomsnittliga perioden mellan den tidpunkt då intyget om en europeisk bevarandeorder utfärdades och den tidpunkt då den efterföljande framställan om utlämnande utfärdades, indelat efter typen av uppgifter som begärts och utfärdande stat.
5. Från och med den 18 August 2027 ska kommissionen senast den 30 juni varje år offentliggöra en rapport med de uppgifter som avses i punkterna 2 och 3, i sammanställd form, uppdelat per medlemsstat och typ av tjänsteleverantör.

Artikel 29

Ändringar av intyg och formulär

Kommissionen ska anta delegerade akter i enlighet med artikel 30 för att ändra bilagorna I, II, III, V och VI i syfte att effektivt åtgärda eventuella behov av förbättringar av innehållet i formulären för intyg om en europeisk utlämnandeorder och intyg om en europeisk bevarandeorder och de formulär som ska användas för att meddela att det är omöjligt att fullfölja ett intyg om en europeisk utlämnandeorder eller ett intyg om en europeisk bevarandeorder, för att bekräfta utfärdandet av en framställan om utlämnande till följd av en europeisk bevarandeorder och för att förlänga bevarandet av elektroniska bevis.

Artikel 30

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 29 ges till kommissionen tills vidare från och med den 18 August 2026.
3. Den delegering av befogenhet som avses i artikel 29 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 29 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 31

Anmälningar till kommissionen

1. Senast den 18 August 2025 ska varje medlemsstat meddela kommissionen om följande:
 - a) Den eller de myndigheter som i enlighet med landets nationella rätt är behöriga i enlighet med artikel 4 att utfärda, godkänna eller översända europeiska utlämnandeorder och europeiska bevarandeorder eller anmälningar därom.
 - b) Den eller de myndigheter som är behöriga att ta emot anmälningar enligt artikel 8 och att verkställa europeiska utlämnandeorder och europeiska bevarandeorder på en annan medlemsstats vägnar, i enlighet med artikel 16.
 - c) Den eller de myndigheter som är behöriga att handlägga motiverade invändningar från mottagarna i enlighet med artikel 17.
 - d) De språk som godtas för anmälan och översändande av ett intyg om en europeisk utlämnandeorder, ett intyg om en europeisk bevarandeorder, en europeisk utlämnandeorder eller en europeisk bevarandeorder vid verkställighet i enlighet med artikel 27.
2. Kommissionen ska göra den information som tas emot enligt denna artikel tillgänglig för allmänheten, antingen på en särskild webbplats eller på webbplatsen för det europeiska straffrättsliga nätverk som avses i artikel 9 i rådets beslut 2008/976/RIF⁽³⁾.

Artikel 32

Förhållande till andra instrument, avtal och överenskommelser

1. Denna förordning påverkar inte unionens instrument eller andra internationella instrument, avtal och överenskommelser beträffande bevisinhämtning som omfattas av denna förordnings tillämpningsområde.
2. Medlemsstaterna ska meddela kommissionen senast den 18 August 2026 om eventuella befintliga instrument, avtal och överenskommelser som avses i punkt 1 och som de kommer att fortsätta att tillämpa. Medlemsstaterna ska också inom tre månader efter det att de har undertecknat nya avtal eller överenskommelser enligt punkt 1 meddela kommissionen om detta.

Artikel 33

Utvärdering

Senast den 18 August 2029 ska kommissionen göra en utvärdering av denna förordning. Kommissionen ska överlämna en utvärderingsrapport till Europaparlamentet, rådet, Europeiska datatillsynsmannen och Europeiska unionens byrå för grundläggande rättigheter. Utvärderingsrapporten ska innehålla en bedömning av tillämpningen av denna förordning och av de resultat som har uppnåtts med avseende på dess mål samt en bedömning av denna förordnings inverkan på de grundläggande rättigheterna. Utvärderingen ska genomföras i enlighet med kommissionens riktlinjer om bättre lagstiftning. Medlemsstaterna ska förse kommissionen med de uppgifter som är nödvändiga för att utarbeta utvärderingsrapporten.

Artikel 34

Ikraftträdande och tillämpning

1. Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

⁽³⁾ Rådets beslut 2008/976/RIF av den 16 december 2008 om det europeiska rättsliga nätverket (EUT L 348, 24.12.2008, s. 130).

28.7.2023

SV

Europeiska unionens officiella tidning

L 191/153

2. Den ska tillämpas från och med den 18 August 2026.

Skyldigheten för behöriga myndigheter och tjänsteleverantörer att använda det decentraliserade it-system som fastställs i artikel 19 för skriftlig kommunikation enligt denna förordning ska dock tillämpas med början ett år efter antagandet av de genomförandeakter som avses i artikel 25.

Denna förordning är till alla delar bindande och direkt tillämplig i medlemsstaterna i enlighet med fördragen.

Utfärdad i Strasbourg den 12 juli 2023.

På Europaparlamentets vägnar

R. METSOLA

Ordförande

På rådets vägnar

P. NAVARRO RÍOS

Ordförande

BILAGA I

INTYG OM EN EUROPEISK UTLÄMNANDEORDER FÖR UTLÄMNANDE AV ELEKTRONISKA BEVIS

I enlighet med Europaparlamentets och rådets förordning (EU) 2023/1543 ⁽¹⁾ ska mottagaren av detta intyg om en europeisk utlämnandeorder fullfölja detta intyg om en europeisk utlämnandeorder och lämna de begärda uppgifterna i enlighet med den tidsfrist eller de tidsfrister som anges i avsnitt C i detta intyg om en europeisk utlämnandeorder till den behöriga myndighet som anges i avsnitt L a i detta intyg om en europeisk utlämnandeorder.

I samtliga fall ska mottagaren vid mottagandet av intyget om en europeisk utlämnandeorder agera skyndsamt för att bevara de begärda uppgifterna, såvida inte informationen i intyget om en europeisk utlämnandeorder inte gör det möjligt att identifiera dessa uppgifter. Uppgifterna ska fortsätta att bevaras till dess att uppgifterna lämnas ut, eller till dess att den utfärdande myndigheten eller, om tillämpligt, den verkställande myndigheten meddelar att det inte längre är nödvändigt att bevara och lämna ut uppgifterna.

Mottagaren ska vidta de nödvändiga åtgärderna för att säkerställa konfidentialiteten, sekretessen och integriteten för intyget om en europeisk utlämnandeorder och för de uppgifter som lämnas ut eller bevaras.

AVSNITT A: Utfärdande/godkännande myndighet

Utfärdande stat:

Utfärdande myndighet

Godkännande myndighet (om tillämpligt):

ANM.: uppgifter om utfärdande och godkännande myndighet ska lämnas i slutet (avsnitten I och J)

Den utfärdande myndighetens ärendenummer:

Den godkännande myndighetens ärendenummer:

AVSNITT B: Mottagare

Mottagare:

Utsett verksamhetsställe

Rättsligt ombud

Detta intyg har utfärdats i en nödsituation till den angivna mottagaren eftersom det utsedda verksamhetsstället eller det rättsliga ombudet för en tjänsteleverantör inte reagerade på intyget om en europeisk utlämnandeorder inom de tidsfrister som anges i artikel 10 i förordning (EU) 2023/1543 eller inte har utsetts inom de tidsfrister som anges i Europaparlamentets och rådets direktiv (EU) 2023/1544 ⁽²⁾

Adress:

Tfn/fax/e-post (om känt):

Kontaktperson (om känt):

Mottagarens ärendenummer (om känt):

Berörd tjänsteleverantör (om annan än mottagaren):

Alla övriga relevanta uppgifter:

⁽¹⁾ Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden (EUT L 191, 28.7.2023, s. 118).

⁽²⁾ Europaparlamentets och rådets direktiv (EU) 2023/1544 av den 12 juli 2023 om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden (EUT L 191, 28.7.2023, s. 181).

AVSNITT C: Tidsfrister (kryssa i lämplig ruta och fyll i där så krävs)

Vid mottagandet av intyget om en europeisk utlämnandeorder ska de begärda uppgifterna lämnas ut:

- så snart som möjligt, inom tio dagar (ingen anmälan till den verkställande myndigheten)
- vid anmälan till den verkställande myndigheten: vid utgången av de tio dagarna, om den verkställande myndigheten inte har åberopat en vägransgrund inom denna tidsfrist, eller efter det att den verkställande myndigheten före utgången av de tio dagarna bekräftat att den inte kommer att åberopa någon vägransgrund, så snart som möjligt och senast vid utgången av de tio dagarna.
- utan onödigt dröjsmål och inom åtta timmar i en nödsituation som innebär
- en omedelbar fara för en persons liv, fysiska integritet eller säkerhet
- en omedelbar fara för kritisk infrastruktur enligt definitionen i artikel 2 a i rådets direktiv 2008/114/EG ^(?), om en driftsstörning vid eller en förstörelse av sådan kritisk infrastruktur skulle leda till en omedelbar fara för en persons liv, fysiska integritet eller säkerhet, inbegripet genom allvarlig skada på tillhandahållandet av basförmödenheter till befolkningen eller på utövandet av statens kärnfunktioner.

Ange om det finns några tidsfrister i förfarandet eller andra tidsfrister som bör beaktas vid fullföljandet av detta intyg om en europeisk utlämnandeorder:

Lämna i förekommande fall ytterligare information:

AVSNITT D: Förhållande till en tidigare framställan om utlämnande/bevarande (kryssa i och fyll i om tillämpligt och i förekommande fall)

- De begärda uppgifterna har helt/delvis bevarats i enlighet med en tidigare framställan om bevarande utfärdad av (ange myndighet och ärendenummer) den (ange datum för utfärdande av framställan) och översänd den (ange datum för översändande av framställan) till (ange den tjänsteleverantör/ det rättsliga ombud/ det utsedda verksamhetsställe/den behöriga myndighet som framställan översändes till och, om tillgängligt, det ärendenummer som mottagaren angett).
- De begärda uppgifterna avser en tidigare framställan om utlämnande utfärdad av (ange myndighet och ärendenummer) den (ange datum för utfärdande av framställan) och översänd den (ange datum för översändande av framställan) till (ange den tjänsteleverantör/ det rättsliga ombud/ det utsedda verksamhetsställe/den behöriga myndighet som den översändes till och, om tillgängligt, det ärendenummer som mottagaren angett).
- Annan relevant information:

^(?) Rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet (EUT L 345, 23.12.2008, s. 75).

AVSNITT E: Information som möjliggör identifiering av de begärda uppgifterna (fyll i, i den mån denna information är känd och där så krävs, för att identifiera uppgifterna)

IP-adress(er) och tidsstämplar (inkl. datum och tidszon):

Tfn:

E-postadress(er):

IMEI-nummer (ett eller flera):

MAC-adress(er):

Användare eller andra unika identifierare såsom användarnamn, inloggnings-ID eller kontobeteckning(ar):

Benämning(ar) på relevant(a) tjänst(er):

Övrigt:

Om tillämpligt, tidsintervallet för de uppgifter för vilka utlämnande begärs:

.....

Ytterligare information vid behov:

AVSNITT F: Elektroniska bevis som ska lämnas ut

Detta intyg om en europeisk utlämnandeorder gäller (kryssa i relevant(a) ruta/rutor):

a) abonnentuppgifter:

namn, födelsedatum, postadress eller geografisk adress, kontaktuppgifter (e-postadress, telefonnummer) och annan relevant information om användarens/abonnentens identitet

dag och tidpunkt för den första registreringen, typ av registrering, kopia av kontrakt, kontroll av identitet vid tidpunkten för registrering, kopior av handlingar som abonnenten tillhandahållit

typ av tjänst och dess varaktighet, inbegripet identifierare som används av eller tillhandahålls abonnenten vid tidpunkten för den första registreringen eller aktiveringen (t.ex. telefonnummer, SIM-kortnummer, MAC-adress) och tillhörande utrustning

profilinformation (t.ex. användarnamn, skärmmamn, profilbild)

uppgifter om validering av användningen av tjänster, såsom en alternativ e-postadress som anges av användaren/abonnenten

betal- eller kreditkortsuppgifter (som tillhandahålls av användaren för faktureringsändamål) inklusive andra betalningsmedel

PUK-koder

övrigt:

- b) uppgifter som begärs med det enda syftet att identifiera användaren enligt definitionen i artikel 3.10 i förordning (EU) 2023/1543:
- IP-förbindelseuppgifter såsom IP-adresser/loggar/åtkomstnummer tillsammans med andra tekniska identifierare, såsom källportar och tidsstämplar eller motsvarande, användar-ID och det gränssnitt som används i samband med användningen av tjänsten – ange, vid behov, följande:
 - tidsintervallet för de uppgifter för vilka utlämnande begärs (om annat än avsnitt E):
 - övrigt:
- c) trafikuppgifter:
- i) för (mobil) telefoni:
 - utgående (A) och inkommande (B) identifierare (telefonnummer, IMSI, IMEI)
 - tidpunkt och varaktighet för förbindelsen eller förbindelserna
 - uppringsningsförsök
 - basstationens ID, inklusive geografisk information (X/Y-koordinater) vid tidpunkten för inledande och avslutande av förbindelsen
 - leverantör/teletjänst som används (t.ex. UMTS, GPRS)
 - övrigt:
 - ii) för internet:
 - ruttuppgifter (avsändar- och mottagar-IP-adress(er), portnummer, webbläsare, e-postrubrikinformation, meddelandentifiering)
 - basstationens ID, inklusive geografisk information (X/Y-koordinater) vid tidpunkten för inledande och avslutande av förbindelsen eller förbindelserna
 - datavolymer
 - dag och tidpunkt för förbindelsen eller förbindelserna
 - varaktighet för förbindelsen eller åtkomstsessionen/åtkomstsessionerna
 - övrigt:
 - iii) för värdtjänster:
 - loggfiler
 - ärenden
 - övrigt:
 - iv) övrigt:
 - inköphistoria

faktureringshistoria för förbetalt saldo

övrigt:

d) innehållsdata:

(webb)brevlådedump

minnesdump (användargenererade data)

siddump

meddelandelogg/backup

röstbrevlådedump

serverinnehåll

anordningsbackup

kontaktlista

övrigt:

Ytterligare information vid behov för att (närmare) precisera eller begränsa omfattningen av de begärda uppgifterna:

AVSNITT G: Information om bakomliggande förhållanden

a) Detta intyg om en europeisk utlämnandeorder gäller (kryssa i relevant(a) ruta/rutor):

straffrättsliga förfaranden avseende ett eller flera brott,

verkställighet av ett fängelsestraff eller annan frihetsberövande åtgärd i minst fyra månader till följd av straffrättsliga förfaranden som inte beslutats genom en dom där personen inte var personligen närvarande vid förhandlingen, i fall där den dömda personen undandragit sig lagföring.

b) Beskaffenhet och brottsrubricering för det eller de brott som intyget om en europeisk utlämnandeorder utfärdas för och tillämplig lagbestämmelse (*):

.....

c) Detta intyg om en europeisk utlämnandeorder utfärdas för trafikuppgifter som inte begärs med det enda syftet att identifiera användaren, eller för innehållsdata, eller båda, och avser (kryssa i relevant(a) ruta/rutor om tillämpligt):

brott för vilka maximistraftet i den utfärdande staten är fängelse eller annan frihetsberövande åtgärd i minst tre år,

(*) För verkställighet av ett fängelsestraff eller annan frihetsberövande åtgärd för trafikuppgifter som inte begärs med det enda syftet att identifiera användaren, eller innehållsdata, ange i b) och c) det brott för vilket straffet utdöms.

- en eller flera av följande brott, om de helt eller delvis begås med hjälp av ett informationssystem:
- brott enligt definitionen i artiklarna 3–8 i Europaparlamentets och rådets direktiv (EU) 2019/713 ⁽⁵⁾,
 - brott enligt definitionen i artiklarna 3–7 i Europaparlamentets och rådets direktiv 2011/93/EU ⁽⁶⁾,
 - brott enligt definitionen i artiklarna 3–8 i Europaparlamentets och rådets direktiv 2013/40/EU ⁽⁷⁾,
 - brott enligt definitionen i artiklarna 3–12 och 14 i Europaparlamentets och rådets direktiv (EU) 2017/541 ⁽⁸⁾.

d) Personuppgiftsansvarig/personuppgiftsbiträde:

Europeiska utlämnandeorder ska ställas till tjänsteleverantörer som agerar som personuppgiftsansvariga. Undantagsvis får den europeiska utlämnandeordern ställas direkt till den tjänsteleverantör som behandlar uppgifterna på den personuppgiftsansvariges vägnar.

Kryssa i lämplig ruta:

- Detta intyg om en europeisk utlämnandeorder är ställt till den tjänsteleverantör som agerar som personuppgiftsansvarig.
- Detta intyg om en europeisk utlämnandeorder är ställt till den tjänsteleverantör som, i situationer där den personuppgiftsansvarige inte kan identifieras, eventuellt behandlar uppgifterna på den personuppgiftsansvariges vägnar, eftersom
 - den personuppgiftsansvarige inte kan identifieras trots att rimlig ansträngning gjorts från den utfärdande myndighetens sida
 - det kan vara till skada för utredningen att rikta sig till den personuppgiftsansvarige

Om detta intyg om en europeisk utlämnandeorder är ställt till den tjänsteleverantör som behandlar uppgifter på den personuppgiftsansvariges vägnar ska

- personuppgiftsbiträdet informera den personuppgiftsansvarige om utlämnandet av uppgifter
- personuppgiftsbiträdet tills vidare inte informera den personuppgiftsansvarige om utlämnandet av uppgifter, eftersom det skulle vara till skada för utredningen. Skriv en kort motivering ⁽⁹⁾:

e) Annan relevant information:

AVSNITT H: Information till användaren

Mottagaren ska under alla omständigheter avhålla sig från att informera den person vars uppgifter begärs. Det är den utfärdande myndighetens ansvar att utan onödigt dröjsmål informera personen om utlämnandet av uppgifter.

⁽⁵⁾ Europaparlamentets och rådets direktiv (EU) 2019/713 av den 17 april 2019 om bekämpande av bedrägeri och förfalskning som rör andra betalningsmedel än kontanter och om ersättande av rådets rambeslut 2001/413/RIF (EUT L 123, 10.5.2019, s. 18).

⁽⁶⁾ 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).

⁽⁷⁾ 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).

⁽⁸⁾ Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF (EUT L 88, 31.3.2017 s. 6).

⁽⁹⁾ Den utfärdande myndigheten ska ange skälen till förseningen i ärendet; endast en kort motivering ska läggas till i intyget om en europeisk utlämnandeorder.

Observera att (kryssa i lämplig ruta):

- den utfärdande myndigheten kommer att vänta med att informera den person vars uppgifter begärs så länge ett eller flera av följande villkor är uppfyllda:
- det är nödvändigt för att undvika att hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden
- det är nödvändigt för att undvika att inverka menligt på förebyggande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder
- det är nödvändigt för att skydda den allmänna säkerheten
- det är nödvändigt för att skydda den nationella säkerheten
- det är nödvändigt för att skydda andra människors fri- och rättigheter

AVSNITT I: Närmare uppgifter om den utfärdande myndigheten

Typ av utfärdande myndighet (kryssa i relevant(a) ruta/rutor):

- domare, domstol eller undersökningsdomare
- allmän åklagare
- annan behörig myndighet, enligt den utfärdande statens definition

Om godkännande krävs, fyll också i avsnitt J.

Observera att (kryssa i om tillämpligt):

- Detta intyg om en europeisk utlämnandeorder utfärdades för abonnentuppgifter eller för uppgifter som begärts med det enda syftet att identifiera användaren i en vederbörligen motiverad nödsituation utan förhandsgodkännande, eftersom godkännandet inte skulle kunna ha erhållits i tid, eller båda. Den utfärdande myndigheten bekräftar att den skulle kunna utfärda en order i ett liknande inhemskt fall utan godkännande, och att efterhandsgodkännande kommer att begäras utan onödigt dröjsmål, inom 48 timmar (notera att mottagaren inte kommer att informeras).

Närmare uppgifter om den utfärdande myndigheten eller dess företrädare, eller båda, som intygar att innehållet i intyget om en europeisk utlämnandeorder är riktigt och korrekt:

Myndighetens namn:

Myndighetsföreträdarens namn:

Befattning (titel/grad):

Ärendenummer:

Adress:

Tfn: (landsnummer) (riktnummer)

Fax: (landsnummer) (riktnummer)

E-post:

28.7.2023

SV

Europeiska unionens officiella tidning

L 191/161

Språkkunskaper:

Om annan än ovan, myndighet/kontaktpunkt (t.ex. centralmyndighet) som kan kontaktas för alla frågor som rör fullföljandet av intyget om en europeisk utlämnandeorder:

Myndighetens namn/Namn:

Adress:

Tfn: (landsnummer) (riktnummer)

Fax: (landsnummer) (riktnummer)

E-post:

Den utfärdande myndighetens eller dess företrädares underskrift, som intygar att innehållet i intyget om en europeisk utlämnandeorder är riktigt och korrekt:

Datum:

Underskrift ⁽¹⁰⁾:

AVSNITT J): Närmare uppgifter om den godkännande myndigheten (fyll i om tillämpligt)

Typ av godkännande myndighet

domare, domstol eller undersökningsdomare

allmän åklagare

Närmare uppgifter om den godkännande myndigheten eller dess företrädare, eller båda, som intygar att innehållet i intyget om en europeisk utlämnandeorder är riktigt och korrekt:

Myndighetens namn:

Myndighetsföreträdares namn:

Befattning (titel/grad):

Ärendenummer:

Adress:

Tfn: (landsnummer) (riktnummer)

Fax: (landsnummer) (riktnummer)

E-post:

Språkkunskaper:

⁽¹⁰⁾ Om det decentraliserade it-systemet inte används, lägg också till en officiell stämpel, elektronisk stämpel eller likvärdig autentisering.

