Yttrande nr 23/2018 över kommissionens förslag om europeiska utlämnandeorder och bevarandeorder för elektroniska bevis i straffrättsliga förfaranden (artikel 70.1 b)

Antaget den 26 september 2018

Innehåll

Inledning ... 3

1. Rättslig grund för förslaget till förordning (artikel 82 i EUF-fördraget) ... 4

2. Behovet av e-bevisning jämfört med avtal om ömsesidig rättslig hjälp och en europeisk utredningsorder ... 5

   a) Behovet av e-bevisning jämfört med de skyddsåtgärder som föreskrivs i direktivet om en europeisk utredningsorder och avtal om ömsesidig rättslig hjälp ... 5

   b) Avskaffandet av principen om dubbel straffbarhet ... 6

   c) Konsekvenser av att rikta sig direkt till företagen ... 7

3. Den nya behörighetsgrunden och platskriteriernas så kallade försvinnande ... 8

4. Begreppet ”tjänsteleverantörer” bör begränsas eller kompletteras med ytterligare garantier för de registrerades rättigheter ... 9

5. Begreppen ”verksamhetsställe” och ”rättslig företrädare” i samband med dessa förslag bör vara klart åtskilda från dessa begrepp inom ramen för den allmänna dataskyddsförordningen ... 11

   a) Verksamhetsställe ... 11

   b) Rättslig företrädare ... 11

6. Nya uppgiftskategorier ... 12

7. Analys av förfarandena för europeiska utlämnandeorder och bevarandeorder ... 13

   a) Trösklarna för utfärdande av order bör höjas och order ska utfärdas eller godkännas av domstolar ... 14

   b) Tidsfrister för utlämnande av uppgifter ska motiveras ... 16

   c) Europeiska utlämnandeorder och bevarandeorder får inte användas för att begära uppgifter om en registrerad i en annan medlemsstat utan att åtminstone informera de behöriga myndigheterna i den medlemsstaten, särskilt när det gäller innehållsdata ... 16

   d) Europeiska bevarandeorder får inte användas för att kringgå tjänsteleverantörernas lagringsskyldigheter ... 17

   e) Sekretess och användarinformation ... 17

   f) Förfarande för verkställighet av en order när tjänsteleverantören vägrar att verkställa den ... 18

   g) Verkställighet av order och motstridiga skyldigheter enligt lagstiftningen i tredjeländer (artiklarna 15–16) ... 18

   h) Säkerhet vid överföring av uppgifter när en order besvaras ... 20

Slutsatser ... 20

Europeiska dataskyddsstyrelsen

har med beaktande av artikel 70.1 b i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG

ANTAGIT FÖLJANDE YTTRANDE:

Inledning

I april 2018 lade kommissionen fram ett förslag till förordning om europeiska utlämnandeorder och bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och ett förslag till direktiv om fastställande av harmoniserade bestämmelser för utseende av rättsliga företrädare för insamling av bevisning i straffrättsliga förfaranden. De två förslagen COM(2018) 225 final och COM(2018) 226 final kompletterar varandra. Den övergripande målsättningen är att förbättra samarbetet mellan medlemsstaternas myndigheter och tjänsteleverantörer, inklusive sådana som är baserade i länder utanför EU, och att föreslå lösningar på problemet med att fastställa och verkställa jurisdiktion i cyberrymden.

I förslaget till förordning fastställs regler och förfaranden för att utfärda, delge och verkställa bevarandeorder och utlämnandeorder för leverantörer av elektroniska kommunikationstjänster, och i förslaget till direktiv föreskrivs minimiregler för utseendet av en rättslig företrädare för tjänsteleverantörer som inte är etablerade i EU.

I november 2017[1] påminde artikel 29-gruppen, innan kommissionen hade lagt fram några utkast till förslag, om nödvändigheten av att se till att alla lagförslag till fullo följer EU:s befintliga regelverk för dataskydd i synnerhet, samt EU:s lagstiftning och rättspraxis i allmänhet.

Artikel 29-gruppen varnade särskilt för begränsningar av rätten till uppgiftsskydd och integritet när det gäller uppgifter som behandlas av leverantörer av telekomtjänster och informationssamhällets tjänster, särskilt när de behandlas ytterligare av de brottsbekämpande myndigheterna, påminde om behovet av att säkerställa att alla EU:s instrument överensstämmer med Europarådets befintliga Budapestkonvention om it-brottslighet och med EU:s direktiv om en europeisk utredningsorder, och rekommenderade ett förtydligande av förfaranderegleрna för tillgång till e-bevisning på nationell nivå och EU-nivå för att se till att det nya instrumentet inte ger myndigheterna nya befogenheter de inte skulle ha internt. Utöver dessa allmänna anmärkningar yttrade sig artikel 29-gruppen om de lagstiftningsalternativ som kommissionen vid den tidpunkten övervägde avseende berörda datakategorier och motsvarande garantier för att få tillgång till dem, om möjligheten att rikta utlämnandeorder/framställningar till tjänsteleverantörer för att ålägga dem att tillhandahålla uppgifter utanför EU, och om de materiella och formella villkor som krävs som garantier vid direkt tillgång till uppgifter.

Eftersom de konkreta förslagen om e-bevisning nu har lagts fram vill Europeiska dataskyddsstyrelsen presentera en mer detaljerad analys av de föreslagna rättsliga instrumenten från dataskyddssynpunkt.

[1] Se artikel 29-gruppens yttrande (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801).

1. Rättslig grund för förslaget till förordning (artikel 82 i EUF-fördraget)

Den rättsliga grunden för förslaget till förordning om e-bevisning är artikel 82.1 i EUF-fördraget, som rör straffrättsligt samarbete. Den har följande lydelse:

> 1. Det straffrättsliga samarbetet inom unionen ska bygga på principen om ömsesidigt erkännande av domar och rättsliga avgöranden och inbegripa en tillnärmning av medlemsstaternas lagar och andra författningar på de områden som avses i punkt 2 och artikel 83.
>
> Europaparlamentet och rådet ska i enlighet med det ordinarie lagstiftningsförfarandet besluta om åtgärder för att
>
> a) fastställa regler och förfaranden för att säkerställa att alla former av domar och rättsliga avgöranden erkänns i hela unionen,
>
> b) förebygga och lösa behörighetskonflikter mellan medlemsstaterna,
>
> c) stödja utbildningen av domare och övrig personal inom rättsväsendet,
>
> d) underlätta samarbetet mellan rättsliga eller likvärdiga myndigheter i medlemsstaterna inom ramen för lagföring och verkställighet av beslut.

Som kommissionen betonar i den konsekvensbedömning som åtföljer förslagen anges det i artikel 82.1 att det straffrättsliga samarbetet ska bygga på principen om ömsesidigt erkännande. Denna rättsliga grund skulle omfatta eventuell lagstiftning om direkt samarbete med tjänsteleverantörer, då myndigheten i den utfärdande medlemsstaten skulle vända sig direkt till ett företag (tjänsteleverantören) i den verkställande staten och även ålägga den skyldigheter. Detta skulle ge det ömsesidiga erkännandet en ny dimension utöver det traditionella rättsliga samarbetet i unionen, som hittills har byggt på förfaranden med två rättsliga myndigheter, en i den utfärdande staten och en i den verkställande staten.

Med tanke på att denna rättsliga grund inte har använts tidigare inom ramen för direkta framställningar mellan offentliga myndigheter och privata aktörer beklagar Europeiska dataskyddsstyrelsen att kommissionen inte har gjort någon ytterligare analys eller bedömning.

Som redan har framhållits i arbetsgruppens tidigare yttrande understryker fortfarande Europeiska dataskyddsstyrelsen att den inte är säker på att denna rättsliga grund är lämplig, vilket stöds av EU-domstolens och dess generaladvokats analys i yttrande nr 1/15. När det gäller artikel 82 som rättslig grund för utkastet till avtal om passageraruppgifter mellan EU och Kanada underströk EU-domstolen att den behöriga kanadensiska myndigheten inte utgör en rättslig myndighet och inte heller utgör en likvärdig myndighet[2]. I samband med förslagen om e-bevisning tycks ett av huvudmålen enligt kommissionen vara att undvika ”alltför besvärligt” rättsligt samarbete. Förslaget bygger följaktligen på principen att samarbete bör ske mellan en myndighet och en tjänsteleverantör i stället för mellan två myndigheter. Det planerade förfarandet gör framför allt att privata enheter kan vara den mottagande parten och besvara framställningar från rättsliga myndigheter.

[2] Se punkt 103 i yttrande nr 1/15 och punkt 108 i generaladvokatens yttrande i detta ärende.

Europeiska dataskyddsstyrelsen noterar att processen för att verkställa utlämnandeorder eller bevarandeorder kan innebära medverkan av en mottagande myndighet när den mottagande tjänsteleverantören inte fullgör sina skyldigheter, vilket gör det nödvändigt att begära verkställighet av ordern i efterhand. Eftersom det främsta syftet med det förfarande som införts just är att inte anlita en mottagande myndighet betvivlar dock Europeiska dataskyddsstyrelsen att detta kompletterande förfarande skulle kunna motivera användningen av artikel 82 som enda rättsliga grund för instrumentet.

