



EUROPEISKA
KOMMISSIONEN

Strasbourg den 17.4.2018
COM(2018) 225 final

2018/0108 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

**om europeiska utlämnandeorder och bevarandeorder för elektroniska bevis i
straffrättsliga förfaranden**

{SWD(2018) 118 final} - {SWD(2018) 119 final}

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

Det är i dag allmänt förekommande i många delar av världen att använda sociala medier, webbaserad e-post, meddelandetjänster och applikationer ("appar") för att kommunicera, arbeta, umgås och hämta information. Dessa tjänster förbinder hundratals miljoner användare med varandra. De genererar avsevärda vinster för användarnas ekonomiska och sociala välfärd inom hela unionen och utanför. De kan emellertid också användas som verktyg för att begå eller underlätta brott, inklusive allvarliga brott, såsom terroristattacker. När detta inträffar är dessa tjänster och applikationer ofta det enda ställe där brottsutredare kan finna ledtrådar för att avgöra vem som har begått ett brott, samt inhämta bevis som kan användas i domstol.

Eftersom internet är gränslöst kan sådana tjänster tillhandahållas var som helst i världen och kräver inte nödvändigtvis en fysisk infrastruktur, ett företag eller personal i de medlemsstater där tjänsterna erbjuds, eller på den inre marknaden som helhet. De kräver inte heller en särskild plats för lagring av uppgifter, vilken ofta väljs av tjänsteleverantören på grundval av berättigade överväganden, t.ex. datasäkerhet, stordriftsfördelar och snabb tillgång. Detta medför i ett växande antal brottmål som rör alla typer av brott¹ att medlemsstaternas myndigheter behöver ha tillgång till uppgifter som kan tjäna som bevismaterial och som lagras utanför det berörda landet och/eller av tjänsteleverantörer i andra medlemsstater eller i tredjeländer.

För situationer där antingen bevisen finns eller tjänsteleverantören är etablerad någon annanstans, utformades mekanismerna för samarbete mellan länder för flera årtionden sedan². Trots återkommande reformer står dessa samarbetsmekanismer under ökat tryck från det växande behovet av snabb, gränsöverskridande tillgång till elektroniska bevis. För att åtgärda detta har ett antal medlemsstater och tredjeländer beslutat att utöka sina nationella verktyg. Den resulterande fragmenteringen skapar rättsosäkerhet och motstridiga förpliktelser och väcker frågor om skyddet av grundläggande rättigheter och processuella garantier för personer som berörs av sådana begäranden.

År 2016 efterlyste rådet konkreta åtgärder på grundval av en gemensam EU-strategi för att göra den ömsesidiga rättsliga hjälpen effektivare, förbättra samarbetet mellan medlemsstaternas myndigheter och tjänsteleverantörer baserade i länder utanför EU, och föreslå lösningar på problemet med att fastställa och verkställa jurisdiktion³ i cyberrymden⁴. Europaparlamentet framhöll också de utmaningar som det för närvarande splittrade regelverket kan medföra för tjänsteleverantörer som vill följa framställningar på brottsbekämpningsområdet, och efterlyste en europeisk rättslig ram med garantier för rättigheter och friheter för alla berörda parter⁵.

¹ Se avsnitten 2.1.1 och 2.3 i konsekvensbedömningen.

² Inom unionen, regler för ömsesidigt erkännande, som numera grundar sig på direktivet om en europeisk utredningsorder; med tredjeländer, mekanismer för ömsesidig rättslig hjälp.

³ I detta dokument avses med termen "verkställande jurisdiktion" de relevanta myndigheternas behörighet att vidta en utredningsåtgärd.

⁴ [Slutsatser från Europeiska unionens råd om förbättrad straffrätt i cyberrymden](#) ST9579/16.

⁵ [P8_TA\(2017\)0366](#)

Det föreliggande förslaget är inriktat på det specifika problem som uppstår genom den elektroniska bevisningens flyktiga karaktär och dess internationella dimension. Det syftar till att anpassa samarbetsmekanismerna till den digitala tidsåldern, för att ge rättsväsendet och de brottsbekämpande myndigheterna möjligheter att hantera hur brottslingar kommunicerar i dag, samt bekämpa moderna former av brottslighet. Sådana verktyg måste samtidigt villkoras av ett starkt skydd av grundläggande rättigheter. Syftet med detta förslag är att förbättra den rättsliga förutsebarheten för myndigheter, tjänsteleverantörer och berörda personer och att upprätthålla en hög standard för framställningar på brottsbekämpningsområdet, vilket garanterar skydd av de grundläggande rättigheterna, transparens och ansvarighet. Det påskyndar också processen för att säkra och inhämta bevis i elektronisk form som lagras och/eller som innehas av tjänsteleverantörer som är etablerade i en annan jurisdiktion. Detta instrument kommer att samexistera med gällande rättsliga samarbetsinstrument som fortfarande är relevanta och som kan användas av de behöriga myndigheterna när så är lämpligt. Samtidigt arbetar kommissionen för att stärka de befintliga mekanismerna för rättsligt samarbete genom åtgärder såsom inrättandet av en säker plattform för snabbt utbyte av framställningar mellan rättsliga myndigheter inom EU, och en investering på 1 miljon euro för att utbilda rättstillämpare från alla medlemsstater i ömsesidig rättslig hjälp och samarbete, med särskild inriktning på Förenta staterna i egenskap av det tredjeland som tar emot det största antalet framställningar från EU⁶.

För delgivning och verkställande av order inom ramen för detta instrument bör myndigheterna förlita sig på den rättsliga företrädare som utsetts av tjänsteleverantörerna. Kommissionen lägger i dag fram ett förslag för att säkerställa att sådana rättsliga företrädare utses. Förslaget tillhandahåller en gemensam, EU-omfattande lösning för att hantera delgivning av order till tjänsteleverantörer genom en rättslig företrädare.

- **Förenlighet med EU:s befintliga rättsliga ram på det berörda politikområdet och Europarådets Budapestkonvention**

EU:s befintliga rättsliga ram består av unionens samarbetsinstrument på det straffrättsliga området, såsom direktiv 2014/41/EU om en europeisk utredningsorder på det straffrättsliga området⁷, konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater⁸, rådets beslut 2002/187/RIF om inrättande av Eurojust⁹, förordning (EU) 2016/794 om Europol¹⁰, rådets rambeslut 2002/465/RIF om gemensamma utredningsgrupper¹¹, samt bilaterala avtal mellan unionen och tredjeländer, såsom avtalet om

⁶ https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

⁷ [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).

⁸ [Rådets akt av den 29 maj 2000](#) om att i enlighet med artikel 34 i Fördraget om Europeiska unionen upprätta konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater.

⁹ [Rådets beslut 2002/187/RIF](#) av den 28 februari 2002 om inrättande av Eurojust för att stärka kampen mot grov brottslighet. Kommissionen antog 2013 [ett förslag till förordning](#) om att reformera Eurojust (Förslag till Europaparlamentets och rådets förordning om Europeiska unionens byrå för straffrättsligt samarbete (Eurojust), COM/2013/0535 final).

¹⁰ [Europaparlamentets och rådets förordning \(EU\) 2016/794](#) av den 11 maj 2016 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) och om ersättande och upphävande av rådets beslut 2009/371/RIF, 2009/934/RIF, 2009/935/RIF, 2009/936/RIF och 2009/968/RIF.

¹¹ [Rådets rambeslut 2002/465/RIF](#) av den 13 juni 2002 om gemensamma utredningsgrupper.

ömsesidig rättslig hjälp mellan Europeiska unionen och Amerikas förenta stater¹² och avtalet om ömsesidig rättslig hjälp mellan Europeiska unionen och Japan¹³.

Genom att införa europeiska utlämnandeorder och europeiska bevarandeorder underlättar förslaget att i samband med straffrättsliga förfaranden säkra och samla in elektroniska bevis som lagras eller innehas av tjänsteleverantörer i en annan jurisdiktion. Direktivet om en europeisk utredningsorder, vilket i stor utsträckning har ersatt konventionen om ömsesidig rättslig hjälp i brottmål, omfattar alla typer av utredningsåtgärder¹⁴. Detta innebär tillgång till elektroniska bevis, men direktivet om en europeisk utredningsorder innehåller inga särskilda bestämmelser om denna typ av bevis¹⁵. Det nya instrumentet kommer inte att ersätta den europeiska utredningsordern i ärenden som kräver inhämtande av elektroniska bevis, utan utgör ett kompletterande instrument för myndigheterna. 'Det kan uppstå situationer där den europeiska utredningsordern kan vara förstahandsvalet för offentliga myndigheter, till exempel när flera utredningsåtgärder måste genomföras i den verkställande medlemsstaten. Att skapa ett nytt instrument för elektroniska bevis är ett bättre alternativ än att ändra direktivet om en europeisk utredningsorder, med hänsyn till de särskilda utmaningar som inhämtning av elektroniska bevis innebär. En sådan lösning påverkar inte andra utredningsåtgärder i direktivet om en europeisk utredningsorder.

För att underlätta gränsöverskridande insamling av elektronisk bevisning kommer det nya instrumentet att bygga på principen om ömsesidigt erkännande. En myndighet i det land där mottagaren av ordern befinner sig måste inte delta i och genomföra ordern direkt, utom om bristande efterlevnad föreligger. I sådant fall kommer verkställighet att krävas och den behöriga myndigheten i det land där ombudet är etablerat ska ingripa. Instrumentet kräver därför en uppsättning kraftfulla skyddsåtgärder och bestämmelser, såsom validering av en rättslig myndighet i varje enskilt fall. Exempelvis får utlämnandeorder på unionsnivå gällande transaktioner eller innehållsdata (i motsats till abonnent- och åtkomstdata) endast utfärdas för brott som i den utfärdande staten är belagda med ett maximalt frihetsstraff på minst 3 år, eller för specifika brott som är beroende av eller möjliggörs av internetbaserad verksamhet eller terroristrelaterad brottslighet, som avses i förslaget.

Personuppgifter som omfattas av detta förslag är skyddade och får endast behandlas i enlighet med den allmänna dataskyddsförordningen¹⁶ och dataskyddsdirektivet för polis och straffrättsliga myndigheter¹⁷. Den allmänna dataskyddsförordningen kommer att börja

¹² [Rådets beslut 2009/820/Gusp](#) av den 23 oktober 2009 om ingående på Europeiska unionens vägnar av avtalet om utlämning mellan Europeiska unionen och Amerikas förenta stater och av avtalet om ömsesidig rättslig hjälp mellan Europeiska unionen och Amerikas förenta stater.

¹³ [Rådets beslut 2010/616/EU](#) av den 7 oktober 2010 om ingående av avtalet mellan Europeiska unionen och Japan om ömsesidig rättslig hjälp i brottmål.

¹⁴ Med undantag av gemensamma utredningsgrupper (se artikel 3 i direktivet om en europeisk utredningsorder); alla medlemsstater deltar inte i direktivet om en europeisk utredningsorder (Irland, Danmark).

¹⁵ Med undantag av en hänvisning till identifiering av en person som har ett abonnemang för en viss IP-adress i artikel 10.2 e, för vilken dubbel straffbarhet inte kan åberopas som grund för vägran att erkänna eller verkställa begäran.

¹⁶ [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.

¹⁷ [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.

tillämpas den 25 maj 2018, medan dataskyddsdirektivet för brottsbekämpning måste införlivas av medlemsstaterna senast den 6 maj 2018.

Europarådets Budapestkonvention om it-relaterad brottslighet (CETS nr 185), som ratificerats av de flesta EU-medlemsstater, inrättar internationella mekanismer för samarbete mot it-brottslighet¹⁸. Konventionen behandlar brott som begås via internet och andra elektroniska nätverk. Den krävs också att parterna fastställer befogenheter och förfaranden för inhämtande av bevis i elektronisk form och att ge varandra ömsesidig rättslig hjälp som inte begränsas till it-brott. Konventionen ålägger särskilt parterna att införa utlämnandeorder för att samla in datauppgifter från tjänsteleverantörer inom deras territorium och abonnentuppgifter från tjänsteleverantörer som tillhandahåller tjänster på deras territorium. I konventionen föreskrivs dessutom bevarandeorder när det finns skäl att anse att datorbehandlingsbara uppgifter är särskilt utsatta för förlust eller ändring. Delgivning och verkställighet av nationella beslut om utlämnandeorder gentemot tjänsteleverantörer med säte utanför en part till konventionen väcker ytterligare frågeställningar. I detta avseende övervägs för närvarande ytterligare åtgärder för att förbättra gränsöverskridande tillgång till elektroniskt bevismaterial¹⁹.

• **Sammanfattning av den föreslagna förordningen**

Genom den föreslagna förordningen införs bindande europeiska utlämnandeorder och bevarandeorder. Båda typerna av order måste utfärdas eller godkännas av en rättslig myndighet i en medlemsstat. En order kan utfärdas för att uppnå bevarande eller utlämnande av uppgifter som lagras av en tjänsteleverantör som är etablerad i en annan jurisdiktion, och som är nödvändiga som bevis i brottsutredningar eller straffrättsliga förfaranden. Sådana order får endast utfärdas om en liknande bestämmelse finns för samma brott i en jämförbar inhemsk situation i den utfärdande staten. Båda ordena kan delges leverantörer av elektroniska kommunikationstjänster, sociala nätverk, elektroniska marknadsplatser, andra värdtjänstleverantörer och leverantörer av internetinfrastruktur såsom IP-adress och domännamnsregister, eller deras rättsliga företrädare när sådana finns. Den europeiska bevarandeordern, i likhet med den europeiska utlämnandeordern, riktar sig till den rättsliga företrädaren utanför den utfärdande medlemsstatens jurisdiktion, och har till syfte att bevara uppgifterna med avseende på en senare begäran att lägga fram dessa uppgifter, exempelvis via ömsesidig rättslig hjälp i fråga om tredjeländer, eller via en europeisk utredningsorder mellan de deltagande medlemsstaterna. Till skillnad från övervakningsåtgärder eller lagringsskyldigheter som fastställs i lag, vilka inte behandlas i denna förordning, är den europeiska bevarandeordern ett föreläggande som utfärdats eller godkänts av en rättslig myndighet i ett straffrättsligt förfarande efter en individuell bedömning av proportionaliteten och nödvändigheten i varje enskilt fall. I likhet med den europeiska utlämnandeordern avses specifika kända eller okända förövare av en straffbar gärning som redan har ägt rum. Den europeiska bevarandeordern gör det endast möjligt att bevara uppgifter som redan har lagrats vid tidpunkten för ordermottagandet, men ger inte tillgång till uppgifter vid en framtida tidpunkt efter mottagandet av bevarandeordern.

¹⁸ I 2013 års EU-strategi för cybersäkerhet erkändes Budapestkonventionen som den viktigaste multilaterala ramen i kampen mot it-brottslighet – Gemensamt meddelande från kommissionen och Europeiska unionens höga representant för utrikes frågor och säkerhetspolitik om EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd (JOIN(2013) 1 final).

¹⁹ Vid sin 17:e plenarsession (juni 2017) antog kommittén för konventionen om it-brottslighet (T-CY) riktlinjer för utarbetandet av ett andra tilläggsprotokoll till konventionen (nedan kallade *andra tilläggsprotokollet*) som ska utarbetas och färdigställas senast i december 2019. Syftet är att i minskande utsträckning låta platsen för datalagring vara en avgörande faktor.

Båda ordena får endast användas i straffrättsliga förfaranden, från den inledande utredningsfasen före rättegång fram till avslutandet av förfarandet genom dom eller annat beslut. De utlämnandeorder som gäller uppgifter om abonnenter och åtkomstdata kan utfärdas för alla brott, medan utlämnandeorder om transaktionsdata eller innehållsdata endast får utfärdas för brott som i den utfärdande staten är belagda med ett maximalt frihetsstraff på minst 3 år, eller för vissa brott som anges i förslaget och där det finns en särskild koppling till elektroniska verktyg och brott som omfattas av direktiv (EU) 2017/541 om bekämpande av terrorism.

Med hänsyn till graden av intrång hos de åtgärder som införts i förhållande till de uppgifter som eftersträvas, fastställer förslaget ett antal villkor och skyddsåtgärder. Dessa innebär skyldigheten att inhämta förhandsvalidering av order från en rättslig myndighet. Förslaget gäller endast för lagrade uppgifter. Avlyssning av telekommunikationer i realtid omfattas inte av detta förslag. Åtgärden är begränsad till vad som är nödvändigt och proportionerligt för relevanta straffrättsliga förfaranden. Det gör det också möjligt för tjänsteleverantörerna att söka förtydliganden från utfärdande myndigheter om så krävs. Om dessa frågor inte kan lösas och den utfärdande myndigheten beslutar att verkställa ordern får tjänsteleverantörerna åberopa samma skäl för att motsätta sig verkställighet genom sina egna myndigheter. Dessutom upprättas ett särskilt förfarande för situationer där skyldigheten att lämna uppgifter strider mot en skyldighet som följer av lagstiftningen i ett tredjeland.

EU:s lagstiftning skyddar rättigheterna för misstänkta och tilltalade i straffrättsliga förfaranden, och det finns redan regler för skydd av personuppgifter. För de personer vars uppgifter efterfrågas erbjuder dessa ytterligare skyddsåtgärder i förslaget processuella rättigheter för dessa personer inom eller utanför de straffrättsliga förfarandena. Detta innebär möjligheten att bestrida orderns lagenlighet, nödvändighet och proportionalitet, utan att begränsa skälen för bestridandet i enlighet med nationell lagstiftning. De rättigheter som anges i den verkställande statens lagstiftning respekteras fullt ut genom att säkerställa att immunitet och privilegier som skyddar de efterfrågade uppgifterna i tjänsteleverantörens medlemsstat beaktas i den utfärdande staten. Detta är särskilt fallet när de erbjuder ett högre skydd än lagstiftningen i den utfärdande staten.

Ordena enligt den föreslagna förordningen är verkställbara på samma sätt som jämförbara inhemska order i den jurisdiktion där tjänsteleverantören delges ordern. I förordningen föreskrivs att medlemsstaterna ska inrätta effektiva och proportionerliga påföljder.

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

• Rättslig grund

Den rättsliga grunden för att besluta om åtgärder på området är artikel 82.1 i fördraget om Europeiska unionens funktionssätt. I artikel 82.1 föreskrivs att åtgärder får antas i enlighet med det ordinarie lagstiftningsförfarandet för att fastställa regler och förfaranden för att säkerställa erkännande i hela unionen av alla former av domar och rättsliga avgöranden. Åtgärder får också vidtas för att underlätta samarbetet mellan rättsliga eller likvärdiga myndigheter i medlemsstaterna inom ramen för lagföring och verkställighet av beslut.

Denna rättsliga grund är tillämplig på de mekanismer som omfattas av denna förordning. Artikel 82.1 säkerställer ömsesidigt erkännande av rättsliga avgöranden varigenom en rättslig myndighet i den utfärdande staten riktar sig till en juridisk person i en annan medlemsstat och även ålägger den skyldigheter, utan föregående ingripande av en rättslig myndighet i den

andra medlemsstaten. Den europeiska utlämnandeordern eller bevarandeordern kan leda till ingripande av en rättslig myndighet i den verkställande staten när så är nödvändigt för att verkställa beslutet.

- **Val av instrument**

Artikel 82.1 i EUF-fördraget ger unionens lagstiftare möjlighet att anta förordningar och direktiv.

Eftersom förslaget avser gränsöverskridande förfaranden där enhetliga regler krävs, finns det inget behov av att lämna en marginal för medlemsstaterna att införliva sådana bestämmelser. En förordning är direkt tillämplig, vilket ger klarhet och större rättssäkerhet, och man undviker olika tolkningar i olika medlemsstater och andra problem som varit förknippade med införlivandet av rambesluten om ömsesidigt erkännande av domar och rättsliga avgöranden. En förordning möjliggör dessutom att samma skyldighet införs på ett enhetligt sätt i unionen. Av dessa skäl anses den lämpligaste formen för detta instrument för ömsesidigt erkännande vara en förordning.

- **Subsidiaritetsprincipen**

Med tanke på den gränsöverskridande dimensionen hos de frågor som hanteras, måste de åtgärder som ingår i förslaget antas på unionsnivå för att uppnå målen. De brott för vilka elektroniska bevis föreligger gäller ofta situationer där infrastrukturen för förvaring av elektroniskt bevismaterial och den tjänsteleverantör som driver infrastrukturen lyder under en annan nationell rättslig ram, inom eller utanför unionen, än den nationella rättsliga ramen för offret och förövaren av brottet. Därför kan det bli mycket tidskrävande och svårt för det behöriga landet att på ett effektivt sätt få tillgång till elektroniska bevis över gränserna utan gemensamma minimiregler. Särskilt medlemsstater som agerar på egen hand skulle ha svårt att ta itu med följande frågor:

- Fragmenteringen av rättsliga ramar i medlemsstaterna, vilket identifierades som en viktig utmaning för tjänsteleverantörer som försöker följa framställningar på grundval av olika nationella lagar.
- Bättre effektivitet i det rättsliga samarbetet på grundval av befintlig unionslagstiftning, särskilt via den europeiska utredningsordern.