Datum:

Underskrift ⁽¹⁾:

AVSNITT K: Anmälan och närmare uppgifter om den verkställande myndighet som mottagit anmälan (om tillämpligt)

Detta intyg om en europeisk utlämnandeorder anmäls till följande verkställande myndighet:

.....

Ange kontaktuppgifter till den verkställande myndighet som mottagit anmälan (om tillgängliga):

Den verkställande myndighetens namn

Adress:

Tfn: (landsnummer) (riktnummer)

Fax: (landsnummer) (riktnummer)

E-post:

AVSNITT L: Överföring av uppgifter

a) Myndighet till vilken uppgifterna ska överföras

utfärdande myndighet

godkännande myndighet

annan behörig myndighet (t.ex. centralmyndighet)

Namn och kontaktuppgifter

b) Föredraget format eller tillvägagångssätt som ska tillämpas vid överföring av uppgifterna (om tillämpligt):

AVSNITT M: Ytterligare information som ska ingå (sänds inte till mottagaren – ska lämnas till den verkställande myndigheten om anmälan till den verkställande myndigheten krävs)

Skälen till att fastställa att den europeiska bevarandeordern uppfyller villkoren för att vara nödvändig och proportionell:

.....

En kortfattad beskrivning av ärendet:

.....

⁽¹⁾ Om det decentraliserade it-systemet inte används, lägg också till en officiell stämpel, elektronisk stämpel eller likvärdig autentisering.

Är straffet för det brott för vilket den europeiska utlämnandeordern utfärdas i den utfärdande staten fängelse eller annan frihetsberövande åtgärd i minst tre år, och ingår det i den förteckning över brott som anges nedan (kryssa i relevant(a) ruta/rutor)?

- Deltagande i en kriminell organisation.
- Terrorism.
- Människohandel.
- Sexuell exploatering av barn samt barnpornografi.
- Olaglig handel med narkotika och psykotropa ämnen.
- Olaglig handel med vapen, ammunition och sprängämnen.
- Korruption.
- Bedrägeri, inbegripet bedrägeri och andra brott som riktar sig mot unionens finansiella intressen enligt definitionen i Europaparlamentets och rådets direktiv (EU) 2017/1371 ⁽¹²⁾.
- Penningtvätt.
- Penningförfalskning, inklusive förfalskning av euron.
- It-brottslighet.
- Miljöbrott, inklusive olaga handel med hotade djurarter och utrotningshotade växtarter och växtsorter.
- Hjälp till olovlig inresa och olovlig vistelse.
- Mord eller grov misshandel.
- Olaglig handel med mänskliga organ och vävnader.
- Människorov, olaga frihetsberövande eller tagande av gisslan.
- Rasism och främlingsfientlighet.
- Organiserad stöld eller väpnat rån.
- Olaglig handel med kulturföremål, inklusive antikviteter och konstverk.
- Svindleri.
- Beskyddarverksamhet och utpressning.
- Varumärkesförfalskning och piratkopiering.
- Förfalskning av administrativa dokument och handel med sådana förfalskningar.
- Förfalskning av betalningsmedel.
- Olaglig handel med hormonpreparat och andra tillväxsubstanser.

⁽¹²⁾ Europaparlamentets och rådets direktiv (EU) 2017/1371 av den 5 juli 2017 om bekämpande genom straffrättsliga bestämmelser av bedrägeri som riktar sig mot unionens finansiella intressen (EUT L 198, 28.7.2017, s. 29).

- Olaglig handel med nukleära och radioaktiva ämnen.
- Handel med stulna fordon.
- Våldtäkt.
- Mordbrand.
- Brott som omfattas av Internationella brottmålsdomstolens jurisdiktion.
- Kapning av flygplan eller fartyg.
- Sabotage.

Lägg i förekommande fall till ytterligare information som den verkställande myndigheten kan behöva för att bedöma möjligheten att åberopa vägransgrunder:

.....

BILAGA II

INTYG OM EN EUROPEISK BEVARANDEORDER FÖR BEVARANDE AV ELEKTRONISKA BEVIS

Enligt Europaparlamentets och rådets förordning (EU) 2023/1543 ⁽¹⁾ ska mottagaren av detta intyg om en europeisk bevarandeorder utan onödigt dröjsmål efter att ha mottagit intyget om en europeisk bevarandeorder bevara de uppgifter som begärs. Bevarandet ska upphöra efter 60 dagar, såvida inte den utfärdande myndigheten förlänger bevarandeperioden med ytterligare 30 dagar eller bekräftar att en efterföljande framställan om utlämnande har utfärdats. Om den utfärdande myndigheten inom dessa tidsperioder bekräftar att en efterföljande framställan om utlämnande har utfärdats ska mottagaren bevara uppgifterna under så lång tid som krävs för att lämna ut dessa när framställan om utlämnande mottas.

Mottagaren ska vidta de nödvändiga åtgärderna för att säkerställa konfidentialiteten, sekretessen och integriteten för intyget om en europeisk bevarandeorder och för de uppgifter som bevaras.

AVSNITT A: Utfärdande/godkännande myndighet

Utfärdande stat:

Utfärdande myndighet:

Godkännande myndighet (om tillämpligt):

ANM.: uppgifter om utfärdande och godkännande myndighet ska lämnas i slutet (avsnitten F och G)

Den utfärdande myndighetens ärendenummer:

Den godkännande myndighetens ärendenummer:

AVSNITT B: Mottagare:

Mottagare:

Utsett verksamhetsställe

Rättsligt ombud

Detta intyg har utfärdats i en nödsituation till den angivna mottagaren eftersom det utsedda verksamhetsstället eller det rättsliga ombudet för en tjänsteleverantör inte reagerade på intyget om en europeisk bevarandeorder inom tidsfristerna eller inte har utsetts inom de tidsfrister som anges i Europaparlamentets och rådets direktiv (EU) 2023/1544 ⁽²⁾

⁽¹⁾ Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden (EUT L 191, 28.7.2023, s. 118).

⁽²⁾ Europaparlamentets och rådets direktiv (EU) 2023/1544 av den 12 juli 2023 om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden (EUT L 191, 28.7.2023, s. 181).

Adress:

Tfn/fax/e-post (om känd):.....

Kontaktperson (om känd):.....

Mottagarens ärendenummer (om känt):.....

Berörd tjänsteleverantör (om annan än mottagaren):

Eventuella andra relevanta uppgifter:

AVSNITT C: Information som möjliggör identifiering av de uppgifter som framställan om bevarande gäller (fyll i i den mån denna information är känd och där så krävs för att identifiera uppgifterna)

IP-adress(er) och tidsstämplar (inkl. datum och tidszon):.....

Tfn:.....

E-postadress(er):.....

IMEI-nummer (ett eller flera):.....

MAC-adress(er):.....

Användare av tjänsten eller andra unika identifierare såsom användarnamn, inloggnings-ID eller kontobeteckning(ar):

Benämning(ar) på relevant(a) tjänst(er):.....

Övrigt:.....

Om tillämpligt, tidsintervallet för de uppgifter för vilka bevarande begärs:

Ytterligare information vid behov:.....

AVSNITT D: Elektroniska bevis som ska bevaras

Detta intyg om en europeisk bevarandeorder gäller (kryssa i relevant(a) ruta/rutor):

a) abonnentuppgifter:

namn, födelsedatum, postadress eller geografisk adress, kontaktuppgifter (e-postadress, telefonnummer) och annan relevant information om användarens/abonnentens identitet

dag och tidpunkt för den första registreringen, typ av registrering, kopia av kontrakt, kontroll av identitet vid tidpunkten för registrering, kopior av handlingar som abonnenten tillhandahållit

- typ av tjänst och dess varaktighet, inbegripet identifierare som används av eller tillhandahålls av abonnenten vid tidpunkten för den första registreringen eller aktiveringen (t.ex. telefonnummer, SIM-kortnummer, MAC-adress) och tillhörande utrustning
 - profilinformation (t.ex. användarnamn, skärmbild, profilbild)
 - uppgifter om validering av användningen av tjänster, såsom en alternativ e-postadress som anges av användaren/abbonenten
 - betal- eller kreditkortsuppgifter (som tillhandahålls av användaren för faktureringsändamål) inklusive andra betalningsmedel
 - PUK-koder
 - övrigt:
- b) uppgifter som begärs med det enda syftet att identifiera användaren enligt definitionen i artikel 3.10 i förordning (EU) 2023/1543:
- IP-förbindelseuppgifter såsom IP-adresser/loggar/åtkomstnummer tillsammans med andra identifierare, såsom källportar och tidsstämplar eller motsvarande, användar-ID och det gränssnitt som används i samband med användningen av tjänsten och som är strängt nödvändiga för identifieringsändamål; precisera vid behov: ...
 - tidsintervallet för de uppgifter för vilka bevarande begärs (om annat än i avsnitt C):.....
 - övrigt:
- c) trafikuppgifter:
- i) för (mobil) telefoni:
- utgående (A) och inkommande (B) identifierare (telefonnummer, IMSI, IMEI)
 - tidpunkt och varaktighet för förbindelsen eller förbindelserna
 - uppringningsförsök
 - basstationens ID, inklusive geografisk information (X/Y-koordinater) vid tidpunkten för inledande och avslutande av förbindelsen
 - leverantör/teletjänst som används (t.ex. UMTS, GPRS)
 - övrigt:
- ii) för internet:
- ruttuppgifter (avsändar- och mottagar-IP-adress(er), portnummer, webbläsare, e-postrubrikinformation, meddelandekodning)
 - basstationens ID, inklusive geografisk information (X/Y-koordinater) vid tidpunkten för inledande och avslutande av förbindelsen eller förbindelserna

<input type="checkbox"/> datavolym
<input type="checkbox"/> dag och tidpunkt för förbindelsen/förbindelserna
<input type="checkbox"/> varaktighet för förbindelsen eller åtkomstsessionen/åtkomstsessionerna
<input type="checkbox"/> övrigt:.....
iii) för värdtjänster:
<input type="checkbox"/> loggfiler
<input type="checkbox"/> ärenden
<input type="checkbox"/> övrigt:.....
iv) Övrigt
<input type="checkbox"/> inköphistoria
<input type="checkbox"/> faktureringshistoria för förbetalt saldo
<input type="checkbox"/> övrigt:.....
d <input type="checkbox"/> innehållsdata:
<input type="checkbox"/> (webb)brevlådedump
<input type="checkbox"/> minnesdump (användargenererade data)
<input type="checkbox"/> siddump
<input type="checkbox"/> meddelandelogg/backup
<input type="checkbox"/> röstbrevlådedump
<input type="checkbox"/> serverinnehåll
<input type="checkbox"/> anordningsbackup
<input type="checkbox"/> kontaktlista
<input type="checkbox"/> övrigt:.....
<input type="checkbox"/> Ytterligare information vid behov för att precisera eller begränsa omfattningen av de begärda uppgifterna:.....

28.7.2023

SV

Europeiska unionens officiella tidning

L 191/169

AVSNITT E: Information om bakomliggande förhållanden

a) Detta intyg om en europeisk bevarandeorder gäller (kryssa i relevant(a) ruta/rutor):

- straffrättsliga förfaranden avseende ett eller flera brott,
- verkställighet av ett fängelsestraff eller annan frihetsberövande åtgärd i minst fyra månader till följd av straffrättsliga förfaranden som inte beslutats genom en dom där personen inte var personligen närvarande vid förhandlingen, i fall där den dömda personen undandragit sig lagföring.

b) Beskaffenhet och brottsrubricering för det eller de brott som intyget om en europeisk bevarandeorder utfärdas för samt tillämplig lagbestämmelse ^(?).....

AVSNITT F: Närmare uppgifter om den utfärdande myndigheten

Typ av utfärdande myndighet (kryssa i relevant(a) ruta/rutor):

- domare, domstol eller undersökningsdomare
- allmän åklagare
- annan behörig myndighet enligt den utfärdande statens rätt

Om godkännande krävs, fyll också i avsnitt G.

Observera att (kryssa i om tillämpligt):

- Detta intyg om en europeisk bevarandeorder utfärdades för abonnentuppgifter eller uppgifter som begärts med det enda syftet att identifiera användaren i en vederbörligen motiverad nödsituation utan förhandsgodkännande, eftersom godkännandet inte skulle kunna ha erhållits i tid, eller båda. Den utfärdande myndigheten bekräftar att den skulle kunna utfärda en order i ett liknande inhemskt fall utan godkännande, och att efterhandsgodkännande kommer att begäras utan onödigt dröjsmål, inom 48 timmar (notera att mottagaren inte kommer att informeras).

Nödsituationen avser en situation där det råder ett överhängande hot mot en persons liv, fysiska integritet eller säkerhet eller ett överhängande hot mot en kritisk infrastruktur enligt definitionen i artikel 2 a i rådets direktiv 2008/114/EG ^(*), om en driftsstörning vid eller en förstörelse av sådan kritisk infrastruktur skulle leda till en omedelbar fara för en persons liv, fysiska integritet eller säkerhet, inbegripet genom allvarlig skada på tillhandahållandet av basförnödenheter till befolkningen eller på utövandet av statens kärnfunktioner.

Närmare uppgifter om den utfärdande myndigheten och/eller dess företrädare som intygar att innehållet i intyget om en europeisk bevarandeorder är riktigt och korrekt:

Myndighetens namn:.....

Myndighetsföreträdarens namn:.....

Befattning (titel/grad):.....

^(?) För verkställighet av ett fängelsestraff eller annan frihetsberövande åtgärd, ange det brott som straffet utdömts för.

^(*) Rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur (EUT L 345, 23.12.2008, s. 75).

Ärendenummer:

Adress:

Tfn: (landsnummer) (riktnummer)

Fax: (landsnummer) (riktnummer)

E-post:

Språkkunskaper:

Om annan än ovan, myndighet/kontaktpunkt (t.ex. centralmyndighet) som kan kontaktas för alla frågor som rör fullföljandet av intyget om en europeisk bevarandeorder:

Myndighetens namn/Namn:

Adress:

Tfn: (landsnummer) (riktnummer)

Fax: (landsnummer) (riktnummer)

E-post:

Den utfärdande myndighetens eller dess företrädares underskrift, som intygar att innehållet i intyget om en europeisk bevarandeorder är riktigt och korrekt:

Datum:

Underskrift (⁵):.....

AVSNITT G: Uppgifter om den godkännande myndigheten (fyll i om tillämpligt)

Typ av godkännande myndighet:

domare, domstol eller undersökningsdomare

allmän åklagare

Närmare uppgifter om den godkännande myndigheten eller dess företrädare, eller både och, som intygar att innehållet i intyget om en europeisk bevarandeorder är riktigt och korrekt:

Myndighetens namn:

Myndighetsföreträdares namn:

Befattning (titel/grad):.....

(⁵) Om det decentraliserade it-systemet inte används, lägg också till en officiell stämpel, elektronisk stämpel eller likvärdig autentisering.

Ärendenummer:.....
Adress:
Tfn: (landsnummer) (riktnummer).....
Fax: (landsnummer) (riktnummer).....
E-post:
Språkkunskaper:
Datum:.....
Underskrift ⁽⁶⁾ :.....

⁽⁶⁾ Om det decentraliserade it-systemet inte används, lägg också till en officiell stämpel, elektronisk stämpel eller likvärdig autentisering.

BILAGA III

INFORMATION OM OMÖJLIGHETEN ATT FULLFÖLJA ETT INTYG OM EN EUROPEISK UTLÄMNANDEORDER/ETT INTYG OM EN EUROPEISK UTLÄMNANDEORDER

Om mottagaren inte kan fullgöra sin skyldighet att bevara de uppgifter som begärs enligt ett intyg om en europeisk bevarandeorder eller lämna ut dem enligt ett intyg om en europeisk utlämnandeorder, inte kan iakta den angivna tidsfristen eller inte tillhandahåller uppgifterna i deras helhet, ska detta formulär enligt Europaparlamentets och rådets förordning (EU) 2023/1543 ⁽¹⁾ fyllas i av mottagaren och utan onödigt dröjsmål skickas tillbaka till den utfärdande myndigheten samt, om en anmälan har skett till den verkställande myndigheten och i övriga tillämpliga fall, till den verkställande myndighet som avses i intyget om en europeisk utlämnandeorder.

Där så är möjligt ska mottagaren bevara de begärda uppgifterna även om ytterligare information behövs för att exakt identifiera dem, såvida inte informationen i intyget om en europeisk utlämnandeorder/intyget om en europeisk bevarandeorder är otillräcklig för detta syfte. Om det behövs klargöranden från den utfärdande myndigheten ska mottagaren utan onödigt dröjsmål begära sådana med hjälp av detta formulär.

AVSNITT A: Berörd order

Följande uppgifter gäller:

- ett intyg om en europeisk utlämnandeorder
- ett intyg om en europeisk bevarandeorder

AVSNITT B: Behörig(a) myndighet(er)

Utfärdande myndighet:

Den utfärdande myndighetens ärendenummer:

Om tillämpligt, den godkännande myndigheten:

Om tillämpligt, den godkännande myndighetens ärendenummer:

Datum för utfärdande av intyget om en europeisk utlämnandeorder/intyget om en europeisk bevarandeorder:

Datum för mottagande av intyget om en europeisk utlämnandeorder/intyget om en europeisk bevarandeorder:

Om tillämpligt, den verkställande myndigheten:

Om tillgängligt, den verkställande myndighetens ärendenummer:

AVSNITT C: Mottagare av intyget om en europeisk utlämnandeorder/intyget om en europeisk bevarandeorder:

Mottagare av intyget om en europeisk utlämnandeorder/intyget om en europeisk bevarandeorder:

Mottagarens ärendenummer:

⁽¹⁾ Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden (EUT L 191, 28.7.2023, s. 118).

AVSNITT D: Skäl för uteblivet fullföljande

a) Intyget om en europeisk utlämnandeorder/intyget om en europeisk bevarandeorder kan inte fullföljas eller kan inte fullföljas inom den angivna tidsfristen av följande skäl:

- det är ofullständigt
- det innehåller uppenbara fel
- det innehåller inte tillräckliga uppgifter
- det gäller inte uppgifter som lagras av eller på uppdrag av tjänsteleverantören vid den tidpunkt då intyget om en europeisk utlämnandeorder/intyget om en europeisk bevarandeordermottas
- andra skäl som avser en faktisk omöjlighet till följd av omständigheter som inte beror på mottagaren eller tjänsteleverantören vid den tidpunkt då intyget om en europeisk utlämnandeorder/intyget om en europeisk bevarandeordermottas
- den europeiska utlämnandeorden/den europeiska bevarandeorden har inte utfärdats eller godkänts av en utfärdande myndighet enligt artikel 4 i förordning (EU) 2023/1543.
- den europeiska utlämnandeorden för att inhämta trafikuppgifter som inte begärs med det enda syftet att identifiera användaren enligt definitionen i artikel 3.10 i förordning (EU) 2023/1543, eller för att inhämta innehållsdata, har utfärdats för ett brott som inte omfattas av artikel 5.4 i förordning (EU) 2023/1543
- tjänsten omfattas inte av förordning (EU) 2023/1543
- de begärda uppgifterna skyddas av immunitet eller privilegier som beviljas enligt den verkställande statens rätt, eller de begärda uppgifterna omfattas av reglerna för fastställande eller begränsning av straffrättsligt ansvar som hänför sig till tryckfrihet eller yttrandefrihet i andra medier och som hindrar den europeiska utlämnandeorden/den europeiska bevarandeorden från att verkställas
- efterlevnad av den europeiska utlämnandeorden skulle strida mot ett tredjelands tillämpliga lagstiftning. Fyll också i avsnitt E.

b) Redogör närmare för skälen till sådant uteblivet fullföljande som avses i led i, och ange och förklara vid behov eventuella andra skäl än de som anges i led i:

.....

SECTION E: Motstridiga skyldigheter som följer av ett tredjelands rätt

I händelse av motstridiga skyldigheter som följer av ett tredjelands rätt, vänligen lämna följande information:

— lagrubrik(er) i tredjelandet:

.....

— tillämplig(a) lagbestämmelse(r) och texten i relevanta bestämmelser:

.....

— vari den motstridiga skyldigheten består, inbegripet intressen som skyddas av tredjelands rätt:

enskildas grundläggande rättigheter (precisera):

.....

grundläggande intressen för tredjelandet som rör nationell säkerhet och försvar (precisera):

.....

övriga intressen (precisera):

 — förklara varför lagen är tillämplig i detta fall:

 — förklara varför en konflikt anses föreligga i detta fall:

 — förklara kopplingen mellan tjänsteleverantören och tredjelandet i fråga:

 — möjliga konsekvenser för mottagaren av att efterleva den europeiska utlämnandeordern, inklusive sanktioner som kan komma i fråga:

 Eventuell ytterligare relevant information:

AVSNITT F: Framställan om ytterligare information/förtydligande (fyll i, om tillämpligt)
 Det behövs ytterligare information från den utfärdande myndigheten för att intyget om en europeisk utlämnandeorder/intyget om en europeisk bevarandeorder ska fullföljas:

AVSNITT G: Bevarande av uppgifter
 De begärda uppgifterna (kryssa i relevant ruta och fyll i):
 ska bevaras till dess att uppgifterna lämnas ut, eller till dess att den utfärdande myndigheten eller, om tillämpligt, den verkställande myndigheten meddelar att det inte längre är nödvändigt att bevara och lämna ut uppgifter eller till dess att den utfärdande myndigheten tillhandahåller nödvändig information som gör det möjligt att begränsa de uppgifter som ska bevaras/lämnas ut
 ska inte bevaras (detta bör ske endast i undantagsfall, t.ex. om tjänsteleverantören inte har uppgifterna vid den tidpunkt då framställan mottas eller inte kan identifiera de begärda uppgifterna i tillräcklig grad)

AVSNITT H: Kontaktuppgifter till tjänsteleverantörens utsedda verksamhetsställe/rättsliga ombud
 Namn på tjänsteleverantörens utsedda verksamhetsställe/rättsliga ombud:

 Kontaktperson:
 Befattning:
 Adress:
 Tfn: (landsnummer) (riktnummer)
 Fax: (landsnummer) (riktnummer)
 E-post:
 Den bemyndigade personens namn:
 Datum
 Underskrift (?):

(?) Om det decentraliserade it-systemet inte används, lägg också till en officiell stämpel, elektronisk stämpel eller likvärdig autentisering.