För att artikel 82 ska kunna användas som rättslig grund anser därför Europeiska dataskyddsstyrelsen att de viktigaste stegen i samarbetet ska äga rum mellan två rättsliga myndigheter och att en annan rättslig grund bör användas för denna typ av samarbete.

2. Behovet av e-bevisning jämfört med avtal om ömsesidig rättslig hjälp och en europeisk utredningsorder

Europeiska dataskyddsstyrelsen noterar att kommissionen har åtagit sig att se över hinder för brottsutredningar, framför allt i fråga om tillgång till elektroniska bevis. I sin motivering beskriver kommissionen förslagets sammanhang och betonar de elektroniska bevisens flyktiga karaktär, deras internationella dimension samt behovet av att anpassa samarbetsmekanismen till den digitala tidsåldern. Förslagen till en förordning och ett direktiv för överföring av och tillgång till elektroniska bevis syftar inte till att ersätta tidigare instrument för samarbete i straffrättsliga frågor, såsom Budapestkonventionen, avtal om ömsesidig rättslig hjälp och direktivet om en europeisk utredningsorder. Enligt kommissionen syftar förslagen om e-bevisning till att förbättra det straffrättsliga samarbetet mellan myndigheter och tjänsteleverantörer inom EU och med tredjeländer, särskilt Förenta staterna.

Eftersom dessa nya verktyg kommer att vara specifikt avsedda för tillgång till och överföring av elektroniska bevis ska Europeiska dataskyddsstyrelsen bedöma mervärdet av instrumenten i förhållande till direktivet om en europeisk utredningsorder och avtal om ömsesidig rättslig hjälp.

a) Behovet av e-bevisning jämfört med de skyddsåtgärder som föreskrivs i direktivet om en europeisk utredningsorder och avtal om ömsesidig rättslig hjälp

Kommissionens viktigaste argument för förslagen om e-bevisning är att det påskyndar arbetet med att säkra och inhämta bevis i elektronisk form som lagras och/eller som innehas av tjänsteleverantörer i en annan jurisdiktion.

Europeiska dataskyddsstyrelsen beklagar dock att behovet av ett nytt instrument för tillgång till elektroniska bevis inte påvisades i konsekvensbedömningen. Det påvisas inte i förslagen att andra, mindre inkräktande medel inte hade kunnat användas för att uppnå målet med förslaget om e-bevisning, medan alternativa lösningar kunde ha övervägts. Exempelvis skulle möjligheten att ändra och förbättra direktivet om en europeisk utredningsorder ha kunnat undersökas och skulle även ha tillgodosett det särskilda kravet enligt direktivet om en europeisk utredningsorder om att utvärdera behovet av att ändra texten senast den 21 maj 2019[3]. En annan möjlighet skulle ha varit att föreskriva användning av bevarandeorder för att frysa uppgifterna under den tid en formell begäran

[3] Se artikel 37 i direktivet om en europeisk utredningsorder.

på grundval av ett avtal om ömsesidig rättslig hjälp utfärdas. Dessa alternativ skulle ha gjort det möjligt att bibehålla de skyddsåtgärder som föreskrivs i dessa instrument och samtidigt se till att de berörda personuppgifterna inte raderas.

Europeiska dataskyddsstyrelsen noterar att de tidsfrister som fastställs i direktivet om en europeisk utredningsorder är längre än i förslaget om e-bevisning. Den verkställande myndigheten har 30 dagar på sig att fatta beslut om erkännande av begäran[4] och ska därefter verkställa ordern inom 90 dagar[5]. Europeiska dataskyddsstyrelsen anser att det är en mycket viktig skyddsåtgärd att tillåta 30 dagars betänketid för de verkställande myndigheterna i den europeiska utredningsordern, vilket gör att de kan bedöma om begäran om verkställighet är välgrundad och om alla villkor för utfärdande och översändande av en utredningsorder är uppfyllda[6].

Europeiska dataskyddsstyrelsen är oroad över att den tidsfrist på tio dagar som föreslås i förslagen om e-bevisning för att verkställa intyget om en europeisk utlämnandeorder (EPOC), utan någon tid för eftertanke, hindrar en korrekt bedömning av huruvida intyget uppfyller samtliga kriterier och är rätt ifylld.

Därför rekommenderar Europeiska dataskyddsstyrelsen att mottagaren av intyget får mer tid på sig att avgöra huruvida ordern ska verkställas eller inte.

När det gäller intyg om en europeisk bevarandeorder (EPOC-PR) noterar Europeiska dataskyddsstyrelsen att det inte finns någon garanti för att bevarandet begränsas till sådana uppgifter som är nödvändiga att lämna ut. Tiden för bevarandet av uppgifter kan överstiga 60 dagar, eftersom den utfärdande myndigheten inte har någon tidsfrist för att underrätta adressaten om att avstå från att utfärda eller återkalla en utlämnandeorder. Därför rekommenderar Europeiska dataskyddsstyrelsen åtminstone att den utfärdande myndigheten har en tidsfrist för att inte bevilja eller återkalla utlämnandeordern, i linje med principen om uppgiftsminimering i den allmänna dataskyddsförordningen[7].

Slutligen konstaterar Europeiska dataskyddsstyrelsen att det i direktivet om en europeisk utredningsorder fastställs att den utfärdande staten kan vara tvungen att återlämna bevis till den verkställande myndigheten[8]. I förslaget till förordning om e-bevisning nämns dock inte denna möjlighet. Vad som händer med de elektroniska bevisen efter att de överlämnas till den utfärdande myndigheten är oklart.

Därför rekommenderar Europeiska dataskyddsstyrelsen att förslaget till förordning ger mer information om användningen av elektroniska bevis efter överlämnandet till den utfärdande myndigheten, för att följa den allmänna dataskyddsförordningen och principen om öppenhet[9] samt principen om specificitet enligt avtalen om ömsesidig rättslig hjälp.

b) Avskaffandet av principen om dubbel straffbarhet

Europeiska dataskyddsstyrelsen inser att ömsesidigt erkännande är beroende av tillämpningen av dubbel straffbarhet, som gör det möjligt för medlemsstaterna att behålla sin suveränitet. Dubbel straffbarhet ses dock i allt högre grad som ett hinder för ett smidigt rättsligt samarbete. EU:s

[4] Artikel 12.3 i direktivet om en europeisk utredningsorder.
[5] Artikel 12.4 i direktivet om en europeisk utredningsorder.
[6] Artikel 6 i direktivet om en europeisk utredningsorder.
[7] Artikel 5.1 c i den allmänna dataskyddsförordningen.
[8] Artikel 13.3 och 13.4 i direktivet om en europeisk utredningsorder.
[9] Artikel 5.1 a i den allmänna dataskyddsförordningen.

medlemsstater är alltmer samarbetsbenägna även om utredningsåtgärderna avser handlingar som inte betraktas som ett brott i deras nationella rätt. Europeiska dataskyddsstyrelsen påminner dock om att syftet med principen om dubbel straffbarhet är att ge en ytterligare garanti för att en stat inte kan förlita sig på hjälpen från en annan stat i tillämpningen av en straffrättslig påföljd som inte finns i den andra medlemsstatens lagstiftning. Detta skulle till exempel hindra en stat från att kräva hjälp av en annan stat för att fängsla någon på grund av personens politiska åsikter, om dessa åsikter inte är ett brott i den anmodade staten, eller åtala någon för abort, om denna person är bosatt i en annan medlemsstat där det inte är olagligt. Principen om dubbel straffbarhet åtföljs ofta även av ytterligare begränsningar eller garantier i fråga om påföljder, om dessa skiljer sig alltför mycket åt mellan den anmodande och den verkställande staten. Det främsta exemplet är åtagandet att inte tillämpa dödsstraff i vissa avtal om ömsesidig rättslig hjälp när det inte finns i en av de två parternas lagstiftning.

Europeiska dataskyddsstyrelsen noterar att principen om dubbel straffbarhet utesluts i förslaget till förordning om e-bevisning. Det leder dock inte endast till att sedvanliga formaliteter för ömsesidigt erkännande stryks, utan även till att skyddsåtgärder kopplade till principen om dubbel straffbarhet i sig tas bort.

Europeiska dataskyddsstyrelsen konstaterar att det inte hänvisas till rätten i det land där den anmodade tjänsteleverantören är etablerad, och att order om bevarande av uppgifter samt utlämnande av abonnent- eller åtkomstdata får utfärdas för alla brott[10], oavsett om liknande brott betraktas som sådana i andra medlemsstater.

Utlämnandeorder får endast utfärdas och verkställas om en liknande åtgärd finns tillgänglig för samma brott i en jämförbar inhemsk situation i den utfärdande staten[11]. Som kommissionen förklarar i motiveringen till förslaget till förordning anses dessutom transaktionsuppgifter och innehållsdata vara mer känsliga. Order om transaktionsuppgifter eller innehållsdata får endast utfärdas för brott som är belagda med ett maximalt frihetsstraff på minst 3 år, för att säkerställa respekt för proportionalitetsprincipen och de berörda personernas rättigheter[12]. Europeiska dataskyddsstyrelsen understryker dock att ingen harmonisering inom EU ännu har ägt rum för brott som är belagda med ett maximalt frihetsstraff på minst 3 år.

