Udtalelse 23/2018 om Kommissionens forslag om europæiske editions- og sikringskendelser om elektronisk bevismateriale i straffesager (artikel 70.1.b)

Vedtaget den 26. september 2018

Indholdsfortegnelse

Det Europæiske Databeskyttelsesråd har —

under henvisning til artikel 70, stk. 1, litra b) i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF —

VEDTAGET FØLGENDE UDTALELSE:

Indledning

I april 2018 fremlagde Kommissionen et forslag til en forordning om europæiske editions- og sikringskendelser om elektronisk bevismateriale i straffesager og et forslag til et direktiv om harmoniserede regler for udnævnelse af juridiske repræsentanter med henblik på indsamling af bevismaterialer i straffesager. De to forslag COM (2018) 225 final og COM (2018) 226 final er komplementære. Kommissionens overordnede mål er at forbedre samarbejdet mellem medlemsstaternes myndigheder og tjenesteudbydere, herunder dem, der er baseret i tredjelande, og at foreslå løsninger på problemet med at fastslå og håndhæve kompetence i cyberspace.

Mens udkastet til forordningen indeholder de regler og procedurer, der gælder i forbindelse med udstedelse, forkyndelse og fuldbyrdelse af editions- og sikringskendelser til udbydere af elektroniske kommunikationstjenester, indeholder udkastet til direktivet minimumsregler for udpegelse af en juridisk repræsentant for tjenesteudbydere, der ikke er etableret i EU.

I november 2017[1], inden Kommissionen forelagde et udkast til forslag, mindede Artikel 29-Gruppen (WP29) om nødvendigheden af at sikre, at ethvert lovgivningsforslag fuldt ud overholder især gældende EU-databeskyttelses*ret* samt EU-lovgivningen og retspraksis generelt.

Artikel 29-Gruppen advarede især mod begrænsninger af rettighederne i forbindelse med databeskyttelse og privatlivets fred med hensyn til data, der behandles af telekommunikationsudbydere og udbydere i informationssamfundet, især når dataene blev behandlet yderligere af retshåndhævende myndigheder, mindede om nødvendigheden af at sikre sammenhæng i alle EU-instrumenter med Europarådets eksisterende Budapestkonvention om cyberkriminalitet og med EU-direktivet om den europæiske efterforskningskendelse og anbefalede at præcisere de respektive proceduremæssige regler for adgang til elektronisk bevismateriale på nationalt og EU-plan med henblik på at sikre, at det nye instrument ikke giver myndighederne nye beføjelser, som de ikke ville have internt. Ud over disse generelle bemærkninger kommenterede Artikel 29-Gruppen på de lovgivningsmæssige muligheder, som Kommissionen på det tidspunkt overvejede, vedrørende de pågældende datakategorier og de tilsvarende garantier for at få adgang til dem, muligheden for at håndtere editionskendelser/anmodninger om at pålægge tjenesteydere at levere data, der er placeret uden for EU, og om de indholdsmæssige og proceduremæssige garantier, som er nødvendige for at beskytte den direkte adgang til data.

[1] Se Artikel 29-Gruppens erklæring (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801)

Med de konkrete forslag om elektronisk bevismateriale, der er til rådighed på nuværende tidspunkt, ønsker det Europæiske Databeskyttelsesråd at give en mere detaljeret analyse af de foreslåede retsakter ud fra et databeskyttelsessynspunkt.

1. Retsgrundlag for forordningsforslaget (artikel 82 i TEUF)

Det foreslåede retsgrundlag for udkastet til forordning om elektronisk bevismateriale er artikel 82, stk. 1, i TEUF om strafferetsligt samarbejde, hvori det fastsættes:

> "1. Det retlige samarbejde i straffesager i Unionen bygger på princippet om gensidig anerkendelse af domme og retsafgørelser og omfatter indbyrdes tilnærmelse af medlemsstaternes love og administrative bestemmelser på de områder, der er nævnt i stk. 2 og i artikel 83.
>
> Europa-Parlamentet og Rådet vedtager efter den almindelige lovgivningsprocedure foranstaltninger med henblik på:
>
> (a) at fastlægge regler og procedurer, der skal sikre anerkendelse af alle former for domme og retsafgørelser i hele Unionen
>
> (b) at forebygge og løse konflikter mellem medlemsstaterne om retternes kompetence
>
> (c) at støtte uddannelse af dommere og anklagere samt andet personale i retsvæsenet
>
> (d) at fremme samarbejdet mellem judicielle eller tilsvarende myndigheder i medlemsstaterne i forbindelse med strafforfølgning og fuldbyrdelse af afgørelser."