Med hänsyn till mångfalden av rättssystem, antalet berörda politikområden (säkerhet, grundläggande rättigheter, inbegripet processuella rättigheter och skydd av personuppgifter, ekonomiska frågor) och det stora antalet aktörer, är unionslagstiftning det lämpligaste sättet att hantera de konstaterade problemen.

- **Proportionalitetsprincipen**

I förslaget fastställs regler enligt vilka en behörig myndighet i unionen får ålägga en tjänsteleverantör som tillhandahåller tjänster i unionen och som inte är etablerad i samma medlemsstat, att lämna ut eller bevara elektroniskt bevismaterial. Huvuddragen i förslaget, t.ex. det materiella tillämpningsområdet för den europeiska utlämnandeordern, villkor som garanterar hövlighet, sanktionsmekanismen och systemet för säkerhetsgarantier och rättsmedel, begränsar förslaget till vad som är nödvändigt för att uppnå dess huvudsakliga mål. Förslaget är särskilt begränsat till begäranden om lagrade uppgifter (uppgifter från avlyssning av telekommunikationer i realtid omfattas inte) och till order som utfärdas i straffrättsliga förfaranden för ett specifikt brott under utredning. Det omfattar därmed inte

förebyggande av brottslighet eller andra typer av förfaranden eller överträdelser (till exempel administrativa förfaranden för överträdelser av rättsregler) och innehåller inte något krav på att leverantörerna systematiskt samlar in eller lagrar ytterligare uppgifter annat än av affärsmässiga skäl eller för att uppfylla andra rättsliga krav. Även om utlämnandeorderna för abonnentuppgifter och åtkomstuppgifter kan utfärdas för alla brott, får utlämnandeorder för transaktionsuppgifter eller innehållsdata endast utfärdas för brott som i den utfärdande staten är belagda med ett maximalt frihetsstraff på minst 3 år, eller för särskilda cyberrelaterade brott och brott med koppling till terrorism. Slutligen klargör förslaget förfaranderegler och garantier som gäller för gränsöverskridande tillgång till elektroniska bevis, men sträcker sig inte till att harmonisera de nationella åtgärderna. Förslaget är begränsat till vad som är nödvändigt och proportionellt för att tillgodose behoven hos brottsbekämpande myndigheter och rättsliga myndigheter i den digitala tidsåldern.

3. RESULTAT AV EFTERHANDSUTVÄRDERINGAR, SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

• Samråd med berörda parter

Under ett och ett halvt år samrådde kommissionen med alla berörda parter för att identifiera problem och lösningar. Detta skedde genom undersökningar, från ett öppet offentligt samråd till riktade undersökningar med relevanta offentliga myndigheter. Expertgruppmöten och bilaterala möten anordnades också för att diskutera de potentiella effekterna av unionslagstiftning. Konferenser om gränsöverskridande tillgång till elektroniska bevis användes också för att samla in synpunkter på initiativet.

På det hela taget ansåg deltagarna i undersökningen att ökad användning av informationstjänster utgör en utmaning för de brottsbekämpande myndigheterna, som ofta är dåligt rustade för att hantera bevis på nätet. Den utdragna processen för inhämtande av bevis erkänns också som ett av de viktigaste hindren. Andra viktiga frågor som offentliga myndigheter lyfte fram är bland annat bristen på tillförlitligt samarbete med tjänsteleverantörer, bristande insyn och rättsosäkerhet i fråga om jurisdiktion för utredningsåtgärder. Direkt gränsöverskridande samarbete mellan brottsbekämpande organ och leverantörer av digitala tjänster ansågs tillföra ett mervärde i brottsutredningar. Tjänsteleverantörer och vissa av det civila samhällets organisationer pekade på behovet att garantera rättssäkerheten vid samarbete med offentliga myndigheter och att undvika lagkonflikter. Vad gäller farhågor om hur en ny EU-lagstiftning kan påverka rättigheter, ansåg de berörda parterna att särskilt skydd bör garanteras som en förutsättning för alla gränsöverskridande instrument.

Inkomna synpunkter från den inledande konsekvensbedömningen visade att berörda parter ansåg att insatser för att komma till rätta med bristerna i det nuvarande systemet för ömsesidig rättslig hjälp skulle göra det effektivare och förbättra rättssäkerheten. Vissa av det civila samhällets organisationer motsatte sig lagstiftning på EU-nivå om direkt samarbete. De föredrog att EU:s åtgärder skulle begränsas till att förbättra förfarandena för ömsesidig rättslig hjälp. Denna idé kommer att utvecklas som en del av de praktiska åtgärder som godkändes av rådet i juni 2016.

Genom en riktad undersökning till offentliga myndigheter i medlemsstaterna framgick också att det inte fanns någon gemensam strategi för att få gränsöverskridande tillgång till elektroniskt bevismaterial, eftersom varje medlemsstat har sin egen nationella praxis. Tjänsteleverantörer reagerar också olika på förfrågningar från utländska brottsbekämpande

myndigheter och svarstiderna varierar beroende på den anmodande medlemsstaten. Detta skapar rättsosäkerhet för alla berörda parter.

I allmänhet visade samrådet med berörda parter att den nuvarande rättsliga ramen är fragmentarisk och komplex. Detta kan medföra förseningar under genomförandefasen och brist på effektiv utredning och lagföring av brott som inbegriper gränsöverskridande tillgång till elektroniska bevis.

- **Konsekvensbedömning**

Nämnden för lagstiftningskontroll avgav ett positivt yttrande om den konsekvensbedömning som ligger till grund för detta förslag²⁰ och lämnade flera förslag till förbättringar²¹. Efter detta yttrande ändrades konsekvensbedömningen för att ytterligare diskutera frågor om grundläggande rättigheter i samband med det gränsöverskridande utbytet av uppgifter, i synnerhet sambandet mellan de olika åtgärder som ingår i det rekommenderade alternativet. Bedömningen ändrades också för att bättre återspegla de berörda parternas och medlemsstaternas synpunkter och hur de har beaktats. Dessutom såg man över den politiska bakgrunden för att inkludera ytterligare hänvisningar till olika aspekter, t.ex. diskussioner i expertgrupper som bidragit till utarbetandet av initiativet. Komplementariteten mellan olika åtgärder (särskilt direktivet om en europeisk utredningsorder, förhandlingar om ett tilläggsprotokoll till Budapestkonventionen och den gemensamma översynen av avtalet om ömsesidig rättslig hjälp mellan EU och USA) har förtydligats i fråga om räckvidd, tidpunkt och omfattning. Grundscenariot har också reviderats för att bättre återspegla den sannolika utveckling som är oberoende av antagandet av de föreslagna åtgärderna. Slutligen har flödesscheman lagts till för att bättre beskriva arbetsflödet för datadelning.

Fyra huvudalternativ övervägdes förutom grundscenariot (alternativ O): Ett antal praktiska åtgärder för att förbättra både förfaranden för rättsligt samarbete och direkt samarbete mellan offentliga myndigheter och tjänsteleverantörer (alternativ A: icke lagstiftande). Ett alternativ som kombinerar de praktiska åtgärderna enligt alternativ A med internationella lösningar på bilateral eller multilateral nivå (alternativ B: lagstiftning). Ett alternativ som kombinerar de tidigare åtgärderna i alternativ B med en europeisk utlämnandeorder och en åtgärd för att förbättra tillgången till databaser som på förfrågan lämnar information om abonnenter, t.ex. Domain Name Whois (alternativ C: lagstiftning). Ett alternativ som kombinerar alla tidigare åtgärder som ingår i alternativ C med lagstiftning om direkt tillgång till uppgifter som lagras på distans (alternativ D: lagstiftning)²².

Om inga åtgärder vidtas (alternativ O) kommer ett ökande antal förfrågningar att förvärra situationen. Alla andra alternativ gör det möjligt att uppnå initiativets mål, men i varierande

²⁰ Arbetsdokument från kommissionens avdelningar – Konsekvensbedömning som åtföljer förslaget till förordning om europeiska utlämnandeorder och bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och förslaget till direktiv om fastställande av harmoniserade regler för utseende av rättsliga företrädare i syfte att samla bevis i straffrättsliga förfaranden, SWD(2018) 118.

²¹ Europeiska kommissionens nämnd för lagstiftningskontroll – Yttrande om konsekvensbedömningen – Förslag till förordning om europeiska utlämnandeorder och bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och förslag till direktiv om fastställande av harmoniserade regler för utseende av rättsliga företrädare för insamling av bevis i straffrättsliga förfaranden, SEC(2018) 199.

²² För närmare information, se Arbetsdokument från kommissionens avdelningar – Konsekvensbedömning som åtföljer förslaget till förordning om europeiska utlämnandeorder och bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och förslaget till direktiv om fastställande av harmoniserade regler för utseende av rättsliga företrädare i syfte att samla bevis i straffrättsliga förfaranden, SWD(2018) 118.

omfattning. Alternativ A skulle förbättra effektiviteten i nuvarande förfaranden, t.ex. genom att förbättra kvaliteten på förfrågningarna, men utrymmet för förbättringar skulle begränsas genom de strukturella bristerna i det nuvarande systemet.

Alternativ B skulle leda till flera förbättringar genom att tillhandahålla internationellt vedertagna lösningar, men resultatet av dessa internationella lösningar skulle i stor utsträckning vara beroende av tredjeländer. Lösningarna är därför osäkra och kommer sannolikt inte att vara lika effektiva och erbjuda lika många garantier som en lösning på unionsnivå.

Alternativ C skulle klart innebära ett mervärde jämfört med de föregående alternativen genom att även föreskriva ett EU-internt instrument för direkt samarbete med tjänsteleverantörer. Detta skulle lösa de flesta av de problem som konstaterats när en tjänsteleverantör innehar de berörda uppgifterna.

Alternativ D är den mest omfattande paketlösningen. Utöver de tidigare åtgärderna rör det sig om en lagstiftningsåtgärd om direkt tillgång i situationer där en tjänsteleverantör inte behöver medverka.

Föreliggande lagstiftningsinitiativ som läggs fram av kommissionen grundar sig på resultaten av konsekvensbedömningen. Denna lagstiftning kommer att kompletteras med de praktiska åtgärder som beskrivs i konsekvensbedömningen och fortsatt arbete för ett tilläggsprotokoll till Budapestkonventionen. På grundval av sitt lagstiftningsförslag kommer kommissionen också att med USA och andra tredjeländer diskutera möjligheten av framtida bilaterala eller multilaterala avtal om gränsöverskridande tillgång till elektroniska bevis, med åtföljande säkerhetsåtgärder. Vad gäller åtgärder för direkt tillgång och åtkomst till databaser, vilket ingår i alternativ D, föreslår kommissionen för närvarande inte någon lagstiftning, men kommer att fundera vidare på den bästa vägen framåt i dessa två frågor.

Initiativet förväntas möjliggöra mer effektiva och ändamålsenliga utredningar och åtal, samtidigt som insynen och ansvarigheten förbättras och respekten för grundläggande rättigheter säkras. Det förväntas också bidra till att skapa förtroende på den digitala inre marknaden genom att förbättra säkerheten och minska känslan av straffrihet för brott som begås med eller via nätverksenheter.

Vad gäller offentliga myndigheter förväntas initiativet medföra genomförandekostnader till en början, vilket på lång sikt skulle uppvägas av besparingar i löpande kostnader. De nationella myndigheterna måste anpassa sig till nya förfaranden och anordna fortbildning. Därefter skulle myndigheterna dock gynnas av rationalisering och centralisering och en tydlig rättslig ram som reglerar förfrågningar om tillgång till uppgifter, eftersom detta sammantaget bör skapa effektivitetsvinster. På samma sätt skulle det rekommenderade alternativet minska trycket på kanalerna för rättsligt samarbete, och de länder som mottar framställningar bör se en minskning av antalet förfrågningar som de är skyldiga att behandla.

Tjänsteleverantörer skulle behöva anpassa sig till den nya rättsliga ramen genom att införa (nya) förfaranden och fortbilda sin personal. Å andra sidan skulle en harmoniserad ram kunna minska bördan för de leverantörer som för närvarande besvarar förfrågningar om icke-innehållsdata och ska bedöma dem enligt medlemsstaternas olika lagar. Rättsäkerhet och standardisering av förfaranden bör också ha en positiv inverkan på små och medelstora företag, eftersom detta bör minska den administrativa bördan och främja konkurrenskraften. På det hela taget förväntas också initiativet medföra besparingar för dem.

- **Grundläggande rättigheter**

Förslaget skulle kunna påverka ett antal grundläggande rättigheter:

rättigheter för den person vars uppgifter hämtas, rätten till skydd av personuppgifter, rätten till respekt för privatlivet och familjelivet, rätten till yttrandefrihet, rätten till försvar, rätt till ett effektivt rättsmedel och till en opartisk domstol,

tjänsteleverantörens rättigheter, näringsfriheten, rättsskipning,

alla medborgares rättigheter, rätt till frihet och säkerhet.

Med beaktande av unionens regelverk i fråga om uppgiftsskydd inkluderas tillräckliga och viktiga skyddsåtgärder i den föreslagna förordningen för att se till att dessa personers rättigheter skyddas.

Eftersom ordena endast får utfärdas i straffrättsliga förfaranden och om det finns jämförbara nationella situationer, är alla straffrättsliga processuella skyddsåtgärder tillämpliga, både under förundersökningen och under själva rättegången. Detta innefattar särskilt rätten till en rättvis rättegång som förankras i artikel 6 i Europakonventionen och i artiklarna 47 och 48 i stadgan om de grundläggande rättigheterna. Det innefattar också den relevanta lagstiftningen på EU-nivå om processuella rättigheter i straffrättsliga förfaranden: Direktiv 2010/64/EU om rätt till tolkning och översättning vid straffrättsliga förfaranden, direktiv 2012/13/EU om rätten till information vid straffrättsliga förfaranden, direktiv 2013/48/EU om rätt till tillgång till försvarare och rätt att kontakta tredje parter och konsulära myndigheter under frihetsberövandet, direktiv (EU) 2016/343 om förstärkning av vissa aspekter av oskuldspresumtionen och av rätten att närvara vid rättegången, direktiv (EU) 2016/800 om rättssäkerhetsgarantier för barn och direktiv (EU) 2016/1919 om rättshjälp för misstänkta och tilltalade i straffrättsliga förfaranden och för eftersökta personer i förfaranden i samband med en europeisk arresteringsorder.

Närmare bestämt säkerställer en föregående prövning av ordern genom en rättslig myndighet att lagenligheten av denna åtgärd och dess nödvändighet och proportionalitet i det aktuella fallet har kontrollerats. Detta säkerställer också att ordern inte i onödan inkräktar på grundläggande rättigheter, inbegripet rättsliga principer såsom rätten till förtrolig kommunikation mellan advokat och klient. Den utfärdande myndigheten är skyldig att i det enskilda fallet säkerställa att åtgärden är nödvändig och proportionell, särskilt med tanke på allvaret i det brott som utreds. Förslaget innehåller även trösklar för transaktionsdata och innehållsdata, för att säkerställa att den europeiska utlämnandeordern endast tillämpas för mer allvarliga former av brott i samband med sådana data.

Rätten till ett effektivt rättsmedel för personer vars uppgifter begärs tas också upp uttryckligen. Immunitet och privilegier för vissa yrken, t.ex. advokat, beviljas samtidigt som grundläggande nationella säkerhets- eller försvarsintressen i mottagarens stat också måste beaktas vid rättegång i den utfärdande staten. Översyn genom en rättslig myndighet fungerar här som en ytterligare skyddsåtgärd.

Eftersom ordern är en bindande åtgärd påverkar den också tjänsteleverantörernas rättigheter, särskilt näringsfriheten. Förslaget innehåller en rätt för tjänsteleverantören att väcka vissa anspråk i den utfärdande medlemsstaten, t.ex. om ordern inte har utfärdats eller godkänts av en rättslig myndighet. Om ordern översänds till den verkställande staten för verkställighet, får den verkställande myndigheten besluta att inte erkänna eller verkställa beslutet, om vid mottagandet någon av de begränsade grunderna för invändning är uppenbart tillämplig, dock först efter samråd med den utfärdande myndigheten. Om förfarandet för verkställighet inleds

kan dessutom adressaten själv motsätta sig ordern inför den verkställande myndigheten på grundval av sådana begränsade grunder. Detta innebär till exempel fall där det är uppenbart att ordern inte har utfärdats eller godkänts av en behörig myndighet, eller där efterlevnad uppenbart skulle strida mot stadgan eller utgöra uppenbart missbruk. Detta utesluter dock inte adressatens rätt till ett effektivt rättsmedel mot ett beslut att ålägga en påföljd.

Ett potentiellt problem i samband med EU:s åtgärder på detta område är att det kan leda till att tredjeländer inför ömsesidiga skyldigheter för EU:s tjänsteleverantörer som inte är förenliga med de grundläggande rättigheterna, inbegripet den höga skyddsnivå för personuppgifter som garanteras av EU:s regelverk. Förslaget hanterar denna situation på två sätt: För det första, genom en åtgärd som innehåller ett omfattande skydd och uttryckliga hänvisningar till de villkor och skyddsåtgärder som redan finns i EU:s regelverk, och på så sätt fungerar som en modell för utländsk lagstiftning. För det andra, genom att införa en särskild klausul om motstridiga skyldigheter som gör det möjligt för tjänsteleverantörer att identifiera och ta upp motstridiga skyldigheter, vilket utlöser en domstolsprövning. Denna klausul är utformad för att säkerställa respekt både för både allmänna blockerande stadgar, t.ex. U.S. Electronic Communications Privacy Act (ECPA) som förbjuder delgivning av innehållsdata inom dess geografiska räckvidd med begränsade undantag, liksom för lagar som inte generellt förbjuder delgivning, men kan göra det i enskilda fall. I de fall som rör ECPA kan för närvarande åtkomst för innehållsdata förhindras i vissa situationer, och ömsesidig rättslig hjälp bör därför förbli det viktigaste verktyget för att få tillgång till sådana data. I och med de ändringar som antagandet av U.S. CLOUD Act²³ innebär kan den blockerande stadgan provisoriskt upphävas, om EU uppnår ett avtal med Förenta staterna. Ytterligare internationella avtal med andra viktiga partner kan ytterligare minska omfattningen av lagkonflikter.

Mot bakgrund av ovanstående är åtgärderna i detta förslag förenliga med de grundläggande rättigheterna.

4. BUDGETKONSEKVENSER

Förslaget till förordning påverkar inte unionens budget.

5. ÖVRIGA INSLAG

- **Genomförandeplaner samt åtgärder för övervakning, utvärdering och rapportering**

Förordningen är direkt tillämplig inom EU. Den kommer att tillämpas direkt av rättstillämpare, utan att interna rättssystem behöver ändras.

Förordningen kommer att utvärderas och kommissionen ska lägga fram en rapport för Europaparlamentet och rådet senast 5 år efter det att den har trätt i kraft. På grundval av resultatet i rapporten, särskilt om huruvida förordningen lämnar eventuella luckor som är praktiskt relevanta, och med hänsyn till den tekniska utvecklingen, kommer kommissionen att bedöma behovet av att utvidga tillämpningsområdet för förordningen. Vid behov kommer kommissionen att lägga fram förslag till ändring av denna förordning. Medlemsstaterna ska förse kommissionen med de uppgifter som är nödvändiga för att utarbeta denna rapport.

²³ Den 23 mars 2018 antogs i Förenta staterna Clarifying Lawful Overseas (CLOUD) Act. CLOUD Act finns [här](#).

Medlemsstaterna ska samla in de uppgifter som krävs för den årliga uppföljningen av förordningen.

Kommissionen kommer vid behov att utfärda riktlinjer för att tjänsteleverantörer ska kunna fullgöra sina skyldigheter enligt förordningen.

- **Ingående redogörelse för de specifika bestämmelserna i förslaget**

	FÖRESKRIFTER	
	Artikel	Skäl
I. Syfte, definitioner och tillämpningsområde	1. Syfte	1–15
	2. Definitioner	16–23
	3. Tillämpningsområde	24–27
II. Europeisk utlämnandeorder, europeisk bevarandeorder och intyg, rättslig företrädare	4. Utfärdande myndighet	30
	5. Villkor för utfärdande av en europeisk utlämnandeorder	28–29, 31–35
	6. Villkor för utfärdande av en europeisk bevarandeorder	36
	7. Mottagare av en europeisk utlämnandeorder och en europeisk bevarandeorder	37
	8. Intyg om en europeisk utlämnandeorder och europeisk bevarandeorder	38–39
	9. Genomförande av en EPOC	40–41
	10. Genomförande av en EPOC-PR	42
	11. Sekretess och användarinformation	43
	12. Ersättning för kostnader	Saknas
III. Påföljder och verkställighet	13. Sanktioner	Saknas
	14. Verkställighetsförfarande	44–45, 55
IV. Rättsmedel	15. och 16. Prövning i händelse av motstridiga krav från ett tredjeland	47–53
	17. Effektiva rättsmedel	54

	18. Säkerställa immunitet och privilegier enligt lagen i den verkställande staten	35
V. Slutbestämmelser	19. Övervakning och rapportering	58
	20. Ändringar av intyg och formulär	59–60
	21. Utövande av delegeringen	60
	22. Anmälan	Saknas
	23. Förhållande till europeiska utredningsorder	61
	24. Utvärdering	62
	25. Ikraftträdande	Saknas

Kapitel 1: Syfte, definitioner och tillämpningsområde

Artikel 1: Syfte

I denna artikel fastställs förslagets räckvidd och syfte, vilket är att fastställa regler enligt vilka en behörig rättslig myndighet i Europeiska unionen får beordra en tjänsteleverantör som erbjuder sina tjänster i unionen att lämna ut eller bevara elektroniska bevis genom en europeisk utlämnandeorder eller bevarandeorder. Dessa instrument får endast användas i gränsöverskridande situationer, det vill säga i situationer där tjänsteleverantören är etablerad eller företrädd i en annan medlemsstat.