Europeiska dataskyddsstyrelsen motsätter sig avskaffandet av principen om dubbel straffbarhet, som syftar till att säkerställa att en stat inte kan förlita sig på andras hjälp för att dess nationella straffrätt ska tillämpas utanför statens territorium av en stat som inte har samma förhållningssätt, särskilt med tanke på bortfallet av andra traditionella viktiga garantier på det straffrättsliga området (se punkt 3 om platskriterier och punkt 7 g om potentiella konflikter med tredjeländers lagstiftning).

c) Konsekvenser av att rikta sig direkt till företagen

Europeiska dataskyddsstyrelsen medger att elektroniska bevis allt oftare finns tillgängliga på privat infrastruktur och kan vara placerade utanför det utredande landet, hos tjänsteleverantörerna.

I kölvattnet efter besluten i Yahoo[13]!- och Skype[14]-målen i Belgien och mot bakgrund av terroristattackerna noterar Europeiska dataskyddsstyrelsen att det krävs ett smidigare och snabbare

[10] Artikel 5.3 och artikel 6.2 i den föreslagna förordningen om e-bevisning.
[11] Artikel 5.2 i den föreslagna förordningen om e-bevisning.
[12] Artikel 5.4 a i den föreslagna förordningen om e-bevisning.
[13] Hof van Cassatie i Belgien, YAHOO! Inc., nr P.13.2082.N av den 1 december 2015.
[14] Correctionele rechtbank van Antwerpen, afdeling Mechelen, Belgien, ME20.F1.105151-12 av den 27 oktober 2016 (Skype har överklagat beslutet).

samarbete mellan offentliga och privata enheter. I konsekvensbedömningen hänvisar kommissionen till tre typer av processuella instrument som omfattar både offentliga myndigheter och tjänsteleverantörer. Dessa är rättsligt samarbete, direkt samarbete och direkt tillgång. I det första fallet läggs inte ansvaret för att verkställa den europeiska utredningsordern på tjänsteleverantören, utan på den verkställande myndigheten[15], men det andra, direkt samarbete, bygger på tjänsteleverantörens samarbete. Ur tjänsteleverantörens perspektiv är det mest inkräktande direkt tillgång, eftersom de offentliga myndigheterna kan få tillgång till uppgifter utan hjälp av en mellanhand.

Därför befarar Europeiska dataskyddsstyrelsen att tjänsteleverantörerna, när de kontaktas direkt, inte kommer att säkerställa skyddet av personuppgifter lika effektivt som de offentliga myndigheterna har möjlighet och skyldighet att göra, och betonar att det också leder till att vissa processuella garantier inom ramen för det rättsliga samarbetet för enskilda personer och för företagen själva inte kan tillämpas[16]. En anmodad tjänsteleverantör skulle exempelvis behöva gå till domstol i en annan (medlems)stat för att bestrida ordern, medan den i samband med rättsligt samarbete skulle möta sina egna myndigheter. Europeiska dataskyddsstyrelsen rekommenderar att ytterligare garantier införs i förslaget till förordning för tjänsteleverantörernas skydd av enskildas grundläggande rättigheter, som skyddet av personuppgifter och respekten för privat- och familjeliv, samt att den behöriga dataskyddsmyndigheten underrättas för att se till att det finns möjlighet till kontroll.

3. Den nya behörighetsgrunden och platskriteriernas så kallade försvinnande

Europeiska dataskyddsstyrelsen noterar att kommissionen framhåller att en av de stora förändringarna med detta förslag är att platskriterierna har försvunnit och att behöriga myndigheter har möjlighet att begära bevarande och utlämnande av uppgifter, oavsett var dessa uppgifterna faktiskt lagras.

Ur ett dataskyddsperspektiv är det inget nytt att EU:s dataskyddslagstiftning gäller oavsett var personuppgifterna är lagrade. Huruvida den allmänna dataskyddsförordningen kan tillämpas beror antingen på om den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerade inom EU, eller om uppgifter som avser registrerade i unionen behandlas, även om den personuppgiftsansvarige eller personuppgiftsbiträdet inte är etablerade i EU[17], i vilket fall de också måste utse en rättslig företrädare i EU[18]. Ur ett dataskyddsperspektiv är det viktigt att notera att det utvidgade territoriella tillämpningsområdet syftar till att ge ett mer fullständigt skydd för registrerade i EU, oavsett var det företag som behandlar uppgifterna är etablerat.

Även om det kan vara en nyhet på det straffrättsliga området att platskriterierna har slopats, framstår detta därför inte som en stor förändring ur ett dataskyddsperspektiv. Dessutom konstaterar Europeiska dataskyddsstyrelsen också att det fortfarande finns en koppling till EU:s territorium, eftersom endast tjänsteleverantörer som erbjuder tjänster i unionen omfattas av förslagen, och det

[15] Artiklarna 10–16.

[16] Se även, ur ett internationellt dataskyddsperspektiv, arbetsdokumentet om standarder för dataskydd och personlig integritet vid gränsöverskridande framställningar om uppgifter i brottsbekämpningssyfte, Berlingruppen, 63:e sammanträdet, den 9–10 april 2018, Budapest (Ungern).

[17] Se artikel 3, särskilt 3.2.

[18] Se artikel 27.

faktum att framställningar endast kan användas i samband med brottsutredningar innebär att det finns en koppling till EU (antingen på grund av att brottet har begåtts inom en medlemsstats territorium eller på grund av att brottsoffret eller gärningsmannen var medborgare i en medlemsstat).

Om slopandet av platskriterierna nu ska tillämpas inom straffrätten är den viktigaste frågan för Europeiska dataskyddsstyrelsen hur man ska se till att en sådan utveckling inte är till skada för uppgiftsskyddet och de registrerades och de anmodade tjänsteleverantörernas straffrättsliga processuella rättigheter. Ur detta perspektiv medger Europeiska dataskyddsstyrelsen att rättssäkerhetsgarantierna inom EU åtminstone delvis har harmoniserats och måste tillhandahållas i enlighet med den europeiska konventionen om de mänskliga rättigheterna. Det kan således hävdas att slopandet av platskriterierna troligen har mer begränsade konsekvenser när bevisen begärs inom EU än när myndigheter från tredjeländer begär uppgifter från företag som är etablerade inom EU enligt de villkor som anges i förslaget till förordning om e-bevisning. Europeiska dataskyddsstyrelsen är särskilt oroad över att detta skulle kunna leda till mer problematiska situationer. I detta sammanhang kan myndigheter från ett tredjeland, där andra och potentiellt svagare rättssäkerhetsgarantier tillämpas på det straffrättsliga området, få tillgång till uppgifter som skulle vara skyddade av ytterligare garantier inom EU. Ur detta perspektiv påminner Europeiska dataskyddsstyrelsen om sina farhågor om dubbla måttstockar och en försvagning av de grundläggande rättigheterna när tjänsteleverantörer och registrerade inte omfattas av unionsrättens rättssäkerhetsgarantier, om framställningen kommer från en myndighet i ett tredjeland.

Eftersom denna nya grund för behörighet ”oavsett var uppgifterna är” kombineras med ett förfarande som främst bygger på direkta framställningar från behöriga myndigheter till tjänsteleverantörer, är Europeiska dataskyddsstyrelsen dessutom oroad över att dataskyddet kanske inte tillämpas av privata företag som mottar begäran och som inte är bundna av ett rättsligt instrument som ett avtal om ömsesidig rättslig hjälp, som traditionellt styr utbytet av uppgifter mellan rättsliga myndigheter och omfattar garantier. Särskilt i samband med avtal om ömsesidig rättslig hjälp innebär minsta dataskyddsgarantier exempelvis tystnadsplikt och principen om specificitet, som innebär att personuppgifterna inte kommer att behandlas i andra syften.

Europeiska dataskyddsstyrelsen påminner därför om att åtminstone det skydd som föreskrivs i direktiv (EU) 2016/680 ska tillämpas, inbegripet när det gäller uppgiftsöverföringar, särskilt artikel 39 i de fall tjänsteleverantören skulle vara etablerad i ett tredjeland utan ett beslut om adekvat skyddsnivå på detta område. Europeiska dataskyddsstyrelsen betonar särskilt att denna bestämmelse kräver att den behöriga dataskyddsmyndigheten i den utfärdande myndighetens medlemsstat underrättas och att överföringen dokumenteras, bl.a. när det gäller motiveringen av att en överföring till den behöriga myndigheten i tredjelandet inte är till någon nytta eller är olämplig.