Som Kommissionen understreger i konsekvensanalysen, der ledsager forslagene, "præciseres det i artikel 82, stk. 1, at det strafferetlige samarbejde skal baseres på princippet om gensidig anerkendelse. Dette retsgrundlag vil omfatte mulig lovgivning om direkte samarbejde med tjenesteudbydere, hvor myndighederne i den udstedende medlemsstat direkte henvender sig til en virksomhed (tjenesteyderen) i fuldbyrdelsesstaten og endog pålægger den forpligtelser. Dette ville indføre en ny dimension inden for gensidig anerkendelse ud over det traditionelle retslige samarbejde i Unionen, der hidtil har været baseret på procedurer, som involverer to retslige myndigheder, en i udstedelsesstaten og en anden i fuldbyrdelsesstaten."(fremhævelse tilføjet)

Eftersom brugen af dette retsgrundlag i forbindelse med direkte anmodninger mellem offentlige myndigheder og private parter er nyt, beklager det Europæiske Databeskyttelsesråd, at Kommissionen ikke kommer med nogen yderligere analyse eller vurdering.

Som arbejdsgruppen allerede understregede i sin tidligere erklæring, understreger det Europæiske Databeskyttelsesråd, at det fortsat nærer tvivl om hensigtsmæssigheden af dette retsgrundlag, hvilket understøttes af EU-Domstolens og dens generaladvokats analyse i udtalelsen 1/15. Som et eksempel på udviklingen vedrørende gyldigheden af artikel 82 som retsgrundlag for udkastet til aftalen om PNR-oplysninger mellem EU og Canada understregede Domstolen, at den canadiske kompetente myndighed "*ikke udgør en retslig myndighed og heller ikke udgør en tilsvarende myndighed*"[2]. I forbindelse med forslagene om elektronisk bevismateriale synes et af hovedmålene som anført af Kommissionen at være at undgå det "alt for besværlige" retslige samarbejde. Forslaget er derfor baseret på princippet om, at samarbejdet skal finde sted mellem en myndighed og en tjenesteyder

[2] Se punkt 103 i udtalelse 1/15 og punkt 108 i generaladvokatens udtalelse i denne sag.

snarere end mellem to myndigheder. Den fastsatte procedure gør primært private enheder til den modtagende part, som besvarer de anmodninger, der udgår fra retslige myndigheder.

Det Europæiske Databeskyttelsesråd bemærker, at processen for fuldbyrdelse af editions- og sikringskendelser kan indebære inddragelse af en modtagende myndighed i de situationer, hvor den modtagende tjenesteudbyder ikke overholder sine forpligtelser og således gør det nødvendigt at kræve efterfølgende fuldbyrdelse af kendelsen. Men da hovedformålet med proceduren netop er ikke at involvere en modtagende myndighed, tvivler Det Europæiske Databeskyttelsesråd på, at denne supplerende procedure kan retfærdiggøre anvendelsen af artikel 82 som eneste retsgrundlag for instrumentet.

Det Europæiske Databeskyttelsesråd er derfor af den opfattelse, at forudsætningen for at anvende artikel 82 som retsgrundlag er, at de vigtigste proceduremæssige trin i samarbejdet finder sted mellem to retslige myndigheder, og at der bør anvendes et andet retsgrundlag for denne form for samarbejde.