BILAGA IV

KATEGORIER AV BROTT SOM AVSES I ARTIKEL 12.1 D

1. Deltagande i en kriminell organisation.
2. Terrorism.
3. Människohandel.
4. Sexuellt utnyttjande av barn samt barnpornografi.
5. Olaglig handel med narkotika och psykotropa ämnen.
6. Olaglig handel med vapen, ammunition och sprängämnen.
7. Korruption.
8. Bedrägeri, inbegripet bedrägeri och andra brott som riktar sig mot unionens finansiella intressen enligt definitionen i Europaparlamentets och rådets direktiv (EU) 2017/1371 ⁽¹⁾.
9. Penningtvätt.
10. Penningförfalskning, inklusive förfalskning av euron.
11. It-brottslighet.
12. Miljöbrott, inklusive olaga handel med hotade djurarter och utrotningshotade växtarter och växtsorter.
13. Hjälp till olovlig inresa och olovlig vistelse.
14. Mord eller grov misshandel.
15. Olaglig handel med mänskliga organ och vävnader.
16. Människorov, olaga frihetsberövande eller tagande av gisslan.
17. Rasism och främlingsfientlighet.
18. Organiserad stöld eller väpnat rån.
19. Olaglig handel med kulturföremål, inklusive antikviteter och konstverk.
20. Svindleri.
21. Beskyddarverksamhet och utpressning.
22. Förfalskning och piratkopiering.

⁽¹⁾ Europaparlamentets och rådets direktiv (EU) 2017/1371 av den 5 juli 2017 om bekämpande genom straffrättsliga bestämmelser av bedrägeri som riktar sig mot unionens finansiella intressen (EUT L 198, 28.7.2017, s. 29).

23. Förfalskning av administrativa dokument och handel med sådana förfalskningar.
 24. Förfalskning av betalningsmedel.
 25. Olaglig handel med hormonsubstanser och andra tillväxsubstanser.
 26. Olaglig handel med nukleära och radioaktiva ämnen.
 27. Handel med stulna fordon.
 28. Våldtäkt.
 29. Mordbrand.
 30. Brott som omfattas av Internationella brottmålsdomstolens behörighet.
 31. Kapning av flygplan eller fartyg
 32. Sabotage.
-

BILAGA V

BEKRÄFTELSE PÅ UTFÄRDANDE AV EN FRAMSTÄLLAN OM UTLÄMNANDE TILL FÖLJD AV EN EUROPEISK BEVARANDEORDER

Enligt Europaparlamentets och rådets förordning (EU) 2023/1543 ⁽¹⁾ ska mottagaren av intyget om en europeisk bevarandeorder utan onödigt dröjsmål bevara de uppgifter som begärs. Bevarandet ska upphöra efter 60 dagar, såvida inte den utfärdande myndigheten förlänger bevarandeperioden med ytterligare 30 dagar eller bekräftar att en efterföljande framställan om utlämnande har utfärdats med hjälp av det formulär som anges i denna bilaga.

Efter en sådan bekräftelse ska mottagaren bevara uppgifterna under så lång tid som krävs för att lämna ut dessa när framställan om utlämnande mottas.

AVSNITT A: Utfärdande myndighet för intyget om en europeisk bevarandeorder

Utfärdande stat:

Utfärdande myndighet:

Om annan än den kontaktpunkt som anges i intyget om en europeisk bevarandeorder, den myndighet/kontaktpunkt (t.ex. centralmyndighet) som kan kontaktas för alla frågor som rör fullföljandet av intyget om en europeisk bevarandeorder:

Namn och kontaktuppgifter

AVSNITT B: Mottagare av intyget om en europeisk bevarandeorder:

Mottagare:

Adress:

Tfn/fax/e-post (om känd):

Kontaktperson (om känd):

Mottagarens ärendenummer (om känt)

Berörd tjänsteleverantör (om annan än mottagaren):

Eventuella andra relevanta uppgifter:

⁽¹⁾ Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden (EUT L 191, 28.7.2023, s. 118).

AVSNITT C: Information om intyget om en europeisk bevarandeorder:

Uppgifterna bevaras i enlighet med intyget om en europeisk bevarandeorder som utfärdades den..... (ange datum för utfärdande av ordern) och som översändes den..... (ange datum för översändande av ordern) med ärendenummer..... (ange ärendenummer).

Den förlängdes med 30 dagar av den utfärdande myndigheten...., ärendenummer... den (kryssa i rutan och ange, om tillämpligt).

AVSNITT D: Bekräftelse

Detta bekräftar att följande utlämnandeorder har utfärdats (kryssa i lämplig ruta och fyll i vid behov):

Intyg om en europeisk utlämnandeorder som utfärdats av (ange myndighet) den..... (ange datum för utfärdande av ordern) och som översändes den..... (ange datum för översändande av ordern) med ärendenummer (ange ärendenummer) till (ange den tjänsteleverantör/det utsedda verksamhetsställe/det rättsliga ombud/den behöriga myndighet som den översändes till och, om tillgängligt, det ärendenummer som mottagaren angett).

En europeisk utredningsorder som utfärdats av (ange myndighet) den..... (ange datum för utfärdande av ordern) och som översändes den..... (ange datum för översändande av ordern) med ärendenummer (ange ärendenummer) till..... (ange den stat och behöriga myndighet som den översändes till och, om tillgängligt, det ärendenummer som de anmodade myndigheterna angett).

Framställning om ömsesidig rättslig hjälp som utfärdats av..... (ange myndighet) den..... (ange datum för utfärdande av framställningen) och som översändes den..... (ange datum för översändande av framställningen) med ärendenummer (ange ärendenummer) till..... (den stat och behöriga myndighet som framställningen överlämnades till och, om tillgängligt, det ärendenummer som de anmodade myndigheterna uppgivit).

Underskrift av den utfärdande myndigheten och/eller dess företrädare:

Namn:

Datum:

Underskrift (?):.....

(?) Om det decentraliserade it-systemet inte används, lägg också till en officiell stämpel, elektronisk stämpel eller likvärdig autentisering.

BILAGA VI

FÖRLÄNGNING AV BEVARANDET AV ELEKTRONISKA BEVIS

Enligt Europaparlamentets och rådets förordning (EU) 2023/1543 ⁽¹⁾ ska mottagaren av intyget om en europeisk bevarandeorder utan onödigt dröjsmål bevara de uppgifter som begärs. Bevarandet ska upphöra efter 60 dagar, såvida inte den utfärdande myndigheten bekräftar att en efterföljande utlämnandeorder har utfärdats. Inom 60 dagar får den utfärdande myndigheten förlänga bevarandeperioden med ytterligare 30 dagar om det är nödvändigt för att göra det möjligt att utfärda en efterföljande utlämnandeorder, med hjälp av det formulär som anges i denna bilaga.

AVSNITT A: Utfärdande myndighet för intyget om en europeisk bevarandeorder

Utfärdande stat:

Utfärdande myndighet:

Den utfärdande myndighetens ärendenummer:

Om annan än den kontaktpunkt som anges i intyget om en europeisk bevarandeorder, den myndighet/kontaktpunkt (t.ex. centralmyndighet) som kan kontaktas för alla frågor som rör fullföljandet av intyget om en europeisk bevarandeorder:

Namn och kontaktuppgifter:

AVSNITT B: Mottagare av intyget om en europeisk bevarandeorder:

Mottagare:

Adress:

Tfn/fax/e-post (om känd):

Kontaktperson (om känd):

Mottagarens ärendenummer (om känt)

Berörd tjänsteleverantör (om annan än mottagaren)

Eventuella andra relevanta uppgifter:

AVSNITT C: Information om tidigare intyg om en europeisk bevarandeorder:

Uppgifternas bevaras i enlighet med det intyg om en europeisk bevarandeorder som utfärdades den (ange datum för utfärdande av ordern) och som översändes den (ange datum för översändande av ordern) med ärendenummer (ange ärendenummer) till

⁽¹⁾ Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden (EUT L 191, 28.7.2023, s. 118).

AVSNITT D: Förlängning av tidigare bevarandeorder

Skyldigheten att bevara uppgifter enligt det intyg om en europeisk bevarandeorder som anges i avsnitt C förlängs härmed med ytterligare 30 dagar.

Underskrift av den utfärdande myndigheten och/eller dess företrädare:

Namn: ...

Datum: ...

Underskrift (²):

(²) Om det decentraliserade it-systemet inte används, lägg också till en officiell stämpel, elektronisk stämpel eller likvärdig autentisering.

Europaparlamentets och rådets direktiv (EU) 2023/1544

DIREKTIV

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2023/1544

av den 12 juli 2023

om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artiklarna 53 och 62,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ⁽¹⁾,i enlighet med det ordinarie lagstiftningsförfarandet ⁽²⁾, och

av följande skäl:

- (1) Nätverksbaserade tjänster kan tillhandahållas från vilken plats som helst och kräver inte fysisk infrastruktur, lokaler eller personal i det land där den aktuella tjänsten erbjuds, eller på den inre marknaden i sig. Detta innebär att det kan vara svårt att tillämpa och säkra efterlevnaden av skyldigheter som föreskrivs i nationell rätt och unionsrätt som är tillämplig på de berörda tjänsteleverantörerna, i synnerhet skyldigheten att efterleva ett föreläggande från eller ett beslut av en rättslig myndighet. Detta är fallet i synnerhet inom straffrätten, där det är svårt för medlemsstaternas myndigheter att delge, säkerställa efterlevnad av och verkställa sina beslut, särskilt när de aktuella tjänsterna tillhandahålls från en plats utanför deras territorium. Mot denna bakgrund har medlemsstaterna vidtagit en rad olikartade åtgärder för att kunna tillämpa och genomdriva sin lagstiftning på ett mer effektivt sätt. Detta omfattar åtgärder för att begära att tjänsteleverantörer inhämtar elektroniska bevis som är av betydelse för straffrättsliga förfaranden. I detta syfte har vissa medlemsstater antagit, eller överväger att anta, lagstiftning som föreskriver obligatorisk juridisk representation inom sitt eget territorium för ett antal tjänsteleverantörer som erbjuder tjänster på det territoriet. Sådana krav skapar hinder för det fria tillhandahållandet av tjänster på den inre marknaden.
- (2) Det finns en risk för att medlemsstaterna, i avsaknad av en enhetlig unionsansats, kommer att försöka åtgärda befintliga brister i samband med insamlingen av elektroniska bevis i straffrättsliga förfaranden genom att införa olikartade nationella skyldigheter. Sådana olikartade nationella skyldigheter skulle skapa hinder för det fria tillhandahållandet av tjänster på den inre marknaden.
- (3) Avsaknaden av en enhetlig unionsansats leder till en osäkerhet om rättsläget som påverkar både tjänsteleverantörer och nationella myndigheter. Olikartade och eventuellt motstridiga skyldigheter är tillämpliga på tjänsteleverantörer som är etablerade eller erbjuder tjänster i olika medlemsstater, vilket leder till att sådana tjänsteleverantörer blir föremål för olika sanktioner vid överträdelser. Sådana skillnader i ramverket för straffrättsliga förfaranden kommer sannolikt att öka ytterligare på grund av den ökande betydelsen av kommunikationstjänster och informationssamhällestjänster i våra dagliga liv och i våra samhällen. Sådana skillnader utgör inte bara ett hinder för en väl fungerande inre marknad utan medför också problem för upprättandet av unionens område med frihet, säkerhet och rättvisa och för att det ska kunna fungera korrekt.
- (4) För att undvika skillnader i det rättsliga ramverket och för att säkerställa att företag som bedriver verksamhet på den inre marknaden har samma eller liknande skyldigheter har unionen antagit ett antal rättsakter inom närliggande områden såsom dataskydd, nämligen Europaparlamentets och rådets förordning (EU) 2016/679 ⁽³⁾ och

⁽¹⁾ EUT C 367, 10.10.2018, s. 88.

⁽²⁾ Europaparlamentets ståndpunkt av den 13 juni 2023 (ännu inte offentliggjord i EUT) och rådets beslut av den 27 juni 2023.

⁽³⁾ 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).

Europaparlamentets och rådets direktiv 2002/58/EG⁽⁴⁾. För att höja skyddsnivån för de registrerade föreskrivs i förordning (EU) 2016/679 att personuppgiftsansvariga eller personuppgiftsbiträden som inte är etablerade i unionen men som erbjuder varor eller tjänster till registrerade i unionen eller övervakar de registrerades beteende om detta utövas inom unionen, ska utse en rättslig företrädare i unionen, såvida inte behandlingen av uppgifterna är tillfällig, inte omfattar behandling i stor skala av särskilda kategorier av personuppgifter eller behandling av personuppgifter som rör fällande domar i brottmål och överträdelse, och det är osannolikt att den leder till en risk för fysiska personers rättigheter och friheter, med beaktande av behandlingens art, sammanhang, omfattning och ändamål eller om den personuppgiftsansvarige eller personuppgiftsbiträdet är en offentlig myndighet eller ett offentligt organ.

- (5) Genom att fastställa harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för vissa tjänsteleverantörer i unionen när det gäller mottagande, efterlevnad och verkställighet av beslut och förelägganden som utfärdats av behöriga myndigheter i medlemsstaterna, i syfte att samla in elektroniska bevis i straffrättsliga förfaranden, bör de befintliga hindren för det fria tillhandahållandet av tjänster undanröjas, och införandet av olikartade nationella ansatser i detta avseende i framtiden bör förhindras. Det bör därför skapas likvärdiga förutsättningar för tjänsteleverantörer. Beroende på om tjänsteleverantörerna är etablerade i unionen eller inte bör medlemsstaterna säkerställa att de utser ett utsett etableringsställe eller ett rättsligt ombud. Dessa harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud bör inte påverka tjänsteleverantörernas skyldigheter enligt annan unionslagstiftning. Dessutom bör en effektivare brottsbekämpning inom unionens område med frihet, säkerhet och rättvisa underlättas.
- (6) De utsedda verksamhetsställen och rättsliga ombud som föreskrivs i detta direktiv bör fungera som mottagare för beslut och förelägganden för insamling av elektroniska bevis på grundval av Europaparlamentets och rådets förordning (EU) 2023/1543⁽⁵⁾, Europaparlamentets och rådets direktiv 2014/41/EU⁽⁶⁾ och den konvention som upprättats av rådet i enlighet med artikel 34 i fördraget om Europeiska unionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater⁽⁷⁾, även när dessa beslut och förelägganden översänds i form av ett intyg.

Användningen av det utsedda verksamhetsstället eller det rättsliga ombudet bör ske i enlighet med de förfaranden som anges i de instrument och lagar som är tillämpliga i det rättsliga förfarandet, även när instrumenten medger direkt överföring av förelägganden i gränsöverskridande situationer till tjänsteleverantörens utsedda verksamhetsställe eller rättsliga ombud eller grundas på samarbete mellan behöriga rättsliga myndigheter. De behöriga myndigheterna i den medlemsstat där det utsedda verksamhetsstället är etablerat eller där det rättsliga ombudet har sin hemvist bör agera i enlighet med den roll som fastställs för dem i respektive instrument där inblandning föreskrivs. Medlemsstaterna bör också kunna rikta beslut och förelägganden, i syfte att samla in elektroniska bevis på grundval av nationell rätt, till en fysisk eller juridisk person som agerar som rättsligt ombud eller som utsett verksamhetsställe åt en tjänsteleverantör på deras territorium.

- (7) Medlemsstaterna bör säkerställa att tjänsteleverantörer som erbjuder tjänster i unionen den 18 februari 2026 är skyldiga att utse minst ett utsett verksamhetsställe eller minst ett rättsligt ombud senast den 18 augusti 2026 och att tjänsteleverantörer som börjar erbjuda tjänster i unionen efter den dagen utser minst ett utsett verksamhetsställe eller minst ett rättsligt ombud inom sex månader efter den dag då de börjar erbjuda tjänster i unionen. Utan att det påverkar tillämpningen av dataskyddsgarantier kan ett sådant utsett verksamhetsställe eller rättsligt ombud delas mellan flera olika tjänsteleverantörer, i synnerhet tjänsteleverantörer som är små eller medelstora företag.
- (8) Skyldigheten att utse ett utsett verksamhetsställe eller ett rättsligt ombud bör gälla för tjänsteleverantörer som erbjuder tjänster i unionen, det vill säga i en eller flera medlemsstater. Situationer i vilka en tjänsteleverantör är etablerad på en medlemsstats territorium och erbjuder tjänster uteslutande på den medlemsstats territorium bör inte omfattas av detta direktiv.

⁽⁴⁾ 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).

⁽⁵⁾ Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff till följd av straffrättsliga förfaranden (se sidan 118 i detta nummer av EUT).

⁽⁶⁾ Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området (EUT L 130, 1.5.2014, s. 1).

⁽⁷⁾ Konvention, upprättad av rådet i enlighet med artikel 34 i Fördraget om Europeiska unionen, om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater (EGT C 197, 12.7.2000, s. 3) och dess protokoll (EGT C 326, 21.11.2001, s. 2).

- (9) I syfte att samla in elektroniska bevis i straffrättsliga förfaranden bör medlemsstaterna kunna fortsätta att rikta framställningar till tjänsteleverantörer som är etablerade på deras territorium för rent inhemska situationer i enlighet med unionsrätten och deras respektive nationella rätt. Även om det enligt den inhemska rätten finns möjligheter att rikta framställningar till tjänsteleverantörer på sitt eget territorium bör medlemsstaterna inte kringgå de principer som ligger till grund för detta direktiv eller förordning (EU) 2023/1543.
- (10) För att fastställa om en tjänsteleverantör erbjuder tjänster i unionen krävs en bedömning av huruvida tjänsteleverantören gör det möjligt för fysiska eller juridiska personer i en eller flera medlemsstater att använda dess tjänster. Enbart det faktum att ett onlinegränssnitt är tillgängligt i unionen, till exempel genom en tjänsteleverantörs eller en mellanhands webbplats eller en e-postadress eller andra kontaktpuffgifter, bör dock inte i sig anses vara tillräckligt för att fastställa att en tjänsteleverantör erbjuder tjänster i unionen i den mening som avses i detta direktiv.
- (11) För att fastställa huruvida en tjänsteleverantör erbjuder tjänster i unionen krävs, utöver en bedömning av huruvida tjänsteleverantören gör det möjligt för fysiska eller juridiska personer i en eller flera medlemsstater att använda dess tjänster, att man fastställer huruvida det finns en betydande anknytning till unionen. En sådan betydande anknytning till unionen bör anses föreligga om tjänsteleverantören har ett verksamhetsställe i unionen. I avsaknad av ett sådant verksamhetsställe bör kriteriet för en betydande anknytning baseras på specifika faktiska kriterier, såsom att det finns ett betydande antal användare i en eller flera medlemsstater eller att verksamheten är inriktad på en eller flera medlemsstater. Huruvida verksamheten är inriktad på en eller flera medlemsstater bör fastställas på grundval av alla relevanta omständigheter, inbegripet faktorer som användningen av ett språk eller en valuta som allmänt används i den medlemsstaten, eller möjligheten att beställa varor eller tjänster.

Att verksamheten är inriktad på en medlemsstat skulle också kunna härledas från det faktum att det finns en app i den berörda nationella appbutiken, att lokal marknadsföring eller reklam görs på det språk som allmänt används i den medlemsstaten eller att kundkontakter, till exempel kundtjänst, sköts på det språk som allmänt används i den medlemsstaten. En betydande anknytning bör också anses föreligga när en tjänsteleverantör riktar sin verksamhet mot en eller flera medlemsstater enligt Europaparlamentets och rådets förordning (EU) nr 1215/2012⁽⁹⁾. Däremot bör tillhandahållande av en tjänst enbart i syfte att efterleva det förbud mot diskriminering som fastställs i Europaparlamentets och rådets förordning (EU) 2018/302⁽⁹⁾ inte utan ytterligare skäl anses innebära att verksamheten är inriktad på ett visst territorium i unionen. Samma överväganden bör tillämpas för att fastställa huruvida en tjänsteleverantör erbjuder tjänster på en medlemsstats territorium.