4. Begreppet ”tjänsteleverantörer” bör begränsas eller kompletteras med ytterligare garantier för de registrerades rättigheter

När det gäller tjänsteleverantörer välkomnar Europeiska dataskyddsstyrelsen den breda definition som gör det möjligt att inbegripa både kommunikationstjänster och OTT-leverantörer, eftersom alla dessa tjänster är funktionsmässigt likvärdiga och de planerade åtgärderna därför kan ha en liknande inverkan på rätten till integritet och rätten till konfidentialitet vid kommunikation, vilket betonades i

artikel 29-gruppens yttrande och tidigare i yttrande nr 1/2017 över förslaget till en förordning om integritet och elektronisk kommunikation. Förslaget till förordning om elektroniska bevis omfattar tjänsteleverantörer som erbjuder elektroniska kommunikationstjänster enligt definitionen i artikel 2.4 i direktivet om inrättande av en europeisk kodex för elektronisk kommunikation, informationssamhällets tjänster enligt definitionen i artikel 1.1 b i direktiv (EU) 2015/1535, ”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”, eller tjänster för internetdomännamn och ip-numrering, ”såsom ip-adressleverantörer, domännamnsregister, domännamnsregistratorer samt relaterade integritets- och proxytjänster”[19].

En tjänsteleverantör i den mening som avses i förslaget till förordning är dock ”en fysisk eller juridisk person som tillhandahåller en eller flera av följande kategorier av tjänster”, så Europeiska dataskyddsstyrelsen befarar att detta instrument skulle kunna omfatta både personuppgiftsansvariga och personuppgiftsbiträden i den mening som avses i den allmänna dataskyddsförordningen. Eftersom ”erbjuda tjänster” enligt artikel 2.4 i förslaget till förordning omfattar både att göra det möjligt för juridiska och fysiska personer i en eller flera medlemsstater att använda de tjänster som anges, och att ha en väsentlig anknytning till den eller de medlemsstater som avses, omfattar detta verksamhet som utförs av ett personuppgiftsbiträde för en personuppgiftsansvarig, t.ex. lagring av uppgifter.

Därför befarar Europeiska dataskyddsstyrelsen att registrerades rättigheter skulle kunna kringgås om det saknas begränsningar för tjänsteleverantörer som agerar som personuppgiftsansvariga i den mening som avses i den allmänna dataskyddsförordningen, och utan någon särskild skyldighet för ett personuppgiftsbiträde att meddela den personuppgiftsansvarige när biträdet tar emot en utlämnandeorder eller bevarandeorder. Detta gäller särskilt eftersom de rättsliga myndigheterna i förslaget till förordning också uppmuntras att vid eventuella motstridiga skyldigheter, som hindrar adressaten att delge mottagna order, rikta sig till den lämpligaste aktören oavsett tillämpliga regler om uppgiftsskydd, särskilt med tanke på att vilka uppgifter som helst kan begäras, och inte endast personuppgifter som omfattas av den allmänna dataskyddsförordningen[20].

Enligt den allmänna dataskyddsförordningen agerar ett personuppgiftsbiträde endast enligt den personuppgiftsansvariges instruktioner. Därför är det den personuppgiftsansvariges ansvar att se till att de registrerades rättigheter respekteras, och att ge dem relevant information, inbegripet vad gäller mottagarna av deras uppgifter, exempelvis inom ramen för utövandet av rätten till tillgång. Personuppgiftsbiträdet kommer inte att ta emot dessa framställningar från registrerade och kommer inte att kunna svara, om detta inte uttryckligen begärs av den personuppgiftsansvarige.

Såvida inte deras rättigheter har begränsats genom tillämpning av den allmänna dataskyddsförordningen betonar följaktligen Europeiska dataskyddsstyrelsen att registrerade som omfattas av den allmänna dataskyddsförordningen inte kan utöva sina rättigheter på ett effektivt sätt om den personuppgiftsansvarige inte är i stånd att lämna fullständiga uppgifter. Europeiska dataskyddsstyrelsen noterar också att risken för att det saknas uppgifter är ännu högre utan någon särskild skyldighet för personuppgiftsbiträdet att informera den personuppgiftsansvarige när de begärda uppgifterna avser registrerade personer som inte åtnjuter skydd enligt den allmänna dataskyddsförordningen. De rättsliga myndigheter som begär uppgifterna är inte nödvändigtvis skyldiga att underrätta de registrerade om sin egen ytterligare behandling i detta fall. Europeiska

[19] Artikel 2.3 c i den föreslagna förordningen om e-bevisning.
[20] Se artikel 7.3 och 7.4.

dataskyddsstyrelsen efterlyser därför en begränsning av tillämpningsområdet till personuppgiftsansvariga i den mening som avses i den allmänna dataskyddsförordningen, eller en bestämmelse som klargör att tjänsteleverantören ska underrätta den personuppgiftsansvarige, om den tjänsteleverantör som kontaktas inte är personuppgiftsansvarig.

5. Begreppen ”verksamhetsställe” och ”rättslig företrädare” i samband med dessa förslag bör vara klart åtskilda från dessa begrepp inom ramen för den allmänna dataskyddsförordningen

Med tanke på att platskriterierna inte kan tillämpas när det gäller uppgifter är mottagarna av utlämnandeorder eller bevarandeorder inom ramen för den föreslagna förordningen begränsade till tjänsteleverantörer som erbjuder tjänster i unionen, oavsett om de är etablerade i EU eller ej, med skyldighet att utse en rättslig företrädare, enligt de bestämmelser som föreslås i förslaget till direktiv. Begreppen ”verksamhetsställe” och ”rättslig företrädare” definieras därför i utkasten till instrument.

Europeiska dataskyddsstyrelsen noterar att dessa begrepp även förekommer i samband med andra EU-instrument, särskilt i samband med den allmänna dataskyddsförordningen. Följaktligen måste definitionen och avgränsningen av dessa begrepp i utkasten till förslag och i den allmänna dataskyddsförordningen förtydligas.

a) Verksamhetsställe

Europeiska dataskyddsstyrelsen påminner också om att begreppet ”verksamhetsställe” i förslaget till förordning inte får förväxlas med samma begrepp i den allmänna dataskyddsförordningen. I förslaget till förordning är begreppet verksamhetsställe enligt definitionen i artikel 2.5 mer omfattande än i den allmänna dataskyddsförordningen, eftersom det omfattar ”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”, oavsett om behandlingen av personuppgifter sker inom ramen för denna verksamhet. Om ”verksamhetsställe” i den mening som avses i den allmänna dataskyddsförordningen utan tvekan skulle omfattas av begreppet verksamhetsställe i förslaget till förordning, kan det hända att motsatsen inte är fallet.

Europeiska dataskyddsstyrelsen uppmärksammar därför att villkoren för tillämpning av den allmänna dataskyddsförordningen enligt artikel 3.1 inte nödvändigtvis måste vara uppfyllda för tjänsteleverantörers verksamhetsställen i den mening som avses i förslaget till förordning. I detta sammanhang uppmanas därför personuppgiftsansvariga och personuppgiftsbiträden att kontrollera om den allmänna dataskyddsförordningens tillämplighet inte härrör från artikel 3.2, vilket skulle innebära att en rättslig företrädare utses i EU och att en gemensam kontaktpunkt saknas.

b) Rättslig företrädare

I sitt yttrande betonade artikel 29-gruppen att all sammanblandning bör undvikas mellan skyldigheten att utse en rättslig företrädare enligt artikel 27 i den allmänna dataskyddsförordningen och den rättsliga företrädare som avses i förslaget till förordning om e-bevisning.

Med hänsyn till utkastet till förslag skulle Europeiska dataskyddsstyrelsen vilja påminna om dessa rekommendationer, och särskilt understryka att den rättsliga företrädaren i den mening som avses i

förslaget till direktiv om utseende av rättsliga företrädare inom ramen för förslagen om e-bevisning ska utses under alla förhållanden, ha särskilda funktioner, oberoende av ett uppdrag från tjänsteleverantören, ha befogenhet att besvara framställningar och att agera för tjänsteleverantörens räkning och ha ett större ansvar än den rättsliga företrädaren i den allmänna dataskyddsförordningen.

Europeiska dataskyddsstyrelsen betonar dessutom att skyldigheten att under alla förhållanden utse en rättslig företrädare enligt utkasten till förslag om e-bevisning, oavsett om tjänsteleverantören är etablerad i EU eller inte, möjligheten att utse flera rättsliga företrädare för samma tjänsteleverantör enligt förslaget till direktiv om e-bevisning, och skyldigheten att anmäla utseendet av den rättsliga företrädaren till medlemsstaternas myndigheter skiljer sig från den allmänna dataskyddsförordningen, i vilken det inte föreskrivs någon skyldighet att anmäla en utsedd rättslig företrädare, undantag från utseendet och begränsat ansvar för den rättsliga företrädaren.

Med tanke på de viktiga skillnaderna i fråga om uppgifter, ansvar och förhållande till tjänsteleverantörens övriga verksamhetsställen, i det ena fallet, och personuppgiftsansvarig eller personuppgiftsbiträde, i det andra, rekommenderar Europeiska dataskyddsstyrelsen därför, då tjänsteleverantören inte är etablerad i EU men omfattas av både den allmänna dataskyddsförordningen enligt artikel 3.2 och förordningen om e-bevisning, att två olika rättsliga företrädare utses, med tydligt skilda funktioner beroende på vilket instrument som är grundvalen.