Denna förordning ska ge ytterligare verktyg till de undersökande myndigheterna för att erhålla elektroniska bevis, utan att begränsa de befogenheter som redan anges i nationell lagstiftning för att ålägga tjänsteleverantörer som är etablerade eller företrädda på deras territorium att lämna ut uppgifter. Om tjänsteleverantören är etablerad eller företrädd i samma medlemsstat ska myndigheterna i den medlemsstaten därför använda nationella myndigheter för att tvinga tjänsteleverantören.

De uppgifter som begärs genom en europeisk utlämnandeorder bör tillhandahållas myndigheterna direkt, utan inblandning av myndigheterna i den medlemsstat där tjänsteleverantören är etablerad eller företrädd. Förordningen låter också i minskande utsträckning platsen för datalagring vara en avgörande faktor, eftersom datalagring normalt inte leder till kontroll från den stat på vars territorium uppgifter lagras. Sådan lagring beslutas i flertalet fall av leverantören ensam, på grundval av affärsmässiga överväganden²⁴.

Förordningen är dessutom även tillämplig om tjänsteleverantörerna inte är etablerade eller företrädda i unionen, men erbjuder tjänster i unionen. Detta återspeglas i artikel 3.1.

²⁴ Konsekvensbedömningen omfattar ytterligare förklaringar.

Om förslaget avser en tjänsteleverantör som är etablerad eller företrädd i en medlemsstat genom en utsedd rättslig företrädare, utgör utseendet av en rättslig företrädare inte en etablering för tjänsteleverantören i den mening som avses i denna förordning.

I artikel 1.2 erinras om att denna förordning inte får ändra skyldigheten att respektera de grundläggande rättigheter och rättsliga principer som anges i artikel 6 i EU-fördraget.

Artikel 2: Definitioner

I denna artikel anges definitioner som gäller genomgående för instrumentet.

Följande typer av tjänsteleverantörer omfattas av förordningens tillämpningsområde: leverantörer av elektroniska kommunikationstjänster, leverantörer av informationssamhällstjänster för vilka datalagring är en grundläggande komponent i den tjänst som tillhandahålls användaren, inbegripet sociala nätverk i den utsträckning dessa inte räknas som elektroniska kommunikationstjänster, internetbaserade marknadsplatser som underlättar transaktioner mellan användarna (till exempel konsumenter eller företag) och andra värdtjänsteleverantörer och leverantörer av domännamn och numreringstjänster.

Förordningens tillämpningsområde omfattar leverantörer av elektroniska kommunikationstjänster enligt definitionen [i direktivet om inrättande av en europeisk kodex för elektronisk kommunikation]. Traditionella telekommunikationstjänster, konsumenter och företag förlitar sig i ökande utsträckning på nya internetbaserade tjänster för interpersonell kommunikation, såsom IP-telefoni, snabbmeddelandetjänster och e-posttjänster i stället för traditionella kommunikationstjänster. Dessa tjänster, tillsammans med sociala nätverk, exempelvis Twitter och Facebook, som låter användare dela innehåll, bör därför omfattas av detta förslag.

I många fall lagras uppgifter inte längre på användarens enhet, utan görs tillgänglig på en molnbaserad infrastruktur som i princip kan nå överallt. Tjänsteleverantörer behöver inte vara etablerade eller ha servrar i varje jurisdiktion, utan snarare använda en centraliserad förvaltning och decentraliserade system för att lagra uppgifter och tillhandahålla tjänster. Detta görs för att optimera lastbalanseringen och snabbare möta användarnas databehov. Nätverk för innehållsleverans utvecklas vanligen för att påskynda innehållsleverans genom att kopiera innehåll i flera servrar som är fördelade runtom i världen. Detta gör att företag kan hämta innehåll från den server som är närmast användaren, eller som leda kommunikationen genom ett mindre trafikerat nätverk. För att ta hänsyn till denna utveckling omfattar definitionen moln- och andra värdtjänster som tillhandahåller en mångfald av datorresurser, såsom nätverk, servrar eller annan infrastruktur, lagring, appar och tjänster som gör det möjligt att lagra data för olika syften. Instrumentet tillämpas också på internetbaserade marknadsplatser som låter konsumenter och/eller företag ingå transaktioner eller tjänstekontrakt via försäljning online. Sådana transaktioner genomförs antingen på den internetbaserade marknadsplatsens hemsida eller på en handlares hemsida som använder datortjänster genom en internetbaserad marknadsplats. Det är därmed denna marknadsplats som innehar elektroniska bevis som kan behövas under en brottsutredning.

Tjänster för vilka datalagring inte är en grundläggande komponent omfattas inte av detta förslag. Även om flertalet tjänster som tillhandahålls av leverantörer omfattar någon form av datalagring, särskilt när de levereras via internet på distans, kan tjänster urskiljas för vilka datalagring inte är ett utmärkande drag och därför av underordnad natur, inbegripet rättsliga, arkitekt-, ingenjör- och bokföringstjänster som tillhandahålls via internet på distans.

Data som innehas av leverantörer av internetinfrastrukturtjänster, såsom domännamnsregistratorer och domännamnsregister och leverantörer av proxytjänster, eller regionala internetregister för IP-adresser, kan vara relevanta för brottsutredningar eftersom de kan ge indikationer för att identifiera en person eller en enhet som är inblandad i brottslig verksamhet.

De datakategorier som behöriga myndigheter kan erhålla genom en europeisk utlämnandeorder omfattar abonnentuppgifter, åtkomstuppgifter, transaktionsuppgifter (de tre kategorier som vanligen gemensamt kallas *icke-innehållsdata*) och lagrade innehållsdata. Denna distinktion, med undantag av åtkomstuppgifter, existerar i flertalet medlemsstaters rättsordningar och även inom rättsliga ramar utanför EU.

Alla kategorier innehåller personuppgifter och omfattas därmed av skyddsåtgärderna under EU:s regelverk för dataskydd. Graden av inverkan på de grundläggande rättigheterna varierar, särskilt mellan abonnentuppgifter å ena sidan, och transaktions- och innehållsdata å andra sidan. Det är viktigt att alla dessa kategorier omfattas av instrumentet: Abonnent- och åtkomstuppgifter är ofta utgångspunkten för att finna ledtrådar i en undersökning av en misstänkts identitet. Samtidigt kan transaktions- och innehållsdata vara mest relevanta som bevismaterial. Beroende på de olika nivåerna av inverkan på grundläggande rättigheter är det motiverat att koppla olika villkor till abonnentuppgifter å ena sidan och transaktions- och innehållsdata å andra sidan, vilket görs i flera bestämmelser i förordningen.

Det är lämpligt att särskilja åtkomstuppgifter som en särskild datakategori som används i denna förordning. Åtkomstuppgifter som de definieras här efterfrågas i samma syfte som abonnentuppgifter, dvs. att identifiera användaren, och nivån på inverkan på grundläggande rättigheter är snarlik. De bör därför vara föremål för samma villkor som abonnentuppgifter. Därför inför detta förslag en ny datakategori som ska behandlas på samma sätt som abonnentuppgifter om samma mål eftersträvas.

I artikel 2 anges de medlemsstater och myndigheter som skulle kunna involveras i förfarandet. En definition av den utfärdande myndigheten anges i artikel 4.

Nödsituationer är exceptionella situationer som regelbundet kräver snabb respons från tjänsteleverantörer och för vilka särskilda villkor ska tillämpas. Dessa definieras därför separat i denna artikel.

Artikel 3: Tillämpningsområde

Denna artikel fastställer förslagets tillämpningsområde. Förordningen är tillämplig på alla tjänsteleverantörer som erbjuder tjänster i unionen, inbegripet tjänsteleverantörer som inte är etablerade i unionen. Aktivt erbjudande av tjänster i unionen, med alla tillhörande fördelar, motiverar även att dessa tjänsteleverantörer är föremål för förordningen och skapar lika villkor för deltagare på samma marknader. Att inte låta dessa tjänsteleverantörer omfattas skulle skapa ett kryphål och underlätta för brottslingar att kringgå förordningens tillämpningsområde.

För att fastställa huruvida tjänster erbjuds måste myndigheterna bedöma om tjänsteleverantören gör det möjligt för juridiska eller fysiska personer i en eller flera medlemsstater att använda dess tjänster. Endast tjänstens tillgänglighet (som även kan härröra från tjänsteleverantörens eller en mellanhands webbplats tillgänglighet, eller genom en e-postadress och annan kontaktinformation) bör dock inte vara ett tillräckligt villkor för denna förordnings tillämplighet. Det krävs därför en väsentlig anknytning till dessa medlemsstater

för att fastställa en tillräcklig förbindelse mellan leverantören och det territorium där den erbjuder sina tjänster. En sådan väsentlig anknytning existerar om tjänsteleverantören är etablerad i en eller fler medlemsstater. I avsaknad av en etablering i unionen bör kriteriet för en väsentlig anknytning till unionen bedömas på grundval av ett betydande antal användare i en eller flera medlemsstater, eller verksamhet som är inriktad på en eller flera medlemsstater. Huruvida verksamheten är inriktad på en eller flera medlemsstater kan fastställas på grundval av alla relevanta omständigheter, inbegripet faktorer såsom ett språk eller en valuta som är allmänt förekommande i en medlemsstat. Verksamhet som inriktas på en medlemsstat kan också härledas från tillgängligheten av en app i en relevant nationell appbutik som erbjuder lokal annonsering eller annonser på det språk som används i medlemsstaten, från användning av information från personer i medlemsstaterna i deras verksamhet, eller från hantering av kundrelationer, till exempel genom kundtjänst på det språk som allmänt används i en medlemsstat. En väsentlig anknytning kan också antas existera om en tjänsteleverantör inriktar sin verksamhet på en eller flera av de medlemsstater som anges i artikel 17.1 c i förordning 1215/2012 om domstols behörighet och om erkännande och verkställighet av domar på privaträttens område.

En europeisk utlämnandeorder och en europeisk bevarandeorder är utredningsåtgärder som kan vidtas endast i brottsutredningar eller straffrättsliga förfaranden i konkreta brottmål. Anknytningen till en konkret utredning särskiljer dem från lagstadgade förebyggande åtgärder eller lagringsskyldigheten och som säkerställer tillämpning av de processuella rättigheter som gäller i straffrättsliga förfaranden. Behörighet att inleda utredning av ett specifikt brott är därför en förutsättning för tillämpning av förordningen.

Ett ytterligare krav är att de uppgifter som efterfrågas måste vara relaterade till tjänster som tjänsteleverantören erbjuder i unionen.

Kapitel 2: Europeisk utlämnandeorder, europeisk bevarandeorder och intyg

Artikel 4: Utfärdande myndighet

Vid utfärdande av en europeisk utlämnandeorder eller en bevarandeorder måste den rättsliga myndigheten alltid vara involverad i egenskap av antingen utfärdande eller godkännande myndighet. En domare eller en domstol krävs för att ordena ska leda till utlämnande av transaktions- eller innehållsdata. När det gäller abonnent- eller åtkomstdata kan detta även åstadkommas av åklagare.

Artikel 5: Villkor för utfärdande av en europeisk utlämnandeorder

I artikel 5 anges villkoren för utfärdande av en europeisk utlämnandeorder. Dessa ska bedömas av den utfärdande rättsliga myndigheten.

En europeisk utlämnandeorder får endast utfärdas om den är nödvändig för och proportionell till det enskilda fallet. Den får dessutom endast utfärdas om en liknande bestämmelse skulle finnas för samma brott i en jämförbar inhemsk situation i den utfärdande staten.

Utlämnandeorder för abonnentuppgifter och åtkomstuppgifter kan utfärdas för alla brott. Transaktions- och innehållsdata bör vara föremål för strängare krav för att återspegla dessa datas känsligare natur och motsvarande högre invasiva karaktär hos order gällande dessa data, jämfört med abonnent- och åtkomstdata. Utlämnandeorder kan därför endast utfärdas för brott som är belagda med ett maximalt frihetsstraff på minst 3 år eller mer. Fastställandet av en tröskel på grundval av ett maximalt frihetsstraff möjliggör en mer proportionell metod,

tillsammans med att antal andra förhands- och efterhandsvillkor och skyddsåtgärder för att säkerställa proportionalitet och de berörda personernas rättigheter.

Samtidigt bör tröskeln inte underminera instrumentets effektivitet och användning av rättstillämpare. Olika maximistraff tillämpas av medlemsstaterna för domar inom deras nationella system. Nationella straffskalor varierar och är inte harmoniserade. Detta gäller för brott och de påföljder som tillämpas på dem. Nationell straffprocesslagstiftning varierar också vad gäller trösklar för att erhålla transaktions- eller innehållsdata: Vissa länder anger ingen särskild tröskel, medan andra använder en förteckning över brott. En tröskel på tre år begränsar instrumentets tillämpningsområde till allvarligare brott, utan att överdrivet begränsa dess användningsmöjligheter för rättstillämpare. Denna tröskel utesluter ett stort antal brott från tillämpningsområdet, beroende på medlemsstatens strafflagstiftning (till exempel i vissa medlemsstater deltagande i organiserad brottslighet och människorov, men också brott som snatteri, bedrägeri och överfall för vilka användning av en gränsoverskridande utlämnandeorder gällande känsligare data kan anses som oproportionerlig). Å andra sidan omfattar en tröskel på tre år brott som kräver ett effektivare tillvägagångssätt, till exempel medlemskap i en brottsorganisation, finansiering av terroristgrupper, stöd eller publicitet för en brottsorganisation, förberedelse för utförande av terroristhandlingar, vissa brott med terroristuppsåt och förberedelser av brott med terroristuppsåt, eller förberedelser för tagande av gisslan, vilka annars skulle uteslutas om en högre tröskel var tillämplig, beroende på den enskilda medlemsstaten. Denna tröskel har valts för att säkerställa balans i alla medlemsstater mellan effektivitet i brottsutredningar och skydd av rättigheter och proportionalitet. En tröskel har också fördelen att lätt kunna tillämpas i praktiken.

Order om utlämnande av transaktions- och innehållsdata kan dessutom utfärdas för specifika harmoniserade brott som förtecknas i bestämmelsen för vilka bevis i de flesta fall är tillgängliga endast i elektronisk form. Detta motiverar att förordningen tillämpas även i fall där det maximala frihetsstraffet är lägre än i tröskeln ovan. Annars skulle dessa brott inte kunna utredas ordentligt, vilket skulle kunna leda till strafffrihet. Brotten fastställs uttryckligen i: i) rådets rambeslut 2001/413/RIF om bekämpande av bedrägeri och förfalskning som rör andra betalningsmedel än kontanter, ii) direktiv 2011/93/EU om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi och om ersättande av rådets rambeslut 2004/68/RIF och iii) direktiv 2013/40/EU om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF. Order får även utfärdas för brott som förtecknas i direktiv 2017/541/EU om bekämpande av terrorism och om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF. Vissa av dessa brott har minimi/maximitrösklar på minst 1 år, andra på 2 år, men ingen ligger lägre än ett maximistraff på 1 år.

I artikeln anges också obligatorisk information som måste ingå i den europeiska utlämnandeordern för att göra det möjligt för tjänsteleverantören att identifiera och ta fram data som efterfrågas. En motivering med skäl för denna åtgärds nödvändighet och proportionalitet ingår också i den europeiska utlämnandeordern.

Den europeiska utlämnandeordern genomförs genom utfärdande av ett intyg om en europeisk utlämnandeorder (nedan kallat *EPOC*) (se artikel 8) som översätts och översänds till tjänsteleverantören. *EPOC* innehåller samma obligatoriska information som ordern, med undantag av skälen för åtgärdens nödvändighet och proportionalitet eller närmare information om ärendet.

I situationer där de efterfrågade uppgifterna lagras eller behandlas som en del i en infrastruktur som tjänsteleverantören tillhandahåller ett företag, t.ex. när det gäller värdtjänster eller mjukvarutjänster, bör företaget vara den primära adressaten för en begäran från de utredande myndigheterna. Detta kan kräva ett förfarande genom en europeisk utredningsorder eller ömsesidig rättslig hjälp, om företaget inte är en tjänsteleverantör som omfattas av denna förordnings tillämpningsområde. Tjänsteleverantören kan endast vara föremål för en europeisk utlämnandeorder om det inte är lämpligt att rikta begäran till företaget, särskilt om detta skulle riskera att äventyra utredningen, till exempel på grund av att företaget självt är föremål för en utredning.

Innan en europeisk utlämnandeorder utfärdas måste den utfärdande myndigheten även beakta potentiell immunitet och privilegier enligt lagstiftningen i tjänsteleverantörens medlemsstat, eller inverkan på den medlemsstatens grundläggande intressen, såsom nationell säkerhet och försvar. Syftet med denna bestämmelse är att säkerställa att den immunitet och de privilegier som skyddar tjänsteleverantörens data i medlemsstaten beaktas i den utfärdande staten, särskilt när dessa ger stärkare skydd än lagstiftningen i den utfärdande staten.

Artikel 6: Villkor för utfärdande av en europeisk bevarandeorder

En europeisk bevarandeorder är föremål för liknande villkor som den europeiska utlämnandeordern. Den kan utfärdas för varje brott som överensstämmer med de villkor som anges i artikel 6. Dess syfte är att förhindra avlägsnande, radering eller ändring av relevanta data i situationer där det kan ta mer tid att erhålla utlämnande av dessa data, till exempel därför att kanaler för rättsligt samarbete kommer att användas. Eftersom till exempel den europeiska utredningsordern i allmänhet kan utfärdas för samtliga brott utan hänsyn till några trösklar, ska inte heller en europeisk bevarandeorder vara begränsad. Annars skulle detta instrument inte vara ändamålsenligt. För att möjliggöra för utredande myndigheter att agera snabbt och eftersom den relevanta begäran om utlämnande av data är den påföljande begäran där alla villkor kommer att granskas igen, får en europeisk bevarandeorder även utfärdas och godkännas av åklagare.

Artikel 7: Mottagare av en europeisk utlämnandeorder och en europeisk bevarandeorder

En europeisk utlämnandeorder och en europeisk bevarandeorder bör rikta sig till en rättslig företrädare som utses av tjänsteleverantören för att insamla bevis i straffrättsliga förfaranden i enlighet med direktivet om harmoniserade regler för utseendet av rättsliga företrädare för insamling av bevis i straffrättsliga förfaranden. Översändandet kommer att ske i form av ett intyg om en europeisk utlämnandeorder (EPOC) eller ett intyg om en europeisk bevarandeorder (EPOC-PR) som avses i artikel 8. Denna rättsliga företrädare ska ansvara för deras mottagande och fullständiga utförande i rätt tid. Detta ger tjänsteleverantörer möjlighet att själva välja hur de organiserar utlämnandet av de data som begärs av medlemsstaternas myndigheter.

Om ingen rättslig företrädare har utsetts får order riktas till ett av tjänsteleverantörens fasta driftställen i unionen. Detta reservalternativ syftar till att säkerställa systemets ändamålsenlighet om tjänsteleverantören inte (ännu) har utsett en företrädare, till exempel om ingen skyldighet föreligger att utse en rättslig företrädare i enlighet med direktivet, därför att tjänsteleverantörer är etablerade och verksamma endast i en medlemsstat, eller om skyldigheten att utse en rättslig företrädare ännu inte trätt i kraft före direktivets frist om införlivande.

Om den rättsliga företrädaren inte har uppfyllt sina skyldigheter kan den utfärdande myndigheten rikta sig till ett av tjänsteleverantörens driftställen i unionen i två fall: I nödfall enligt artikel 9.2 och i de fall där den rättsliga företrädaren inte uppfyller sina skyldigheter enligt artiklarna 9 och 10, och om den utfärdande myndigheten anser att det finns en klar risk att uppgifter går förlorade.