2. Nødvendigheden af elektronisk bevismateriale i forhold til MLAT'er og den europæiske efterforskningskendelse

Det Europæiske Databeskyttelsesråd bemærker, at Kommissionen har forpligtet sig til at granske hindringer for strafferetlig efterforskning, især vedrørende spørgsmålet om adgang til elektronisk bevismateriale. I sin begrundelse fremsætter Kommissionen forslagets kontekst og understreger elektronisk dokumentations meget ustabile karakter, dets internationale dimension og behovet for at tilpasse samarbejdsmekanismen til den digitale tidsalder. Forslag til en forordning og et direktiv om overførsel af og adgang til elektronisk bevismateriale har ikke til formål at erstatte tidligere samarbejdsinstrumenter i straffesager såsom Budapestkonvention, traktaten om gensidig retshjælp (MLAT) og den europæiske efterforskningskendelse (EIO-direktivet). Ifølge Kommissionen har forslagene om elektronisk bevismateriale til formål at forbedre det retslige samarbejde i straffesager mellem myndigheder og tjenesteydere i Den Europæiske Union samt med tredjelande, især USA.

Da disse nye ekstra værktøjer vil blive målrettet specifikt til adgang og overførsel af elektronisk bevismateriale, vil det Europæiske Databeskyttelsesråd vurdere instrumenternes merværdi med hensyn til EIO-direktivet og MLAT.

a) Behovet for elektronisk bevismateriale i forhold til de garantier, som EIO og MLAT'er indeholder

Hovedargumentet fra Kommissionen til fordel for forslagene om elektronisk bevismateriale er fremskyndelse af processen for sikring og indhentning af elektronisk bevismateriale, der lagres og/eller opbevares af tjenesteudbydere, som er etableret i en anden jurisdiktion.

Det Europæiske Databeskyttelsesråd beklager imidlertid, at behovet for et nyt instrument til at organisere adgangen til elektronisk bevismateriale ikke blev påvist i konsekvensanalysen. Forslagene mangler faktisk dokumentation for, at det ikke var muligt at nå formålet med forslaget om elektronisk bevismateriale med mindre indgribende midler, selv om man kunne have overvejet alternative løsninger. Man kunne f.eks. have undersøgt muligheden for at ændre og forbedre EIO-direktivet, hvilket også ville have opfyldt det specifikke krav i EIO-direktivet om at vurdere behovet for at ændre teksten

inden den 21. maj 2019[3]. En anden mulighed kunne have været at foreskrive anvendelse af sikringskendelser til at fastfryse dataene mens der blev udstedt en formel anmodning baseret på en MLAT. Disse valgmuligheder ville have gjort det muligt at opretholde de garantier, som disse instrumenter indeholder, og samtidig sikre, at de ønskede personoplysninger ikke slettes.

Det Europæiske Databeskyttelsesråd bemærker, at tidsfristerne i EIO-direktivet er længere end i forslaget om elektronisk bevismateriale. Faktisk har den fuldbyrdende myndighed 30 dage til at træffe sin afgørelse om anerkendelse af anmodningen[4] og skal derefter fuldbyrde kendelsen inden for 90 dage[5]. Det er Det Europæiske Databeskyttelsesråds holdning, at det udgør en afgørende sikkerhedsforanstaltning at give de fuldbyrdende myndigheder i EIO 30 dages betænkningstid, så de kan vurdere, om anmodningen om fuldbyrdelse er velbegrundet og opfylder alle betingelserne for udstedelse og overførsel af en EIO[6].

Det Europæiske Databeskyttelsesråd er bekymret for, at den 10-dages frist for udfærdigelse af attesten for en europæisk editionskendelse (EPOC), der er fremsat i forslagene om elektronisk bevismateriale, uden at der gives betænkningstid, forhindrer en korrekt vurdering af, om EPOC'en opfylder alle kravene og er udfyldt korrekt.

Derfor anbefaler det Europæiske Databeskyttelsesråd, at EPOC-modtagere får mere tid til at afgøre, om kendelsen skal fuldbyrdes eller ej.

Det Europæiske Databeskyttelsesråd bemærker, at der i tilfælde af en europæisk sikringskendelse (EPOC-PR) ikke er nogen garanti for, at bevaringen af data vil være begrænset til det nødvendige. Faktisk kan dataopbevaringens varighed overstige 60 dage, da der ikke er nogen frist for, hvornår udstedelsesmyndigheden skal oplyse modtageren om at afstå fra at udstede eller trække en editionskendelse tilbage. Derfor anbefaler det Europæiske Databeskyttelsesråd, at der i det mindste indføres en frist for den udstedende myndighed med hensyn til afståelse fra at udstede eller tilbagetrækning af editionskendelsen med henblik på at overholde princippet om dataminimering som fastlagt i GDPR[7].