6. Nya uppgiftskategorier

I den föreslagna förordningen anges olika uppgiftskategorier i artikel 2: abonnentuppgifter, åtkomstuppgifter, transaktionsuppgifter och innehållsdata. I skäl 20 i kommissionens förslag anges dessutom följande: *”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.”*

I detta sammanhang betonar Europeiska dataskyddsstyrelsen att alla fyra kategorier av uppgifter som nämns ovan ska betraktas som personuppgifter enligt EU:s dataskyddslagstiftning, eftersom de innehåller information som rör en identifierad eller identifierbar fysisk person, oavsett om den registrerade kallas ”abonnent” eller ”användare” i den föreslagna förordningen. Det bör även noteras att ”elektroniska bevis” enligt definitionen i artikel 2.6 i kommissionens förslag omfattar alla fyra kategorier av uppgifter och därför rör personuppgifter. I förslaget till förordning föreskrivs därför inte regler för tillgång till bevisning, som definieras och kvalificeras enligt nationell lagstiftning och rättsliga förfaranden, utan snarare nya materiella och formella villkor för tillgången till personuppgifter.

I förslaget till förordning fastställs nya underkategorier av personuppgifter för vilka olika villkor för tillgång tillämpas, men Europeiska dataskyddsstyrelsen påminner om att det enligt tillämplig rättspraxis EU-domstolen har föga betydelse om uppgifterna om privatlivet är känsliga eller om de berörda har fått utstå eventuella olägenheter på något sätt, när det fastställs att det föreligger ett ingrepp i den grundläggande rätten till respekt för privatlivet.

I förhållande till ”icke-innehållsdata”, som enligt kommissionens förslag omfattar abonnentuppgifter, åtkomstuppgifter och transaktionsuppgifter, påminner dessutom Europeiska dataskyddsstyrelsen om att EU-domstolen i sin dom i de förenade målen C-203/15 och C-698/15, Tele2 Sverige AB, slog fast att metadata, t.ex. trafik- och lokaliseringsuppgifter, gör det möjligt att kartlägga de berörda personerna på ett sätt som är minst lika känsligt från integritetssynpunkt som själva innehållet i kommunikationen[21].

I linje med artikel 29-gruppens yttrande om dataskydd och integritet i gränsöverskridande tillgång till elektroniska bevis av den 29 november 2017 upprepar därför Europeiska dataskyddsstyrelsen sina tvivel och farhågor när det gäller den nuvarande uppdelningen mellan ”icke-innehållsdata” och innehållsdata, samt när det gäller de fyra kategorier av personuppgifter som fastställs i den föreslagna förordningen. De fyra föreslagna kategorierna tycks inte vara tydligt avgränsade, och definitionen av ”åtkomstuppgifter” är fortfarande vag jämfört med övriga kategorier. Europeiska dataskyddsstyrelsen beklagar därför att den logiska grunden för införandet av dessa nya underkategorier av personuppgifter inte underbyggs ytterligare i kommissionens konsekvensbedömning och förslaget, och uttrycker sin oro när det gäller de olika garantierna som rör materiella och formella villkor för tillgång till kategorier av personuppgifter, särskilt med tanke på de praktiska svårigheterna med att utvärdera till vilken uppgiftskategori de begärda uppgifterna ska hänföras i vissa fall. Exempelvis kan IP-adresser betecknas både som transaktionsuppgifter och som abonnentuppgifter.

I detta sammanhang påminner Europeiska dataskyddsstyrelsen också om att kommissionen, i skäl 14 i sitt förslag till förordning om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation (e-integritet), anger följande: ”Data från elektronisk kommunikation bör definieras på ett tillräckligt brett och teknikneutralt sätt, så att begreppet omfattar all information om det innehåll som överförs eller utbyts (elektroniskt kommunikationsinnehåll) och information om slutanvändare av elektroniska kommunikationstjänster som behandlas i syfte att överföra, distribuera eller möjliggöra utbyte av elektroniskt kommunikationsinnehåll. Detta innefattar data för att spåra och identifiera meddelandets källa och adressat samt geografisk lokalisering, datum, varaktighet och typ av kommunikation.” Eftersom den nuvarande och framtida ramen om e-integritet, samt tillhörande begränsningar av rätten till privatliv, kommer att gälla för de regler som styr brottsbekämpande myndigheters tillgång till elektroniska bevis, rekommenderar Europeiska dataskyddsstyrelsen en allmännare definition av data från elektronisk kommunikation i den föreslagna förordningen för att säkerställa att lämpliga garantier och villkor för tillgång alltid omfattar både ”icke-innehållsdata” och ”innehållsdata”.

7. Analys av förfarandena för europeiska utlämnandeorder och bevarandeorder

I stort sett förefaller förfarandet för att hantera en utlämnandeorder eller bevarandeorder vara följande:

- Den behöriga rättsliga myndigheten – den utfärdande myndigheten – beroende på typ av begärda uppgifter och på typ av order, utfärdar ordern enligt de (fåtaliga) villkor som räknas upp i artiklarna 5 och 6 och skickar det med hjälp av ett harmoniserat intyg till

[21] EU-domstolens dom av den 21 december 2016, punkt 99.

tjänsteleverantörens rättsliga företrädare eller till något av dess verksamhetsställen i EU – adressaten.

- När intyget har tagits emot ska adressaten verkställa ordern – vilket innebär att uppgifterna ska översändas inom tio dagar eller sex timmar i nödsituationer, eller bevara dem i upp till 60 dagar – såvida inte detta är omöjligt på grund av att intyget är ofullständigt eller på grund av force majeure eller faktisk omöjlighet för adressaten, eller på grund av att adressaten vägrar med hänvisning till motstridiga skyldigheter, antingen på grundval av grundläggande rättigheter eller ett tredjelands grundläggande intressen eller på andra grunder.
- Om adressaten utan motivering som godtas av den utfärdande myndigheten inte har följt den mottagna ordern, finns det förfaranden för verkställande av order av en behörig verkställande myndighet i den medlemsstat där tjänsteleverantören är företrädd eller etablerad, såvida inte begränsade skäl för vägran är tillämpliga och den verkställande myndigheten invänder mot erkännandet eller verkställandet av ordern.
- Om adressaten utfärdar en motiverad invändning mot ordern på grund av motstridiga skyldigheter ska den utfärdande myndigheten hänskjuta ärendet till den behöriga domstolen i sin medlemsstat, som sedan ska ansvara för bedömningen av den eventuella motstridigheten och för att upprätthålla ordern i avsaknad av en motstridighet. Vid en motstridighet ska den behöriga domstolen antingen vända sig till tredjelandets centrala myndigheter via sina nationella centrala myndigheter, med 15 dagars tidsfrist för svar, vilket kan förlängas med 30 dagar efter en motiverad begäran, i händelse av motstridiga skyldigheter på grundval av grundläggande rättigheter eller ett tredjelands grundläggande intressen, eller själv avgöra huruvida ordern ska upprätthållas eller återkallas på andra grunder för vägran som åberopas av adressaten.
- Utan att det påverkar tillämpningen av tillgängliga rättsmedel enligt den allmänna dataskyddsförordningen och brottsbekämpningsdirektivet ska personer vars uppgifter har erhållits genom en utlämnandeorder även ha rätt till effektiva rättsmedel mot denna order.

Europeiska dataskyddsstyrelsen har bedömt de förfaranden och skyddsåtgärder som föreskrivs i förslaget till förordning med avseende på de olika stegen, och för var och en av de aspekter som tas upp nedan rekommenderar den följande skyddsåtgärder och ändringar.

a) Trösklarna för utfärdande av order bör höjas och order ska utfärdas eller godkännas av domstolar

Vad gäller villkoren för utfärdande av order välkomnar Europeiska dataskyddsstyrelsen principen om starkare skyddsåtgärder för tillgång till transaktionsuppgifter eller innehållsdata. Med tanke på att det saknas en fullständig harmonisering av de straffrättsliga påföljderna mellan medlemsstaterna konstaterar den dock att hänvisningen till ”brott för vilka maximistraffet i den utfärdande staten är fängelse i minst 3 år”[22] fortfarande medför olika trösklar och skillnader i skyddet av registrerades personuppgifter i EU.

Dessutom betonar Europeiska dataskyddsstyrelsen, särskilt med tanke på den allmänna definitionen av abonnentuppgifter, att tröskeln verkar ganska låg för bevarandeorder och för utlämnandeorder om abonnent- eller åtkomstuppgifter, eftersom alla brott i princip kan motivera sådana order. Färre

[22] Se artikel 5.3 a.

myndigheter har rätt att utfärda order om utlämnande av transaktionsuppgifter eller innehållsdata än att utfärda order om bevarande eller utlämnande av abonnent- eller åtkomstuppgifter, eftersom åklagare endast kan utfärda eller godkänna sistnämnda order, medan domare, domstolar eller undersökningsdomare kan utfärda eller godkänna alla order.