Artikel 8: Intyg om en europeisk utlämnandeorder och en europeisk bevarandeorder

Syftet med EPOC och EPOC-PR är att översända ordena till den adressat som anges i artikel 7. Mallar för båda intygen återfinns i bilagorna I och II till denna förordning. Dessa måste översättas till ett officiellt språk i den medlemsstat där adressaten är etablerad. Tjänsteleverantören får ange att order även kommer att godtas på andra officiella språk i unionen. Intygens syfte är att tillhandahålla all nödvändig information som ska översändas till adressaten i ett standardformat för att minimera felkällor, och möjliggöra att enkelt identifiera data och undvika fritext så långt möjligt och därigenom minska översättningskostnaderna. Hela motiveringen och skälen för nödvändighet och proportionalitet eller närmare information om ärendet ska inte inkluderas i intyget, för att inte äventyra utredningen. Den behövs därför endast som en del av ordern för att i ett senare skede låta den tilltalade invända mot den under det straffrättsliga förfarandet.

Vissa tjänsteleverantörer har redan inrättat plattformar för brottsbekämpande myndigheters begäranden. Förordningen ska inte hindra användning av dessa plattformar, eftersom de erbjuder många fördelar, inbegripet möjligheten till enkel autentisering och säker dataöverföring. Dessa plattformar måste dock tillåta inlämning av EPOC och EPOC-PR i det format som anges i bilagorna I och II, utan krav på ytterligare data som gäller för ordern.

Plattformar som inrättas av medlemsstater eller unionsorgan får också tillhandahålla säkra överföringssätt och underlätta autentisering av order och insamling av statistik. Man bör överväga en möjlig expanderings av plattformarna eCodex och Sirius till att omfatta en säker förbindelse till tjänsteleverantörer i syfte att överföra EPOC och EPOC-PR och, i tillämpliga fall, svar från tjänsteleverantörerna.

Artikel 9: Genomförande av en EPOC

I artikel 9 anges adressaternas skyldighet att besvara EPOC inom obligatoriska frister. Den normala fristen är 10 dagar, även om myndigheter får fastställa en kortare frist där detta är motiverat. I nödfall, vilket definieras som en situation med omedelbart hot mot en persons liv eller fysiska integritet, eller mot en kritisk infrastruktur, är fristen 6 timmar.

Bestämmelsen säkerställer också möjligheten till dialog mellan adressaten och den utfärdande myndigheten. Om EPOC är ofullständig, uppenbart felaktig eller saknar tillräcklig information för att tjänsteleverantören ska kunna utföra den, ska adressaten kontakta den utfärdande myndigheten och begära klagorande, med hjälp av formuläret i bilaga III. Den ska också informera den utfärdande myndigheten i de fall där den inte kan tillhandahålla data på grund av force majeure eller faktisk omöjlighet. Detta är fallet till exempel om den person vars data efterfrågas varken var kund för tjänsten i fråga eller – till exempel enligt andra bestämmelser om datasekretess – om uppgifterna lagenligt har raderats av tjänsteleverantören innan den eller dess rättsliga företrädare mottog ordern. Den utfärdande myndigheten måste vara medveten om dessa omständigheter för att reagera snabbt, eventuellt för att samla in elektroniska bevis från en annan tjänsteleverantör och hindra den utfärdande myndigheten från att inleda ett verkställighetsförfarande om detta inte är meningsfullt.

Om adressaten inte tillhandahåller någon information, eller inte tillhandahåller information på ett uttömmande sätt eller i rätt tid, av andra skäl än dem som nämns ovan, ska den underrätta den utfärdande myndigheten om skälen till detta i formuläret i bilaga III. Adressater kan därför ta upp alla frågor som rör verkställigheten av EPOC med den utfärdande myndigheten. Detta gör det möjligt för den utfärdande myndigheten att korrigera eller på nytt överväga EPOC på ett tidigt stadium, före verkställighetsfasen.

Om uppgifter inte omedelbart läggs fram, särskilt om en dialog inleds mellan adressaten och den utfärdande myndigheten, vilket innebär att fristerna i artikel 9.1 inte kommer att hållas, är tjänsteleverantören skyldig att bevara uppgifterna för att undvika att förlora dem, vid mottagandet av EPOC, förutsatt att uppgifterna kan identifieras. Bevarandet kan gälla för den förtydligade EPOC eller efterföljande ömsesidig rättslig hjälp eller en europeisk utredningsorder som ska översändas i stället för den ursprungliga EPOC.

Artikel 10: Verkställighet av en EPOC-PR

Verkställighet av en EPOC-PR kräver bevarande av de uppgifter som är tillgängliga vid tiden för mottagandet av ordern. Tjänsteleverantörer bör bevara uppgifterna så länge som krävs för att lämna ut uppgifterna på begäran, förutsatt att den utfärdande myndigheten inom 60 dagar efter att ha utfärdat ordern bekräftar att den har inlett den efterföljande begäran om utlämnande. Detta kräver att åtminstone vissa formella åtgärder har vidtagits, till exempel översändande av en begäran om ömsesidig rättslig hjälp för översättning.

Å andra sidan bör begäranden om bevarande endast göras eller upprätthållas så länge som är nödvändigt för att möjliggöra en efterföljande begäran om utlämnande av dessa uppgifter. För att undvika onödigt eller överdrivet långvarigt bevarande ska den myndighet som utfärdade den europeiska bevarandeordern underrätta adressaten så snart ett beslut fattats om att avstå utfärdande eller att återkalla en utlämnandeorder eller en begäran om rättsligt samarbete.

Bestämmelsen säkerställer också möjligheten till dialog mellan adressaten och den utfärdande myndigheten, i likhet med bestämmelserna i artikel 9. Om EPOC-PR är ofullständig, uppenbart felaktig eller saknar tillräcklig information för att tjänsteleverantören ska kunna verkställa den, ska adressaten kontakta den utfärdande myndigheten och begära klargörande, med hjälp av formuläret i bilaga III. Den ska också informera den utfärdande myndigheten i de fall där den inte kan tillhandahålla data på grund av omständigheter som betraktas som *force majeure* eller faktisk omöjlighet, eller av andra skäl.

Artikel 11: Sekretess och användarinformation

Sekretessen i pågående undersökning, inbegripet det faktum att en order har utfärdats för att erhålla relevanta data, måste skyddas. Denna artikel är inspirerad av artikel 10 i direktivet om en europeisk utredningsorder. Det föreskriver adressatens, eller i annat fall tjänsteleverantörens, skyldighet att bevara sekretessen för EPOC eller EPOC-PR, särskilt genom att avstå från att informera den person vars data efterfrågas där den utfärdande myndigheten begär det, i syfte att skydda utredningen av brott, i enlighet med artikel 23 i den allmänna dataskyddsförordningen.

Det är å andra sidan viktigt, inbegripet för användningen av rättsmedel, att den person vars data efterfrågas är informerad. Om detta inte görs av tjänsteleverantören på begäran av den utfärdande myndigheten, ska den utfärdande myndigheten underrätta personen i enlighet med artikel 13 i dataskyddsdirektivet för polis och straffrättsliga myndigheter när ingen risk längre föreligger att äventyra utredningen, samt bifoga information om tillgängliga rättsmedel.

Eftersom inverkan på rättigheter är mindre föreskrivs inte sådan information när det gäller en europeisk bevarandeorder, utan endast när det gäller europeiska utlämnandeorder.

Artikel 12: Ersättning för kostnader

Om så föreskrivs i den utfärdande statens lagstiftning för inhemska order i liknande inhemska fall, får tjänsteleverantörer även begära ersättning för kostnader från den utfärdande staten i enlighet med den utfärdande statens nationella lagstiftning. Detta säkerställer lika behandling av tjänsteleverantörer som berörs av en inhemsk order och dem som berörs av en EPOC av samma medlemsstat, om den medlemsstaten har valt att ersätta vissa tjänsteleverantörer. Å andra sidan harmoniserar den föreslagna förordningen inte ersättning av kostnader, eftersom medlemsstaterna har gjort olika val i det avseendet.

Kostnadsersättning kan begäras antingen direkt av tjänsteleverantören eller genom dess rättsliga företrädare. Kostnaderna ersätts endast en gång.

Kapitel 3: Påföljder och verkställighet

Artikel 13: Påföljder

Medlemsstaterna bör säkerställa att det finns effektiva, proportionella och avskräckande böter att tillgå när tjänsteleverantörer inte uppfyller sina skyldigheter enligt artikel 9, 10 eller 11. Detta bör inte påverka tillämpningen av nationell lagstiftning som föreskriver straffrättsliga påföljder i sådana situationer.

Artikel 14: Verkställighetsförfarande

I artikel 14 föreskrivs ett förfarande för att verkställa order i händelse av bristande efterlevnad, med hjälp av den medlemsstat där mottagaren av det översända intyget befinner sig. Beroende på den ursprungliga mottagaren är detta antingen tjänsteleverantörens eller det rättsliga ombudets medlemsstat. Den utfärdande myndigheten överför den fullständiga ordern, inklusive resonemanget kring nödvändighet och proportionalitet, tillsammans med intyget, till den behöriga myndigheten i den verkställande staten, som ska verkställa den i enlighet med sin nationella lagstiftning; vid behov med hjälp av de påföljder som nämns i artikel 13. Om ordern översänds till den verkställande staten för verkställighet, får den verkställande myndigheten besluta att inte erkänna och verkställa ordern, om den vid mottagandet anser att något av de begränsade skälen för invändning är tillämpligt, och efter samråd med den utfärdande myndigheten. Om verkställighetsförfarandet inleds kan dessutom mottagaren själv motsätta sig ordern inför den verkställande myndigheten. Mottagaren kan göra detta på grundval av något av dessa skäl, förutom immunitet och privilegier, men däremot i fall där det är uppenbart att ordern inte har utfärdats eller godkänts av en behörig myndighet, att efterlevnad på ett uppenbart sätt skulle strida mot Europeiska unionens stadga om de grundläggande rättigheterna eller att ordern är tydligt oskäligen. Till exempel skulle en order om utlämnande av innehållsdata avseende en odefinierad grupp människor i ett geografiskt område eller utan koppling till konkreta straffrättsliga förfaranden på ett uppenbart sätt strida mot de villkor som fastställs för utfärdande av en europeisk utlämnandeorder i denna förordning, vilket skulle framgå redan av innehållet i själva intyget. Andra skäl kan endast åberopas av den person vars uppgifter efterfrågas, inom ramen för egna rättsmedel i den utfärdande staten (se artikel 17). Dessutom ska tjänsteleverantörer ha tillgång till ett rättsmedel mot den verkställande myndighetens beslut att ålägga dem böter.

Verkställighetsförfarandet innehåller flera tidsfrister för den verkställande och den utfärdande myndigheten, för att undvika ytterligare förseningar under förfarandet.

Kapitel 4: Rättsmedel

Artiklarna 15 och 16: Prövning i händelse av motstridiga skyldigheter på grundval av ett tredjelandets lagstiftning

I artiklarna 15 och 16 föreskrivs ett prövningsförfarande i händelse av att tjänsteleverantörer med säte i tredjeländer ställs inför motstridiga skyldigheter. Dessa bestämmelser är också mycket viktiga för att säkerställa skyddet av individuella rättigheter och internationell hövlighet. Genom att fastställa en hög standard syftar de till att uppmuntra tredjeländer att införa en liknande skyddsnivå. I motsatt situation, när myndigheterna i ett tredjeland begär uppgifter om en EU-medborgare från en EU-tjänsteleverantör, kan unionens eller medlemsstaternas lagstiftning som skyddar de grundläggande rättigheterna, såsom dataskyddsregelverket, likaledes förhindra röjande. Europeiska unionen förväntar sig att tredjeländer, i likhet med detta förslag, respekterar sådana förbud.

Förfarandet i artikel 15 kan utlösas av mottagaren om efterlevnad av en europeisk utlämnandeorder skulle stå i strid med ett tredjelandets lagstiftning som förhindrar röjande av uppgifterna på grund av att detta är nödvändigt för att antingen skydda de berörda personernas grundläggande rättigheter eller tredjelandets grundläggande intressen i fråga om nationell säkerhet eller försvar. Mottagaren måste informera den utfärdande myndigheten, genom en motiverad invändning, om skälen till slutsatsen att det föreligger motstridiga skyldigheter. En sådan motiverad invändning kan inte grundas enbart på den omständigheten att liknande bestämmelser inte existerar i tredjelandets lagstiftning eller att uppgifterna lagras i ett tredjeland. Den motiverade invändningen ska göras i enlighet med det förfarande som anges i artikel 9.5 för att informera om en avsikt att inte efterleva ordern, med hjälp av det formulär som återges i bilaga III.

På grundval av denna motiverade invändning ska den utfärdande myndigheten ompröva sin egen order. Om den utfärdande myndigheten beslutar att återkalla ordern avslutas förfarandet. Om den utfärdande myndigheten vill upprätthålla ordern överlämnas ärendet till den behöriga domstolen i dess medlemsstat. Domstolen bedömer sedan, på grundval av den motiverade invändningen och med beaktande av alla relevanta omständigheter i målet, om tredjelandets lagstiftning är tillämplig i det aktuella fallet och – om så är fallet – huruvida motstridigheter föreligger i det aktuella fallet. När domstolen gör denna bedömning bör den beakta om tredjelandets lagstiftning, snarare än att vara avsedd att skydda grundläggande rättigheter eller tredjelandets grundläggande intressen i fråga om nationell säkerhet eller försvar, uppenbarligen syftar till att skydda andra intressen eller dölja olaglig verksamhet från brottsbekämpande myndigheters begäranden i samband med brottsutredningar.

Om domstolen fastställer att det faktiskt föreligger motstridiga skyldigheter som följer av lagstiftning som skyddar enskilda personers grundläggande rättigheter eller tredjelandets grundläggande intressen i fråga om nationell säkerhet eller försvar, måste domstolen begära ett yttrande av det berörda tredjelandet via de nationella centralmyndigheterna i tredjelandet. Om tredjelandet vid samråd bekräftar att motstridigheter föreligger och motsätter sig verkställigheten av ordern, måste domstolen återkalla ordern.

Om motstridigheter uppstår till följd av annan tredjelandslagstiftning som inte tjänar till att skydda varken enskilda personers grundläggande rättigheter eller tredjelandets grundläggande intressen i fråga om nationell säkerhet eller försvar, ska domstolen fatta sitt beslut på grundval av en avvägning av intressen som talar för och emot att upprätthålla ordern.

De villkor som anges i artikel 9, i synnerhet de bevarandeskyldigheter som beskrivs i artikel 9.6, ska även tillämpas i situationer där motstridiga skyldigheter som följer av ett tredjelands lagstiftning föreligger. Om domstolen beslutar att ordern ska upprätthållas, informeras den utfärdande myndigheten och tjänsteleverantören för att verkställigheten ska fortskrida. Om ordern upphävs kan en separat europeisk bevarandeorder utfärdas för att säkerställa att uppgifterna finns tillgängliga så att de kan erhållas genom en framställning om ömsesidig rättslig hjälp.

Med tanke på att en europeisk bevarandeorder i sig inte leder till röjande av uppgifter och därför inte ger upphov till liknande problem, gäller prövningsförfarandet endast europeiska utlämnandeorder.

Artikel 17: Effektiva rättsmedel

Denna bestämmelse säkerställer att personer som berörs av en europeisk utlämnandeorder har effektiva rättsmedel. Dessa rättsmedel används i den utfärdande staten i enlighet med nationell lagstiftning. För misstänkta och tilltalade personer utövas rätten till ett effektivt rättsmedel vanligen under de straffrättsliga förfarandena. Inga särskilda rättsmedel görs tillgängliga för den europeiska bevarandeordern, som i sig inte ger tillstånd att röja uppgifter, förutom i de fall när den följs av en europeisk utlämnandeorder eller ett annat instrument som leder till röjande, som i sin tur ger upphov till specifika rättsmedel.

Personer vars uppgifter har efterfrågats utan att de är misstänkta eller tilltalade i straffrättsliga förfaranden bör också ha rätt till ett rättsmedel i den utfärdande staten. Dessa rättigheter påverkar inte tillämpningen av rättsmedel som är tillgängliga inom ramen för direktivet om dataskydd vid brottsbekämpning och den allmänna dataskyddsförordningen.

I motsats till vad som föreskrivs för tjänsteleverantörer begränsar förordningen inte dessa personers möjliga skäl att ifrågasätta orderns lagenlighet. Dessa skäl inbegriper orderns nödvändighet och proportionerlighet.

Användningen av rättsmedel i den utfärdande staten innebär inte en oproportionell börda för berörda personer. I likhet med vad som är fallet med order som verkställs genom andra former av rättsligt samarbete är domstolarna i den utfärdande staten bäst lämpade att granska lagenligheten av europeiska utlämnandeorder som utfärdats av deras egna myndigheter och att bedöma förenligheten med deras egna nationella lagstiftning. Dessutom kan mottagare under verkställighetsstadiet separat motsätta sig verkställigheten av EPOC eller EPOC-PR i sin värdmedlemsstat på grundval av de skäl som förtecknas i förordningen (se artikel 14).

Artikel 18: Säkerställa immunitet och privilegier enligt lagen i den verkställande staten

Denna artikel har samma syfte som artikel 5.7, dvs. att säkerställa att immunitet och privilegier som skyddar de efterfrågade uppgifterna i tjänsteleverantörens medlemsstat beaktas i den utfärdande staten, i synnerhet när det finns skillnader mellan dessa medlemsstater, samt den medlemsstatens grundläggande intressen såsom nationell säkerhet och försvar. I artikel 18 föreskrivs att domstolen i den utfärdande staten måste beakta dem på samma sätt som om de föreskrevs i dess nationella lagstiftning. På grund av skillnaderna mellan medlemsstaterna vid bedömningen av bevisens relevans och godtagbarhet ger artikeln domstolarna en viss flexibilitet vad gäller hur de ska beaktas.

Kapitel 5: Slutbestämmelser

Artikel 19: Övervakning och rapportering

Enligt denna artikel måste medlemsstaterna rapportera specifik information om tillämpningen av förordningen i syfte att bistå kommissionen vid utövandet av dess uppgifter enligt artikel 24. Kommissionen ska upprätta ett detaljerat program för övervakning av resultaten och konsekvenserna av denna förordning.

Artikel 20: Ändringar av intyg och formulär

Det intyg och de formulär som återges i bilagorna I, II och III i detta förslag kommer att göra det enklare att verkställa EPOC och EPOC-PR. Av denna orsak är det nödvändigt att i framtiden kunna åtgärda ett eventuellt behov av att förbättra innehållet i intyget och formuläret så snabbt som möjligt. Ändring av de tre bilagorna genom det ordinarie lagstiftningsförfarandet uppfyller inte detta krav, och bilagorna utgör icke väsentliga delar av lagstiftningsakten, vars väsentliga delar definieras i artikel 8. Ett snabbare och mer flexibelt förfarande för ändringar genom delegerade akter föreskrivs därför i artikel 20.

Artikel 21: Utövande av delegeringen

Denna artikel anger villkoren enligt vilka kommissionen har befogenhet att anta delegerade akter för att göra nödvändiga ändringar av det intyg och de formulär som bifogas förslaget. I artikeln föreskrivs ett standardförfarande för antagande av sådana delegerade akter.

Artikel 22: Anmälningar

Medlemsstaterna måste anmäla till kommissionen vilka de behöriga utfärdande och verkställande myndigheterna är och vilka domstolar som är behöriga att handlägga motiverade invändningar från tjänsteleverantörer i händelse av motstridigheter i lagstiftningen.

Artikel 23: Förhållande till europeiska utredningsorder

I denna artikel klargörs att förordningen inte hindrar medlemsstaternas myndigheter från att utfärda en europeisk utredningsorder i enlighet med direktiv 2014/41/EU för att inhämta elektroniska bevis.

Artikel 24: Utvärdering

I denna artikel fastställs att kommissionen ska göra en utvärdering av förordningen i enlighet med kommissionens riktlinjer om bättre lagstiftning och punkt 22 i det interinstitutionella avtalet av den 13 april 2016²⁵. Kommissionen kommer att rapportera till Europaparlamentet och rådet om resultaten av utvärderingen, med en bedömning av behovet av att utvidga tillämpningsområdet till tjänster som ännu inte omfattas men som kan bli mer relevanta för utredningar, fem år efter det att den föreslagna förordningen har trätt i kraft.

Artikel 25: Ikraftträdande

Den föreslagna förordningen kommer att träda i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*. Förordningen kommer att börja tillämpas sex månader efter dagen för ikraftträdandet.

²⁵ Interinstitutionellt avtal mellan Europaparlamentet, Europeiska unionens råd och Europeiska kommissionen om bättre lagstiftning av den 13 april 2016. EUT L 123, 12.5.2016, s. 1.