- (12) Olika instrument som omfattas av avdelning V kapitel 4 i fördraget om Europeiska unionens funktionssätt är tillämpliga på samarbetet mellan medlemsstaterna vid insamling av bevis i straffrättsliga förfaranden. Till följd av de variationer som föreligger inom unionens område med frihet, säkerhet och rättvisa finns det ett behov att säkerställa att detta direktiv inte underlättar uppkomsten av ytterligare skillnader eller hinder för tillhandahållandet av tjänster på den inre marknaden genom att se till att tjänsteleverantörer som erbjuder tjänster på medlemsstaternas territorium utser utsedda verksamhetsställen eller rättsliga ombud i medlemsstater som inte deltar i de berörda rättsliga instrumenten. Därför bör minst ett utsett verksamhetsställe eller ett rättsligt ombud utses i en medlemsstat som deltar i unionens relevanta rättsliga instrument, för att undvika risken att det utseende som föreskrivs i detta direktiv blir mindre ändamålsenligt och för att utnyttja de synergier som det innebär att ha ett utsett verksamhetsställe eller ett rättsligt ombud för mottagande, efterlevnad och verkställighet av beslut och förelägganden som omfattas av detta direktiv, inbegripet enligt förordning (EU) 2023/1543, direktiv 2014/41/EU och den konvention som upprättats av rådet i enlighet med artikel 34 i fördraget om Europeiska unionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater. Att utse ett utsett verksamhetsställe eller ett rättsligt ombud, som också skulle kunna användas för att säkerställa efterlevnad av nationella rättsliga skyldigheter, skulle dessutom göra det möjligt att dra nytta av de synergier som uppkommer när man har en tydlig kontaktpunkt för att rikta framställningar till tjänsteleverantörer i syfte att samla in bevis i straffrättsliga förfaranden.

⁽⁹⁾ Europaparlamentets och rådets förordning (EU) nr 1215/2012 av den 12 december 2012 om domstols behörighet och om erkännande och verkställighet av domar på privaträttsens område (EUT L 351, 20.12.2012, s. 1).

⁽⁹⁾ Europaparlamentets och rådets förordning (EU) 2018/302 av den 28 februari 2018 om åtgärder mot omotiverad geoblockering och andra former av diskriminering på grund av kunders nationalitet, bostättningsort eller etableringsort på den inre marknaden och om ändring av förordningarna (EG) nr 2006/2004 och (EU) 2017/2394 samt direktiv 2009/22/EG (EUT L 60 I, 2.3.2018, s. 1).

- (13) Det bör stå tjänsteleverantörer fritt att välja i vilken medlemsstat de utser sitt utsedda verksamhetsställe eller, i förekommande fall, sitt rättsliga ombud, och medlemsstaterna bör inte kunna begränsa denna valfrihet, till exempel genom att införa en skyldighet att utse det utsedda verksamhetsstället eller det rättsliga ombudet på deras territorium. Detta direktiv bör dock också innehålla vissa begränsningar av tjänsteleverantörernas valfrihet, i synnerhet att det utsedda verksamhetsstället bör vara etablerat – eller, i förekommande fall, det rättsliga ombudet ha sin hemvist – i en medlemsstat där tjänsteleverantören tillhandahåller tjänster eller är etablerad, samt fastställa en skyldighet att utse ett utsett verksamhetsställe eller ett rättsligt ombud i en av de medlemsstater som deltar i ett rättsligt instrument som avses i detta direktiv. Enbart det faktum att ett rättsligt ombud har utsetts bör inte anses utgöra etablering av tjänsteleverantören.
- (14) De tjänsteleverantörer som är mest relevanta när det gäller insamling av bevis i straffrättsliga förfaranden är leverantörer av elektroniska kommunikationstjänster och specifika leverantörer av informationssamhällets tjänster som underlättar interaktion mellan användare. Båda dessa grupper bör därför omfattas av detta direktiv. Elektroniska kommunikationstjänster definieras i Europaparlamentets och rådets direktiv (EU) 2018/1972⁽¹⁰⁾ och omfattar interpersonella kommunikationstjänster såsom VoIP, meddelandetjänster och e-posttjänster. Det här direktivet bör vara tillämpligt på andra leverantörer av informationssamhällets tjänster i den mening som avses i Europaparlamentets och rådets direktiv (EU) 2015/1535⁽¹¹⁾ som inte kan betecknas som leverantörer av elektroniska kommunikationstjänster men som erbjuder sina användare möjligheten att kommunicera med varandra eller erbjuder sina användare tjänster som kan användas för att lagra eller på annat sätt behandla uppgifter för deras räkning. Detta skulle vara i linje med de begrepp som används i Europarådets konvention om it-relaterad brottslighet (ETS nr 185), utfärdad i Budapest den 23 november 2001, även kallad Budapestkonventionen. Uppgiftsbehandling bör förstås i teknisk mening, alltså som skapande eller manipulation av uppgifter, det vill säga teknisk bearbetning för att framställa eller ändra uppgifter med hjälp av datorernas bearbetningskapacitet.

De kategorier av tjänsteleverantörer som omfattas av det här direktivet bör till exempel inkludera marknadsplatser online som ger konsumenter och företag möjlighet att kommunicera med varandra och andra värdtjänster, även när tjänsten tillhandahålls via molntjänster, liksom plattformar för onlinespel. Om en leverantör av informationssamhällets tjänster inte ger sina användare möjlighet att kommunicera med varandra utan endast med tjänsteleverantören, eller inte ger en möjlighet att lagra eller på annat sätt behandla uppgifter, eller om lagringen av uppgifter inte är en avgörande komponent, det vill säga en väsentlig del, av den tjänst som tillhandahålls användarna, såsom juridiska tjänster, dataarkitekturtjänster och bokföringstjänster som tillhandahålls online på distans, bör den inte omfattas av definitionen av tjänsteleverantör i det här direktivet, även om de tjänster som tillhandahålls av den tjänsteleverantören är informationssamhällets tjänster i den mening som avses i direktiv (EU) 2015/1535.

- (15) Leverantörer av internetinfrastruktur tjänster som rör tilldelning av namn och nummer, såsom domännamnsregister och domännamnsregistratorer samt leverantörer av integritetstjänster och proxytjänster, eller regionala internetregister över IP-adresser, är särskilt relevanta när det gäller att identifiera aktörer bakom skadliga eller komprometterade webbplatser. De innehar uppgifter som skulle kunna göra det möjligt att identifiera en person eller enhet som ligger bakom en webbplats som används för brottslig verksamhet, eller offret för brottslig verksamhet.
- (16) Medlemsstaterna bör säkerställa att tjänsteleverantörer som är etablerade eller erbjuder tjänster på deras territorium ger sina utsedda verksamhetsställen och rättsliga ombud de befogenheter och resurser som krävs för att efterleva beslut och förelägganden som omfattas av detta direktiv och som mottas från en medlemsstat. Medlemsstaterna bör också kontrollera att de utsedda verksamhetsställena eller rättsliga ombuden med hemvist på deras territorium av tjänsteleverantörerna har fått de befogenheter och resurser som krävs för att efterleva beslut och förelägganden som omfattas av detta direktiv och som mottas från en medlemsstat och att de samarbetar med de behöriga myndigheterna vid mottagandet av dessa beslut och förelägganden, i enlighet med den tillämpliga rättsliga ramen. Avsaknad av sådana åtgärder eller brister i dem bör inte kunna anföras som skäl för att rättfärdiga bristande efterlevnad av beslut eller förelägganden som omfattas av detta direktiv.

⁽¹⁰⁾ 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).

⁽¹¹⁾ 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).

Dessutom bör tjänsteleverantörer inte kunna rättfärdiga sin bristande efterlevnad av skyldigheter som följer av den tillämpliga rättsliga ramen vid mottagande av beslut eller förelägganden som omfattas av detta direktiv med hänvisning till att interna rutiner saknas eller är ineffektiva, eftersom de är ansvariga för att tillhandahålla de befogenheter och resurser som krävs för att garantera efterlevnad av sådana beslut och förelägganden. Utsedda verksamhetsställen eller rättsliga ombud bör inte heller kunna rättfärdiga sådan bristande efterlevnad genom att till exempel hävda att de inte har befogenhet att lämna uppgifter. I detta syfte bör medlemsstaterna säkerställa att både det utsedda verksamhetsstället eller det rättsliga ombudet och tjänsteleverantören kan hållas solidariskt ansvariga för bristande efterlevnad av de skyldigheter som följer av den tillämpliga rättsliga ramen vid mottagande av beslut och förelägganden som omfattas av detta direktiv, så att var och en av dem kan bli föremål för sanktioner för att någon av dem brutit i efterlevnad. I synnerhet bör det inte vara möjligt för tjänsteleverantören eller det utsedda verksamhetsstället, eller i förekommande fall det rättsliga ombudet, att använda avsaknaden av lämpliga interna rutiner mellan tjänsteleverantören och det utsedda verksamhetsstället eller det rättsliga ombudet som motivering för sin bristande efterlevnad av dessa skyldigheter. Solidariskt ansvar bör inte gälla för något som tjänsteleverantören eller det utsedda verksamhetsstället, eller i förekommande fall det rättsliga ombudet, har gjort eller försummat att göra som utgör ett brott i den medlemsstat som tillämpar sanktionerna.

- (17) Medlemsstaterna bör säkerställa att varje tjänsteleverantör som är etablerad eller erbjuder tjänster på deras territorium skriftligen underrättar centralmyndigheten, som utsetts i enlighet med detta direktiv, i den medlemsstat där dess utsedda verksamhetsställe är etablerat eller dess rättsliga ombud har sin hemvist om kontaktpuppgifterna för det utsedda verksamhetsstället eller rättsliga ombudet och om eventuella ändringar av dessa. Underretelsen bör också innehålla information om på vilka språk en framställan kan riktas till det utsedda verksamhetsstället eller det rättsliga ombudet, vilket bör inbegripa ett eller flera av de officiella språken som fastställs i nationell rätt i den medlemsstat där det utsedda verksamhetsstället är etablerat eller det rättsliga ombudet har sin hemvist, men kan också inbegripa andra officiella språk i unionen, såsom språket i den medlemsstat där de har sitt säte. Om en tjänsteleverantör utser flera utsedda verksamhetsställen eller flera rättsliga ombud i enlighet med detta direktiv bör medlemsstaterna säkerställa att en sådan tjänsteleverantör för varje utsett verksamhetsställe eller rättsligt ombud anger det exakta territoriella tillämpningsområdet för sitt utseende. Territoriet i samtliga medlemsstater som deltar i de instrument som omfattas av detta direktiv bör omfattas. Medlemsstaterna bör säkerställa att deras respektive behöriga myndigheter riktar alla sina beslut och förelägganden enligt detta direktiv till det utsedda verksamhetsställe eller det rättsliga ombud som tjänsteleverantören har angett. Medlemsstaterna bör säkerställa att den information som de underrättas om i enlighet med detta direktiv är allmänt tillgänglig på en särskild webbsida hos det europeiska straffrättsliga nätverket i syfte att underlätta samordningen mellan medlemsstaterna och användningen av de utsedda verksamhetsställena eller det rättsliga ombudet av myndigheter från en annan medlemsstat. Medlemsstaterna bör säkerställa att sådan information uppdateras regelbundet. Det bör också vara möjligt att ytterligare sprida informationen för att göra det lättare för behöriga myndigheter att få tillgång till denna information, till exempel via särskilda interna webbplatser eller forum och plattformar.
- (18) Medlemsstaterna bör fastställa regler om sanktioner för överträdelse av nationella bestämmelser som antagits enligt detta direktiv och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna bör vara effektiva, proportionella och avskräckande. Medlemsstaterna bör senast den dag som anges i detta direktiv anmäla dessa regler och åtgärder till kommissionen samt utan dröjsmål eventuella ändringar som berör dem. Medlemsstaterna bör också årligen informera kommissionen om tjänsteleverantörer som inte uppfyller kraven, relevanta verkställighetsåtgärder som vidtagits mot dem och påförda sanktioner. Sanktionerna bör under inga omständigheter leda till ett permanent eller tillfälligt förbud mot tillhandahållande av tjänster. Medlemsstaterna bör samordna sina åtgärder för tillsyn av efterlevnaden när en tjänsteleverantör erbjuder tjänster i flera medlemsstater. Centralmyndigheter bör samarbeta för att säkerställa ett enhetligt och proportionellt tillvägagångssätt. Kommissionen bör vid behov underlätta sådan samordning och bör under alla omständigheter hållas underrättad om överträdelser. Detta direktiv reglerar inte avtalsarrangemangen för överföring eller ändring av ekonomiska konsekvenser mellan tjänsteleverantörer, utsedda verksamhetsställen och rättsliga ombud av sanktioner som påförs dem.
- (19) Vid fastställandet av lämpliga sanktioner för tjänsteleverantörers överträdelser bör de behöriga myndigheterna beakta alla relevanta omständigheter, såsom tjänsteleverantörens ekonomiska kapacitet, överträdelsens art, allvarlighetsgrad och varaktighet, huruvida den begåtts uppsåtligt eller av oaksamhet samt huruvida tjänsteleverantören har hållits ansvarig för liknande tidigare överträdelser. I detta sammanhang bör särskild uppmärksamhet ägnas åt mikroföretag.
- (20) Detta direktiv påverkar inte nationella myndigheters befogenheter i civilrättsliga eller administrativa förfaranden, inte heller där sådana förfaranden kan leda till sanktioner.

- (21) För att säkerställa en enhetlig tillämpning av detta direktiv bör ytterligare mekanismer för samordning mellan medlemsstaterna inrättas. För detta ändamål bör medlemsstaterna utse en eller flera centralmyndigheter som kan ge information och stöd till centralmyndigheter i andra medlemsstater i samband med tillämpningen av detta direktiv, i synnerhet när verkställighetsåtgärder enligt detta direktiv övervägs. Samordningsmekanismen bör säkerställa att berörda medlemsstater informeras om en medlemsstats avsikt att vidta en verkställighetsåtgärd. Dessutom bör medlemsstaterna säkerställa att centralmyndigheter kan förse varandra med all relevant information och stöd i en sådan situation och samarbeta med varandra där så är relevant. Samarbete mellan centralmyndigheter i samband med verkställighetsåtgärder kan innefatta samordning av en verkställighetsåtgärd mellan behöriga myndigheter i olika medlemsstater. Ett sådant samarbete bör syfta till att undvika positiva och negativa behörighetskonflikter. Vid samordning av verkställighetsåtgärder bör centralmyndigheterna vid behov även involvera kommissionen. Dessa myndigheters skyldighet att samarbeta bör inte påverka en enskild medlemsstats rätt att besluta om sanktioner mot tjänsteleverantörer som inte fullgör sina skyldigheter enligt detta direktiv. Att centralmyndigheter utses och information om dem offentliggörs skulle underlätta tjänsteleverantörernas anmälningar om att de har utsett sitt utsedda verksamhetsställe eller rättsliga ombud och lämnande av kontaktoppgifter för detta till den medlemsstat där deras utsedda verksamhetsställe är etablerat eller deras rättsliga ombud har sin hemvist. I detta syfte bör medlemsstaterna underrätta kommissionen om sin eller sina utsedda centralmyndigheter, och kommissionen bör översända en förteckning över utsedda centralmyndigheter till medlemsstaterna och göra den tillgänglig för allmänheten.
- (22) Eftersom målet för detta direktiv, nämligen att undanröja hinder för det fria tillhandahållandet av tjänster inom ramen för insamling av elektroniska bevis i straffrättsliga förfaranden, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av dessa tjänsters gränslösa karaktär, 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.
- (23) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725⁽¹²⁾ och avgav ett yttrande den 6 november 2019⁽¹³⁾.
- (24) Kommissionen bör göra en utvärdering av detta direktiv, vilken bör grunda sig på de fem kriterierna effektivitet, ändamålsenlighet, relevans, enhetlighet och EU-mervärde, och den utvärderingen bör ligga till grund för konsekvensbedömningar av möjliga framtida åtgärder. Utvärderingen bör ha slutförts senast den 18 augusti 2029, för att möjliggöra insamling av tillräckliga uppgifter om dess praktiska genomförande. Information bör samlas in regelbundet för att utgöra underlag för utvärderingen av detta direktiv.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Innehåll och tillämpningsområde

1. I detta direktiv fastställs regler för att utse utsedda verksamhetsställen och rättsliga ombud för vissa tjänsteleverantörer som erbjuder tjänster i unionen, för mottagande, efterlevnad och verkställighet av beslut och förelägganden som utfärdas av behöriga myndigheter i medlemsstaterna i syfte att samla in elektroniska bevis i straffrättsliga förfaranden.

2. Detta direktiv är tillämpligt på beslut och förelägganden för insamling av elektroniska bevis på grundval av förordning (EU) 2023/1543, direktiv 2014/41/EU och den konvention som upprättats av rådet i enlighet med artikel 34 i fördraget om Europeiska unionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater. Detta direktiv är även tillämpligt på beslut och förelägganden för insamling av elektroniska bevis på grundval av nationell rätt som en medlemsstat riktar till en fysisk eller juridisk person som agerar som rättsligt ombud eller som utsett verksamhetsställe åt en tjänsteleverantör på den medlemsstats territorium.

⁽¹²⁾ 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).

⁽¹³⁾ EUT C 32, 31.1.2020, s. 11.

3. Detta direktiv påverkar inte de nationella myndigheternas befogenheter att i enlighet med unionsrätten och nationell rätt rikta framställningar direkt till tjänsteleverantörer som är etablerade på deras territorium i syfte att samlas in elektroniska bevis i straffrättsliga förfaranden.
4. Medlemsstaterna får inte ålägga tjänsteleverantörer ytterligare skyldigheter utöver dem som följer av detta direktiv, i synnerhet i fråga om att utse utsedda verksamhetsställen eller rättsliga ombud, för de ändamål som anges i punkt 1.
5. Detta direktiv är tillämpligt på tjänsteleverantörer enligt definitionen i artikel 2.1 som erbjuder sina tjänster i unionen. Det är inte tillämpligt på tjänsteleverantörer som är etablerade på en enda medlemsstats territorium och som erbjuder tjänster uteslutande på den medlemsstats territorium.

Artikel 2

Definitioner

I detta direktiv gäller följande definitioner:

1. *tjänsteleverantör*: en fysisk eller juridisk person som tillhandahåller en eller flera av följande kategorier av tjänster, med undantag för finansiella tjänster som avses i artikel 2.2 b i Europaparlamentets och rådets direktiv 2006/123/EG ⁽¹⁴⁾:
 - a) Elektroniska kommunikationstjänster enligt definitionen i artikel 2.4 i direktiv (EU) 2018/1972.
 - b) Tjänster för internetdomännamn och IP-numrering, såsom tjänster för tilldelning av IP-adresser, tjänster för domännamnsregister, tjänster för domännamnsregistratorer och domännamnsrelaterade integritets- och proxytjänster.
 - c) Andra av informationssamhällets tjänster enligt artikel 1.1 b i direktiv (EU) 2015/1535 som
 - i) gör det möjligt för användarna att kommunicera med varandra, eller
 - ii) gör det möjligt att lagra eller på annat sätt behandla uppgifter på uppdrag av de användare till vilka tjänsten tillhandahålls, förutsatt att datalagringen är en avgörande komponent i den tjänst som tillhandahålls användaren.
2. erbjudande av tjänster på en medlemsstats territorium:
 - a) att göra det möjligt för fysiska eller juridiska personer i en medlemsstat att använda de tjänster som förtecknas i punkt 1, och
 - b) att ha en betydande anknytning, baserad på specifika faktiska kriterier, till den medlemsstat som avses i led a; en sådan betydande anknytning ska anses föreligga om tjänsteleverantören har ett verksamhetsställe i den medlemsstaten eller, i avsaknad av ett sådant verksamhetsställe, om det finns ett betydande antal användare den medlemsstaten eller om verksamheten är inriktad på den medlemsstaten.
3. erbjuda tjänster i unionen:
 - a) att göra det möjligt för fysiska eller juridiska personer i en medlemsstat att använda de tjänster som förtecknas i punkt 1, och
 - b) att ha en betydande anknytning, baserad på specifika faktiska kriterier, till den medlemsstat som avses i led a; en sådan betydande anknytning ska anses föreligga om tjänsteleverantören har ett verksamhetsställe i en medlemsstat eller, i avsaknad av ett sådant verksamhetsställe, om det finns ett betydande antal användare i en eller flera medlemsstater eller om verksamheten är inriktad på en eller flera medlemsstater.

⁽¹⁴⁾ Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden (EUT L 376, 27.12.2006, s. 36).

4. *verksamhetsställe*: en enhet som de facto utövar ekonomisk verksamhet under en obegränsad tid genom en stabil infrastruktur varifrån tillhandahållandet av tjänster genomförs eller verksamheten förvaltas.
5. *utsett verksamhetsställe*: ett verksamhetsställe med ställning som juridisk person vilket skriftligen utsetts av en tjänsteleverantör som är etablerad i en medlemsstat, och vilket deltar i ett rättsligt instrument som avses i artikel 1.2, för de ändamål som avses i artiklarna 1.1 och 3.1.
6. *rättsligt ombud*: en fysisk eller juridisk person som skriftligen utsetts av en tjänsteleverantör som inte är etablerad i en medlemsstat, och som deltar i ett rättsligt instrument som avses i artikel 1.2, för de ändamål som avses i artiklarna 1.1 och 3.1.