Europeiska dataskyddsstyrelsen beklagar särskilt att den lägsta tröskeln för att brottsbekämpande myndigheter ska ha möjlighet att begära tillgång till abonnent- och åtkomstuppgifter för alla brott bygger på en motsatsvis tolkning av EU-domstolens rättspraxis (som är inriktad på de andra uppgifterna) för att göra skillnad mellan skyddsåtgärderna. När det gäller trafik- och lokaliseringsuppgifter betonade EU-domstolen särskilt att de behöriga myndigheternas tillgång enbart ska vara begränsad till bekämpning av grov brottslighet[23]. Europeiska dataskyddsstyrelsen kan förstå att förslaget, i avsaknad av förhandstillstånd från en domstol, skulle ge möjlighet att begära tillgång till mycket grundläggande information som endast gör det möjligt att identifiera en person utan att avslöja kommunikationsuppgifter. Den beklagar emellertid kommissionens allmänna motsatsvisa tolkning av detta beslut och efterlyser starkare skyddsåtgärder för att begränsa grunderna för tillgång till andra abonnentuppgifter och åtkomstuppgifter. Europeiska dataskyddsstyrelsen föreslår att tillgången till dessa uppgifter ska begränsas antingen till en förteckning över brott som anges i förslaget till förordning, eller åtminstone till ”grova brott”, särskilt med tanke på den lägre tröskeln för förhandstillstånd för dessa uppgifter.

Dessutom understryker Europeiska dataskyddsstyrelsen att denna motsatsvisa tolkning också leder till att förslaget gör det möjligt för åklagare att utfärda eller godkänna utfärdandet av order. Med undantag av framställningar om mycket grundläggande information som skulle göra det möjligt att identifiera en person utan att avslöja eventuella kommunikationsuppgifter anser Europeiska dataskyddsstyrelsen att detta utgör ett steg tillbaka jämfört med EU-domstolens rättspraxis om tillgång till kommunikationsuppgifter. I sin rättspraxis om tillgång till kommunikationsuppgifter för brottsbekämpande ändamål har EU-domstolen begränsat möjligheten till sådan tillgång, bland andra kriterier, och ”*utom i vederbörligen motiverade brådskande fall*”[24], till en ”*förhandskontroll utförd av en domstol eller en oberoende myndighet*”, ”*efter det att nämnda myndigheter framställt en motiverad ansökan inom ramen för ett förfarande för förebyggande, avslöjande eller lagföring av brott*”.[25]

Europeiska dataskyddsstyrelsen påminner om att begreppet ”domstol” är ett självständigt begrepp i unionsrätten och att EU-domstolen konsekvent har betonat och påmint om de kriterier som ska vara uppfyllda för att en domstol ska betraktas som en sådan, inbegripet kriterierna för oberoende[26], vilket inte förefaller vara fallet för åklagare, vilket även Europadomstolen påpekar i sin rättspraxis[27].

Följaktligen leder artiklarna 4.1 a och 4.1 b samt 3 a och 3 b till förfaranden där betydligt mindre garantier är tillämpliga för abonnent- och åtkomstuppgifter, eftersom en åklagare ensam kan begära uppgifter, utan någon ytterligare kontroll från myndigheten i den stat där de begärda uppgifterna är eller från myndigheten där den rättsliga företrädaren för det anmodade företaget kommer att vara, eller någon kontroll från en oberoende myndighet.

Dessutom noterar Europeiska dataskyddsstyrelsen den så kallade ytterligare skyddsåtgärd som föreskrivs i artikel 5.2, enligt vilken en utlämnandeorder endast får utfärdas om en liknande åtgärd

[23] Se mål C-203/15, punkt 125.
[24] Se mål C-203/15, punkt 120.
[25] Se de förenade målen C-293/12 och C-594/12, punkt 62.
[26] Se t.ex. mål C-203/14.
[27] Se t.ex. målet Moulin mot Frankrike, den 23 november 2010.

skulle finnas att tillgå för samma brott i en jämförbar inhemsk situation. Den varnar dock för den kontraproduktiva effekten av en sådan bestämmelse: snarare än att ge ytterligare skydd förefaller det uppmuntra medlemsstaterna att utvidga de nationella möjligheterna att begära ett utlämnande av abonnent- eller åtkomstuppgifter, för att se till att utlämnandeorder kan utfärdas enligt denna förordning.

b) Tidsfrister för utlämnande av uppgifter ska motiveras

Europeiska dataskyddsstyrelsen konstaterar att europeiska utlämnandeorder ska besvaras senast inom tio dagar efter mottagandet av intyget, såvida inte den utfärdande myndigheten anger skäl för att lämna ut uppgifterna tidigare, och senast inom sex timmar i nödsituationer, enligt vad som föreskrivs i artikel 9.1 och 9.2.

Europeiska dataskyddsstyrelsen har dock inte sett några kriterier för utformning av myndigheternas skyldighet att visa att det är brådskande att lägga fram uppgifterna, även i efterhand, för att möjliggöra en eventuell kontroll av användningen av detta mycket snabba förfarande, medan sex timmars tidsfrist sannolikt innebär en mycket lätt kontroll innan uppgifterna lämnas ut, eller till och med avsaknad av kontroll från tjänsteleverantörens sida. I konsekvensbedömningen betonas behovet av att behöriga myndigheter får tillgång till uppgifter i tid. De exempel som anges i konsekvensbedömningen rör dock i samtliga fall bevis som krävs vid grova brott (terroristdåd med gisslantagande, pågående sexuella övergrepp mot barn), men hänvisningen till bevisningens flyktiga karaktär tycks inte vara tillräcklig när det inte finns någon särskild brådskande anledning utöver denna potentiellt flyktiga karaktär hos uppgifterna. Dessutom ger uppgifternas flyktiga karaktär ingen ytterligare motivering till proportionaliteten i att få tillgång till uppgifter med lägre skyddsnivå i dessa situationer, när det inte finns någon annan brådskande anledning än uppgifternas flyktiga karaktär.

Dessutom betvivlar Europeiska dataskyddsstyrelsen att det krävs en tidsfrist på sex timmar, när denna tidsfrist inte skulle tillämpas förrän den utfärdande myndigheten ger ytterligare förtydliganden ”inom fem dagar” om tjänsteleverantören inte kan fullgöra sin skyldighet.

Europeiska dataskyddsstyrelsen efterlyser därför ytterligare inslag i konsekvensbedömningen för att motivera behovet av dessa tidsfrister i fall där det brott som begås eller beivras inte är grovt, och om inte sådana detaljerade inslag tillhandahålls, tydliga kriterier för att motivera brådskan om europeiska utlämnandeorder utfärdas. Exempelvis kan det vara tänkbart med samma modell som i direktivet om en europeisk utredningsorder. I direktivet om en europeisk utredningsorder föreskrivs en kortare tidsfrist när detta är berättigat ”på grund av tidsfrister i förfarandet, brottets svårhetsgrad eller andra särskilt brådskande omständigheter” (se artikel 12.2), eller en 24-timmars tidsfrist för beslut om provisoriska åtgärder (se artikel 32.2). I konsekvensbedömningen av förslaget till förordning föreskrivs inte detaljerade inslag som motiverar varför dessa tidsfrister inte är effektiva. De enda inslag som understryks är att antalet framställningar överbelastar de mottagande rättsliga myndigheterna, som inte kan iaktta tidsfristerna.

c) Europeiska utlämnandeorder och bevarandeorder får inte användas för att begära uppgifter om en registrerad i en annan medlemsstat utan att åtminstone informera de behöriga myndigheterna i den medlemsstaten, särskilt när det gäller innehållsdata

Europeiska dataskyddsstyrelsen påminner om att rättsligt samarbete och därmed ytterligare garantier föreskrivs i befintliga instrument, särskilt för att kontrollera framställningarnas nödvändighet och proportionalitet, och understryker att dessa garantier är desto mer berättigade då

de begärda uppgifterna är innehållsdata, som är förknippade med fler begränsningar av de registrerades rätt till skydd av sina personuppgifter och personliga integritet. I detta avseende påminner Europeiska dataskyddsstyrelsen om att direktivet om en europeisk utredningsorder även ger möjlighet att avlyssna telekommunikation med tekniskt bistånd av en annan medlemsstat (se artikel 30) och omfattar en skyldighet att informera den behöriga myndigheten i en annan medlemsstat från vilken bistånd inte behövs om avlyssning av data, när den berörda personen befinner sig eller kommer att befinna sig på den medlemsstatens territorium (se artikel 31).

Europeiska dataskyddsstyrelsen ser inga skäl till det förfarande som anges i förslaget till förordning om e-bevisning för att möjliggöra utlämnande av innehållsdata utan medverkan av åtminstone de behöriga myndigheterna i den medlemsstat där den registrerade befinner sig.

d) Europeiska bevarandeorder får inte användas för att kringgå tjänsteleverantörernas lagringsskyldigheter

Europeiska dataskyddsstyrelsen noterar att huvudsyftet med europeiska bevarandeorder är att förhindra radering av uppgifter.