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om europeiska utlämnandeorder och bevarandeorder för elektroniska bevis i 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 yttrande²⁶,
i enlighet med det ordinarie lagstiftningsförfarandet, 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 att möjliggöra brottsutredningar och åtal i hela unionen. Effektiva mekanismer för att inhämta elektroniska bevis är ytterst viktiga för att bekämpa brottslighet, under förutsättningar som säkerställer full överensstämmelse med de grundläggande rättigheter och principer som erkänns i Europeiska unionens stadga om de grundläggande rättigheterna i enlighet med fördragen, i synnerhet principerna om nödvändighet och proportionalitet, rättssäkerhet, dataskydd, brevhemlighet och integritet.
- (3) I det gemensamma uttalandet från EU:s ministrar med ansvar för rättsliga och inrikes frågor och företrädare för EU-institutionerna om terrorattackerna i Bryssel av den 22 mars 2016 poängterades behovet av att, som en prioritering, finna sätt att snabbare och effektivare säkra och inhämta digital bevisning samt fastställa konkreta åtgärder för att ta itu med denna komplicerade fråga.
- (4) I rådets slutsatser av den 9 juni 2016 framhölls den allt större betydelsen av e-bevisning i straffrättsliga förfaranden samt vikten av att skydda cyberrymden från oegentligheter och brottslig verksamhet, för våra ekonomiers och samhällets skull, och därmed behovet inom brottsbekämpningen och rättsväsendet av effektiva verktyg för att utreda och lagföra it-relaterade brott.

²⁶

EUT C , , s. .

- (5) I det gemensamma meddelandet om resiliens, avskräckning och försvar av den 13 september 2017²⁷ 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 sker ibland snabbare än dagens förfaranden kan hantera, vilket skapar särskilda behov av snabbt samarbete över gränserna.
- (6) Europaparlamentet uttryckte samma farhågor i sin resolution om kampen mot it-brottslighet av den 3 oktober 2017²⁸, där det konstaterade att det befintliga fragmenterade regelverket kan skapa problem för tjänsteleverantörer som försöker svara på framställningar på brottsbekämpningsområdet och uppmanade kommissionen att lägga fram ett förslag till en europeisk rättslig ram för e-bevisning, med lämpliga skyddsåtgärder för alla berörda parter rättigheter och friheter.
- (7) Nätverksbaserade tjänster kan tillhandahållas från vilken plats som helst och kräver inte fysisk infrastruktur, lokaler eller personal i det relevanta landet. Till följd av detta lagras relevanta bevis ofta utanför den utredande staten eller av en tjänsteleverantör som har ett verksamhetsställe utanför den staten. Ofta finns det ingen annan anknytning mellan det fall som utreds i den berörda staten och den stat där lagringen sker eller där tjänsteleverantören har sitt huvudsakliga verksamhetsställe.
- (8) På grund av denna brist på anknytning riktas begäranden om rättsligt samarbete ofta till stater där många tjänsteleverantörer är etablerade, men som inte har någon annan relation till det aktuella fallet. Dessutom har antalet begäranden ökat mångfaldigt vartefter som användningen av nätverksbaserade, av naturen gränslösa, tjänster har ökat. Detta leder till att det ofta tar lång tid att inhämta elektroniska bevis med hjälp av kanaler för rättsligt samarbete – kanske längre tid än de ledtrådar bevisen kan ge är tillgängliga. Dessutom finns ingen tydlig ram för samarbete med tjänsteleverantörer, då vissa leverantörer i tredjeländer tar emot direkta begäranden om icke-innehållsdata i enlighet med vad som tillåts enligt tillämplig nationell lagstiftning. Följaktligen förlitar sig alla medlemsstater på samarbetskanaler med tjänsteleverantörer när sådana finns tillgängliga, och använder sig därvid av olika nationella verktyg, villkor och förfaranden. Dessutom har vissa medlemsstater vidtagit ensidiga åtgärder för innehållsdata, medan andra fortfarande förlitar sig på rättsligt samarbete.
- (9) Det fragmenterade regelverket skapar problem för tjänsteleverantörer som försöker svara på framställningar på brottsbekämpningsområdet. Därför finns det ett behov av att inrätta en europeisk rättslig ram för elektroniska bevis i syfte att ålägga tjänsteleverantörer som omfattas av instrumentets tillämpningsområde en skyldighet att svara myndigheterna direkt utan att blanda in en rättslig myndighet i tjänsteleverantörens medlemsstat.
- (10) Order enligt denna förordning bör ställas till de rättsliga ombud som tjänsteleverantörerna har utsett för detta ändamål. Om en tjänsteleverantör med verksamhet i unionen inte har utsett ett ombud kan ordern ställas till något av denna tjänsteleverantörs verksamhetsställen i unionen. Detta reservalternativ syftar till att säkerställa systemets effektivitet även om tjänsteleverantören inte (ännu) har utsett ett särskilt ombud.

²⁷ JOIN(2017) 450 final.

²⁸ 2017/2068(INI).

- (11) Mekanismen med en europeisk utlämnandeorder och en europeisk bevarandeorder för elektroniska bevis på det straffrättsliga området kan endast fungera om den bygger på en hög nivå av ömsesidigt förtroende mellan medlemsstaterna, vilket är en avgörande förutsättning för att detta instrument ska fungera ordentligt.
- (12) Denna förordning är förenlig med de grundläggande rättigheter och de principer som erkänns särskilt i Europeiska unionens stadga om de grundläggande rättigheterna. Hit hör bland annat 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 inte bli dömd eller straffad två gånger för samma brott. Om den utfärdande medlemsstaten har uppgifter som tyder på att parallella straffrättsliga förfaranden pågår i en annan medlemsstat, ska den samråda med myndigheterna i den medlemsstaten i enlighet med rådets rambeslut 2009/948/RIF²⁹.
- (13) För att garantera full respekt för de grundläggande rättigheterna hänvisas i denna förordning uttryckligen till de standarder som krävs i fråga om inhämtande av personuppgifter, behandling av sådana uppgifter, rättslig prövning av användningen av den utredningsåtgärd som föreskrivs i detta instrument samt tillgängliga rättsmedel.
- (14) Tillämpningen av denna förordning bör inte påverka de processuella rättigheter i straffrättsliga förfaranden som fastställs i Europaparlamentets och rådets direktiv 2010/64/EU³⁰, 2012/13/EU³¹, 2013/48/EU³², 2016/343³³, 2016/800³⁴ och 2016/1919³⁵.
- (15) I detta instrument fastställs regler enligt vilka en behörig rättslig myndighet i Europeiska unionen kan beordra en tjänsteleverantör som erbjuder tjänster i unionen att lämna ut eller bevara elektroniska bevis genom en europeisk utlämnandeorder eller bevarandeorder. Denna förordning ska tillämpas i samtliga fall när en tjänsteleverantör har ett verksamhetsställe eller är representerad i en annan medlemsstat. I nationella situationer där de instrument som inrättas genom denna förordning inte kan användas bör förordningen inte begränsa de befogenheter som de nationella behöriga myndigheterna redan har enligt nationell lagstiftning att ålägga skyldigheter för tjänsteleverantörer som har ett verksamhetsställe eller är representerade på deras territorium.

²⁹ [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).

³⁰ [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).

³¹ [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).

³² [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).

³³ [Europaparlamentets och rådets direktiv \(EU\) 2016/343](#) av den 9 mars 2016 om förstärkning av vissa aspekter av oskuldspresumptionen och av rätten att närvara vid rättegången i straffrättsliga förfaranden (EUT L 65, 11.3.2016, s. 1).

³⁴ [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).

³⁵ [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).

- (16) De tjänsteleverantörer som är mest relevanta för 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. Leverantörer av elektroniska kommunikationstjänster definieras i förslaget till direktiv om inrättande av en europeisk kodex för elektronisk kommunikation. Hit hör interpersonell kommunikation som VoIP, meddelandetjänster och e-posttjänster. De kategorier av informationssamhällets tjänster som omfattas här är sådana för vilka datalagring är en väsentlig del av den tjänst som tillhandahålls användaren, och avser särskilt sociala nätverk som inte kan klassas som elektroniska kommunikationstjänster, nätbaserade marknadsplatser som underlättar transaktioner mellan användare (såsom konsumenter eller företag) och andra värdtjänster, även när tjänsten tillhandahålls via molntjänster. Sådana av informationssamhällets tjänster för vilka datalagring inte är en väsentlig del av den tjänst som tillhandahålls användaren, utan för vilka den endast är av underordnad betydelse – t.ex. rättsliga tjänster, arkitektjänster, ingenjörstjänster och bokföringstjänster som tillhandahålls online på distans – bör undantas från denna förordnings tillämpningsområde, även om de kan omfattas av definitionen av informationssamhällets tjänster enligt direktiv (EU) 2015/1535.
- (17) I många fall lagras och behandlas uppgifter 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 servrar 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.
- (18) Tjänsteleverantörer av internetinfrastruktur som rör tilldelning av namn och nummer, såsom domännamnsregistratorer, domännamnsregister, leverantörer av integritetstjänster och proxytjänster eller regionala internetregister för ip-adresser, är särskilt relevanta när det gäller att identifiera aktörer bakom skadliga eller hackade webbplatser. De innehar uppgifter som är speciellt relevanta för straffrättsliga förfaranden, eftersom de kan göra det möjligt att identifiera en person eller enhet som ligger bakom en webbplats som används för brottslig verksamhet, eller offret för brottslig verksamhet när det gäller en hackad webbplats som kapats av brottslingar.
- (19) Genom denna förordning regleras endast insamling av lagrade uppgifter, dvs. de uppgifter som tjänsteleverantören innehar vid den tidpunkt då den mottar ett intyg om en europeisk utlämnandeorder eller bevarandeorder. Den föreskriver ingen allmän datalagringskyldighet och ger inte heller rätt till dataavlyssning eller inhämtande av uppgifter som lagras vid en senare tidpunkt än vid mottagandet av ett intyg om en europeisk utlämnandeorder eller bevarandeorder. Uppgifter bör tillhandahållas oavsett om de är krypterade eller inte.
- (20) Denna förordning omfattar uppgiftskategorier såsom abonnentuppgifter, åtkomstuppgifter, transaktionsuppgifter (dessa tre kategorier kallas gemensamt ”icke-innehållsdata”) och innehållsdata. Denna skillnad existerar, förutom för åtkomstuppgifter, i många medlemsstaters lagstiftning och även i den nuvarande amerikanska rättsliga ram som gör det möjligt för tjänsteleverantörer att dela icke-innehållsdata med utländska brottsbekämpande myndigheter på frivillig basis.
- (21) Det är lämpligt att avgränsa åtkomstuppgifter som en särskild uppgiftskategori som används i denna förordning. Åtkomstuppgifter efterfrågas för samma ändamål som abonnentuppgifter, nämligen för att identifiera den bakomliggande användaren, och de

medför en liknande grad av ingrepp i de grundläggande rättigheterna som abonnentuppgifter. Åtkomstuppgifter registreras vanligen som en del av registreringen av en händelse (dvs. en serverlogg) för att ange när en användares åtkomst till en tjänst börjar och slutar. De utgörs ofta av en enskild ip-adress (statisk eller dynamisk) eller annan identifierare som utpekar det nätverksgränssnitt som använts under åtkomstsessionen. Om användaren är okänd måste de ofta inhämtas innan de abonnentuppgifter som har anknytning till identifieraren i fråga kan begäras från tjänsteleverantören.

- (22) Transaktionsuppgifter, å andra sidan, efterfrågas i allmänhet för att få information om användarens kontakter och vistelseort och kan användas för att fastställa en berörd persons profil. Åtkomstuppgifter kan dock inte i sig användas för att fastställa liknande information, t.ex. avslöjar de ingenting om användarens kontakter. Därför införs i detta förslag en ny uppgiftskategori, som ska behandlas som abonnentuppgifter om inhämtandet av uppgifter har ett liknande syfte.
- (23) Alla uppgiftskategorier innehåller personuppgifter och omfattas därmed av skyddsåtgärder enligt unionens dataskyddsregelverk, men graden av inverkan på de grundläggande rättigheterna varierar, i synnerhet mellan abonnentuppgifter och åtkomstuppgifter, å ena sidan, och transaktionsuppgifter och innehållsdata, å andra sidan. Abonnentuppgifter och åtkomstuppgifter är användbara för att vid en utredning få de första ledtrådarna om en misstänkt persons identitet, medan transaktionsuppgifter och innehållsdata är mest relevanta som bevismaterial. Det är därför viktigt att alla dessa uppgiftskategorier omfattas av rättsakten. På grund av den varierande graden av ingrepp i de grundläggande rättigheterna införs olika villkor för inhämtande av abonnentuppgifter och åtkomstuppgifter, å ena sidan, och transaktionsuppgifter och innehållsdata, å andra sidan.
- (24) En europeisk utlämnandeorder och en europeisk bevarandeorder är utredningsåtgärder som endast bör utfärdas inom ramen för specifika straffrättsliga förfaranden mot specifika kända eller fortfarande okända gärningsmän som begått ett konkret brott som redan har ägt rum, efter en individuell bedömning av proportionaliteten och nödvändigheten i varje enskilt fall.
- (25) Denna förordning påverkar inte myndigheternas utredningsbefogenheter i civilrättsliga eller administrativa förfaranden, inte heller då sådana förfaranden kan leda till påföljder.
- (26) Denna förordning bör tillämpas på tjänsteleverantörer som erbjuder tjänster i unionen, och de order som föreskrivs i denna förordning får endast utfärdas för uppgifter som hänför sig till tjänster som erbjuds i unionen. Tjänster som erbjuds uteslutande utanför unionen omfattas inte av denna förordning, även om tjänsteleverantören har ett verksamhetsställe i unionen.
- (27) För att fastställa om en tjänsteleverantör erbjuder tjänster i unionen krävs en bedömning av huruvida tjänsteleverantören gör det möjligt för juridiska eller fysiska personer i en eller flera medlemsstater att använda dess tjänster. Blotta åtkomsten till ett onlinegränssnitt, t.ex. åtkomst till tjänsteleverantörens eller en mellanhands webbplats eller en e-postadress och andra kontaktuppgifter i en eller flera medlemsstater, bör dock inte i sig räcka som villkor för att denna förordning ska tillämpas.
- (28) En väsentlig anknytning till unionen bör också vara relevant för att fastställa tillämpningsområdet för den här förordningen. En sådan väsentlig anknytning till

unionen bör anses föreligga om tjänsteleverantören har ett verksamhetsställe i unionen. I avsaknad av ett sådant verksamhetsställe bör kriteriet avseende en väsentlig anknytning bedömas på grundval av om det finns ett betydande antal användare i en eller flera medlemsstater, eller om verksamheten är fokuserad på en eller flera medlemsstater. Fokusering av verksamheten på en eller flera medlemsstater kan fastställas på grundval av alla relevanta omständigheter, t.ex. faktorer som användning av ett språk eller en valuta som i allmänhet används i den medlemsstaten, eller möjligheten att beställa varor eller tjänster. Fokusering av verksamheten på en medlemsstat kan även härledas från att en app finns tillgänglig i den berörda nationella appbutiken, att lokal marknadsföring eller reklam görs på det språk som används i medlemsstaten eller att kundkontakter, t.ex. kundtjänst, sköts på det språk som vanligen används i den medlemsstaten. En väsentlig anknytning ska också antas föreligga om en tjänsteleverantör riktar sin verksamhet till en eller flera medlemsstater i enlighet med artikel 17.1 c i förordning nr 1215/2012 om domstols behörighet och om erkännande och verkställighet av domar på privaträttens område³⁶. Å andra sidan kan tillhandahållande av tjänsten enbart i syfte att efterleva det förbud mot diskriminering som fastställs i förordning (EU) 2018/302³⁷ inte, bara på grund av detta, anses innebära att verksamhet riktas till eller fokuseras på ett visst territorium inom unionen.

- (29) En europeisk utlämnandeorder bör endast utfärdas om det är nödvändigt och proportionerligt. Vid bedömningen bör hänsyn tas till om ordern är begränsad till vad som är nödvändigt för att uppnå det legitima målet att endast inhämta de relevanta och nödvändiga uppgifterna för att utgöra bevis i det enskilda fallet.
- (30) När en europeisk utlämnandeorder eller bevarandeorder utfärdas bör en rättslig myndighet alltid delta antingen i utfärdandet eller godkännandet av ordern. Med tanke på den mer känsliga karaktären hos transaktionsuppgifter och innehållsdata kräver utfärdande eller godkännande av en europeisk utlämnandeorder för dessa kategorier prövning av en domare. Eftersom abonnentuppgifter och åtkomstuppgifter är mindre känsliga kan en europeisk utlämnandeorder om utlämnande av dessa uppgifter dessutom utfärdas eller godkännas av behöriga åklagare.
- (31) Av samma orsak måste en avgränsning göras avseende det materiella tillämpningsområdet för denna förordning: Order om utlämnande av abonnentuppgifter och åtkomstuppgifter kan utfärdas för alla brott, medan tillgång till transaktionsuppgifter och innehållsdata bör vara föremål för striktare krav med tanke på att dessa uppgifter är känsligare. Ett tröskelvärde möjliggör en mer proportionerlig hållning, tillsammans med ett antal andra förhands- och efterhandsvillkor och skyddsåtgärder som föreskrivs i förordningen för att säkerställa respekt för proportionalitetsprincipen och de berörda personernas rättigheter. Samtidigt bör tröskelvärdet inte begränsa instrumentets effektivitet och dess användning bland berörda aktörer. Genom att tillåta utfärdande av order för utredningar av brott med maximistraff på minst tre års fängelse begränsas instrumentets tillämpningsområde till

³⁶ [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 (EUT L 351, 20.12.2012, s. 1).

³⁷ [Europaparlamentets och rådets förordning \(EU\) 2018/302](#) av den 28 februari 2018 om åtgärder mot omotiverad geoblocking och andra former av diskriminering på grund av kunders nationalitet, boplatssort 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 601, 2.3.2018, s. 1).

allvarligare brott, utan att i alltför hög grad påverka aktörernas möjligheter att använda instrumentet. Tillämpningsområdet omfattar därmed inte ett betydande antal brott som medlemsstaterna anser vara mindre allvarliga, vilket uttrycks genom kortare maximistraff. Tack vare detta blir förordningen också lätt att tillämpa i praktiken.

- (32) Vid vissa typer av brott finns bevisen vanligen endast tillgängliga i elektronisk form, vilket kan göra dem särskilt kortlivade. Detta är fallet när det gäller it-relaterade brott – även sådana som inte kan betraktas som allvarliga i sig, men som kan orsaka omfattande eller betydande skador, däribland särskilt fall 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 för det mesta leda till strafffrihet. Detta motiverar att förordningen tillämpas på sådana brott även när maximistraffet understiger tre års fängelse. Terrorismrelaterade brott som beskrivs i direktiv (EU) 2017/541 kräver inte heller ett lägsta maximistraff på tre år.
- (33) Det är dessutom nödvändigt att föreskriva att en europeisk utlämnandeorder endast får utfärdas om en liknande order finns att tillgå för samma brott i en jämförbar inhemsk situation i den utfärdande staten.
- (34) Om de efterfrågade uppgifterna lagras eller behandlas som en del av en infrastruktur som en tjänsteleverantör tillhandahåller ett företag eller en annan enhet än fysiska personer, t.ex. värdtjänster, får den europeiska utlämnandeordern endast användas om andra utredningsåtgärder som kan riktas mot företaget eller enheten inte är lämpliga, i synnerhet om de kan riskera att äventyra utredningen. Detta är relevant framför allt när det gäller större enheter, såsom bolag eller offentliga organ, som utnyttjar tjänsteleverantörers tjänster för att tillhandahålla verksamhetens it-infrastruktur eller tjänster eller både och. Den första mottagaren av en europeisk utlämnandeorder bör i sådana fall vara företaget eller enheten. Företaget eller enheten i fråga kan vara en tjänsteleverantör som inte omfattas av denna förordnings tillämpningsområde. Om det inte är lämpligt att rikta sig till enheten, t.ex. för att den misstänks vara inblandad i det aktuella fallet eller för att det finns tecken på maskopi med föremålet för utredningen, bör de behöriga myndigheterna emellertid kunna rikta begäran om uppgifter till den tjänsteleverantör som tillhandahåller den berörda infrastrukturen. Denna bestämmelse påverkar inte rätten att beordra tjänsteleverantören att bevara uppgifterna.
- (35) Det hänvisas till immunitet och privilegier, som kan avse kategorier av personer (t.ex. diplomater) eller särskilt skyddade förhållanden (t.ex. rätten till förtrolig kommunikation mellan advokat och klient), i andra instrument för ömsesidigt erkännande, såsom den europeiska utredningsordern. Deras omfattning och effekter varierar beroende på den tillämpliga nationella lagstiftning som bör beaktas vid tidpunkten för utfärdandet av ordern, eftersom den utfärdande myndigheten endast får utfärda ordern om en liknande order skulle kunna användas i en jämförbar inhemsk situation. Utöver denna grundläggande princip bör immunitet och privilegier som skyddar åtkomstuppgifter, transaktionsuppgifter och innehållsdata i tjänsteleverantörens medlemsstat i möjligaste mån beaktas i den utfärdande staten på samma sätt som om de vore föreskrivna i den utfärdande statens nationella lagstiftning. Detta är särskilt relevant om lagen i den mottagande tjänsteleverantörens eller dess rättsliga ombuds medlemsstat föreskriver en högre skyddsnivå än den utfärdande statens lagstiftning. Bestämmelsen säkerställer också respekt för fall där röjandet av uppgifterna kan påverka medlemsstatens grundläggande intressen, såsom nationell säkerhet och försvar. Som en ytterligare skyddsåtgärd bör dessa aspekter inte bara beaktas när ordern utfärdas, utan även senare, då de berörda uppgifternas relevans

och godtagbarhet bedöms i det relevanta skedet av det straffrättsliga förfarandet och, om ett verkställighetsförfarande äger rum, av den verkställande myndigheten.