Artikel 3

Utsetta verksamhetsställen och rättsliga ombud

1. Medlemsstaterna ska säkerställa att tjänsteleverantörer som erbjuder tjänster i unionen utser minst en mottagare för mottagande, efterlevnad och verkställighet av beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 (*beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2*) som utfärdats av medlemsstaternas behöriga myndigheter för insamling av bevis i straffrättsliga förfaranden, enligt följande:
 - a) För tjänsteleverantörer som är etablerade i unionen och som är juridiska personer ska de medlemsstater där tjänsteleverantörerna är etablerade säkerställa att dessa tjänsteleverantörer utser det eller de utsetta verksamhetsställen som ansvarar för den verksamhet som beskrivs i inledningen till denna punkt.
 - b) För tjänsteleverantörer som inte är etablerade i unionen och som är juridiska personer ska medlemsstaterna säkerställa att sådana tjänsteleverantörer som erbjuder tjänster på deras territorium utser det eller de rättsliga ombud som ansvarar för den verksamhet som beskrivs i inledningen till denna punkt i de medlemsstater som deltar i de instrument som avses i artikel 1.2.
 - c) För tjänsteleverantörer som är etablerade i medlemsstater som inte deltar i de instrument som avses i artikel 1.2 ska medlemsstaterna säkerställa att de tjänsteleverantörer som erbjuder tjänster på deras territorium utser det eller de rättsliga ombud som ansvarar för den verksamhet som beskrivs i inledningen till denna punkt i de medlemsstater som deltar i sådana instrument.
2. Medlemsstaterna ska säkerställa att de mottagare som avses i punkt 1
 - a) är etablerade eller har sin hemvist i en medlemsstat där tjänsteleverantörerna erbjuder sina tjänster, och
 - b) kan bli föremål för verkställighetsförfaranden.
3. Medlemsstaterna ska säkerställa att beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 riktas till det utsetta verksamhetsställe eller rättsliga ombud som utsetts för det ändamålet i enlighet med punkt 1 i den här artikeln.
4. Medlemsstaterna ska säkerställa att tjänsteleverantörer som är etablerade eller erbjuder tjänster på deras territorium ger sina utsetta verksamhetsställen och rättsliga ombud de befogenheter och resurser som krävs för att efterleva beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2 och som mottas från en medlemsstat. Medlemsstaterna ska också kontrollera att de utsetta verksamhetsställen som är etablerade på eller rättsliga ombud som har sin hemvist på deras territorium av tjänsteleverantörerna har fått de befogenheter och resurser som krävs för att efterleva dessa beslut och förelägganden som mottas från en medlemsstat och att de samarbetar med de behöriga myndigheterna vid mottagandet av dessa beslut och förelägganden, i enlighet med den tillämpliga rättsliga ramen.
5. Medlemsstaterna ska säkerställa att både det utsetta verksamhetsstället eller det rättsliga ombudet och tjänsteleverantören kan hållas solidariskt ansvariga för bristande efterlevnad av de skyldigheter som följer av den tillämpliga rättsliga ramen vid mottagande av beslut och förelägganden som omfattas av det tillämpningsområde som fastställs i artikel 1.2, så att var och en av dem kan bli föremål för sanktioner för att någon av dem brustit i efterlevnad. Medlemsstaterna ska i synnerhet säkerställa att det inte är möjligt för tjänsteleverantören eller det utsetta

verksamhetsstället, eller i förekommande fall det rättsliga ombudet, att använda avsaknaden av lämpliga interna rutiner mellan tjänsteleverantören och det utsedda verksamhetsstället eller det rättsliga ombudet för att rättfärdiga sin bristande efterlevnad av dessa skyldigheter. Solidariskt ansvar ska inte gälla för något som antingen tjänsteleverantören eller det utsedda verksamhetsstället, eller det rättsliga ombudet i förekommande fall, har gjort eller försummat att göra och som utgör ett brott i den medlemsstat som påför sanktionerna.

6. Medlemsstaterna ska säkerställa att tjänsteleverantörer som erbjuder tjänster i unionen den 18 februari 2026 är skyldiga att utse utsedda verksamhetsställen eller rättsliga ombud senast den 18 augusti 2026 och att tjänsteleverantörer som börjar erbjuda tjänster i unionen efter den 18 februari 2026 är skyldiga att utse utsedda verksamhetsställen eller rättsliga ombud inom sex månader efter den dag då de börjar erbjuda tjänster i unionen.

Artikel 4

Underrättelser och språk

1. Medlemsstaterna ska säkerställa att varje tjänsteleverantör som är etablerad eller erbjuder tjänster på deras territorium skriftligen underrättar den centralmyndighet som utsetts i enlighet med artikel 6 i den medlemsstat där dess utsedda verksamhetsställe är etablerat eller där dess rättsliga ombud har sin hemvist om kontaktoppgifterna för det verksamhetsstället eller rättsliga ombudet och om eventuella ändringar av dessa.

2. I den underrättelse som avses i punkt 1 ska det anges på vilket eller vilka av unionens officiella språk, i enlighet med rådets förordning nr 1⁽¹⁵⁾, som framställningar kan riktas till det rättsliga ombudet eller utsedda verksamhetsstället. Dessa språk ska inbegripa ett eller flera av de officiella språk som fastställs i nationell rätt i den medlemsstat där det utsedda verksamhetsstället är etablerat eller det rättsliga ombudet har sin hemvist.

3. Om en tjänsteleverantör utser flera utsedda verksamhetsställen eller flera rättsliga ombud i enlighet med artikel 3.1 ska medlemsstaterna säkerställa att en sådan tjänsteleverantör i den underrättelse som avses i punkt 1 i den här artikeln anger det exakta territoriella tillämpningsområdet för utseendet av dessa utsedda verksamhetsställen eller rättsliga ombud. I underrättelsen ska det anges på vilket eller vilka av de officiella språken i unionen eller medlemsstaterna som framställningar kan riktas till vart och ett av de utsedda verksamhetsställena eller de rättsliga ombuden.

4. Medlemsstaterna ska säkerställa att den information som de underrättas om i enlighet med denna artikel offentliggörs på en särskild webbsida hos det europeiska straffrättsliga nätverket. Medlemsstaterna ska säkerställa att denna information uppdateras regelbundet. Informationen får spridas vidare i syfte att underlätta de behöriga myndigheternas åtkomst till den.

Artikel 5

Sanktioner

Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av nationella bestämmelser som antagits enligt artiklarna 3 och 4 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 18 februari 2026 samt utan dröjsmål eventuella ändringar som berör dem. Medlemsstaterna ska också årligen informera kommissionen om tjänsteleverantörer som inte uppfyller kraven, relevanta verkställighetsåtgärder som vidtagits mot dem och påförda sanktioner.

Artikel 6

Centralmyndigheter

1. Medlemsstaterna ska i enlighet med sina rättssystem utse en eller flera centralmyndigheter för att säkerställa att detta direktiv tillämpas på ett enhetligt och proportionellt sätt.

2. Medlemsstaterna ska underrätta kommissionen om den eller de centralmyndigheter som de utser enligt punkt 1. Kommissionen ska översända en förteckning över utsedda centralmyndigheter till medlemsstaterna och göra den tillgänglig för allmänheten.

⁽¹⁵⁾ Rådets förordning nr 1 om vilka språk som skall användas i Europeiska ekonomiska gemenskapen (EGT 17, 6.10.1958, s. 385).

3. Medlemsstaterna ska säkerställa att deras centralmyndigheter samordnar och samarbetar med varandra och vid behov med kommissionen, och att centralmyndigheterna förser varandra med lämplig information och lämpligt stöd i syfte att tillämpa detta direktiv på ett enhetligt och proportionellt sätt. Sådan samordning, sådant samarbete och sådant tillhandahållande av information och stöd ska i synnerhet omfatta verkställighetsåtgärder.

Artikel 7

Införlivande

1. Medlemsstaterna ska senast den 18 februari 2026 sätta i kraft de bestämmelser i lagar och andra författningar som är nödvändiga för att följa detta direktiv. De ska genast underrätta kommissionen om texten till dessa bestämmelser.
2. När en medlemsstat antar dessa bestämmelser 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.
3. Medlemsstaterna ska underrätta kommissionen om texten till de bestämmelser i nationell rätt som de antar inom det område som omfattas av detta direktiv.

Artikel 8

Utvärdering

Senast den 18 augusti 2029 ska kommissionen göra en utvärdering av detta direktiv. Kommissionen ska översända utvärderingsrapporten till Europaparlamentet och rådet. Utvärderingen ska genomföras i enlighet med kommissionens riktlinjer om bättre lagstiftning. Medlemsstaterna ska förse kommissionen med de uppgifter som är nödvändiga för att utarbeta denna rapport.

Artikel 9

Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 10

Adressater

Detta direktiv riktar sig till medlemsstaterna i enlighet med fördragen.

Utfärdat i Strasbourg den 12 juli 2023.

På Europaparlamentets vägnar

R. METSOLA

Ordförande

På rådets vägnar

P. NAVARRO RÍOS

Ordförande

Andra tilläggsprotokollet till konventionen om it-brottslighet om utökat samarbete och utlämnande av elektroniska bevis

II

(Icke-lagstiftningsakter)

INTERNATIONELLA AVTAL

ÖVERSÄTTNING

Andra tilläggsprotokollet till konventionen om it-brottslighet om utökad samarbete och utlämnande av elektroniska bevis**Ingress**

EUROPARÅDETS MEDLEMSSTATER OCH ÖVRIGA STATER SOM ÄR PARTER I KONVENTIONEN om it-brottslighet (ETS nr 185, nedan kallad *konventionen*), vilken öppnades för undertecknande i Budapest den 23 november 2001, och som undertecknat detta protokoll,

SOM BETÄNKER konventionens räckvidd och inverkan i alla regioner i världen,

SOM ERINRAR OM att konventionen redan kompletteras av tilläggsprotokollet om kriminalisering av gärningar av rasistisk och främlingsfientlig natur som begås med hjälp av ett datorsystem (ETS nr 189), öppnat för undertecknande i Strasbourg den 28 januari 2003 (nedan kallat *det första protokollet*), mellan parterna i det protokollet,

SOM BEAKTAR Europarådets befintliga fördrag om straffrättsligt samarbete samt andra avtal och arrangemang om straffrättsligt samarbete mellan parterna i konventionen,

SOM ÄVEN TAR HÄNSYN till konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS nr 108), i dess ändrade lydelse genom dess ändringsprotokoll (CETS nr 223), öppnad för undertecknande i Strasbourg den 10 oktober 2018, och till vilken alla stater kan inbjudas att ansluta sig,

SOM ERKÄNNER den ökande användningen av informations- och kommunikationsteknik, inbegripet internettjänster, och den ökande it-brottsligheten, som utgör ett hot mot demokratin och rättsstatsprincipen och som många stater också anser utgör ett hot mot de mänskliga rättigheterna,

SOM OCKSÅ ERKÄNNER det växande antalet offer för it-brottslighet och vikten av att skipa rättvisa för dessa offer,

SOM ERINRAR OM att regeringar har ansvar för att skydda samhälle och enskilda mot brott, inte bara offline utan även online, inbegripet genom effektiva brottsutredningar och åtal,

SOM ÄR MEDVETNA OM att bevis för brott i allt högre grad lagras i elektronisk form i datorsystem i utländska eller okända jurisdiktioner, eller flera olika jurisdiktioner, och som är övertygade om att det krävs ytterligare åtgärder för att lagligen erhålla sådan bevisning för att möjliggöra effektiva straffrättsliga åtgärder och upprätthålla rättsstatsprincipen,

SOM ERKÄNNER behovet av ökat och effektivare samarbete mellan stater och den privata sektorn och att det i detta sammanhang behövs större klarhet eller rättssäkerhet för tjänsteleverantörer och andra enheter när det gäller de omständigheter under vilka de kan svara på direkta framställningar från andra parter straffrättsliga myndigheter om utlämnande av elektroniska data,

SOM DÄRFÖR HAR SOM MÅL att ytterligare stärka samarbetet om it-brottslighet och insamling av bevis i elektronisk form för brott i samband med särskilda brottsutredningar eller straffrättsliga förfaranden genom ytterligare verktyg för effektivare ömsesidig rättslig hjälp och andra former av samarbete mellan behöriga myndigheter, samarbete i nödsituationer, och direkt samarbete mellan behöriga myndigheter och tjänsteleverantörer och andra enheter som innehar eller kontrollerar relevant information,

SOM ÄR ÖVERTYGADE OM att ett effektivt gränsöverskridande samarbete för lagföringsändamål, även mellan den offentliga och den privata sektorn, gynnas av effektiva villkor och garantier för skyddet av de mänskliga rättigheterna och de grundläggande friheterna,

SOM ERKÄNNER att insamling av elektroniska bevis för brottsutredningar ofta rör personuppgifter och som vidare erkänner att många parter är förpliktade att skydda integritet och personuppgifter för att uppfylla sina konstitutionella och internationella skyldigheter, och

SOM ÄR UPPMÄRKSAMMA på behovet av att säkerställa att effektiva straffrättsliga åtgärder mot it-brottslighet och insamling av bevis i elektronisk form omfattas av villkor och garantier som ska säkerställa ett adekvat skydd av de mänskliga rättigheterna och de grundläggande friheterna, inbegripet rättigheter som följer av skyldigheter som stater har åtagit sig enligt tillämpliga internationella människorättsinstrument, såsom Europarådets konvention om skydd för de mänskliga rättigheterna och de grundläggande friheterna från 1950 (ETS nr 5), Förenta nationernas internationella konvention om medborgerliga och politiska rättigheter från 1966, den afrikanska stadgan om mänskliga rättigheter och folkens rättigheter från 1981, den amerikanska konventionen om mänskliga rättigheter från 1969 samt andra internationella människorättsfördrag,

HAR ENATS OM FÖLJANDE:

Kapitel I

Gemensamma bestämmelser

Artikel 1

Syfte

Syftet med detta protokoll är att komplettera

- a. konventionen mellan parterna i detta protokoll, och
- b. det första protokollet mellan de parter i det här protokollet som också är parter i det första protokollet.

Artikel 2

Tillämpningsområde

1. Om inte annat anges i detta protokoll ska de åtgärder som beskrivs här tillämpas
 - a. mellan de parter i konventionen som är parter i detta protokoll, på särskilda brottsutredningar eller straffrättsliga förfaranden om brott relaterade till datorsystem och datorbehandlingsbara uppgifter och på insamling av bevis i elektronisk form på brott, och
 - b. mellan de parter i det första protokollet som är parter i det här protokollet, vid särskilda brottsutredningar eller straffrättsliga förfaranden rörande brott som fastställts enligt det första protokollet.
2. Varje part ska anta den lagstiftning och de andra åtgärder som krävs för att fullgöra de skyldigheter som anges i detta protokoll.

Artikel 3

Definitioner

1. Definitionerna i artiklarna 1 och 18.3 i konventionen ska gälla för detta protokoll.

2. I detta protokoll gäller följande ytterligare definitioner:
- centralmyndighet*: den eller de myndigheter som utsetts enligt ett fördrag eller arrangemang om ömsesidig rättslig hjälp på grundval av gällande enhetlig eller ömsesidig lagstiftning mellan de berörda parterna eller, i avsaknad av sådana, den eller de myndigheter som utsetts av en part enligt artikel 27.2 a i konventionen.
 - behörig myndighet*: en rättslig, administrativ eller annan brottsbekämpande myndighet som enligt nationell rätt har befogenhet att beordra, godkänna eller genomföra åtgärder enligt detta protokoll i syfte att samla in eller lägga fram bevis i samband med särskilda brottsutredningar eller straffrättsliga förfaranden.
 - nödsituation*: en situation där det föreligger en betydande och överhängande risk för en fysisk persons liv eller säkerhet.
 - personuppgifter*: information som avser en identifierad eller identifierbar fysisk person.
 - överförande part*: den part som överför uppgifter som svar på en framställning eller som en del av en gemensam utredningsgrupp eller, vid tillämpning av kapitel II avsnitt 2, en part på vars territorium en överförande tjänsteleverantör eller enhet som tillhandahåller domännamnregistreringstjänster är belägen.

Artikel 4

Språk

- Framställningar, order och åtföljande information som lämnas till en part ska vara avfattade på ett språk som godtas av den anmodade parten eller den part som underrättas enligt artikel 7.5, eller åtföljas av en översättning till ett sådant språk.
- Order enligt artikel 7 och framställningar enligt artikel 6 samt eventuell åtföljande information ska
 - lämnas in på ett av den andra partens språk på vilket tjänsteleverantören eller enheten godtar ett jämförbart nationellt förfarande,
 - lämnas in på ett annat språk som tjänsteleverantören eller enheten kan godta, eller
 - åtföljas av en översättning till ett av de språk som avses i punkt 2 a eller 2 b.

KAPITEL II

Åtgärder för utökat samarbete

Avsnitt 1

Allmänna principer som är tillämpliga med avseende på kapitel II

Artikel 5

Allmänna principer som är tillämpliga med avseende på kapitel II

- Parterna ska i största möjliga utsträckning samarbeta i enlighet med bestämmelserna i detta kapitel.
- Avsnitt 2 i detta kapitel består av artiklarna 6 och 7. Det föreskriver förfaranden som förbättrar det direkta samarbetet med leverantörer och enheter på en annan parts territorium. Avsnitt 2 är tillämpligt oavsett om det finns ett fördrag eller arrangemang om ömsesidig rättslig hjälp på grundval av gällande enhetlig eller ömsesidig lagstiftning mellan de berörda parterna.

3. Avsnitt 3 i detta kapitel består av artiklarna 8 och 9. Det föreskriver förfaranden som syftar till att förbättra det internationella samarbetet mellan myndigheter när det gäller utlämnande av lagrade datorbehandlingsbara uppgifter. Avsnitt 3 är tillämpligt oavsett om det finns ett fördrag eller arrangemang om ömsesidig rättslig hjälp på grundval av gällande enhetlig eller ömsesidig lagstiftning mellan den ansökande och den anmodade parten.
4. Avsnitt 4 i detta kapitel består av artikel 10. Det föreskriver förfaranden för ömsesidig rättslig hjälp i nödsituationer. Avsnitt 4 är tillämpligt oavsett om det finns ett fördrag eller arrangemang om ömsesidig rättslig hjälp på grundval av gällande enhetlig eller ömsesidig lagstiftning mellan den ansökande och den anmodade parten.
5. Avsnitt 5 i detta kapitel består av artiklarna 11 och 12. Avsnitt 5 är tillämpligt om det inte finns ett fördrag eller arrangemang om ömsesidig rättslig hjälp på grundval av gällande enhetlig eller ömsesidig lagstiftning mellan den ansökande och den anmodade parten. Bestämmelserna i avsnitt 5 ska inte tillämpas när det finns ett sådant fördrag eller arrangemang, med undantag för vad som föreskrivs i artikel 12.7. De berörda parterna får emellertid ömsesidigt besluta att tillämpa bestämmelserna i avsnitt 5 i stället för detta, om fördraget eller arrangemanget inte förbjuder det.
6. Om den anmodade parten, i enlighet med bestämmelserna i detta protokoll, får göra samarbetet beroende av dubbel straffbarhet, ska detta villkor anses vara uppfyllt, oavsett om dess lagstiftning placerar brottet i samma brottskategori eller rubricerar brottet med samma termer som den ansökande parten, om det handlande som ligger till grund för det brott för vilket rättslig hjälp begärs är ett brott enligt dess lagstiftning.
7. Bestämmelserna i detta kapitel innebär ingen begränsning av samarbete mellan parterna, eller mellan parter och tjänsteleverantörer eller andra enheter, som bygger på andra tillämpliga avtal, arrangemang eller praxis eller tillämplig nationell rätt.

Avsnitt 2

Förfaranden som förbättrar det direkta samarbetet med leverantörer och enheter i andra parter

Artikel 6

Framställning om information om domännamsregistrering

1. Varje part ska anta den lagstiftning och de andra åtgärder som krävs för att ge sina behöriga myndigheter befogenhet att, i samband med särskilda brottsutredningar eller straffrättsliga förfaranden, rikta en framställning till en enhet som tillhandahåller tjänster för domännamsregistrering på en annan parts territorium om information som enheten innehar eller kontrollerar, för att identifiera eller kontakta registraren av ett domännamn.
2. Varje part ska anta den lagstiftning och de andra åtgärder som krävs för att göra det möjligt för en enhet på dess territorium att lämna ut sådan information som svar på en framställning enligt punkt 1, med förbehåll för rimliga villkor i nationell rätt.
3. Framställningen enligt punkt 1 ska inkludera
 - a. datum för utfärdande av framställningen samt identitet på och kontaktuppgifter för den behöriga myndighet som utfärdat framställningen,
 - b. det domännamn om vilket information söks och en detaljerad förteckning över den information som söks, inklusive de särskilda dataelementen,
 - c. en förklaring om att framställningen görs enligt detta protokoll, att behovet av information uppstår på grund av dess relevans för en specifik brottsutredning eller ett specifikt straffrättsligt förfarande och att informationen endast kommer att användas för den specifika brottsutredningen eller det specifika straffrättsliga förfarandet, och
 - d. den tidsram inom vilken och det sätt på vilket informationen ska lämnas ut samt eventuella andra särskilda förfarandeinstruktioner.
4. Om det är godtagbart för enheten får en part lämna in en framställning enligt punkt 1 i elektronisk form. Lämpliga säkerhets- och autentiseringsnivåer får krävas.

5. Om en enhet som beskrivs i punkt 1 inte samarbetar får en ansökande part begära att enheten anger skälen till att den inte lämnar ut den begärda informationen. Den ansökande parten får samråda med den part i vilken enheten är belägen för att fastställa vilka åtgärder som är tillgängliga för att få ut informationen.
6. Varje part ska vid tidpunkten för undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeinstrument, eller vid någon annan tidpunkt, meddela Europarådets generalsekreterare den myndighet som utsetts för samråd enligt punkt 5.
7. Europarådets generalsekreterare ska upprätta ett register över de myndigheter som parterna har utsett enligt punkt 6, och hålla det uppdaterat. Varje part ska säkerställa att de uppgifter som den har lämnat till registret vid varje tidpunkt är korrekta.