Även om Europeiska dataskyddsstyrelsen medger att det kan vara nödvändigt och proportionellt i vissa fall beklagar den bristen på garantier i samband med utfärdandet av sådana order. När bevarandeorder endast avser vissa uppgifter, när förslaget verkar möjliggöra allmänna framställningar och när sådana order utfärdas för uppgifter som ska raderas i enlighet med datalagringsprincipen rekommenderar Europeiska dataskyddsstyrelsen särskilt att ordern aldrig får utgöra en grund för tjänsteleverantörens behandling av uppgifterna efter det första raderingsdatumet. Med andra ord bör uppgifterna vara ”frysta”.

Dessutom bör man stärka kopplingen mellan bevarandeordern och den efterföljande begäran om att uppgifter ska lämnas ut, antingen genom en europeisk utlämnandeorder, en begäran om en europeisk utredningsorder eller en begäran om ömsesidig rättslig hjälp, för att se till att europeiska bevarandeorder endast utfärdas när den andra begäran är säker (och inte bara övervägs som en möjlighet) och att bevarandeordern också upphör att gälla när den andra begäran avslås, utan att man ska behöva vänta i 60 dagar[28] om den efterföljande begäran avslås tidigare.

e) Sekretess och användarinformation

Europeiska dataskyddsstyrelsen noterar att en särskild artikel[29] om sekretess för order har införts i förslaget till förordning. För att undvika förvirring och missförstånd när det gäller rätten till dataskydd påminner Europeiska dataskyddsstyrelsen om att det i den allmänna dataskyddsförordningen visserligen föreskrivs att begränsningar av registrerades rättigheter för att säkerställa förebyggande, utredning, avslöjande eller lagföring av straffrättsliga sanktioner bör föreskrivas i lag och därför vara allmänt tillgängliga[30] och att dessa lagstiftningsåtgärder ska innehålla särskilda bestämmelser om de registrerades rätt att bli informerade om begränsningen, såvida detta inte kan inverka menligt på begränsningen[31], men att det inte föreskrivs någon skyldighet att individuellt informera registrerade om varje begäran om tillgång som görs av brottsbekämpande myndigheter.

[28] Se artikel 10.1.
[29] Se artikel 11.
[30] Se artikel 23.1 d.
[31] Se artikel 23.2 h.

Europeiska dataskyddsstyrelsen påminner dock om att dataskyddsdirektivet föreskriver denna rätt till information för registrerade från de behöriga myndigheterna själva, såvida inte denna rätt har begränsats, utan att begränsa denna rätt endast till registrerade som är bosatta på EU:s territorium.

f) Förfarande för verkställighet av en order när tjänsteleverantören vägrar att verkställa den

Europeiska dataskyddsstyrelsen noterar att det i artikel 14 i förslaget till förordning föreskrivs ett förfarande för att säkerställa verkställighet av en order om adressaten inte rättar sig efter den, genom ett rättsligt samarbete mellan den utfärdande myndigheten och en behörig myndighet i den verkställande staten.

Detta förfarande tycks dock inte göra det möjligt för den verkställande myndigheten att vägra att verkställa ordern på andra grunder än rent formella (samma som adressaten, framför allt vad gäller avsaknaden av uppgifter eller faktisk omöjlighet att tillhandahålla uppgifter), om de berörda uppgifterna skyddas av immunitet eller privilegier enligt nationell lagstiftning, eller om ett röjande av uppgifterna kan påverka grundläggande intressen såsom nationell säkerhet och försvar[32].

Europeiska dataskyddsstyrelsen upprepar därför sin oro när det gäller avlägsnandet av den verkställande behöriga myndighetens dubbelkontroll av den översända ordern, jämfört med övriga instrument. Även grunden för att vägra att verkställa en order med motiveringen att det skulle strida mot stadgan förefaller högre än den klassiska tröskeln avseende en kränkning av den berörda personens grundläggande rättigheter. I linje med den europeiska arresteringsordern, som föreskriver både obligatoriska och frivilliga grunder för vägran, eller åtminstone direktivet om en europeisk utredningsorder, i vilket det generellt föreskrivs att presumtionen enligt vilken "skapandet av ett område med frihet, säkerhet och rättvisa inom unionen är grundat på ömsesidigt förtroende och presumtionen om andra medlemsstaters efterlevnad av unionsrätten och, i synnerhet, respekt för de grundläggande rättigheterna" kan motbevisas[33], bör följaktligen förslaget till förordning åtminstone omfatta det minsta klassiska undantaget, nämligen att verkställigheten av en order bör vägras om det finns tungt vägande skäl att anta att verkställandet av ordern skulle leda till en kränkning av den berörda personens grundläggande rättigheter och att den verkställande staten skulle åsidosätta sina skyldigheter avseende det skydd av grundläggande rättigheter som erkänns i stadgan.

g) Verkställighet av order och motstridiga skyldigheter enligt lagstiftningen i tredjeländer (artiklarna 15–16)

Europeiska dataskyddsstyrelsen välkomnar att förslaget till förordning gör det möjligt för adressaterna att vägra att verkställa en order på grund av att det skulle strida mot grundläggande rättigheter, eftersom det syftar till att ge garantier i händelse av motstridiga skyldigheter. Den anser det också vara väsentligt att förslaget föreskriver samråd med tredjeländers myndigheter, åtminstone vid en motstridighet, samt skyldigheten att häva ordern när en tredjelandsmyndighet gör en invändning.

Därför bör förfarandet för att vägra att verkställa en order på grund av motstridiga skyldigheter enligt lagstiftningen i tredjeländer förbättras avsevärt.

För det första konstaterar Europeiska dataskyddsstyrelsen att ett privat företag, som mottagare av en utlämnandeorder, enligt förslaget till förordning ska bedöma huruvida denna order strider mot

[32] Se artikel 14.2.
[33] Se skäl 19 i direktivet om en europeisk utredningsorder.

tillämplig lagstiftning i ett tredjeland som förbjuder utlämnande av de begärda uppgifterna. Företaget måste lämna en motiverad invändning med all relevant information om tredjelandets lagstiftning, dess tillämpbarhet i det aktuella fallet och de motstridiga skyldigheternas karaktär.

Europeiska dataskyddsstyrelsen är oroad över att behörig domstol i den utfärdande myndighetens medlemsstat ensam ska bedöma huruvida en motstridighet föreligger eller inte vid en sådan invändning, eftersom det endast är om domstolen slår fast att en motstridighet föreligger som den ska ta kontakt med myndigheterna i tredjeland. Den behöriga EU-domstolen ges därför befogenhet att slutgiltigt tolka lagstiftningen i ett tredjeland i detta sammanhang, utan att vara särskilt specialiserad på sakinnehållet. Europeiska dataskyddsstyrelsen anser att skyldigheten att samråda med de behöriga myndigheterna i tredjelandet därför är alltför begränsad i det nuvarande förslaget. I fråga om dataskydd riktar Europeiska dataskyddsstyrelsen lagstiftarens uppmärksamhet på att om en behörig domstol i ett tredjeland skulle tolka den allmänna dataskyddsförordningen för att bedöma huruvida den strider mot de egna kraven, skulle EU:s dataskyddsmyndigheter och behöriga domstolar fortfarande vara behöriga att bedöma överföringens lagenlighet på grundval av domstolsbeslut eller beslut från myndigheter i ett tredjeland där det krävs överföring eller utlämnande av personuppgifter som omfattas av den allmänna dataskyddsförordningen[34].

Dessutom understryker Europeiska dataskyddsstyrelsen att bedömningen av tredjelandets lagstiftning av behörig domstol i den anmodande medlemsstaten måste grunda sig på objektiva faktorer, och oroas av de kriterier som den behöriga domstolen ska beakta vid bedömningen av lagstiftningen i tredjelandet enligt artiklarna 15.4 och 16.5 a i förslaget till förordning. Domstolen skulle behöva bedöma om lagstiftningen, ”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” eller ”det intresse som skyddas genom tredjelandets relevanta lagstiftning, inklusive tredjelandets intresse av att förhindra röjande av uppgifterna”. Även om bedömningen pga. all tillgänglig information, och med tanke på ett sådant besluts potentiella effekter, i princip bör vara evidensbaserad verkar åtminstone t.ex. formuleringen (”syftar till att”) oklar och bör anpassas (”har som mål/syfte att”).

Europeiska dataskyddsstyrelsen beklagar att det enda fallet där myndigheterna i ett tredjeland skulle höras och kunna invända mot verkställigheten av en utlämnandeorder, skulle vara då denna behöriga domstol i EU anser att det föreligger en relevant motstridighet, översänder alla element till de centrala myndigheterna i det berörda tredjelandet och den centrala myndigheten i detta tredjeland invänder inom de snäva tidsfristerna på högst 50 dagar (15 dagar, som kan förlängas med 30 dagar, och efter en sista påminnelse med ytterligare fem dagar). I alla övriga fall skulle den behöriga domstolen kunna fastställa utlämnandeordern och utfärda böter för den tjänsteleverantör som vägrar att verkställa ordern. Europeiska dataskyddsstyrelsen är följaktligen oroad över att behöriga domstolar inom EU inte har en större skyldighet att samråda med behöriga myndigheter i berörda tredjeländer för att se till att förfarandet mer systematiskt säkerställer att båda parternas argument beaktas och att visa ännu större respekt för tredjeländers lagstiftning.