- (36) En europeisk bevarandeorder kan utfärdas för alla brott. Dess syfte är att förhindra avlägsnande, radering eller ändring av relevanta uppgifter i situationer där utlämnandet av dessa uppgifter kan ta längre tid, till exempel därför att rättsliga samarbetskanaler kommer att användas.
- (37) Europeiska utlämnandeorder och bevarandeorder bör ställas till det rättsliga ombud som utsetts av tjänsteleverantören. Om ett rättsligt ombud inte har utsetts kan ordern ställas till något av tjänsteleverantörens verksamhetsställen i unionen. Detta kan vara fallet om tjänsteleverantören inte har någon rättslig skyldighet att utse ett rättsligt ombud. Vid bristande efterlevnad från det rättsliga ombudets sida i nödsituationer kan den europeiska utlämnandeordern eller bevarandeordern också ställas till tjänsteleverantören samtidigt som eller i stället för att man eftersträvar verkställighet av den ursprungliga ordern enligt artikel 14. Vid bristande efterlevnad från det rättsliga ombudets sida i situationer som inte är nödsituationer, men där det finns en klar risk för att uppgifter kan gå förlorade, kan en europeisk utlämnandeorder eller bevarandeorder också ställas till något av tjänsteleverantörens verksamhetsställen i unionen. På grund av dessa olika möjliga scenarier används den allmänna termen ”mottagare” i bestämmelserna. Om en skyldighet, t.ex. om sekretess, är tillämplig inte bara på mottagaren utan även en tjänsteleverantör som inte är mottagaren specificeras detta i respektive bestämmelse.
- (38) Den europeiska utlämnandeordern och bevarandeordern ska översändas till tjänsteleverantören genom ett intyg om en europeisk utlämnandeorder eller ett intyg om en europeisk bevarandeorder, vilket bör översättas. Intyget bör innehålla samma obligatoriska information som ordern, med undantag för skälen till att åtgärden är nödvändig och proportionerlig eller närmare detaljer om ärendet för att undvika att äventyra utredningarna. Men eftersom de utgör en del av själva ordern är det möjligt för den misstänkta personen att bestrida dem senare under det straffrättsliga förfarandet. Vid behov bör ett intyg översättas till det officiella språket (eller ett av dem) i mottagarens medlemsstat, eller till ett annat officiellt språk som tjänsteleverantören har uppgett att den godtar.
- (39) Den behöriga utfärdande myndigheten bör översända intyget om en europeisk utlämnandeorder eller intyget om en europeisk bevarandeorder direkt till mottagaren på ett sätt som gör det möjligt att få en skriftlig uppteckning och som ger förutsättningar för tjänsteleverantören att fastställa äktheten, såsom per rekommenderat brev, säkrad e-post och säkrade plattformar eller via andra säkra kommunikationskanaler, även sådana som tjänsteleverantören tillhandahåller, i enlighet med reglerna om skydd av personuppgifter.
- (40) De begärda uppgifterna bör översändas till myndigheterna senast inom tio dagar efter mottagandet av intyget om en europeisk utlämnandeorder. Leverantören bör respektera kortare tidsfrister i nödsituationer och om den utfärdande myndigheten anger andra skäl att avvika från tidsfristen på tio dagar. Förutom överhängande risk för radering av begärda uppgifter kan dessa skäl vara omständigheter som hänför sig till en pågående utredning, till exempel om de begärda uppgifterna har anknytning till andra brådskande utredningsåtgärder som inte kan genomföras utan de uppgifter som saknas eller på annat sätt är beroende av dem.
- (41) För att göra det möjligt för tjänsteleverantörer att hantera formella problem är det nödvändigt att upprätta ett förfarande för kommunikation mellan tjänsteleverantören

och den utfärdande rättsliga myndigheten i de fall där intyget om en europeisk utlämnandeorder är ofullständigt, innehåller uppenbara fel eller saknar information som krävs för att verkställa ordern. Om tjänsteleverantören 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 lagen i ett tredjeland eller att den europeiska utlämnandeordern inte har utfärdats i enlighet med de villkor som fastställs i denna förordning, bör den svara de utfärdande myndigheterna med vederbörliga motiveringar. I breda ordalag bör kommunikationsförfarandet alltså göra det möjligt för den utfärdande myndigheten att korrigera eller ompröva intyget om en europeisk utlämnandeorder i ett tidigt skede. För att garantera att uppgifterna finns tillgängliga bör tjänsteleverantören bevara uppgifterna om den kan identifiera vilka uppgifter som efterfrågas.

- (42) Vid mottagande av ett intyg om en europeisk bevarandeorder bör tjänsteleverantören bevara de begärda uppgifterna i högst 60 dagar, såvida inte den utfärdande myndigheten informerar tjänsteleverantören om att den har inlett förfarandet med att utfärda en efterföljande begäran om utlämnande, varvid bevarandet bör fortsätta. Perioden på 60 dagar har beräknats för att göra det möjligt att sätta i gång en officiell begäran. Detta förutsätter att åtminstone några formella åtgärder har vidtagits, t.ex. att en begäran om ömsesidig rättslig hjälp har skickats till översättning. Efter att informationen har mottagits bör uppgifterna bevaras så länge som krävs för att lämna ut uppgifterna inom ramen för en efterföljande begäran om utlämnande.
- (43) Tjänsteleverantörer och deras rättsliga ombud bör säkerställa sekretessen och, när så begärs av den utfärdande myndigheten, avstå från att informera den person vars uppgifter begärs i syfte att skydda brottsutredningen, i enlighet med artikel 23 i förordning (EU) 2016/679³⁸. Användarinformation är dock en nödvändig förutsättning för granskning och rättslig prövning och bör därför tillhandahållas av myndigheten om tjänsteleverantören har ombetts att inte informera användaren, ifall det inte finns någon risk för att äventyra pågående utredningar, i enlighet med de nationella bestämmelser som införlivar artikel 13 i direktiv (EU) 2016/680³⁹.
- (44) Vid bristande efterlevnad från mottagarens sida får den utfärdande myndigheten överföra den fullständiga ordern inklusive resonemanget kring nödvändighet och proportionalitet, tillsammans med intyget, till den behöriga myndigheten i den medlemsstat där mottagaren av intyget bor eller har ett verksamhetsställe. Medlemsstaten bör verkställa den i enlighet med sin nationella lagstiftning. Medlemsstaterna bör föreskriva effektiva, proportionerliga och avskräckande böter vid överträdelse av de skyldigheter som införs genom denna förordning.
- (45) Verkställighetsförfarandet är ett förfarande som gör det möjligt för mottagaren att motsätta sig verkställighet på grundval av vissa begränsade skäl. Den verkställande myndigheten får vägra att erkänna och verkställa ordern på grundval av samma skäl, eller om immunitet och privilegier enligt den nationella lagstiftningen är tillämpliga eller om röjandet kan påverka dess grundläggande intressen såsom nationell säkerhet

³⁸ [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).

³⁹ [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).

och försvar. Den verkställande myndigheten bör samråda med den utfärdande myndigheten innan den vägrar att erkänna eller verkställa ordern på grundval av dessa skäl. Vid bristande efterlevnad kan myndigheter utdöma påföljder. Dessa påföljder bör vara proportionerliga även med tanke på särskilda omständigheter såsom upprepad eller systematisk bristande efterlevnad.

- (46) Vid sidan av deras dataskyddsskyldigheter bör tjänsteleverantörer inte hållas ansvariga i medlemsstaterna för nackdelar som drabbar 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.
- (47) Utöver de enskilda personer vars uppgifter begärs kan tjänsteleverantörerna och tredjeländer påverkas av utredningsåtgärden. För att säkerställa samförstånd i fråga om tredjeländers suveräna intressen, skydda den berörda personen och hantera tjänsteleverantörers motstridiga skyldigheter, föreskriver detta instrument en särskild mekanism för rättslig prövning om efterlevnad av en europeisk utlämnandeorder skulle hindra tjänsteleverantörer från att uppfylla rättsliga skyldigheter enligt lagstiftningen i ett tredjeland.
- (48) I detta syfte bör en mottagare som anser att den europeiska utlämnandeordern i ett visst fall skulle medföra en överträdelse av en rättslig skyldighet enligt lagstiftningen i ett tredjeland informera den utfärdande myndigheten genom en motiverad invändning med hjälp av de formulär som tillhandahålls. Den utfärdande myndigheten bör därefter ompröva den europeiska utlämnandeordern mot bakgrund av den motiverade invändningen, med beaktande av samma kriterier som behörig domstol skulle tvingas följa. Om myndigheten beslutar att upprätthålla ordern bör förfarandet hänskjutas till behörig domstol, enligt den berörda medlemsstatens anmälan, som därpå granskar ordern.
- (49) När den behöriga domstolen avgör om det föreligger en motstridig skyldighet i de särskilda omständigheterna i det aktuella fallet bör den förlita sig på lämplig extern sakkunskap när så behövs, t.ex. om prövningen väcker frågor om tolkningen av lagstiftningen i det berörda tredjelandet. Detta kan omfatta samråd med centralmyndigheterna i det landet.
- (50) Sakkunskap om tolkning kan också tillhandahållas genom expertutlåtanden, om sådana finns tillgängliga. Information och rättspraxis avseende tolkningen av tredjeländers lagstiftning och om konfliktförfaranden i medlemsstaterna bör göras tillgänglig på en central plattform såsom Sirius-projektet och/eller det europeiska rättsliga nätverket. Detta bör göra det möjligt för domstolarna att dra nytta av erfarenheter och sakkunskap som samlats in av andra domstolar om samma eller liknande frågor. Det bör inte förhindra ett förnyat samråd med tredjelandet i tillämpliga fall.
- (51) Om motstridiga skyldigheter föreligger bör domstolen avgöra om tredjelandets motstridiga bestämmelser förhindrar röjande av de berörda uppgifterna på grund av att detta är nödvändigt för att antingen skydda de berörda personernas grundläggande rättigheter eller tredjelandets grundläggande intressen i fråga om nationell säkerhet eller försvar. När domstolen gör denna bedömning bör den beakta om tredjelandets lagstiftning, snarare än att vara avsedd att skydda grundläggande rättigheter eller tredjelandets grundläggande intressen i fråga om nationell säkerhet eller försvar, uppenbarligen syftar till att skydda andra intressen eller dölja olaglig verksamhet från brottsbekämpande myndigheters begäranden i samband med brottsutredningar. Om domstolen bedömer att tredjelandets motstridiga bestämmelser förhindrar röjande av

de berörda uppgifterna på grund av att detta är nödvändigt för att antingen skydda de berörda personernas grundläggande rättigheter eller tredjelandets grundläggande intressen i fråga om nationell säkerhet eller försvar, bör den samråda med tredjelandet via dess centralmyndigheter, som redan inrättats för ömsesidig rättslig hjälp i de flesta delar av världen. Den bör fastställa en tidsfrist inom vilken tredjelandet kan invända mot verkställigheten av den europeiska utlämnandeordern. Om tredjelandets myndigheter inte svarar inom den (förlängda) tidsfristen, trots en påminnelse med information om vad som händer vid uteblivet svar, upprätthåller domstolen ordern. Om tredjelandets myndigheter invänder mot röjande bör domstolen upphäva ordern.

- (52) I alla andra fall av motstridiga skyldigheter, som inte rör personens grundläggande rättigheter eller tredjelandets grundläggande intressen i fråga om nationell säkerhet eller försvar, bör domstolen fatta beslut om huruvida den ska upprätthålla den europeiska utlämnandeordern genom att väga ett antal element som är avsedda att avgöra styrkan i anknytningen till endera av de två berörda jurisdiktionerna, intressena av att inhämta respektive förhindra röjande av uppgifterna samt möjliga konsekvenser för tjänsteleverantören om den måste rätta sig efter ordern. Av betydelse för it-relaterade brott är att den plats där brottet begicks omfattar både den eller de platser där handlingen skedde och den eller de platser där brottets följder uppstod.
- (53) De villkor som anges i artikel 9 ska tillämpas även när motstridiga skyldigheter som följer av ett tredjelands lagstiftning föreligger. Under detta förfarande bör uppgifterna bevaras. Om ordern upphävs kan en ny bevarandeorder utfärdas för att göra det möjligt för den utfärdande myndigheten att begära utlämnande av uppgifterna via andra kanaler, såsom ömsesidig rättslig hjälp.
- (54) 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 Europeiska unionens stadga om de grundläggande rättigheterna. För misstänkta och tilltalade personer bör rätten till ett effektivt rättsmedel utövas under de straffrättsliga förfarandena. Detta kan påverka möjligheterna att använda de bevis som inhämtats på detta sätt, eller i förekommande fall bevisens betydelse i förfarandet. Dessutom kan de utnyttja alla förfarandegarantier som är tillämpliga på dem, såsom rätten till information. Andra personer, som varken är misstänkta eller tilltalade, bör också ha rätt till ett effektivt rättsmedel. Därför bör minimikravet vara att det tillhandahålls en möjlighet att ifrågasätta lagenligheten av en europeisk utlämnandeorder, inklusive dess nödvändighet och proportionalitet. Denna förordning bör inte begränsa de möjliga skälen att ifrågasätta lagenligheten av ordern. Dessa rättsmedel bör användas i den utfärdande staten i enlighet med nationell lagstiftning. Bestämmelser om interimistiska åtgärder bör regleras av nationell lagstiftning.
- (55) Utöver detta kan mottagaren under verkställighetsförfarandet och vid användning av påföljande rättsmedel motsätta sig verkställigheten av en europeisk utlämnandeorder eller bevarandeorder av ett antal begränsade skäl, däribland att den inte har utfärdats eller godkänts av en behörig myndighet, att den på ett uppenbart sätt strider mot Europeiska unionens stadga om de grundläggande rättigheterna eller att den är uppenbart oskälig. Till exempel skulle en order om utlämnande av innehållsdata avseende en odefinierad grupp människor i ett geografiskt område eller utan koppling till konkreta straffrättsliga förfaranden på ett uppenbart sätt strida mot villkoren för utfärdande av en europeisk utlämnandeorder.
- (56) Skyddet av fysiska personer vid behandling av personuppgifter är en grundläggande rättighet. I enlighet med artikel 8.1 i Europeiska unionens stadga om de grundläggande

rättigheterna och artikel 16.1 i EUF-fördraget har var och en rätt till skydd av de personuppgifter som rör dem. Vid genomförandet av denna förordning bör medlemsstaterna säkerställa att personuppgifter skyddas och endast får behandlas i enlighet med förordning (EU) 2016/679 och direktiv (EU) 2016/680.

- (57) Personuppgifter som inhämtas i enlighet med denna förordning bör endast behandlas om det är nödvändigt och proportionerligt i förhållande till ändamålen förebyggande, utredning, upptäckt och lagföring av brott eller verkställande av straffrättsliga påföljder och utövande av rätten till försvar. Medlemsstaterna bör i synnerhet säkerställa att lämpliga strategier och åtgärder för dataskydd tillämpas på överföringen av personuppgifter från behöriga myndigheter till tjänsteleverantörer vid tillämpningen av denna förordning, inklusive åtgärder för att säkerställa uppgifternas säkerhet. Tjänsteleverantörer bör säkerställa detsamma för överföringen av personuppgifter till behöriga myndigheter. Endast behöriga personer bör ha tillgång till information som innehåller personuppgifter, vilket kan uppnås genom autentiseringsförfaranden. Man bör överväga att använda mekanismer för att säkerställa autentisering, t.ex. sådana anmälda nationella system för elektronisk identifiering eller betrodda tjänster som avses i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.
- (58) Kommissionen bör göra en utvärdering av denna förordning vilken bör grunda sig på de fem kriterierna effektivitet, ändamålsenlighet, relevans, enhetlighet och mervärde för EU samt ligga till grund för konsekvensbedömningar av eventuella ytterligare åtgärder. Information bör samlas in regelbundet för utvärderingen av denna förordning.
- (59) Användningen av redan översatta och standardiserade formulär underlättar samarbetet och informationsutbytet mellan rättsliga myndigheter och tjänsteleverantörer genom att göra det möjligt för dem att säkra och översända elektroniska bevis snabbare och effektivare samtidigt som de nödvändiga säkerhetskraven uppfylls på ett användarvänligt sätt. Sådana formulär minskar översättningskostnaderna och bidrar till en hög kvalitetsstandard. Svarsformulär bör likaledes möjliggöra ett standardiserat informationsutbyte, i synnerhet i de fall där tjänsteleverantörerna inte kan tillmötesgå begäran eftersom kontot inte existerar eller det inte finns några tillgängliga uppgifter. Formulären bör också underlätta insamlingen av statistik.
- (60) För att effektivt hantera eventuella behov av förbättringar när det gäller innehållet i intyg om en europeisk utlämnandeorder och intyg om en europeisk bevarandeorder och det formulär som ska användas för att meddela att det inte är möjligt att verkställa intyget om en europeisk utlämnandeorder eller intyget om en europeisk bevarandeorder, bör befogenheten att anta akter i enlighet med artikel 290 i fördraget om Europeiska unionens funktionssätt delegeras till kommissionen med avseende på ändringar av bilagorna I, II och III till den här förordningen. 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 om bättre lagstiftning av den 13 april 2016⁴⁰. För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter,

⁴⁰

EUT L 123, 12.5.2016, s. 1.

och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

- (61) En åtgärd som grundar sig på denna förordning bör inte ersätta en europeisk utredningsorder i enlighet med Europaparlamentets och rådets direktiv 2014/41/EU⁴¹ vad gäller inhämtande av elektroniska bevis. Medlemsstaternas myndigheter bör välja det verktyg som är bäst lämpat för deras situation – de kan föredra att använda en europeisk utredningsorder när de begär flera olika typer av utredningsåtgärder som omfattar utlämnande av elektroniska bevis från en annan medlemsstat men även andra åtgärder.
- (62) Den tekniska utvecklingen kan leda till att nya former av kommunikationsverktyg används om några år, och det kan uppstå luckor i tillämpningen av denna förordning. Det är därför viktigt att föreskriva en översyn av dess tillämpning.
- (63) Eftersom målet för denna förordning, nämligen att förbättra säkring och inhämtande av elektroniska bevis över gränserna, på grund av dess gränsöverskridande karaktär inte i tillräcklig utsträckning kan uppnås av medlemsstaterna, utan bättre kan uppnås på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen som fastställs i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå dessa mål.
- (64) I enlighet med artikel 3 i protokollet om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, *[har Förenade kungariket/Irland meddelat att det önskar delta i antagandet och tillämpningen av detta direktiv] eller [och utan att det påverkar tillämpningen av artikel 4 i protokollet, deltar Förenade kungariket/Irland inte i antagandet av detta direktiv, som därför inte är bindande för eller tillämpligt för Förenade kungariket/Irland]*.
- (65) I enlighet med artiklarna 1 och 2 i protokoll nr 22 om Danmarks ställning, fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, deltar Danmark inte i antagandet av denna förordning, som inte är bindande för eller tillämplig på Danmark.
- (66) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i Europaparlamentets och rådets förordning (EG) nr 45/2001⁴² och avgav ett yttrande den (...) ⁴³.

⁴¹ [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).

⁴² Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

⁴³ EUT C , , s. .

Kapitel 1: Syfte, definitioner och tillämpningsområde

Artikel 1

Syfte

1. I denna förordning fastställs regler enligt vilka en medlemsstats myndighet får beordra en tjänsteleverantör som erbjuder tjänster i unionen att lämna ut eller bevara elektroniska bevis, oavsett var uppgifterna finns. Denna förordning påverkar inte de nationella myndigheternas befogenheter att ålägga tjänsteleverantörer som har ett verksamhetsställe eller är representerade på deras territorium skyldigheter att följa liknande nationella åtgärder.
2. Denna förordning ska inte medföra någon ändring av skyldigheten att respektera de grundläggande rättigheter och rättsprinciper som återges i artikel 6 i EU-fördraget, bland annat rätten till försvar för personer som är föremål för straffrättsliga förfaranden, och alla skyldigheter som åligger brottsbekämpande eller rättsliga myndigheter i detta avseende ska kvarstå opåverkade.

Artikel 2

Definitioner

I denna förordning gäller följande definitioner:

- (1) *europaisk utlämnandeorder*: ett bindande beslut av en utfärdande myndighet i en medlemsstat varigenom en tjänsteleverantör som erbjuder tjänster i unionen och som har ett verksamhetsställe eller är representerad i en annan medlemsstat åläggs att lämna ut elektroniska bevis.
- (2) *europaisk bevarandeorder*: ett bindande beslut av en utfärdande myndighet i en medlemsstat varigenom en tjänsteleverantör som erbjuder tjänster i unionen och har ett verksamhetsställe eller är representerad i en annan medlemsstat åläggs att bevara elektroniska bevis i avvaktan på en efterföljande begäran om utlämnande.
- (3) *tjänsteleverantör*: 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 om inrättande av en europeisk kodex för elektronisk kommunikation].
 - (b) Informationssamhällets tjänster enligt definitionen i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535⁴⁴, för vilka datalagring är en väsentlig del av den tjänst som tillhandahålls användaren, t.ex. sociala nätverk, nätbaserade marknadsplatser som underlättar transaktioner mellan användarna och andra värdtjänsteleverantörer.