Artikel 7

Utlämnande av abonnemangsuppgifter

1. Varje part ska anta den lagstiftning och de andra åtgärder som krävs för att ge sina behöriga myndigheter befogenhet att utfärda en order som ska lämnas direkt till en tjänsteleverantör på en annan parts territorium, i syfte att få till stånd utlämnande av specificerade, lagrade abonnemangsuppgifter i den tjänsteleverantörens besittning eller kontroll, om abonnemangsuppgifterna behövs för den utfärdande partens specifika brottsutredningar eller straffrättsliga förfaranden.
2.
 - a. Varje part ska anta den lagstiftning och de andra åtgärder som krävs för att en tjänsteleverantör inom dess territorium ska kunna lämna ut abonnemangsuppgifter som svar på en order enligt punkt 1.
 - b. Vid tidpunkten för undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeinstrument får en part – med avseende på order som utfärdats till tjänsteleverantörer inom dess territorium – avge följande förklaring: "Ordern enligt artikel 7.1 ska utfärdas av eller under överinseende av en åklagare eller annan rättslig myndighet eller på annat sätt utfärdas under oberoende tillsyn."
3. Ordern enligt punkt 1 ska ange
 - a. utfärdande myndighet och datum för utfärdande,
 - b. en förklaring om att ordern utfärdas enligt detta protokoll,
 - c. namn på och adress till den eller de tjänsteleverantörer som ska delges ordern,
 - d. det eller de brott som är föremål för brottsutredningen eller det straffrättsliga förfarandet,
 - e. den myndighet som söker de specifika abonnemangsuppgifterna, om det inte är den utfärdande myndigheten, och
 - f. en detaljerad beskrivning av de specifika abonnemangsuppgifter som söks.
4. Ordern enligt punkt 1 ska åtföljas av följande kompletterande information:
 - a. De rättsliga grunderna enligt nationell rätt för myndighetens befogenhet att utfärda ordern.
 - b. En hänvisning till rättsliga bestämmelser om och tillämpliga påföljder för det brott som utreds eller lagförs.
 - c. Kontaktoppgifter till den myndighet till vilken tjänsteleverantören ska skicka abonnemangsuppgifter, från vilken den kan begära kompletterande information eller till vilken den ska svara på annat sätt.
 - d. Den tidsram inom vilken och det sätt på vilket abonnemangsuppgifterna ska skickas.
 - e. Uppgift om huruvida bevarande av uppgifterna redan har begärts, inbegripet datum för begäran och eventuella referensnummer.

- f. Eventuella särskilda förfarandeanvisningar.
- g. I tillämpliga fall, en förklaring om att en samtidig underrättelse har lämnats enligt punkt 5.
- h. Annan information som kan vara till hjälp för att få abonnemangsuppgifterna utlämnade.
- 5.
- a. En part får vid tidpunkten för undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeinstrument och vid varje annan tidpunkt underrätta Europarådets generalsekreterare om att parten, när en order utfärdas enligt punkt 1 till en tjänsteleverantör på dess territorium, i varje enskilt fall eller under vissa fastställda omständigheter, kräver samtidig underrättelse om ordern, den kompletterande informationen och en sammanfattning av de sakförhållanden som har samband med utredningen eller förfarandet.
- b. Oavsett om en part kräver underrättelse enligt punkt 5 a eller inte, får den kräva att tjänsteleverantören under vissa fastställda omständigheter samråder med partens myndigheter innan uppgifter lämnas ut.
- c. De myndigheter som underrättats enligt punkt 5 a eller med vilka samråd skett enligt punkt 5 b får utan onödigt dröjsmål uppmana tjänsteleverantören att inte lämna ut abonnemangsuppgifterna om
- i. utlämnande kan skada brottsutredningar eller straffrättsliga förfaranden i den parten, eller
 - ii. villkor eller vägransgrunder skulle vara tillämpliga enligt artikel 25.4 och artikel 27.4 i konventionen för det fall att abonnemangsuppgifterna hade begärts inom ramen för ömsesidig rättslig hjälp.
- d. De myndigheter som underrättats enligt punkt 5 a eller med vilka samråd skett enligt punkt 5 b
- i. får begära kompletterande information från den myndighet som avses i punkt 4 c för tillämpningen av punkt 5 c och får inte lämna ut den till tjänsteleverantören utan den myndighetens samtycke, och
 - ii. ska omgående informera den myndighet som avses i punkt 4 c om tjänsteleverantören har uppmanats att inte lämna ut abonnemangsuppgifterna och ange skälen till detta.
- e. En part ska utse en enda myndighet som ska ta emot underrättelser enligt punkt 5 a och vidta de åtgärder som föreskrivs i punkterna 5 b, 5 c och 5 d. Parten ska, när underrättelse till Europarådets generalsekreterare enligt punkt 5 a först lämnas, meddela generalsekreteraren kontaktuppgifterna för denna myndighet.
- f. Europarådets generalsekreterare ska upprätta ett register över de myndigheter som parterna har utsett enligt punkt 5 e med uppgift om huruvida och under vilka omständigheter de begär underrättelse enligt punkt 5 a, och hålla registret uppdaterat. Varje part ska säkerställa att de uppgifter som den har lämnat till registret vid varje tidpunkt är korrekta.
6. Om tjänsteleverantören finner det godtagbart får en part lämna in en order enligt punkt 1 och kompletterande information enligt punkt 4 i elektronisk form. En part får lämna underrättelse och kompletterande information enligt punkt 5 i elektronisk form. Lämpliga säkerhets- och autentiseringsnivåer får krävas.
7. Om en tjänsteleverantör underrättar myndigheten i punkt 4 c om att den inte kommer att lämna ut de begärda abonnemangsuppgifterna, eller om den inte lämnar ut abonnemangsuppgifter som svar på en order enligt punkt 1 inom 30 dagar från mottagandet av ordern eller inom den tidsfrist som avses i punkt 4 d, beroende på vilken av dessa tidsperioder som är längst, får den utfärdande partens behöriga myndigheter söka verkställa ordern endast genom artikel 8 eller andra former av ömsesidig rättslig hjälp. Parterna får begära att en tjänsteleverantör anger skälen för vägran att lämna ut de abonnemangsuppgifter som begärs i ordern.
8. En part får, vid tidpunkten för undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeinstrument, förklara att en utfärdande part ska begära att abonnemangsuppgifter lämnas ut från tjänsteleverantören innan den begär det enligt artikel 8, såvida inte den utfärdande parten lämnar en rimlig förklaring till varför detta inte har gjorts.

9. Vid tidpunkten för undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeinstrument får en part
- förbehålla sig rätten att inte tillämpa denna artikel, eller
 - om utlämnande av vissa typer av åtkomstnummer enligt denna artikel skulle strida mot de grundläggande principerna i det nationella rättssystemet, förbehålla sig rätten att inte tillämpa denna artikel på sådana nummer.

Avsnitt 3

Förfaranden som förbättrar det internationella samarbetet mellan myndigheter vad gäller utlämnande av lagrade datorbehandlingsbara uppgifter

Artikel 8

Verkställighet av order från en annan part avseende skyndsamt framtagande av abonnemangsuppgifter och trafikuppgifter

1. Varje part ska anta den lagstiftning och de andra åtgärder som krävs för att ge sina behöriga myndigheter befogenhet att utfärda en order som ska överlämnas som en del av en framställning till en annan part i syfte att få en tjänsteleverantör på den anmodade partens territorium att ta fram specificerade och lagrade
- abonnemangsuppgifter, och
 - trafikuppgifter
- som finns i den tjänsteleverantörens besittning eller under dennas kontroll och som krävs för partens specifika brottsutredningar eller straffrättsliga förfaranden.
2. Varje part ska anta den lagstiftning och de andra åtgärder som krävs för att kunna verkställa en order enligt punkt 1 som lämnats in av en ansökande part.
3. I sin framställning ska den ansökande parten bifoga den order som avses i punkt 1, informationsunderlaget och eventuella särskilda förfarandeanvisningar för den anmodade parten.
- I ordern ska följande anges:
 - Utfärdande myndighet och datum för utfärdande av ordern.
 - En förklaring om att ordern inges enligt detta protokoll.
 - Namn på och adress till den eller de tjänsteleverantörer som ska delges ordern.
 - Det eller de brott som är föremål för brottsutredningen eller det straffrättsliga förfarandet.
 - Den myndighet som begär informationen eller uppgifterna, om det inte är den utfärdande myndigheten.
 - En detaljerad beskrivning av den specifika information eller de specifika uppgifter som begärs.
 - I det informationsunderlag som tillhandahålls för att hjälpa den anmodade parten att verkställa ordern och som inte får lämnas ut till tjänsteleverantören utan den ansökande partens samtycke ska följande anges:
 - De rättsliga grunderna enligt nationell rätt för myndighetens befogenhet att utfärda ordern.
 - Lagbestämmelser och tillämpliga påföljder för det eller de brott som utreds eller lagförs.
 - Anledningen till att den ansökande parten bedömer att tjänsteleverantören innehar eller kontrollerar uppgifterna.
 - En sammanfattning av de faktiska omständigheterna bakom utredningen eller förfarandet.
 - Informationens eller uppgifternas relevans för undersökningen eller förfarandet.

- vi. Kontaktuppgifter för en eller flera myndigheter som kan lämna kompletterande information.
 - vii. Uppgift om huruvida bevarande av informationen eller uppgifterna redan har begärts, inbegripet datum för begäran och eventuella referensnummer.
 - viii. Uppgift om huruvida informationen eller uppgifterna redan har begärts på annat sätt och, om så är fallet, hur.
- c. Den ansökande parten får begära att den anmodade parten följer särskilda förfarandeanvisningar.
4. En part får vid tidpunkten för undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeinstrument, och vid varje annan tidpunkt, förklara att ytterligare informationsunderlag krävs för att verkställa order enligt punkt 1.
 5. Den anmodade parten ska godta framställningar i elektronisk form. Den får kräva lämpliga säkerhets- och autentiseringsnivåer innan framställningen godtas.
 6.
 - a. Den anmodade parten ska, från och med dagen för mottagandet av all den information som anges i punkterna 3 och 4, göra rimliga ansträngningar för att delge tjänsteleverantören inom 45 dagar, men helst tidigare, och ska beordra att begärd information eller uppgifter lämnas senast inom
 - i. 20 dagar för abonnemangsuppgifter, och
 - ii. 45 dagar för trafikuppgifter.
 - b. Den anmodade parten ska se till att den information eller de uppgifter som tagits fram översänds till den ansökande parten utan onödigt dröjsmål.
 7. Om den anmodade parten inte kan följa anvisningarna enligt punkt 3 c på det sätt som begärts, ska den omgående underrätta den ansökande parten och, i tillämpliga fall, ange på vilka villkor den kan följa anvisningarna, varefter den ansökande parten ska avgöra om framställningen ändå bör verkställas.
 8. Den anmodade parten får vägra att verkställa en framställning av de skäl som anges i artikel 25.4 eller artikel 27.4 i konventionen eller uppställa villkor som den anser nödvändiga för att framställningen ska kunna verkställas. Den anmodade parten får skjuta upp verkställigheten av framställningar av sådana skäl som anges i artikel 27.5 i konventionen. Den anmodade parten ska så snart som möjligt underrätta den ansökande parten om vägran, villkoren eller uppskjutandet. Den anmodade parten ska också underrätta den ansökande parten om andra omständigheter som riskerar att försena verkställigheten av framställningen avsevärt. Artikel 28.2 b i konventionen ska tillämpas på den här artikeln.
 9.
 - a. Om den ansökande parten inte kan uppfylla ett villkor som uppställts av den anmodade parten enligt punkt 8, ska den omgående underrätta den anmodade parten. Den anmodade parten ska sedan avgöra om informationen eller materialet ändå bör tillhandahållas.
 - b. Om den ansökande parten godtar villkoret ska den vara bunden av det. Den anmodade parten som tillhandahåller information eller material som omfattas av ett sådant villkor får kräva att den ansökande parten i samband med detta villkor förklarar hur informationen eller materialet används.
 10. Varje part ska vid tidpunkten för undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeinstrument meddela Europarådets generalsekreterare kontaktuppgifterna till, och hålla dessa uppgifter uppdaterade, de myndigheter som utsetts
 - a. för att inge en order enligt denna artikel, och
 - b. för att ta emot en order enligt denna artikel.

11. En part får, vid tidpunkten för undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeinstrument, förklara att den kräver att framställningar från andra parter enligt denna artikel ska inges till den, av den ansökande partens centralmyndighet eller av en annan myndighet som parterna gemensamt har fastställt.
12. Europarådets generalsekreterare ska upprätta och uppdatera ett register över de myndigheter som parterna har utsett enligt punkt 10, och hålla det uppdaterat. Varje part ska säkerställa att de uppgifter som den har lämnat till registret vid varje tidpunkt är korrekta.
13. Vid tidpunkten för undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeinstrument får en part förbehålla sig rätten att inte tillämpa denna artikel på trafikuppgifter.

Artikel 9

Påskyndat utlämnande av lagrade datorbehandlingsbara uppgifter i en nödsituation

1.
 - a. Varje part ska anta den lagstiftning och de andra åtgärder som i en nödsituation kan krävas för att dess kontaktpunkt inom det nätverk av ständigt tillgängliga kontaktpunkter som avses i artikel 35 i konventionen (*kontaktpunkten*) ska kunna vidarebefordra en framställning till och ta emot en framställning från en kontaktpunkt i en annan part som begär omedelbar hjälp med att få en tjänsteleverantör på den partens territorium att skyndsamt lämna ut specificerade, lagrade datorbehandlingsbara uppgifter som tjänsteleverantören innehar eller kontrollerar, utan någon framställning om ömsesidig rättslig hjälp.
 - b. En part får, vid tidpunkten för undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeinstrument, förklara att den inte kommer att verkställa framställningar enligt punkt 1 a som endast avser utlämnande av abonnemangsuppgifter.
2. Varje part ska anta den lagstiftning och de andra åtgärder som krävs för att enligt punkt 1 göra det möjligt för
 - a. dess myndigheter att begära ut uppgifter från en tjänsteleverantör på dess territorium efter en framställning enligt punkt 1,
 - b. en tjänsteleverantör på dess territorium att lämna ut begärda uppgifter till sina myndigheter som svar på en framställning enligt punkt 2 a, och
 - c. dess myndigheter att lämna de begärda uppgifterna till den ansökande parten.
3. Framställningen enligt punkt 1 ska ange
 - a. den behöriga myndighet som begär uppgifterna och datum då framställningen utfärdades,
 - b. en förklaring om att framställningen utfärdas enligt detta protokoll,
 - c. namn på och adress till den eller de tjänsteleverantörer som innehar eller kontrollerar de begärda uppgifterna,
 - d. det eller de brott som är föremål för brottsutredningen eller det straffrättsliga förfarandet och en hänvisning till de rättsliga bestämmelser och tillämpliga påföljder som gäller för brottet,
 - e. tillräckliga fakta för att visa att det föreligger en nödsituation och hur de begärda uppgifterna förhåller sig till den,
 - f. en detaljerad beskrivning av de begärda uppgifterna,
 - g. eventuella särskilda förfarandeanvisningar, och
 - h. all annan information som kan vara till hjälp för att få till stånd utlämnande av de begärda uppgifterna.
4. Den anmodade parten ska godta en framställning i elektronisk form. En part får också godta en muntlig framställning och kan därvid kräva bekräftelse i elektronisk form. Den får kräva lämpliga säkerhets- och autentiseringsnivåer innan framställningen godtas.

5. En part får, vid tidpunkten för undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeinstrument, förklara att den ställer som krav att ansökande parter, efter det att framställningen har verkställts, ska lämna in framställningen och eventuell kompletterande information som översänts till stöd för denna i ett sådant format och via en sådan kanal, vilket kan inbegripa ömsesidig rättslig hjälp, som har angetts av den anmodade parten.
6. Den anmodade parten enligt ett skyndsamt förfarande underrätta den ansökande parten om sitt beslut om framställningen enligt punkt 1 och, i tillämpliga fall, ange på vilka villkor den skulle tillhandahålla uppgifterna och varje annan form av samarbete som kan komma i fråga.
7.
 - a. Om en ansökande part inte kan uppfylla ett villkor som uppställts av den anmodade parten enligt punkt 6, ska den omgående underrätta den anmodade parten om detta. Den anmodade parten ska sedan avgöra om informationen eller materialet ändå bör tillhandahållas. Om den ansökande parten godtar villkoret ska den vara bunden av det.
 - b. Den anmodade part som tillhandahåller information eller material som omfattas av ett sådant villkor får kräva att den ansökande parten i samband med detta villkor förklarar hur informationen eller materialet används.

Avsnitt 4

Förfaranden för ömsesidig rättslig hjälp i nödsituationer

Artikel 10

Ömsesidig rättslig hjälp i nödsituationer

1. Varje part får ansöka om ömsesidig rättslig hjälp enligt ett skyndsamt förfarande om den anser att det föreligger en nödsituation. En framställning enligt denna artikel ska, utöver det övriga innehåll som krävs, innefatta en beskrivning av de fakta som visar att en nödsituation föreligger och hur den begärda hjälpen förhåller sig till den.
2. En anmodad part ska godta en sådan framställning i elektronisk form. Den får kräva lämpliga säkerhets- och autentiseringsnivåer innan framställningen godtas.
3. Den anmodade parten får begära kompletterande information enligt ett skyndsamt förfarande för att kunna bedöma framställningen. Den ansökande parten ska tillhandahålla sådan kompletterande information enligt ett skyndsamt förfarande.
4. När den anmodade parten har förvässat sig om att en nödsituation föreligger och övriga krav för ömsesidig rättslig hjälp är uppfyllda ska den besvara framställningen enligt ett skyndsamt förfarande.
5. Varje part ska säkerställa att en person från dess centralmyndighet eller andra myndigheter med ansvar för att besvara framställningar om ömsesidig rättslig hjälp är tillgänglig dygnet runt för att besvara en framställning enligt denna artikel.
6. Centralmyndigheten eller andra myndigheter med ansvar för ömsesidig rättslig hjälp mellan den ansökande och den anmodade parten får gemensamt besluta att resultaten av verkställandet av en framställning enligt denna artikel, eller en förhandskopia av dessa, får lämnas till den ansökande parten via en annan kanal än den som används för framställningen.
7. Om det inte finns något fördrag eller arrangemang om ömsesidig rättslig hjälp på grundval av gällande enhetlig eller ömsesidig lagstiftning mellan den ansökande och den anmodade parten, ska artikel 27.2 b och 27.3–27.8 samt artikel 28.2–28.4 i konventionen tillämpas på den här artikeln.
8. Om det finns ett sådant fördrag eller arrangemang ska denna artikel kompletteras med bestämmelserna i det fördraget eller arrangemanget, såvida inte de berörda parterna ömsesidigt beslutar att i stället tillämpa någon av eller samtliga de konventionsbestämmelser som avses i punkt 7 i denna artikel.

9. Varje part får, vid tidpunkten för undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeminstrument, förklara att framställningar också kan sändas direkt till dess rättsliga myndigheter eller via Internationella kriminalpolisorganisationens (Interpol) kanaler eller till dess ständigt tillgängliga kontaktpunkt som inrättats enligt artikel 35 i konventionen. I sådana fall ska den ansökande partens centralmyndighet samtidigt översända en kopia till den anmodade partens centralmyndighet. Om en framställning sänds direkt till en rättslig myndighet i den anmodade parten och den myndigheten inte är behörig att behandla framställningen, ska den hänskjuta framställningen till den behöriga nationella myndigheten och direkt underrätta den ansökande parten om detta.

Avsnitt 5

Förfaranden för internationellt samarbete i avsaknad av tillämpliga internationella avtal

Artikel 11

Videokonferens

1. En ansökande part får begära och den anmodade parten får medge att vittnesmål och utsagor inhämtas från ett vittne eller en sakkunnig genom videokonferens. Den ansökande parten och den anmodade parten ska samråda för att underlätta lösningen av eventuella problem som kan uppstå i samband med verkställigheten av framställningen, inbegripet, beroende på vad som är tillämpligt, vilken part som ska leda videokonferensen, vilka myndigheter och personer som ska närvara, huruvida den ena eller båda parterna ska ansvara för att ta upp särskilda eder från vittnen och sakkunniga eller varna eller ge anvisningar till dessa, hur förhör med vittnet eller den sakkunniga ska hållas, hur vittnets eller den sakkunnigas rättigheter vederbörligen ska säkerställas, hur anspråk på privilegier eller immunitet ska hanteras, hur invändningar mot frågor eller svar ska hanteras, och huruvida den ena eller båda parterna ska tillhandahålla översättnings-, tolknings- och transkriberingstjänster.

2.

a. Den anmodade och den ansökande partens centralmyndigheter ska kommunicera direkt med varandra vid tillämpningen av denna artikel. En anmodad part får godta en framställning i elektronisk form. Den får kräva lämpliga säkerhets- och autentiseringsnivåer innan framställningen godtas.

b. Den anmodade parten ska underrätta den ansökande parten om skälen till att framställningen inte verkställs eller till att verkställigheten av framställningen försenas. Artikel 27.8 i konventionen ska tillämpas på den här artikeln. Utan att det påverkar andra villkor som en anmodad part kan ställa i enlighet med den här artikeln ska artikel 28.2-28.4 i konventionen tillämpas på den här artikeln.

3. En anmodad part som tillhandahåller rättslig hjälp enligt denna artikel ska sträva efter att få den person vars vittnesmål eller utsaga begärs att närvara. När så är lämpligt får den anmodade parten, i den utsträckning det är möjligt enligt dess lagstiftning, vidta nödvändiga åtgärder för att tvinga ett vittne eller en sakkunnig att inställa sig hos den anmodade parten på en bestämd tid och plats.