Endelig bemærker det Europæiske Databeskyttelsesråd, at EIO-direktivet fastlægger tilbageførelsen af bevismateriale fra udstedelsesstaten til fuldbyrdelsesmyndigheden[8]. Imidlertid indeholder forslaget til regulering af elektronisk bevismateriale intet om en sådan mulighed. Hvad der sker med det elektroniske bevismateriale efter dets fremsendelse til den udstedende myndighed er uklart.

Det Europæiske Databeskyttelsesråd anbefaler derfor, at forordningsforslaget giver flere oplysninger om brugen af elektronisk bevismateriale efter overførsel heraf til udstedelsesmyndigheden med henblik på at overholde GDPR og gennemsigtighedsprincippet[9] samt det specificitetsprincip, der er fastlagt af MLAT'erne.

b) Ophævelse af princippet om dobbelt strafbarhed

Det Europæiske Databeskyttelsesråd erkender, at gensidig anerkendelse er afhængigt af anvendelsen af dobbelt strafbarhed, som er en måde, hvorpå medlemsstaterne kan opretholde deres suverænitet.

[3] Se artikel 37 i EIO-direktivet
[4] Artikel 12, stk. 3 i EIO-direktivet
[5] Artikel 12, stk. 4 i EIO-direktivet
[6] Artikel 6 i EIO-direktivet
[7] Artikel 5, stk. 1, litra c) i GDPR.
[8] Artikel 13, stk. 3 og 4 i EIO-direktivet.
[9] Artikel 5, stk. 1, litra a) i GDPR.

Dobbelt strafbarhed betragtes dog i stigende grad som en hindring for et velfungerende retsligt samarbejde. EU-medlemsstaterne er mere og mere villige til at samarbejde, selv i tilfælde, hvor undersøgelsesforanstaltningerne vedrører handlinger, der ikke betragtes som lovovertrædelser i henhold til deres nationale lovgivning. Det Europæiske Databeskyttelsesråd minder dog om, at formålet med princippet om dobbelt strafbarhed er at tilvejebringe en ekstra sikkerhedsforanstaltning med henblik på at sikre, at en stat ikke kan være afhængig af en anden stats bistand til at pålægge en strafferetlig sanktion, der ikke findes i en anden stats lovgivning. Dette ville eksempelvis forhindre en stat i at forlange hjælp fra en anden stat til at fængsle en person for vedkommendes politiske holdninger, hvis disse udtalelser ikke er kriminaliseret i den anmodede stat, eller at retsforfølge en person for at have fået foretaget en abort, hvis denne person er bosat i en anden stat, hvor dette ikke er ulovligt. Princippet om dobbelt strafbarhed er også ofte ledsaget af yderligere begrænsninger eller garantier vedrørende sanktionerne, hvis disse er for forskellige i den anmodende og fuldbyrdende medlemsstat. Hovedeksemplet er tilsagnet om ikke at anvende dødsstraf i visse MLAT'er, når denne straf ikke findes i lovgivningen hos en af de to parter.

Det Europæiske Databeskyttelsesråd bemærker, at princippet om dobbelt strafbarhed er udelukket i forslaget om elektronisk bevismateriale. Herved fjernes dog ikke blot de sædvanlige formaliteter i forbindelse med gensidig anerkendelse men også garantier i forbindelse med selve princippet om dobbelt strafbarhed.

Det Europæiske Databeskyttelsesråd bemærker, at der ikke henvises til lovgivningen i det land, hvor den anmodede tjenesteudbyder er etableret, og at der kan udstedes påbud om bevarelse af eventuelle data samt fremlæggelse af abonnent- eller adgangsdata for alle lovovertrædelser,[10] uanset om der findes lignende forbrydelser i andre medlemsstater eller ej.