⁴⁴

[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).

- (c) Tjänster för internetdomännamn och ip-numrering, såsom ip-adressleverantörer, domännamnsregister, domännamnsregistratorer samt relaterade integritets- och proxytjänster.
- (4) *erbjuda tjänster i unionen:*
- (a) att göra det möjligt för juridiska och fysiska personer i en eller flera medlemsstater att använda de tjänster som anges i punkt 3, och
- (b) att ha en väsentlig anknytning till den eller de medlemsstater som avses i led a.
- (5) *verksamhet eller verksamhetsställe:* antingen det faktiska utövandet av en ekonomisk verksamhet under en obegränsad tid genom en stabil infrastruktur varifrån tillhandahållandet av tjänster genomförs, eller en stabil infrastruktur varifrån verksamheten förvaltas.
- (6) *elektroniska bevis:* bevis som lagras i elektronisk form av en tjänsteleverantör eller på dennas vägnar vid den tidpunkt då ett intyg om en utlämnandeorder eller bevarandeorder mottas, bestående av lagrade abonnentuppgifter, åtkomstuppgifter, transaktionsuppgifter och innehållsdata.
- (7) *abonnentuppgifter:* alla uppgifter om
- (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, bland annat tekniska data och uppgifter om relaterade tekniska åtgärder eller gränssnitt som använts av eller tillhandahållits abonnenten eller kunden, 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.
- (8) *åtkomstuppgifter:* uppgifter som rör inledande och avslutande av en användares åtkomst till en tjänst, vilka är strängt nödvändiga endast för ändamålet att identifiera tjänstens användare, såsom datum och tid för användningen, eller inloggning i och utloggning från tjänsten, tillsammans med den ip-adress som internetleverantören har tilldelat tjänstens användare, uppgifter som identifierar det gränssnitt som använts och användar-id. Detta innebär inte metadata från elektronisk kommunikation enligt definitionen i artikel 4.3 g i [förordning om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation].
- (9) *transaktionsuppgifter:* uppgifter som rör tillhandahållandet av en tjänst som erbjuds av en tjänsteleverantör och som tjänar till att ge kontext eller ytterligare information om tjänsten och som genereras eller behandlas av tjänsteleverantörens informationssystem, t.ex. källan till eller destinationen för ett meddelande eller en annan typ av interaktion, uppgifter om var utrustningen är belägen, datum, tid, varaktighet, storlek, rutt, format, vilket protokoll som använts och typen av komprimering, förutom om sådana uppgifter utgör åtkomstuppgifter. Detta innebär metadata från elektronisk kommunikation enligt definitionen i artikel 4.3 g i [förordning om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation].
- (10) *innehållsdata:* alla lagrade uppgifter i digital form, t.ex. text, röst, video, bilder och ljud, med undantag för abonnentuppgifter, åtkomstuppgifter och transaktionsuppgifter.

- (11) *informationssystem*: informationssystem enligt definitionen i artikel 2 a i Europaparlamentets och rådets direktiv 2013/40/EU⁴⁵.
- (12) *utfärdande stat*: den medlemsstat i vilken den europeiska utlämnandeordern eller den europeiska bevarandeordern utfärdas.
- (13) *verkställande stat*: den medlemsstat i vilken mottagaren av den europeiska utlämnandeordern eller den europeiska bevarandeordern bor eller har ett verksamhetsställe, och till vilken den europeiska utlämnandeordern och intyget om den europeiska utlämnandeordern eller den europeiska bevarandeordern och intyget om den europeiska bevarandeordern översänds för verkställighet.
- (14) *verkställande myndighet*: den behöriga myndighet i den verkställande staten till vilken den europeiska utlämnandeordern och intyget om den europeiska utlämnandeordern eller den europeiska bevarandeordern och intyget om den europeiska bevarandeordern översänds av den utfärdande myndigheten för verkställighet.
- (15) *nödsituationer*: situationer där det råder ett överhängande hot mot en persons liv eller fysiska integritet eller mot en kritisk infrastruktur enligt definitionen i artikel 2 a i rådets direktiv 2008/114/EG⁴⁶.

Artikel 3 *Tillämpningsområde*

1. Denna förordning ska tillämpas på tjänsteleverantörer som erbjuder tjänster i unionen.
2. Europeiska utlämnandeorder och europeiska bevarandeorder får endast utfärdas inom ramen för straffrättsliga förfaranden, både under förundersöknings- och rättegångsskedet. Order får också utfärdas i förfaranden som rör brott för vilka en juridisk person kan ställas till ansvar eller bestraffas i den utfärdande staten.
3. De order som föreskrivs i denna förordning får endast utfärdas för uppgifter som hänför sig till de tjänster som definieras i artikel 2.3 och som erbjuds i unionen.

Kapitel 2: Europeisk utlämnandeorder, europeisk bevarandeorder och intyg

Artikel 4 *Utfärdande myndighet*

1. En europeisk utlämnandeorder för abonnentuppgifter och åtkomstuppgifter kan utfärdas av
 - (a) en domare, en domstol, en undersökningsdomare eller en åklagare som är behörig i det berörda ärendet, eller

⁴⁵ [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).

⁴⁶ [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).

- (b) en annan behörig myndighet, enligt den utfärdande statens definition, som i det specifika ärendet handlar i egenskap av utredande myndighet i straffrättsliga förfaranden, med behörighet att besluta om bevisinhämtning i enlighet med nationell rätt. En sådan europeisk utlämnandeorder ska, efter granskning av dess överensstämmelse med villkoren för utfärdande av en europeisk utlämnandeorder enligt denna förordning, godkännas av en domare, domstol, undersökningsdomare eller åklagare i den utfärdande staten.
- 2. En europeisk utlämnandeorder för transaktionsuppgifter och 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 specifika ärendet handlar i egenskap av utredande myndighet i straffrättsliga förfaranden, med behörighet att besluta om bevisinhämtning i enlighet med nationell rätt. En sådan europeisk utlämnandeorder ska, 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 kan utfärdas av
 - (a) en domare, en domstol, en undersökningsdomare eller en åklagare som är behörig i det berörda ärendet, eller
 - (b) en annan behörig myndighet, enligt den utfärdande statens definition, som i det specifika ärendet handlar i egenskap av utredande myndighet i straffrättsliga förfaranden, med behörighet att besluta om bevisinhämtning i enlighet med nationell rätt. En sådan europeisk bevarandeorder ska, efter granskning av dess överensstämmelse med villkoren för utfärdande av en europeisk bevarandeorder enligt denna förordning, godkännas av en domare, en domstol, en undersökningsdomare eller en åklagare i den utfärdande staten.
- 4. Om ordern har godkänts av en rättslig myndighet i enlighet med punkterna 1 b, 2 b och 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.

Artikel 5

Villkor för utfärdande av en europeisk utlämnandeorder

- 1. En utfärdande myndighet får endast utfärda en europeisk utlämnandeorder om de villkor som anges i denna artikel är uppfyllda.
- 2. Den europeiska utlämnandeordern ska vara nödvändig och proportionerlig med avseende på de förfaranden som avses i artikel 3.2 och får endast utfärdas om en liknande åtgärd skulle finnas att tillgå för samma brott i en jämförbar inhemsk situation i den utfärdande staten.
- 3. Europeiska utlämnandeorder om abonnentuppgifter eller åtkomstuppgifter kan utfärdas för alla brott.
- 4. Europeiska utlämnandeorder om transaktionsuppgifter eller innehållsdata får endast utfärdas

- (a) för brott för vilka maximistrafvet i den utfärdande staten är fängelse i minst 3 år, eller
 - (b) för följande brott, om de helt eller delvis begås med hjälp av ett informationssystem:
 - Brott enligt definitionen i artiklarna 3, 4 och 5 i rådets rambeslut 2001/413/RIF⁴⁷.
 - Brott enligt definitionen i artiklarna 3–7 i Europaparlamentets och rådets direktiv 2011/93/EU⁴⁸.
 - Brott enligt definitionen i artiklarna 3–8 i Europaparlamentets och rådets direktiv 2013/40/EU.
 - (c) för brott enligt definitionen i artiklarna 3–12 och 14 i Europaparlamentets och rådets direktiv (EU) 2017/541⁴⁹.
5. Den europeiska utlämnandeordern 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) De personer vars uppgifter begärs, förutom när det enda syftet med ordern är att identifiera en person.
 - (d) Kategorin för de uppgifter som begärs (abonnentuppgifter, åtkomstuppgifter, transaktionsuppgifter eller innehållsdata).
 - (e) Om tillämpligt, det tidsintervall som begäran om utlämnande gäller.
 - (f) De tillämpliga bestämmelserna i den utfärdande medlemsstatens straffrätt.
 - (g) Vid nödsituationer eller vid begäran om tidigare utlämnande, orsakerna till detta.
 - (h) I fall där de uppgifter som efterfrågas lagras eller behandlas som en del av en infrastruktur som en tjänsteleverantör tillhandahåller ett företag eller en annan enhet än fysiska personer, en bekräftelse på att ordern har utfärdats i enlighet med punkt 6.
 - (i) Skälen till att åtgärden är nödvändig och proportionerlig.
6. I fall där de uppgifter som efterfrågas lagras eller behandlas som en del av en infrastruktur som en tjänsteleverantör tillhandahåller ett företag eller en annan enhet än fysiska personer, får den europeiska utlämnandeordern endast ställas till tjänsteleverantören om utredningsåtgärder som riktas mot företaget eller enheten inte är lämpliga, framför allt om de kan äventyra utredningen.

⁴⁷ [Rådets rambeslut 2001/413/RIF](#) av den 28 maj 2001 om bekämpning av bedrägeri och förfälskning som rör andra betalningsmedel än kontanter (EGT L 149, 2.6.2001, s. 1).

⁴⁸ [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).

⁴⁹ [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).

7. Om den utfärdande myndigheten har skäl att tro att de begärda transaktionsuppgifterna eller innehållsdata skyddas av immunitet och privilegier som beviljas enligt lagstiftningen i den mottagande tjänsteleverantörens medlemsstat, eller att röjande av dem kan påverka den medlemsstatens grundläggande intressen, såsom nationell säkerhet och försvar, måste den utfärdande myndigheten söka klargöranden före utfärdandet av den europeiska utlämnandeordern, bland annat genom att samråda med de behöriga myndigheterna i den berörda medlemsstaten, antingen direkt eller via Eurojust eller det europeiska rättsliga nätverket. Om den utfärdande myndigheten anser att de begärda åtkomstuppgifterna, transaktionsuppgifterna eller innehållsdata skyddas av sådan immunitet och sådana privilegier eller att röjande av dem skulle påverka den andra medlemsstatens grundläggande intressen, ska den inte utfärda den europeiska utlämnandeordern.

Artikel 6

Villkor för utfärdande av en europeisk bevarandeorder

1. En utfärdande myndighet får endast utfärda en europeisk bevarandeorder om de villkor som anges i denna artikel är uppfyllda.
2. Den kan utfärdas om det är nödvändigt och proportionerligt för att förhindra avlägsnande, radering eller ändring av uppgifter i avvaktan på en efterföljande begäran om utlämnande av dessa uppgifter via ömsesidig rättslig hjälp, en europeisk utredningsorder eller en europeisk utlämnandeorder. Europeiska bevarandeorder för bevarande av uppgifter kan utfärdas för alla brott.
3. Den europeiska bevarandeordern ska innehålla följande information:
 - (a) Den utfärdande myndigheten och i förekommande fall den godkännande myndigheten.
 - (b) Den europeiska bevarandeorderns mottagare i den mening som avses i artikel 7.
 - (c) De personer vars uppgifter ska bevaras, förutom när det enda syftet med ordern är att identifiera en person.
 - (d) Kategorin för de uppgifter som ska bevaras (abonnentuppgifter, åtkomstuppgifter, transaktionsuppgifter eller innehållsdata).
 - (e) Om tillämpligt, det tidsintervall som begäran om bevarande gäller.
 - (f) De tillämpliga bestämmelserna i den utfärdande medlemsstatens straffrätt.
 - (g) Skälen till att åtgärden är nödvändig och proportionerlig.

Artikel 7

Mottagare av en europeisk utlämnandeorder och en europeisk bevarandeorder

1. Den europeiska utlämnandeordern och den europeiska bevarandeordern ska ställas direkt till ett rättsligt ombud som utsetts av tjänsteleverantören i syfte att samla in bevis i straffrättsliga förfaranden.
2. Om inget rättsligt ombud har utsetts kan den europeiska utlämnandeordern och den europeiska bevarandeordern ställas till något av tjänsteleverantörens verksamhetsställen i unionen.

3. Om det rättsliga ombudet inte följer intyget om den europeiska utlämnandeordern i en nödsituation i enlighet med artikel 9.2 får intyget om den europeiska utlämnandeordern ställas till något av tjänsteleverantörens verksamhetsställen i unionen.
4. Om det rättsliga ombudet inte uppfyller sina skyldigheter enligt artikel 9 eller 10 och den utfärdande myndigheten anser att det föreligger en allvarlig risk för att uppgifterna ska gå förlorade, kan den europeiska utlämnandeordern eller den europeiska bevarandeordern ställas till något av tjänsteleverantörens verksamhetsställen i unionen.

Artikel 8

Intyg om en europeisk utlämnandeorder och en europeisk bevarandeorder

1. En europeisk utlämnandeorder eller bevarandeorder ska översändas till mottagaren i enlighet med artikel 7 genom ett intyg om en europeisk utlämnandeorder eller ett intyg om en europeisk bevarandeorder.

Den utfärdande eller godkännande myndigheten ska fylla i det intyg som återges i bilaga I eller det intyg som återges i bilaga II, underteckna det och intyga att dess innehåll är riktigt och korrekt.

2. Intyget om en europeisk utlämnandeorder eller intyget om en europeisk bevarandeorder ska översändas direkt på ett sätt som gör det möjligt att få en skriftlig uppteckning och som ger förutsättningar för mottagaren att fastställa äktheten.

Om tjänsteleverantörer, medlemsstater eller unionsorgan har inrättat särskilda plattformar eller andra säkra kanaler för hantering av begäranden om uppgifter från brottsbekämpande och rättsliga myndigheter, får den utfärdande myndigheten också välja att översända intyget via dessa kanaler.

3. Intyget 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 kontakta den utfärdande myndigheten. Det ska inte innehålla skälen till att åtgärden är nödvändig och proportionerlig eller ytterligare detaljer om utredningarna.
4. Intyget om en europeisk bevarandeorder ska innehålla den information som anges i artikel 6.3 a–f, inklusive tillräcklig information för att göra det möjligt för mottagaren att identifiera och kontakta den utfärdande myndigheten. Det ska inte innehålla skälen till att åtgärden är nödvändig och proportionerlig eller ytterligare detaljer om utredningarna.
5. 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. Om inget språk har angetts ska intyget om en europeisk utlämnandeorder eller intyget om en europeisk bevarandeorder översättas till ett av de officiella språken i den medlemsstat där det rättsliga ombudet bor eller har ett verksamhetsställe.

Artikel 9

Verkställande av ett intyg om en europeisk utlämnandeorder

1. Vid mottagandet av intyget om en europeisk utlämnandeorder ska mottagaren säkerställa att de begärda uppgifterna översänds direkt till den utfärdande myndigheten eller de brottsbekämpande myndigheterna enligt angivelse i intyget senast inom 10 dagar efter mottagandet av intyget, såvida inte den utfärdande myndigheten anger skäl att lämna ut dem tidigare.
2. I nödsituationer ska mottagaren översända de begärda uppgifterna utan onödigt dröjsmål, och senast inom sex timmar efter mottagandet av intyget om en europeisk utlämnandeorder.
3. Om mottagaren inte kan uppfylla sin skyldighet eftersom intyget om en europeisk utlämnandeorder är ofullständigt, innehåller uppenbara fel eller saknar information som krävs för att verkställa intyget, ska mottagaren informera den utfärdande myndighet som anges i intyget utan onödigt dröjsmål och be om förtydligande, med hjälp av det formulär som återges i bilaga III. Den ska informera den utfärdande myndigheten om huruvida det var möjligt att identifiera och bevara uppgifterna i enlighet med punkt 6. Den utfärdande myndigheten ska reagera snabbt och senast inom fem dagar. De tidsfrister som anges i punkterna 1 och 2 ska inte tillämpas förrän förtydliganden ges.
4. Om mottagaren inte kan uppfylla sin skyldighet på grund av force majeure eller faktisk omöjlighet som inte beror på mottagaren eller, om en annan, tjänsteleverantören, i synnerhet om personen vars uppgifter efterfrågas inte är dess kund eller om uppgifterna har raderats innan intyget om en europeisk utlämnandeorder mottogs, ska mottagaren informera den utfärdande myndighet som anges i intyget utan onödigt dröjsmål och förklara orsakerna, med hjälp av det formulär som återges i bilaga III. Om relevanta villkor uppfylls ska den utfärdande myndigheten dra tillbaka intyget om en europeisk utlämnandeorder.
5. I samtliga fall där mottagaren av andra orsaker inte tillhandahåller den begärda informationen, inte tillhandahåller den i sin helhet eller inte tillhandahåller den inom tidsfristen ska den informera den utfärdande myndigheten utan onödigt dröjsmål och senast inom de tidsfrister som anges i punkterna 1 och 2 om orsakerna till detta, med hjälp av formuläret i bilaga III. Den utfärdande myndigheten ska ompröva ordern mot bakgrund av den information som tjänsteleverantören har tillhandahållit och, vid behov, ange en ny tidsfrist inom vilken tjänsteleverantören ska lämna ut uppgifterna.

Om mottagaren anser att intyget om en europeisk utlämnandeorder inte kan verkställas på grund av att det enbart av informationen i intyget framgår att den uppenbart strider mot Europeiska unionens stadga om de grundläggande rättigheterna eller att den är uppenbart oskälig, ska mottagaren också sända formuläret i bilaga III till den behöriga verkställande myndigheten i mottagarens medlemsstat. I sådana fall kan den behöriga verkställande myndigheten begära förtydliganden om den europeiska utlämnandeordern från den utfärdande myndigheten, antingen direkt eller via Eurojust eller det europeiska rättsliga nätverket.
6. Mottagaren ska bevara de begärda uppgifterna, om den inte lämnar ut dem omedelbart, såvida inte informationen i intyget om en europeisk utlämnandeorder är sådan att det inte är möjligt att identifiera vilka uppgifter som begärs, i vilket fall den ska begära förtydliganden i enlighet med punkt 3. Bevarandet ska fortsätta tills uppgifterna lämnas ut, oavsett om det sker på grundval av den förtydligade

europiska utlämnandeordern och dess intyg eller via andra kanaler, såsom ömsesidig rättslig hjälp. Om utlämnandet av uppgifter och dess bevarande inte längre är nödvändigt ska den utfärdande myndigheten och, i tillämpliga fall enligt artikel 14.8, den verkställande myndigheten informera mottagaren utan onödigt dröjsmål.

Artikel 10

Verkställande av ett intyg om en europeisk bevarandeorder

1. Vid mottagande av intyget om en europeisk bevarandeorder ska mottagaren utan onödigt dröjsmål bevara de begärda uppgifterna. Bevarandet ska upphöra efter 60 dagar, såvida inte den utfärdande myndigheten bekräftar att en efterföljande begäran om utlämnande har inletts.
2. Om den utfärdande myndigheten inom den tidsperiod som fastställs i punkt 1 bekräftar att en efterföljande begäran om utlämnande har inletts ska mottagaren bevara uppgifterna så länge som krävs för att lämna ut uppgifterna när begäran om utlämnande väl delges.
3. Om det inte längre är nödvändigt att bevara uppgifterna ska den utfärdande myndigheten informera mottagaren utan onödigt dröjsmål.
4. Om mottagaren inte kan uppfylla sin skyldighet eftersom intyget om en europeisk bevarandeorder är ofullständigt, innehåller uppenbara fel eller saknar information som krävs för att verkställa intyget, ska mottagaren informera den utfärdande myndighet som anges i intyget utan onödigt dröjsmål och be om förtydligande, med hjälp av det formulär som återges i bilaga III. Den utfärdande myndigheten ska reagera snabbt och senast inom fem dagar. Mottagaren ska å sin sida säkerställa att det förtydligande som behövs kan mottas i syfte att uppfylla skyldigheten enligt punkt 1.
5. Om mottagaren inte kan uppfylla sin skyldighet på grund av force majeure eller faktisk omöjlighet som inte beror på mottagaren eller, om en annan, tjänsteleverantören, i synnerhet om personen vars uppgifter efterfrågas inte är dess kund eller om uppgifterna har raderats innan ordern mottogs, ska mottagaren kontakta den utfärdande myndighet som anges i intyget om en europeisk bevarandeorder utan onödigt dröjsmål och förklara orsakerna, med hjälp av det formulär som återges i bilaga III. Om dessa villkor uppfylls ska den utfärdande myndigheten dra tillbaka intyget om en europeisk bevarandeorder.
6. I samtliga fall där mottagaren inte bevarar den begärda informationen, av andra orsaker än de som förtecknas i formuläret i bilaga III, ska mottagaren utan onödigt dröjsmål informera den utfärdande myndigheten om orsakerna till detta med hjälp av det formulär som återges i bilaga III. Den utfärdande myndigheten ska ompröva ordern mot bakgrund av de motiveringar som tjänsteleverantören har tillhandahållit.