4. De förfaranden för genomförande av videokonferensen som anges av den ansökande parten ska följas, utom när de är oförenliga med den anmodade partens nationella rätt. I händelse av oförenlighet, eller i den mån förfarandet inte har specificerats av den ansökande parten, ska den anmodade parten tillämpa det förfarande som föreskrivs i nationell rätt, såvida inte den ansökande och den anmodade parten gemensamt fastställer något annat.

5. Utan att det påverkar någon jurisdiktion enligt den ansökande partens nationella rätt ska vittnet eller den sakkunniga, om vederbörande under videokonferensen

a. avsiktligt lämnar en oriktig uppgift när den anmodade parten i enlighet med sin nationella rätt har ålagt en sådan person att vittna sanningsenligt,

b. vägrar att vittna när den anmodade parten i enlighet med sin nationella rätt har ålagt denna person att vittna, eller

c. gör sig skyldig till annan försummelse som är förbjuden enligt den anmodade partens nationella rätt under sådana förfaranden,

kunna bli föremål för påföljd i den anmodade parten på samma sätt som om handlingen hade begåtts inom ramen för dess nationella förfaranden.

6.

a. Om inte annat fastställs gemensamt mellan den ansökande parten och den anmodade parten ska den anmodade parten bära alla kostnader i samband med verkställigheten av en framställning enligt denna artikel, med undantag för

- i. arvoden till sakkunniga,
- ii. kostnader för översättning, tolkning och transkribering, och
- iii. ovanligt stora kostnader.

b. Om verkställighet av en framställning skulle innebära ovanligt stora kostnader bör den ansökande och den anmodade parten samråda med varandra för att fastställa på vilka villkor framställningen kan verkställas.

7. Om den ansökande och den anmodade parten gemensamt kommit överens om det,

- a. får bestämmelserna i denna artikel tillämpas för att genomföra ljudkonferenser,
- b. får videokonferens teknik användas för andra ändamål, eller förhör, än de som beskrivs i punkt 1, inbegripet för att identifiera personer eller föremål.

8. Om en anmodad part väljer att tillåta att en misstänkt eller tilltalad person hörs, får den kräva särskilda villkor och skyddsåtgärder vad gäller upptagande av vittnesmål eller uttalanden från, underrättelse till eller tillämpning av processuella åtgärder gentemot en sådan person.

Artikel 12

Gemensamma utredningsgrupper och gemensamma utredningar

1. Genom ömsesidig överenskommelse får två eller flera parter behöriga myndigheter inrätta och driva en gemensam utredningsgrupp på sina territorier för att underlätta brottsutredningar eller straffrättsliga förfaranden, om en förstärkt samordning anses vara av särskilt stor nytta. De behöriga myndigheterna ska fastställas av respektive berörd part.

2. Förfarandena och villkoren för gemensamma utredningsgruppers verksamhet, såsom deras särskilda ändamål, sammansättning, funktioner, varaktighet och eventuella förlängningsperioder, lokalisering, organisation, villkor för insamling, överföring och användning av information eller bevis, sekretessvillkor, samt villkor för involvering av en parts deltagande myndigheter i utredningsverksamhet som äger rum på en annan parts territorium, ska vara de som överenskommit mellan dessa behöriga myndigheter.

3. En part får vid undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeinstrument förklara att dess centralmyndighet måste vara signatär till eller på annat sätt ställa sig bakom överenskommelsen om inrättande av gruppen.

4. De behöriga och deltagande myndigheterna ska kommunicera direkt, med undantag för att parterna ömsesidigt får fastställa andra lämpliga kommunikationskanaler när exceptionella omständigheter kräver en mer central samordning.

5. Om utredningsåtgärder behöver vidtas på en av de berörda parternas territorium, får deltagande myndigheter från den parten begära att deras egna myndigheter vidtar dessa åtgärder utan att de andra parterna behöver lämna in en framställning om ömsesidig rättslig hjälp. Dessa åtgärder ska vidtas av den partens myndigheter på dess territorium och på de villkor som gäller enligt nationell rätt i en nationell utredning.

6. Användning av information eller bevis som tillhandahålls av en parts deltagande myndigheter till andra berörda parter deltagande myndigheter får vägras eller begränsas på det sätt som anges i den överenskommelse som beskrivs i punkterna 1 och 2. Om överenskommelsen inte innehåller villkor för att vägra eller begränsa användningen får parterna använda den information eller de bevis som tillhandahålls
- för de ändamål för vilka överenskommelsen har ingåtts,
 - för att upptäcka, utreda och lagföra andra brott än de för vilka överenskommelsen ingicks, med förbehåll för förhandsgodkännande från de myndigheter som tillhandahåller informationen eller bevisen; samtycke ska dock inte krävas om grundläggande rättsprinciper hos den part som använder informationen eller bevisen innebär krav på att parten lämnar ut informationen eller bevisen för att skydda en tilltalads rättigheter i straffrättsliga förfaranden; i sådana fall ska dessa myndigheter utan onödigt dröjsmål underrätta de myndigheter som tillhandahöll informationen eller bevisen; eller
 - för att förhindra en nödsituation. I sådana fall ska de deltagande myndigheter som tog emot informationen eller bevisen utan onödigt dröjsmål underrätta de deltagande myndigheter som tillhandahöll informationen eller bevisen, om inte annat fastställs gemensamt.
7. I avsaknad av en sådan överenskommelse som beskrivs i punkterna 1 och 2 får gemensamma utredningar genomföras enligt gemensamt överenskomna villkor från fall till fall. Den här punkten är tillämplig oavsett om det finns ett fördrag eller arrangemang om ömsesidig rättslig hjälp på grundval av gällande enhetlig eller gemensam lagstiftning mellan de berörda parterna.

KAPITEL III

Villkor och garantier

Artikel 13

Villkor och garantier

I enlighet med artikel 15 i konventionen ska varje part säkerställa att införandet, genomförandet och tillämpningen av de befogenheter och förfaranden som föreskrivs i detta protokoll omfattas av villkor och garantier som föreskrivs i dess nationella rätt, vilka ska säkerställa ett adekvat skydd av mänskliga rättigheter och friheter.

Artikel 14

Skydd av personuppgifter

- Tillämpningsområde
 - Om inte annat föreskrivs i punkt 1 b och 1 c ska vardera parten behandla de personuppgifter som parten tar emot enligt detta protokoll i enlighet med punkterna 2–15 i denna artikel.
 - Om både den överförande parten och den mottagande parten vid tidpunkten för mottagandet av personuppgifter enligt detta protokoll är ömsesidigt bundna av ett internationellt avtal som upprättar en övergripande ram för skydd av personuppgifter mellan dessa parter, vilket är tillämpligt på överföring av personuppgifter i syfte att förebygga, förhindra, upptäcka, utreda och lagföra brott, och där det anges att behandlingen av personuppgifter enligt det avtalet uppfyller kraven i de berörda parternas uppgiftsskyddslagstiftning, ska villkoren i ett sådant avtal, med avseende på de åtgärder som omfattas av tillämpningsområdet för avtalet, tillämpas på personuppgifter som mottas enligt protokollet i stället för punkterna 2–15, om inte annat överenskommit mellan de berörda parterna.
 - Om den överförande parten och den mottagande parten inte är ömsesidigt bundna av ett avtal som beskrivs i punkt 1 b, får de gemensamt besluta att överföringen av personuppgifter enligt detta protokoll kan ske på grundval av andra avtal eller överenskommelser mellan de berörda parterna i stället för punkterna 2–15.

- d. Varje part ska anse att behandlingen av personuppgifter enligt punkterna 1 a och 1 b uppfyller kraven i dess regelverk för skydd av personuppgifter för internationella överföringar av personuppgifter, och inget ytterligare tillstånd för överföring ska krävas enligt regelverket. En part får endast vägra eller förhindra överföring av uppgifter till en annan part enligt detta protokoll av skäl som rör uppgiftsskydd enligt de villkor som anges i punkt 15 när punkt 1 a är tillämplig, eller enligt villkoren i ett sådant avtal eller arrangemang som avses i punkt 1 b eller 1.c, när en av dessa punkter är tillämplig.
- e. Ingenting i denna artikel ska hindra en part från att tillämpa strängare garantier för sina egna myndigheters behandling av personuppgifter som mottagits inom ramen för detta protokoll.

2. Syfte och användning

- a. Den part som har mottagit personuppgifter ska behandla dem för de ändamål som anges i artikel 2. Den ska inte behandla personuppgifterna vidare för ett oförenligt ändamål och ska inte heller behandla uppgifterna vidare om detta inte är tillåtet enligt dess nationella regelverk. Den här artikeln ska inte påverka den överförande partens möjlighet att i ett specifikt fall införa ytterligare villkor enligt detta protokoll, men sådana villkor ska inte inbegripa allmänna villkor för uppgiftsskydd.
- b. Den mottagande parten ska inom ramen för sitt nationella regelverk säkerställa att begärda och behandlade personuppgifter är relevanta och inte mer omfattande än vad som krävs för de ändamål för vilka de behandlas.

3. Kvalitet och integritet

Varje part ska vidta rimliga åtgärder för att säkerställa att personuppgifter bevaras med sådan precision och fullständighet och är så aktuella som är nödvändigt och lämpligt för en laglig behandling av personuppgifterna, med beaktande av de ändamål för vilka de behandlas.

4. Känsliga uppgifter

En part får endast behandla personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller annan övertygelse eller medlemskap i fackförening, genetiska uppgifter, biometriska uppgifter som anses känsliga med hänsyn till riskerna, eller personuppgifter rörande hälsa eller sexualliv om det finns lämpliga garantier som skyddar mot risken för oönskade skadliga effekter av användningen av sådana uppgifter, särskilt mot olaglig diskriminering.

5. Lagringsperioder

Varje part ska lagra personuppgifterna endast så länge som är nödvändigt och lämpligt med tanke på ändamålen med behandlingen av uppgifterna enligt punkt 2. För att uppfylla denna skyldighet ska den i sitt nationella regelverk föreskriva särskilda lagringsperioder eller regelbunden översyn av behovet av ytterligare lagring av uppgifterna.

6. Automatiserade beslut

Beslut som har en betydande negativ inverkan på den berörda personens intressen får inte grunda sig enbart på automatisk behandling av personuppgifter, såvida det inte är tillåtet enligt nationell rätt och det finns lämpliga garantier som inbegriper möjligheten till mänskligt ingripande.

7. Datasäkerhet och säkerhetsincidenter

- a. Varje part ska säkerställa att den har infört lämpliga tekniska, fysiska och organisatoriska åtgärder för skydd av personuppgifter, särskilt mot förlust eller oavsiktlig eller obehörig åtkomst, utlämnande, ändring eller förstöring (säkerhetsincident).
- b. Vid upptäckt av en säkerhetsincident som innebär en betydande risk för fysisk eller icke-fysisk skada för enskilda personer eller för den andra parten, ska den mottagande parten omgående bedöma sannolikheten för och omfattningen av denna och omgående vidta lämpliga åtgärder för att minimera skadan. Sådana åtgärder ska inbegripa underrättelse till den överförande myndigheten eller, med avseende på tillämpningen av kapitel II avsnitt 2, till den eller de myndigheter som utsetts enligt punkt 7 c. Underrättelse kan emellertid innefatta lämpliga begränsningar vad gäller vidare överföring av underrättelsen; den får senareläggas eller utelämnas om en sådan underrättelse kan äventyra den nationella

säkerheten, eller senareläggas om underrättelsen kan äventyra åtgärder för att skydda den allmänna säkerheten. Sådana åtgärder ska också inbegripa underrättelse till den berörda personen, såvida inte parten har vidtagit lämpliga åtgärder så att det inte längre föreligger någon betydande risk. Underrättelse till den berörda personen får senareläggas eller utelämnas på de villkor som anges i punkt 12 a i. Den underrättade parten får begära samråd och kompletterande information om incidenten och de åtgärder som vidtagits.

- c. Varje part ska vid tidpunkten för undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeinstrument meddela Europarådets generalsekreterare den eller de myndigheter som ska underrättas enligt punkt 7 b för de ändamål som avses i kapitel II avsnitt 2; den information som lämnas får senare ändras.

8. Förande av register

Varje part ska föra register eller ha andra lämpliga metoder för att visa hur en enskilds personuppgifter görs tillgängliga, används och lämnas ut i ett specifikt fall.

9. Vidare delning inom en part

- a. När en parts myndighet tillhandahåller personuppgifter som ursprungligen mottagits enligt detta protokoll till en annan myndighet i den parten, ska den andra myndigheten behandla dem i enlighet med denna artikel, om inte annat följer av punkt 9 b.
- b. Trots vad som sägs i punkt 9 a får en part som har gjort ett förbehåll enligt artikel 17 tillhandahålla personuppgifter som den har mottagit till sina delstater eller liknande territoriella enheter, förutsatt att parten har infört åtgärder så att de mottagande myndigheterna fortsätter att effektivt skydda uppgifterna genom att tillhandahålla en skyddsnivå för uppgifterna som är likvärdig med den som föreskrivs i den här artikeln.
- c. Vid indikationer på felaktig tillämpning av denna punkt får den överförande parten begära samråd och relevant information om dessa indikationer.

10. Vidare överföring till en annan stat eller en internationell organisation

- a. Den mottagande parten får överföra personuppgifterna till en annan stat eller till en internationell organisation endast med förhandstillstånd från den överförande myndigheten eller, vid tillämpning av kapitel II avsnitt 2, den eller de myndigheter som utsetts enligt punkt 10 b.
- b. Varje part ska vid tidpunkten för undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeinstrument meddela Europarådets generalsekreterare den eller de myndigheter som ska ge tillstånd för de ändamål som avses i kapitel II avsnitt 2; den information som lämnas får senare ändras.

11. Öppenhet och underrättelse

- a. Varje part ska genom tillkännagivande av allmänna meddelanden eller genom personlig underrättelse meddela den person vars personuppgifter har samlats in
 - i. den rättsliga grunden för och syftet med behandlingen,
 - ii. eventuella lagrings- eller översynsperioder enligt punkt 5, beroende på vad som är tillämpligt,
 - iii. mottagare eller kategorier av mottagare till vilka sådana uppgifter lämnas ut, och
 - iv. möjligheter till åtkomst, rättelse och prövning.
- b. En part får underkasta eventuella krav på personlig underrättelse rimliga begränsningar enligt sitt nationella regelverk enligt villkoren i punkt 12 a i.
- c. Om den överförande partens nationella regelverk kräver personlig underrättelse till den person vars uppgifter har lämnats till en annan part, ska den överförande parten vidta åtgärder så att den andra parten vid tidpunkten för överföringen informeras om detta krav och om lämplig kontaktinformation. Den personliga underrättelsen ska inte lämnas om den andra parten har begärt att tillhandahållandet av uppgifterna hålls konfidentiellt, och förutsättningarna

för begränsningar i punkt 12 a i är tillämpliga. När dessa begränsningar inte längre är tillämpliga och den personliga underrättelsen kan lämnas, ska den andra parten vidta åtgärder så att den överförande parten informeras om detta. Om den överförande parten ännu inte har informerats har den rätt att göra framställningar till den mottagande parten, som ska informera den överförande parten om huruvida begränsningen ska bibehållas.

12. Åtkomst och rättelse

- a. Varje part ska säkerställa att envar vars personuppgifter har mottagits enligt detta protokoll har rätt att, i enlighet med förfaranden som fastställs i dess nationella regelverk och utan onödigt dröjsmål, begära och erhålla
 - i. en skriftlig eller elektronisk kopia av den dokumentation som bevaras om personen i fråga vilken innehåller dennes personuppgifter och tillgänglig information som anger den rättsliga grunden för och syftet med behandlingen, lagringsperioderna och mottagarna eller kategorierna av mottagare av uppgifterna (*åtkomst*), samt information om möjligheter till prövning, förutsatt att åtkomst i ett visst fall kan underkastas tillämpning av proportionella begränsningar som medges enligt det nationella regelverket och som vid tidpunkten för avgörandet behövs för att skydda andra personers rättigheter och friheter eller viktiga mål av allmänt intresse, med vederbörlig hänsyn till den berörda personens legitima intressen,
 - ii. rättelse, om den enskildes personuppgifter är felaktiga eller har behandlats på ett felaktigt sätt; rättelse ska, när så är lämpligt och rimligt med hänsyn till skälen till rättelsen och det särskilda sammanhanget för behandlingen, inbegripa korrigerig, komplettering, radering eller anonymisering, begränsning av behandling eller blockering.
- b. Om åtkomst eller rättelse vägras eller medges endast i begränsad omfattning ska parten, i skriftlig form som får tillhandahållas på elektronisk väg, utan onödigt dröjsmål lämna ett svar till den enskilde om vägran eller begränsningen. Den ska ange skälen för en sådan vägran eller begränsning och ge information om tillgängliga möjligheter till prövning. Eventuella kostnader för att få åtkomst bör vara skäligen och inte överdrivna.

13. Rättsmedel och prövning utanför domstol

Varje part ska ha effektiva rättsmedel och prövningsförfaranden utanför domstol för att ge möjlighet till prövning vid överträdelser av denna artikel.

14. Tillsyn

Varje part ska ha en eller flera offentliga myndigheter som ensamma eller tillsammans utövar oberoende och effektiva tillsynsfunktioner och tillsynsbefogenheter med avseende på de åtgärder som anges i denna artikel. Dessa myndigheters funktioner och befogenheter ska, när myndigheterna agerar ensamma eller tillsammans, inbegripa utredningsbefogenheter, befogenhet att agera med anledning av klagomål och förmåga att vidta korrigerande åtgärder.

15. Samråd och avbrytande

En part får avbryta överföringen av personuppgifter till en annan part om den har konkreta bevis för att den andra parten systematiskt eller väsentligt bryter mot villkoren i denna artikel eller att ett väsentligt brott mot dessa villkor är nära förestående. Den ska inte avbryta överföringar utan rimligt varsel och inte förrän efter det att de berörda parterna har inlett en rimlig samrådsperiod utan att nå en lösning. En part får dock tillfälligt avbryta överföringar i händelse av en systematisk eller väsentlig överträdelse som innebär en betydande och överhängande risk för en fysisk persons liv, säkerhet eller anseende eller för ekonomisk skada för en sådan person, i vilket fall den ska underrätta och inleda samråd med den andra parten omedelbart därefter. Om samrådet inte har lett till en lösning får den andra parten ömsesidigt avbryta överföringarna om den har väsentliga bevis för att den avbrytande partens åtgärd strider mot villkoren i denna punkt. Den avbrytande parten ska häva avbrytandet så snart den överträdelse som motiverar avbrytandet har åtgärdats; varje eventuellt motsvarande avbrytande från den andra parten ska hävas vid den tidpunkten. Personuppgifter som överförts före avbrytandet ska fortsätta att behandlas i enlighet med detta protokoll.

KAPITEL IV

Slutbestämmelser

Artikel 15

Verkningar av detta protokoll

1.
 - a. Artikel 39.2 i konventionen ska tillämpas på detta protokoll.
 - b. Vad gäller parter som är medlemmar i Europeiska unionen får dessa parter i sina ömsesidiga förbindelser tillämpa Europeiska unionens lagstiftning vad gäller frågor som behandlas i detta protokoll.
 - c. Punkt 1 b påverkar inte den fullständiga tillämpningen av detta protokoll mellan parter som är medlemmar i Europeiska unionen och andra parter.
2. Artikel 39.3 i konventionen ska tillämpas på detta protokoll.

Artikel 16

Undertecknande och ikrafträdande

1. Detta protokoll ska stå öppet för undertecknande av parterna i konventionen, som kan uttrycka sitt samtycke till att vara bundna antingen genom
 - a. undertecknande utan förbehåll vad gäller ratificering, godtagande eller godkännande, eller
 - b. undertecknande med förbehåll vad gäller ratificering, godtagande eller godkännande, följt av ratificering, godtagande eller godkännande.
2. Ratifikations-, godtagande- eller godkännandeinstrument ska deponeras hos Europarådets generalsekreterare.
3. Detta protokoll träder i kraft den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då fem parter i konventionen har uttryckt sitt samtycke till att vara bundna av detta protokoll i enlighet med punkterna 1 och 2 i denna artikel.
4. För varje part i konventionen som senare uttrycker sitt samtycke till att vara bunden av detta protokoll ska protokollet träda i kraft den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då parten har uttryckt sitt samtycke till att vara bunden av detta protokoll i enlighet med punkterna 1 och 2 i denna artikel.

Artikel 17

Federal klausul

1. En federal stat får förbehålla sig rätten att åta sig förpliktelser enligt detta protokoll i överensstämmelse med dess grundläggande principer för förhållandet mellan dess centralregering och delstater eller andra jämförbara territoriella enheter, under förutsättning att
 - a. protokollet ska vara tillämpligt för den federala statens centralregering,
 - b. ett sådant förbehåll inte påverkar skyldigheter vad gäller att sörja för det samarbete som andra parter eftersträvar i enlighet med bestämmelserna i kapitel II, och
 - c. bestämmelserna i artikel 13 ska tillämpas på den federala statens delstater eller andra jämförbara territoriella enheter.

2. En annan part får hindra myndigheter, leverantörer eller enheter på sitt territorium från att samarbeta som svar på en framställning eller order som lämnats direkt av delstaten eller annan jämförbar territoriell enhet i en federal stat som har gjort ett förbehåll enligt punkt 1, såvida inte den federala staten underrättar Europarådets generalsekreterare om att en delstat eller annan jämförbar territoriell enhet tillämpar de skyldigheter i detta protokoll som gäller för den federala staten. Europarådets generalsekreterare ska upprätta ett register över sådana underrättelser, och hålla det uppdaterat.