Som redan understrukits i artikel 29-gruppens yttrande och ovan påminner Europeiska dataskyddsstyrelsen om att särskild uppmärksamhet bör ägnas åt tredjeländers antagande av liknande instrument som skulle kunna påverka registrerades rättigheter och deras rätt till personlig integritet inom EU, särskilt risken för liknande instrument som skulle stå i direkt motsättning till EU:s dataskyddslagstiftning.

[34] Se artikel 48 i den allmänna dataskyddsförordningen.

Dessutom understryker Europeiska dataskyddsstyrelsen att den behöriga domstolen i den utfärdande myndighetens medlemsstat kanske inte ens är den domstol som är behörig att verkställa beslutet i enlighet med artikel 14 i förslaget till förordning, vilket till och med skulle öka risken för motstridiga förfaranden och avsaknaden av dubbelkontroller i en situation med motstridiga lagar. Detta beror på att tre stater i vissa fall kan komma i fråga: den utfärdande myndighetens stat, tjänsteleverantörens tredjeland och den medlemsstat där tjänsteleverantörens rättsliga företrädare i EU befinner sig, och där ordern skulle verkställas. Enligt det förfarande som för närvarande planeras kan domstolen för den anmodande myndigheten i medlemsstat A följaktligen göra sin egen tolkning av lagstiftningen i tjänsteleverantörens tredjeland B, utan krav på synpunkter från myndigheterna i detta tredjeland (så länge de skulle ha invänt mot ordern) och begära att en domstol i en annan EU-medlemsstat C verkställer dess beslut utan möjlighet till invändningar.

Dessutom välkomnar Europeiska dataskyddsstyrelsen införandet av särskilda rättsmedel mot utlämnandeorder, utöver de rättsmedel som anges i den allmänna dataskyddsförordningen och i brottsbekämpningsdirektivet. Artikel 29-gruppen har redan efterlyst sådana garantier i sitt tidigare yttrande. Europeiska dataskyddsstyrelsen beklagar dock att sådana rättsmedel inte föreskrivs mot bevarandeorder, eftersom dessa order också kan leda till begränsningar av de grundläggande rättigheterna för de personer vars uppgifter lagras. Bevarandeorder kan faktiskt leda till att uppgifter lagras under längre tid än de skulle ha lagrats enligt dataskyddsreglerna. Därför leder bevarandeordern i sig till en begränsning av den berörda registrerade personens grundläggande rättigheter, vars motivering ska bli föremål för en översyn och för särskilda rättsmedel, särskilt då bevarandeordern har utfärdats tillsammans med en utlämnandeorder för att skaffa fram uppgifterna. Som artikel 29-gruppen rekommenderade i sitt yttrande bör man föreskriva rättsmedel som åtminstone är likvärdiga med dem som är tillgängliga i ett inhemskt ärende.

h) Säkerhet vid överföring av uppgifter när en order besvaras

Europeiska dataskyddsstyrelsen konstaterar att det i förslaget till förordning endast föreskrivs att order ska riktas till mottagare i EU, och att det därför inte föreskrivs någon särskild kanal för överföring av uppgifter mellan adressaterna och tjänsteleverantörer utanför EU.

Även om Europeiska dataskyddsstyrelsen välkomnar avsaknaden av ytterligare undantag från EU:s allmänna ram för dataskydd påminner den om att alla order till en adressat som sedan skulle innebära en överföring utanför EU måste respektera den allmänna dataskyddsförordningens rättsliga ram. Kringgåendet av den rättsliga ramen för rättsligt samarbete, enligt vilken dataskyddsgarantierna ska respekteras, bör inte leda till att även dataöverföringskraven kringgås av dem som mottar utlämnande- eller bevarandeorder, för att de ska kunna följa sådana order.

Även om Europeiska dataskyddsstyrelsen välkomnar avsaknaden av en skyldighet att dekryptera krypterade data[35] är den dessutom oroad över att utkasten till förslag inte innehåller några särskilda krav på att adressaterna ska bedöma uppgifternas äkthet, och understryker att denna bedömning också är ett mervärde av traditionella instrument som bygger på rättsligt samarbete och varnar för de ökade riskerna för berörda registrerade i avsaknad av en sådan bedömning.

Slutsatser

På grundval av denna bedömning riktar Europeiska dataskyddsstyrelsen följande rekommendationer till medlagstiftarna:

[35] Se skäl 19 och sidan 240 i konsekvensbedömningen.

1) Förordningens rättsliga grund bör inte vara artikel 82.1 i EUF-fördraget.
2) Behovet av ett nytt instrument jämfört med det befintliga direktivet om en europeisk utredningsorder eller avtalen om ömsesidig rättslig hjälp bör påvisas bättre, bl.a. genom en detaljerad analys av mindre inkräktande åtgärder när det gäller de grundläggande rättigheterna, såsom ändringar av dessa befintliga instrument eller en begränsning av detta instruments tillämpningsområde till bevarandeorder i kombination med andra befintliga förfaranden för att begära tillgång till uppgifter.
3) I förordningen bör det föreskrivas en längre tidsfrist för att den verkställande tjänsteleverantören ska kunna säkerställa garantier i fråga om skyddet av de grundläggande rättigheterna.
4) Principen om dubbel straffbarhet bör bibehållas, särskilt om uppgifternas platskriterier överges för att upprätthålla skyldigheten att beakta de skyddsåtgärder som föreskrivs i båda de berörda staterna (den anmodande myndighetens stat och den stat där tjänsteleverantören är etablerad).
5) Tillämpningsområdet för denna förordning bör begränsas till personuppgiftsansvariga i den mening som avses i den allmänna dataskyddsförordningen, eller också bör förordningen innehålla en bestämmelse om att personuppgiftsbiträdet är skyldigt att underrätta den personuppgiftsansvarige om den tjänsteleverantör som kontaktas inte är den personuppgiftsansvarige för uppgifterna, utan personuppgiftsbiträdet.
6) Förordningen bör innehålla garantier för uppgiftsöverföringar om tjänsteleverantören är etablerad i ett tredjeland som saknar ett beslut om adekvat skyddsnivå på detta område, eller hänvisa till direktiv (EU) 2016/680, eftersom dessa garantier kommer att vara tillämpliga.
7) Eftersom det obligatoriska utseendet av en rättslig företrädare skiljer sig från den allmänna dataskyddsförordningen bör det i förordningen preciseras att den rättsliga företrädare som utsetts enligt förordningen om e-bevisning bör vara skild från den som utsetts enligt artikel 3.2 i den allmänna dataskyddsförordningen.
8) Förordningen bör innehålla en allmännare definition av data från elektronisk kommunikation för att se till att de lämpliga garantier och villkor för tillgång som ska fastställas omfattar både icke-innehållsdata och innehållsdata.
9) I förordningen bör trösklarna höjas för utfärdande av order, och order ska utfärdas eller godkännas av domstolar, med undantag för abonnentuppgifter om definitionen av denna kategori av uppgifter kraftigt inskränks till mycket grundläggande information som endast gör det möjligt att identifiera en person, utan tillgång till kommunikationsuppgifter.
10) I förordningen bör tillgången till abonnentuppgifter och åtkomstuppgifter begränsas till en strikt förteckning över brott eller åtminstone ”grova brott”.
11) Tidsfristen för att lämna uppgifter, särskilt i nödsituationer, bör motiveras bättre i förordningen, och möjligheten att använda ett snabbt sextimmarsförfarande bör inbegripa en skyldighet för de anmodande myndigheterna att visa att det är brådskande, även i efterhand, för att möjliggöra en kontroll av användningen av sådana särskilda befogenheter.
12) Det förfarande som möjliggör utlämnande av innehållsdata utan medverkan av de behöriga myndigheterna i den medlemsstat där den registrerade befinner sig, bör slopas.
13) Garantierna för utfärdande av europeiska bevarandeorder bör förbättras i förordningen.
14) Förordningen bör åtminstone omfatta det minsta klassiska undantaget, nämligen att verkställigheten av en order bör vägras om det finns tungt vägande skäl att anta att verkställandet av ordern skulle leda till en kränkning av den berörda personens grundläggande rättigheter och att den verkställande staten skulle åsidosätta sina skyldigheter avseende det skydd av grundläggande rättigheter som erkänns i stadgan.

15) För att undvika subjektiva tolkningar från en enda domstol bör det i förordningen föreskrivas en allmännare skyldighet att vid lagkonflikter samråda med behöriga myndigheter i det tredjeland där den tjänsteleverantör som har anmodats att lämna uppgifter befinner sig.
16) Giltigheten och varaktigheten hos bevarandeorder bör i högre grad vara knuten till de utlämnandeorder som åtföljer dem.
17) Säkerheten vid överföring av uppgifter bör garanteras på ett bättre sätt.
18) Det bör föreskrivas att uppgifternas äkthet ska kontrolleras, särskilt om krypterade data kan tillhandahållas.

För Europeiska dataskyddsstyrelsen

Ordföranden

(Andrea Jelinek)