Artikel 11

Sekretess och användarinformation

1. Mottagare och, om dessa inte är samma, tjänsteleverantörer ska vidta nödvändiga åtgärder för att säkerställa sekretessen för intyget om en europeisk utlämnandeorder och intyget om en europeisk bevarandeorder och de uppgifter som lämnas ut eller bevaras och, på begäran av den utfärdande myndigheten, avstå från att informera den

person vars uppgifter efterfrågas för att inte hindra det berörda straffrättsliga förfarandet.

2. Om den utfärdande myndigheten har begärt att mottagaren ska avstå från att informera den person vars uppgifter efterfrågas, ska den utfärdande myndigheten utan onödigt dröjsmål informera den person vars uppgifter efterfrågas genom intyget om en europeisk utlämnandeorder om utlämnandet av uppgifter. Denna information kan skjutas upp så länge som är nödvändigt och proportionerligt för att undvika att hindra det berörda straffrättsliga förfarandet.
3. När personen informeras ska den utfärdande myndigheten inbegripa information om alla tillgängliga rättsmedel i den mening som avses i artikel 17.

Artikel 12

Ersättning för kostnader

Tjänsteleverantören får kräva ersättning för sina kostnader av den utfärdande staten, om detta föreskrivs i den utfärdande statens nationella lagstiftning för inhemska förelägganden i liknande situationer, i enlighet med dessa nationella bestämmelser.

Kapitel 3: Påföljder och verkställighet

Artikel 13

Påföljder

Utan att det påverkar tillämpningen av nationell lagstiftning som föreskriver straffrättsliga påföljder, ska medlemsstaterna fastställa regler om böter som är tillämpliga på överträdelser av de skyldigheter som följer av artiklarna 9, 10 och 11 i denna förordning och ska vidta alla nödvändiga åtgärder för att säkerställa att de genomförs. Böterna ska vara effektiva, proportionerliga och avskräckande. Medlemsstaterna ska utan dröjsmål anmäla dessa regler och åtgärder samt eventuella ändringar som berör dem till kommissionen.

Artikel 14

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, får den utfärdande myndigheten till den behöriga myndigheten i den verkställande staten överföra den europeiska utlämnandeordern med intyget om den europeiska utlämnandeordern eller den europeiska bevarandeordern med intyget om den europeiska bevarandeordern samt det formulär som återges i bilaga III, ifyllt av mottagaren, och alla andra relevanta handlingar i syfte att verkställa ordern, på ett sätt som gör det möjligt att få en skriftlig uppteckning och som ger förutsättningar för den verkställande myndigheten att fastställa äktheten. För detta ändamål ska den utfärdande myndigheten översätta ordern, formuläret och alla andra medföljande handlingar till ett av de officiella språken i denna medlemsstat och ska informera mottagaren om överföringen.

2. Vid mottagandet ska den verkställande myndigheten utan vidare formaliteter erkänna en europeisk utlämnandeorder eller europeisk bevarandeorder som översänts i enlighet med punkt 1 och ska vidta de åtgärder som krävs för att verkställa den, såvida inte den verkställande myndigheten anser att ett av de skäl som anges i punkterna 4 eller 5 är tillämpligt, att de berörda uppgifterna skyddas av immunitet eller privilegier enligt nationell lagstiftning eller att röjande av uppgifterna kan påverka grundläggande intressen såsom nationell säkerhet och försvar. Den verkställande myndigheten ska fatta beslut om att erkänna ordern utan onödigt dröjsmål och senast fem arbetsdagar efter mottagandet av ordern.
3. Om den verkställande myndigheten erkänner ordern ska den formellt kräva att mottagaren uppfyller motsvarande skyldighet, informera mottagaren om möjligheten att invända mot verkställigheten genom att hänvisa till de skäl som anges i punkterna 4 eller 5 och de tillämpliga påföljderna vid bristande efterlevnad, samt fastställa en tidsfrist för efterlevnad eller invändningar.
4. Mottagaren kan endast motsätta sig verkställighet av den europeiska utlämnandeordern på grundval 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 uppfylla intyget om en europeisk utlämnandeorder på grund av faktisk omöjlighet eller force majeure, 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) Det framgår enbart av den information som ingår i intyget om en europeisk utlämnandeorder att den uppenbart strider mot stadgan eller att den är uppenbart oskälig.
5. Mottagaren kan endast motsätta sig verkställighet av den europeiska bevarandeordern på grundval av följande skäl:
 - (a) Den europeiska bevarandeordern har inte utfärdats eller godkänts av en utfärdande myndighet som anges i artikel 4.
 - (b) Tjänsteleverantören kunde inte uppfylla intyget om en europeisk bevarandeorder på grund av faktisk omöjlighet eller force majeure, 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) Det framgår enbart av den information som ingår i intyget om en europeisk bevarandeorder att intyget uppenbart strider mot stadgan eller att det är uppenbart oskäligt.

6. Om mottagaren gör invändningar ska den verkställande myndigheten besluta huruvida ordern ska verkställas på grundval av den 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 verkställa ordern i enlighet med punkterna 2 och 6 ska den samråda med den utfärdande myndigheten på lämpligt sätt. När 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. Alla beslut ska omedelbart meddelas den utfärdande myndigheten och mottagaren på ett sätt som gör det möjligt att få en skriftlig uppteckning.
9. Om den verkställande myndigheten inhämtar uppgifterna från mottagaren ska den översända dem till den utfärdande myndigheten inom två arbetsdagar, såvida inte de berörda uppgifterna skyddas av immunitet eller privilegier enligt dess egna nationella lagstiftning eller utlämnandet påverkar grundläggande intressen såsom nationell säkerhet och försvar. I sådana fall ska den informera den utfärdande myndigheten om orsakerna till att den inte översänder uppgifterna.
10. Om mottagaren inte uppfyller sina skyldigheter enligt en erkänd order vars verkställbarhet har bekräftats av den verkställande myndigheten, ska den myndigheten ålägga böter i enlighet med sin nationella lagstiftning. Ett effektivt rättsmedel ska finnas tillgängligt mot beslutet att ålägga böter.

Kapitel 4: Rättsmedel

Artikel 15

Prövning i händelse av motstridiga skyldigheter på grundval av grundläggande rättigheter eller ett tredjelandets grundläggande intressen

1. Om mottagaren anser att efterlevnaden av en europeisk utlämnandeorder skulle stå i strid med ett tredjelandets tillämpliga lagstiftning som förbjuder röjande av de berörda uppgifterna på grundval av att detta är nödvändigt för att skydda de berörda personernas grundläggande rättigheter eller tredjelandets grundläggande intressen i fråga om nationell säkerhet eller försvar, ska den informera den utfärdande myndigheten om sina skäl till att inte verkställa den europeiska utlämnandeordern i enlighet med det förfarande som avses i artikel 9.5.
2. Motiverade invändningar ska innehålla alla relevanta uppgifter om tredjelandets lagstiftning, dess tillämpning i det aktuella fallet och arten av den motstridiga skyldigheten. De får inte grundas på att liknande bestämmelser om villkor, formaliteter och förfaranden för utfärdande av en utlämnandeorder inte existerar i tredjelandets tillämpliga lagstiftning, eller endast på att uppgifterna lagras i ett tredjeland.
3. Den utfärdande myndigheten ska ompröva den europeiska utlämnandeordern på grundval av den motiverade invändningen. Om den utfärdande myndigheten har för avsikt att upprätthålla den europeiska utlämnandeordern ska den begära en prövning av den behöriga domstolen i sin medlemsstat. Verkställigheten av ordern ska avbrytas i avvaktan på att prövningsförfarandet avslutas.

Den behöriga domstolen ska först bedöma om motstridigheter föreligger, på grundval av en granskning av om

- (a) tredjelandets lagstiftning är tillämplig utifrån de särskilda omständigheterna i ärendet i fråga och i så fall,
 - (b) om tredjelandets lagstiftning, när den tillämpas på de särskilda omständigheterna i ärendet i fråga, förbjuder röjande av de berörda uppgifterna.
4. När domstolen gör denna bedömning bör den beakta om tredjelandets lagstiftning, snarare än att vara avsedd att skydda grundläggande rättigheter eller tredjelandets grundläggande intressen i fråga om nationell säkerhet eller försvar, uppenbarligen syftar till att skydda andra intressen eller dölja olaglig verksamhet från brottsbekämpande myndigheters begäranden i samband med brottsutredningar.
 5. Om den behöriga domstolen anser att det inte föreligger några motstridigheter i den mening som avses i punkterna 1 och 4, ska den upprätthålla ordern. Om den behöriga domstolen fastställer att det föreligger motstridigheter i den mening som avses i punkterna 1 och 4, ska den behöriga domstolen översända alla relevanta uppgifter om de faktiska och rättsliga aspekterna av ärendet, inklusive sin bedömning, till centralmyndigheterna i det berörda tredjelandet via sin nationella centralmyndighet, med en 15 dagars svarsfrist. På en motiverad begäran från tredjelandets centralmyndighet kan tidsfristen förlängas med 30 dagar.
 6. Om tredjelandets centralmyndighet inom tidsfristen meddelar den behöriga domstolen att den motsätter sig verkställigheten av den europeiska utlämnandeordern i detta fall, ska den behöriga domstolen upphäva ordern och informera den utfärdande myndigheten och mottagaren. Om inga invändningar har mottagits inom (den förlängda) tidsfristen, ska den behöriga domstolen skicka en påminnelse och ge tredjelandets centralmyndighet ytterligare fem dagar att svara, samt informera om vad som händer om svaret uteblir. Om inga invändningar har mottagits inom denna ytterligare tidsfrist ska den behöriga domstolen upprätthålla ordern.
 7. Om den behöriga myndigheten bestämmer att ordern ska upprätthållas ska den informera den utfärdande myndigheten och mottagaren, som ska fullfölja verkställigheten av ordern.

Artikel 16

Prövning i händelse av motstridiga skyldigheter på grundval av andra skäl

1. Om mottagaren anser att efterlevnaden av en europeisk utlämnandeorder skulle stå i strid med ett tredjelandets tillämpliga lagstiftning som förbjuder röjande av de berörda uppgifterna av andra skäl än de som anges i artikel 15, ska den informera den utfärdande myndigheten om sina orsaker att inte verkställa den europeiska utlämnandeordern i enlighet med det förfarande som avses i artikel 9.5.
2. Motiverade invändningar ska innehålla alla relevanta uppgifter om tredjelandets lagstiftning, dess tillämpning i det aktuella fallet och arten av den motstridiga skyldigheten. De får inte grundas på att liknande bestämmelser om villkor, formaliteter och förfaranden för utfärdande av en utlämnandeorder inte existerar i tredjelandets tillämpliga lagstiftning, eller endast på att uppgifterna lagras i ett tredjeland.

3. Den utfärdande myndigheten ska ompröva den europeiska utlämnandeordern på grundval av den motiverade invändningen. Om den utfärdande myndigheten har för avsikt att upprätthålla den europeiska utlämnandeordern ska den begära en prövning av den behöriga domstolen i sin medlemsstat. Verkställigheten av ordern ska avbrytas i avvaktan på att prövningsförfarandet avslutas.
4. Den behöriga domstolen ska först bedöma om motstridigheter föreligger, på grundval av en granskning av om
 - (a) tredjelandets lagstiftning är tillämplig utifrån de särskilda omständigheterna i ärendet i fråga och i så fall,
 - (b) om tredjelandets lagstiftning, när den tillämpas på de särskilda omständigheterna i ärendet i fråga, förbjuder röjande av de berörda uppgifterna.
5. Om den behöriga domstolen anser att det inte föreligger några motstridigheter i den mening som avses i punkterna 1 och 4, ska den upprätthålla ordern. Om den behöriga domstolen fastställer att tredjelandets lagstiftning, när den tillämpas på de särskilda omständigheterna i ärendet i fråga, förbjuder röjande av de berörda uppgifterna, ska den behöriga domstolen avgöra om ordern ska upprätthållas eller återkallas, i synnerhet på grundval av följande faktorer:
 - (a) Det intresse som skyddas genom tredjelandets relevanta lagstiftning, inklusive tredjelandets intresse av att förhindra röjande av uppgifterna.
 - (b) Graden av anknytning mellan det brottmål för vilket ordern utfärdades och endera av de två jurisdiktionerna, vilken bland annat kan framgå av plats, medborgarskap och hemvist för den person vars uppgifter efterfrågas och/eller för brottsoffret/offren, platsen där brottet i fråga begicks,
 - (c) graden av anknytning mellan tjänsteleverantören och tredjelandet i fråga; i detta sammanhang räcker inte platsen för lagring av uppgifterna i sig till för att fastställa en betydande grad av anknytning,
 - (d) den utredande statens intresse av att inhämta de aktuella bevisen, utgående från brottets svårhetsgrad och vikten av att inhämta bevis på ett snabbt sätt,
 - (e) möjliga konsekvenser för mottagaren eller tjänsteleverantören av att efterleva den europeiska utlämnandeordern, inklusive påföljder som kan komma i fråga.
6. Om den behöriga domstolen beslutar att upphäva ordern ska den informera den utfärdande myndigheten och mottagaren. Om den behöriga myndigheten bestämmer att ordern ska upprätthållas ska den informera den utfärdande myndigheten och mottagaren, som ska fullfölja verkställigheten av ordern.

Artikel 17 *Effektiva rättsmedel*

1. Misstänkta och tilltalade personer vars uppgifter har inhämtats genom en europeisk utlämnandeorder ska ha rätt till effektiva rättsmedel mot den europeiska utlämnandeordern under det straffrättsliga förfarande för vilket ordern utfärdades,

utan att detta påverkar tillämpningen av tillgängliga rättsmedel enligt direktiv (EU) 2016/680 och förordning (EU) 2016/679.

2. Om den person vars uppgifter har inhämtats inte är misstänkt eller tilltalad i det straffrättsliga förfarande för vilket ordern utfärdades, ska denna person ha rätt till effektiva rättsmedel mot den europeiska utlämnandeordern i den utfärdande staten, utan att detta påverkar tillämpningen av tillgängliga rättsmedel enligt direktiv (EU) 2016/680 och förordning (EU) 2016/679.
3. Denna rätt till ett effektivt rättsmedel ska utövas vid en domstol i den utfärdande staten i enlighet med dess nationella lagstiftning och ska inbegripa möjligheten att bestrida åtgärdens laglighet, inklusive dess nödvändighet och proportionalitet.
4. Utan att det påverkar tillämpningen av artikel 11 ska den utfärdande myndigheten vidta lämpliga åtgärder för att säkerställa att information ges om möjligheterna enligt nationell lagstiftning att utnyttja rättsmedel och säkerställa att de kan utövas på ett effektivt sätt.
5. Samma tidsfrister eller andra villkor för att utnyttja ett rättsmedel ska gälla här som i liknande inhemska ärenden och på ett sätt som garanterar effektivt utövande av dessa rättsmedel för de berörda personerna.
6. Utan att det påverkar nationella förfaranderegler ska medlemsstaterna säkerställa att man vid straffrättsliga förfaranden i den utfärdande staten respekterar rätten till försvar och ett rättvist förfarande vid bedömningen av de bevis som inhämtats genom den europeiska utlämnandeordern.

Artikel 18

Säkerställa immunitet och privilegier enligt lagen i den verkställande staten

Om transaktionsuppgifter eller innehållsdata som inhämtats genom den europeiska utlämnandeordern skyddas av immunitet eller privilegier som beviljas enligt lagstiftningen i mottagarens medlemsstat, eller om de påverkar den medlemsstatens grundläggande intressen såsom nationell säkerhet och försvar, ska domstolen i den utfärdande staten under det straffrättsliga förfarande för vilket ordern utfärdades säkerställa att dessa faktorer beaktas vid bedömningen av de berörda bevisens relevans och godtagbarhet på samma sätt som om de föreskrevs i dess nationella lagstiftning. Domstolen får samråda med myndigheterna i den berörda medlemsstaten, det europeiska straffrättsliga nätverket eller Eurojust.

Kapitel 5: Slutbestämmelser

Artikel 19

Övervakning och rapportering

1. Senast den [datum för tillämpning av denna förordning] 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 andra nödvändiga bevis 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 och de andra bevisen.

2. I alla händelser ska medlemsstaterna samla in och föra uttömmande statistik från de relevanta myndigheterna. De insamlade uppgifterna ska sändas till kommissionen senast den 31 mars varje år för det föregående kalenderåret och ska omfatta följande:
- (a) Antalet intyg om en europeisk utlämnandeorder och intyg om en europeisk bevarandeorder som utfärdats, indelat efter typ av uppgifter som begärts, tjänsteleverantörer som varit mottagare och situation (nödsituation eller inte).
 - (b) Antalet verkställda respektive icke verkställda intyg om en europeisk utlämnandeorder, indelat efter typ av uppgifter som begärts, tjänsteleverantörer som varit mottagare och situation (nödsituation eller inte).
 - (c) För verkställda intyg om en europeisk utlämnandeorder, den genomsnittliga tiden för inhämtande av de begärda uppgifterna, från den tidpunkt då intyget utfärdades till den tidpunkt då uppgifterna erhöles, indelat efter typ av uppgifter som begärts, tjänsteleverantörer som varit mottagare och situation (nödsituation eller inte).
 - (d) Antalet europeiska utlämnandeorder som översänts och mottagits för verkställighet till en verkställande stat, indelat efter typ av uppgifter som begärts, tjänsteleverantörer som varit mottagare och situation (nödsituation eller inte) samt antalet som verkställts.
 - (e) Antalet rättsmedel mot europeiska utlämnandeorder i den utfärdande staten och i den verkställande staten, indelat efter typ av uppgifter som begärts.

Artikel 20

Ändringar av intyg och formulär

Kommissionen ska anta delegerade akter i enlighet med artikel 21 för att ändra bilagorna I, II och III 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 formulär som ska användas för att meddela att det är omöjligt att verkställa intyget om en europeisk utlämnandeorder eller intyget om en europeisk bevarandeorder.

Artikel 21

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 20 ska ges till kommissionen tills vidare från och med den [det datum då denna förordning börjar tillämpas].
3. Den delegering av befogenhet som avses i artikel 20 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 om bättre lagstiftning av den 13 april 2016⁵⁰.
5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.
6. En delegerad akt som antas enligt artikel 20 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 22 *Anmälningar*

1. Senast den [datum för tillämpning av denna förordning] ska varje medlemsstat till kommissionen anmäla följande:
 - (a) De myndigheter som i enlighet med landets nationella lagstiftning är behöriga i enlighet med artikel 4 att utfärda och/eller godkänna europeiska utlämnandeorder och europeiska bevarandeorder.
 - (b) Den eller de verkställande myndigheter som är behöriga att verkställa europeiska utlämnandeorder och europeiska bevarandeorder på en annan medlemsstats vägnar.
 - (c) De domstolar som är behöriga att handlägga motiverade invändningar från mottagarna i enlighet med artiklarna 15 och 16.
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 rättsliga nätverk som avses i artikel 9 i rådets beslut 2008/976/RIF⁵¹.

Artikel 23 *Förhållande till europeiska utredningsorder*

Medlemsstaternas myndigheter får fortsätta att utfärda europeiska utredningsorder i enlighet med direktiv 2014/41/EU för bevisinhämtning som också skulle omfattas av denna förordning.

Artikel 24 *Utvärdering*

Senast den [5 år från datumet för tillämpning av denna förordning] ska kommissionen göra en utvärdering av förordningen och lägga fram en rapport till Europaparlamentet och rådet om tillämpningen av denna förordning, inklusive en bedömning av behovet av att utvidga dess tillämpningsområde. Rapporten ska vid behov åtföljas av lagstiftningsförslag. Utvärderingen

⁵⁰ EUT L 123, 12.5.2016, s. 13.

⁵¹ Rådets beslut 2008/976/RIF av den 16 december 2008 om det europeiska rättsliga nätverket (EUT L 348, 24.12.2008, s. 130).

ska genomföras enligt kommissionens riktlinjer om bättre lagstiftning. Medlemsstaterna ska förse kommissionen med de uppgifter som är nödvändiga för att utarbeta denna rapport.

Artikel 25
Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Den ska tillämpas från och med den [*sex månader efter ikraftträdandet*].

Denna förordning är till alla delar bindande och direkt tillämplig i medlemsstaterna i enlighet med fördragen.

Utfärdad i Bryssel den

På Europaparlamentets vägnar
Ordförande

På rådets vägnar
Ordförande