3. En annan part får inte hindra myndigheter, leverantörer eller enheter på sitt territorium från att samarbeta med en delstat eller annan jämförbar territoriell enhet på grundval av ett förbehåll enligt punkt 1, om en order eller framställning har lämnats in via den centrala regeringen eller om ett avtal om en gemensam utredningsgrupp enligt artikel 12 ingås med deltagande av den centrala regeringen. I sådana situationer ska den centrala regeringen säkerställa att de tillämpliga skyldigheterna i protokollet fullgörs, förutsatt att, vad gäller skyddet av personuppgifter som vidarebefordrats till delstater eller jämförbara territoriella enheter, endast villkoren i artikel 14.9 eller, i tillämpliga fall, villkoren i ett avtal eller arrangemang som beskrivs i artikel 14.1 b eller 14.1 c ska tillämpas.

4. Med avseende på de bestämmelser i detta protokoll vars tillämpning faller under en delstats eller jämförbar territoriell enhets jurisdiktion som enligt den federala statens system inte är skyldig att vidta lagstiftningsåtgärder, ska den federala regeringen informera de behöriga myndigheterna i sådana stater om dessa bestämmelser, och lämna ett positivt yttrande i vilket de uppmanas att vidta lämpliga åtgärder för att ge verkan åt dem.

Artikel 18

Territoriell tillämpning

1. Detta protokoll ska tillämpas på det eller de territorier som anges i en förklaring som avgetts av en part enligt artikel 38.1 eller 38.2 i konventionen, i den mån en sådan förklaring inte har återkallats enligt artikel 38.3.

2. En part får vid undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeinstrument förklara att detta protokoll inte ska tillämpas på ett eller flera av de territorier som anges i partens förklaring enligt artikel 38.1 och/eller 38.2 i konventionen.

3. En förklaring enligt punkt 2 i denna artikel får, med avseende på ett i förklaringen angivet territorium, återtogs genom en underrättelse ställd till Europarådets generalsekreterare. Återtagandet får verkan den första dagen i den månad som följer efter utgången av en period på tre månader räknat från den dag då generalsekreteraren tog emot underrättelsen.

Artikel 19

Förbehåll och förklaringar

1. Genom en skriftlig underrättelse ställd till Europarådets generalsekreterare får varje part i konventionen, vid tidpunkten för undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeinstrument, förklara att den använder sig av de förbehåll som avses i artiklarna 7.9 a, 7.9 b, 8.13 och 17 i detta protokoll. Inga andra förbehåll får göras.

2. Genom en skriftlig underrättelse ställd till Europarådets generalsekreterare får varje part i konventionen, vid tidpunkten för undertecknandet av detta protokoll eller vid deponeringen av sitt ratifikations-, godtagande- eller godkännandeinstrument, avge den eller de förklaringar som anges i artiklarna 7.2 b, 7.8, 8.11, 9.1 b, 9.5, 10.9, 12.3, och 18.2 i detta protokoll.

3. Genom en skriftlig underrättelse ställd till Europarådets generalsekreterare ska varje part i konventionen lämna de förklaringar, underrättelser eller meddelanden som anges i artiklarna 7.5 a, 7.5 e, 8.4, 8.10 a, 8.10 b, 14.7 c, 14.10 b och 17.2 i detta protokoll enligt de villkor som anges däri.

*Artikel 20***Status för och återkallande av förbehåll**

1. En part som har lämnat ett förbehåll i enlighet med artikel 19.1 ska återkalla förbehållet helt eller delvis så snart omständigheterna tillåter det. Ett sådant återkallande får verkan från och med dagen för mottagandet av en underrättelse ställd till Europarådets generalsekreterare. Om det i underrättelsen anges att återkallandet av ett förbehåll ska få verkan ett visst i förbehållet angivet datum, och detta datum infaller senare än den dag underrättelsen tas emot av generalsekreteraren, ska återkallandet få verkan detta senare datum.
2. Europarådets generalsekreterare får regelbundet fråga parter som har lämnat ett eller flera förbehåll i enlighet med artikel 19.1 om utsikterna till återkallande av sådana förbehåll.

*Artikel 21***Ändringar**

1. Ändringar av detta protokoll får föreslås av varje part i detta protokoll och ska meddelas av Europarådets generalsekreterare till Europarådets medlemsstater och till parterna och signatärerna till konventionen samt till varje stat som har inbjudits att ansluta sig till konventionen.
2. Varje ändring som föreslås av en part ska meddelas till Europarådets kommitté för brottsfrågor, som ska lägga fram sitt yttrande om den föreslagna ändringen för ministerkommittén.
3. Ministerkommittén ska överväga den föreslagna ändringen och yttrandet från Europarådets kommitté för brottsfrågor och får, efter samråd med parterna i konventionen, anta ändringen.
4. Texten till eventuella ändringar som har antagits av ministerkommittén i enlighet med punkt 3 ska överlämnas till parterna i detta protokoll för godtagande.
5. Ändringar som har antagits i enlighet med punkt 3 ska träda i kraft den trettonde dagen efter det att alla parter i detta protokoll har underrättat generalsekreteraren om att de godtar ändringen.

*Artikel 22***Twistlösning**

Artikel 45 i konventionen ska tillämpas på detta protokoll.

*Artikel 23***Samråd med parterna och bedömning av genomförandet**

1. Artikel 46 i konventionen ska tillämpas på detta protokoll.
2. Parterna ska regelbundet utvärdera den faktiska användningen och genomförandet av bestämmelserna i detta protokoll. Artikel 2 i arbetsordningen för kommittén för konventionen om it-brottslighet, reviderad den 16 oktober 2020, ska gälla i tillämpliga delar. Parterna ska inledningsvis se över och får i samförstånd ändra förfarandena i den artikeln så som de är tillämpliga med avseende på detta protokoll fem år efter det att detta protokoll har trätt i kraft.
3. Översynen av artikel 14 ska inledas när tio konventionsparter har uttryckt sitt samtycke till att vara bundna av detta protokoll.

*Artikel 24***Frånträdande**

1. Varje part får när som helst frånträda detta protokoll genom en underrättelse ställd till Europarådets generalsekreterare.
2. Ett sådant frånträdande får verkan den första dagen i den månad som följer efter utgången av en period på tre månader räknat från den dag då generalsekreteraren tog emot underrättelsen.
3. Om en part i detta protokoll frånträder konventionen innebär detta att den frånträder detta protokoll.
4. Information eller bevis som överförs före den dag då frånträdandet träder i kraft ska fortsätta att behandlas i enlighet med detta protokoll.

*Artikel 25***Underrättelse**

Europarådets generalsekreterare ska underrätta Europarådets medlemsstater, parterna och signatärerna i konventionen och varje stat som har inbjudits att ansluta sig till konventionen om

- a. varje undertecknande,
- b. varje deponering av ratifikations-, godtagande- eller godkännandeinstrument,
- c. varje datum för detta protokolls ikraftträdande i enlighet med artikel 16.3 och 16.4,
- d. varje förklaring eller förbehåll som lämnats i enlighet med artikel 19 eller återkallande av förbehåll som lämnats i enlighet med artikel 20,
- e. andra åtgärder, underrättelser eller meddelanden som rör protokollet.

Till bevis härpå har undertecknade, därtill vederbörligen befullmäktigade, undertecknat detta protokoll.

Upprättat i Strasbourg den 12 maj 2022 på engelska och franska, vilka båda texter är lika giltiga, i ett enda exemplar, som ska deponeras i Europarådets arkiv. Europarådets generalsekreterare ska översända bestyrkta kopior till varje medlemsstat i Europarådet, till parterna och signatärerna i konventionen och till varje stat som har inbjudits att ansluta sig till konventionen.

Statens offentliga utredningar 2024

Kronologisk förteckning

1. Ett starkare skydd för offentliganställda mot våld, hot och trakasserier. Ju.
2. Ett samordnat vaccinationsarbete – för effektivare hantering av kommande vacciner. Del 1 och 2. S.
3. Ett starkt juridiskt liv för framtida generationer. Nationell strategi för att stärka juridiskt liv i Sverige 2025–2034. Ku.
4. Inskränkningarna i upphovsrätten. Ju.
5. Förbättrad ordning och säkerhet vid förvar. Ju.
6. Steg mot stärkt kapacitet. Fi.
7. Ett säkrare och mer tillgängligt fastighetsregister. Ju.
8. Livsmedelsberedskap för en ny tid. LI.
9. Utvecklat samarbete för verksamhetsförlagd utbildning – långsiktiga åtgärder för sjuksköterskeprogrammen. U.
10. Preskription av avlägsnandebeslut och vissa frågor om återreseförbud. Ju.
11. Rätt frågor på regeringens bord – en ändamålsenlig regeringsprövning på miljöområdet. KN.
12. Mål och mening med integration. A.
13. En effektivare kontaktförbudslagstiftning – ett utökat skydd för utsatta personer. Ju.
14. Arbetslivskriminalitet – myndighets-samverkan, en gemensam tipsfunktion, lärdomar från Belgien och gränsöverskridande arbete. A.
15. Nya regler för arbetskraftsinvandring m.m. Ju.
16. Växla yrke som vuxen – en reformerad vuxenutbildning och en ny yrkesskola för vuxna. U.
17. Skolor mot brott. U.
18. Nya regler om cybersäkerhet. Fö.
19. En ny beredskapssektor – för ökad försörjningsberedskap. KN.
20. Maskinellt värde för vissa industribyggnader – ett undantag från fastighets-skatt. Fi.
21. Ett inkluderande jämställdhetspolitiskt delmål mot våld. A.
22. En ny organisation för förvaltning av EU-medel. Fi.
23. En trygg uppväxt utan nikotin, alkohol och lustgas. S.
24. Ett effektivt straffrättsligt skydd för statliga stöd till företag. Fi.
25. En mer effektiv tillsyn över socialtjänsten. S.
26. En utvärdering av förändringar i sjukförsäkringens regelverk under 2021 och 2022. S.
27. Kamerabevakning i offentlig verksamhet – lättnader och utökade möjligheter. Ju.
28. Offentlighetsprincipen eller insyns-lag. Allmänhetens insyn i enskilda aktörer inom skolväsendet. U.
29. Goda möjligheter till ökat välbefinnande. Fi.
30. En statlig ordning med brottsförebyggande åtgärder för barn och unga. S.
31. En ändamålsenlig vapenlagstiftning. Del 1 och 2. Ju.
32. Åtgärder mot mervärdesskattebedrägerier. Fi.
33. Delad hälsodata – dubbel nytta. Regler för ökad interoperabilitet i hälso- och sjukvården. S.
34. Ansvar och oberoende – public service i oroliga tider. Ku.
35. En framtid för alm och ask – förädling, forskning och finansiering. LI.

36. Förenkla och förbättra! Fi.
37. Förbättrade ränteavdragsregler för företag. Fi.
38. Digitala fastighetsköp & Förköpsrätt vid fastighetstransaktioner. LI.
39. Skärpta regler om ungdomsövervakning och straffreduktion för unga. Ju.
40. Genomförande av lönetransparensdirektivet. A.
41. Styrkraft för lyckad integration. A.
42. Bildning, utbildning och delaktighet – folkbildningspolitik i en ny tid. U.
43. Staten och kommunsektorn – samverkan, självstyrelse, styrning. Fi.
44. Stärkt kontroll av fusk i livsmedelskedjan. LI.
45. Kompletterande bestämmelser till EU:s reviderade förordning om elektronisk identifiering. Fi.
46. Ny lag om internationella sanktioner. Genomförande av EU:s sanktionsdirektiv. UD.
47. Digital myndighetspost. Fi.
48. Ett ändamålsenligt samhällsskydd. Vissa reformer av straff- och straffverkställighetslagstiftningen. Volym 1 och 2. Ju.
49. Arbetslöshetsförsäkringen vid störning, kris eller krig. A.
50. Nätt och jämnt. Likvärdighet och effektivitet i kommunsektorn. Del 1 och 2. Fi.
51. En mer rättssäker och effektiv domstolsprocess. Ju.
52. Allmänna sammankomster och Sveriges säkerhet. Ju.
53. Stöd till invandrades utvandring. Ju.
54. Vagar till ett tryggare samhälle. Åtgärder för att motverka återfall i brott. Ju.
55. En översyn av 23 kap. brottsbalken. Ju.
56. Animalieproduktion med hög konkurrenskraft och gott djurskydd. LI.
57. Ett nytt regelverk för hälsodataregister. S.
58. Ett nytt regelverk mot penningtvätt och finansiering av terrorism. Volym 1 och 2. Fi.
59. Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning. Fö.
60. Stärkt stöd till anhöriga. Ett mer ändamålsenligt stöd till barn och vuxna som är anhöriga. S.
61. Effektivare kontrollmöjligheter i systemen för rot, rut, grön teknik och personalliggare. Fi.
62. En förbättrad modell för presumtionshyra. Ju.
63. Ökat informationsutbyte mellan myndigheter. Behov och föreslagna förändringar. Ju.
64. Motståndskraft i samhällsviktiga tjänster. Fö.
65. Kommuners och regioners grundläggande beredskap inför kris och krig. Fö.
66. Livsviktigt lärande – fler vägar till kunskap för att förebygga suicid. S.
67. Om ekonomiska styrmedel för en mer cirkulär ekonomi. Fi.
68. Mottagandelagen. En ny lag för ordnat asylmottagande och effektivt återvändande. Ju.
69. Ett nytt konsumentkreditdirektiv. Ju.
70. Tiotandvård – ett förstärkt högkostnadsskydd för tandvård. S.
71. Reglering av hushållens skulder. Fi.
72. Stärkt medicinsk kompetens i kommunal hälso- och sjukvård. S.
73. Juridiska personers förvärv av lantbruksegendom genom testamente. LI.
74. Fler vägar till arbetslivet. U.
75. Personuppgifter och mediegrundlagarna. Ju.
76. Från överskottsmål till balansmål. Fi.
77. Ett modernt och anpassat regelverk för krigsmateriel. UD.
78. Ett språkrav för språkutveckling. S.
79. Handlingsoffentlighet och handlingar som inhämtas genom straffprocessuella tvångsmedel. Ju.
80. Vissa åtgärder för stärkt återvändandeverksamhet och utlänningskontroll. Ju.
81. Ämneskunskaper och lärarskicklighet – en reformerad lärarutbildning. U.

82. Ökad va-beredskap. KN.
83. Fler vägar till att äga sitt boende.
Del I. En utvidgning av systemet
med ägarlägenheter.
Del II. En lagreglerad modell
för hyrköp av bostäder. Ju.
84. Skärpt kontroll av utländska
fastighetsförvärv. Fö.
85. Effektivare gränsöverskridande inhämt-
ning av elektroniska bevis. Ju.

Statens offentliga utredningar 2024

Systematisk förteckning

Arbetsmarknadsdepartementet

- Mål och mening med integration. [12]
- Arbetslivskriminalitet – myndighets-samverkan, en gemensam tipsfunktion, lärdomar från Belgien och gränsöver-skridande arbete. [14]
- Ett inkluderande jämställdhetspolitiskt delmål mot våld. [21]
- Genomförande av lönetransparensdirektivet. [40]
- Styrkraft för lyckad integration. [41]
- Arbetslöshetsförsäkringen vid störning, kris eller krig. [49]

Finansdepartementet

- Steg mot stärkt kapacitet. [6]
- Maskinellt värde för vissa industribyggnader – ett undantag från fastighetsskatt. [20]
- En ny organisation för förvaltning av EU-medel. [22]
- Ett effektivt straffrättsligt skydd för statliga stöd till företag. [24]
- Goda möjligheter till ökat välstånd. [29]
- Åtgärder mot mervärdesskattebedrägerier. [32]
- Förenkla och förbättra! [36]
- Förbättrade ränteavdragsregler för företag. [37]
- Staten och kommunsektorn – samverkan, självstyrelse, styrning. [43]
- Kompletterande bestämmelser till EU:s reviderade förordning om elektronisk identifiering. [45]
- Digital myndighetspost. [47]
- Nätt och jämnt. Likvärdighet och effektivitet i kommunsektorn. Del 1 och 2. [50]

- Ett nytt regelverk mot penningtvätt och finansiering av terrorism. Volym 1 och 2. [58]
- Effektivare kontrollmöjligheter i systemen för rot, rut, grön teknik och personal-liggare. [61]
- Om ekonomiska styrmedel för en mer cirkulär ekonomi. [67]
- Reglering av hushållens skulder. [71]
- Från överskottsmål till balansmål. [76]

Försvarsdepartementet

- Nya regler om cybersäkerhet. [18]
- Signalspaning i försvarsunderrättelseverk-samhet – en modern och ändamålsenlig lagstiftning. [59]
- Motståndskraft i samhällsviktiga tjänster. [64]
- Kommuners och regioners grundläggande beredskap inför kris och krig. [65]
- Skärpt kontroll av utländska fastighetsförvärv. [84]

Justitiedepartementet

- Ett starkare skydd för offentliganställda mot våld, hot och trakasserier. [1]
- Inskränkningarna i upphovsrätten. [4]
- Förbättrad ordning och säkerhet vid förvar. [5]
- Ett säkrare och mer tillgängligt fastighetsregister. [7]
- Preskription av avlägsnandebeslut och vissa frågor om återreseförbud. [10]
- En effektivare kontaktförbuds-lagstiftning – ett utökat skydd för utsatta personer. [13]
- Nya regler för arbetskraftsinvandring m.m. [15]

Kamerabevakning i offentlig verksamhet – lättnader och utökade möjligheter. [27]

En ändamålsenlig vapenlagstiftning. Del 1 och 2. [31]

Skärpta regler om ungdomsövervakning och straffreduktion för unga. [39]

Ett ändamålsenligt samhällsskydd. Vissa reformer av straff- och straffverkställighetslagstiftningen. Volym 1 och 2. [48]

En mer rättssäker och effektiv domstolsprocess. [51]

Allmänna sammankomster och Sveriges säkerhet. [52]

Stöd till invandras utvandring. [53]

Vägar till ett tryggare samhälle. Åtgärder för att motverka återfall i brott. [54]

En översyn av 23 kap. brottsbalken. [55]

En förbättrad modell för presumtionshyra. [62]

Ökat informationsutbyte mellan myndigheter. Behov och föreslagna förändringar. [63]

Mottagandelagen. En ny lag för ordnat asylmottagande och effektivt återvändande. [68]

Ett nytt konsumentkreditdirektiv. [69]

Personuppgifter och mediegrundlagarna. [75]

Handlingsoffentlighet och handlingar som inhämtas genom straffprocessuella tvångsmedel. [79]

Vissa åtgärder för stärkt återvändandeverksamhet och utlänningskontroll. [80]

Fler vägar till att äga sitt boende. Del I. En utvidgning av systemet med ägarlägenheter. Del II. En lagreglerad modell för hyrköp av bostäder. [83]

Effektivare gränsöverskridande inhämtning av elektroniska bevis. [85]

Klimat- och näringslivsdepartementet

Rätt frågor på regeringens bord – en ändamålsenlig regeringsprövning på miljöområdet. [11]

En ny beredskapssektor – för ökad försörjningsberedskap. [19]

Ökad va-beredskap. [82]

Kulturdepartementet

Ett starkt judiskt liv för framtida generationer. Nationell strategi för att stärka judiskt liv i Sverige 2025–2034. [3]

Ansvar och oberoende – public service i oroliga tider. [34]

Landsbygds- och infrastrukturdepartementet

Livsmedelsberedskap för en ny tid. [8]

En framtid för alm och ask – förädling, forskning och finansiering. [35]

Digitala fastighetsköp & Förköpsrätt vid fastighetstransaktioner. [38]

Stärkt kontroll av fusk i livsmedelskedjan. [44].

Animalieproduktion med hög konkurrenskraft och gott djurskydd. [56].

Juridiska personers förvärv av lantbruks-egendom genom testamente. [73]

Socialdepartementet

Ett samordnat vaccinationsarbete – för effektivare hantering av kommande vacciner. Del 1 och 2. [2]

En trygg uppväxt utan nikotin, alkohol och lustgas. [23]

En mer effektiv tillsyn över socialtjänsten. [25]

En utvärdering av förändringar i sjukförsäkringens regelverk under 2021 och 2022. [26]

En statlig ordning med brottsförebyggande åtgärder för barn och unga. [30]

Delad hälsodata – dubbel nytta. Regler för ökad interoperabilitet i hälso- och sjukvården. [33]

Ett nytt regelverk för hälsodataregister. [57]

Stärkt stöd till anhöriga. Ett mer ändamålsenligt stöd till barn och vuxna som är anhöriga. [60]

Livsviktigt lärande – fler vägar till kunskap för att förebygga suicid. [66]

Tiotandvård – ett förstärkt högkostnads- skydd för tandvård. [70]

Stärkt medicinsk kompetens i kommunal hälso- och sjukvård. [72]

Ett språkr krav för språkutveckling. [78]

Utbildningsdepartementet

Utvecklat samarbete för verksamhets- förlagd utbildning – långsiktiga åtgärder för sjuksköterskeprogrammen. [9]

Växla yrke som vuxen – en reformerad vuxenutbildning och en ny yrkesskola för vuxna. [16]

Skolor mot brott. [17]

Offentlighetsprincipen eller insynslag. Allmänhetens insyn i enskilda aktörer inom skolväsendet. [28]

Bildning, utbildning och delaktighet – folkbildningspolitik i en ny tid. [42]

Fler vägar till arbetslivet. [74]

Ämneskunskaper och lärarskicklighet – en reformerad lärarutbildning. [81]

Utrikesdepartementet

Ny lag om internationella sanktioner. Genomförande av EU:s sanktions- direktiv. [46]

Ett modernt och anpassat regelverk för krigsmateriel. [77]