Imidlertid kan editionskendelser kun udstedes og fuldbyrdes, hvis der findes en lignende foranstaltning for samme forbrydelse i en sammenlignelig indenlandsk situation i udstedelsesstaten[11]. Som Kommissionen forklarer i begrundelsen til forslaget til forordning, fastlægges transaktions- og indholdsdatas specificitet, da disse anses for at være mere følsomme. Kendelser vedrørende transaktions- eller indholdsdata udstedes på grundlag af en tærskel på en frihedsstraf af en maksimal varighed på mindst tre år for at sikre respekt for proportionaliteten og de berørte personers rettigheder[12]. Det Europæiske Databeskyttelsesråd understreger dog, at der endnu ikke er gennemført nogen harmonisering i EU angående strafbare handlinger, som straffes med en frihedsstraf af mindst 3 års varighed.

Det Europæiske Databeskyttelsesråd modsætter sig ophævelsen af princippet om dobbelt strafbarhed, der har til formål at sikre, at en stat ikke kan forlade sig på andres hjælp til at få sin nationale strafferet anvendt uden for sit territorium af en stat, der ikke deler samme tilgang, især i betragtning af, at andre traditionelle vigtige garantier på det strafferetlige område er forsvundet (se punkt 3 nedenfor om lokaliseringskriterierne og stk. 7, litra g), vedrørende potentielle konflikter med tredjelandes lovgivning).

c) Konsekvensen af at henvende sig direkte til virksomhederne

[10] Artikel 5, stk. 3 og artikel 6, stk. 2, i forslaget til forordning om elektronisk bevismateriale.
[11] Artikel 5, stk. 2 i forslaget til forordning om elektronisk bevismateriale
[12] Artikel 5, stk. 4, litra a) i forslaget til forordning om elektronisk bevismateriale

Det Europæiske Databeskyttelsesråd erkender, at elektronisk bevismateriale i stigende grad er tilgængeligt på privat infrastruktur og kan være placeret uden for det undersøgende land og ejet af tjenesteudbydere.

Det Europæiske Databeskyttelsesråd bemærker, at der efter afgørelserne vedrørende *Yahoo*[13]! og *Skype*[14] i Belgien og i forbindelse med terrorangreb er behov for et smidigere og hurtigere samarbejde mellem offentlige og private enheder. I konsekvensanalysen henviser Kommissionen til tre typer proceduremæssige instrumenter, der involverer både offentlige myndigheder og tjenesteudbydere. Der er tale om retsligt samarbejde, direkte samarbejde og direkte adgang. Hvis det første instrument ikke pålægger tjenesteudbyderen men fuldbyrdelsesmyndigheden[15] ansvaret for at udføre EIO'en, så baseres det andet instrument, direkte samarbejde, på samarbejde fra tjenesteudbyderens side. Det mest indgribende instrument er set fra en tjenesteudbyders perspektiv direkte adgang, fordi offentlige myndigheder kan tilgå data uden hjælp fra en formidler.

Det Europæiske Databeskyttelsesråd frygter derfor, at tjenesteydere ved direkte henvendelse ikke vil sikre beskyttelsen af personoplysninger lige så effektivt, som de offentlige myndigheder er i stand til og forpligtet til at gøre, og understreger, at dette også medfører, at visse proceduremæssige garantier for enkeltpersoner og virksomhederne selv[16] ikke kan anvendes i forbindelse med retligt samarbejde. Eksempelvis skal en anmodet tjenesteudbyder gå til domstolen i en anden (medlems-) stat for at anfægte kendelsen, selv om den i forbindelse med det retslige samarbejde ville benytte sine egne myndigheder. Det Europæiske Databeskyttelsesråd anbefaler, at der indføjes yderligere grunde i forslaget til forordning, som bekræfter, at tjenesteydere vil værne om individuelle grundlæggende rettigheder såsom beskyttelse af personoplysninger og respekt for privatliv og familieliv samt oplysninger fra den kompetente databeskyttelsesmyndighed for at sikre, at kontrol er mulig.

3. Det nye kompetencegrundlag og lokaliseringskriteriernes såkaldte forsvinden

Det Europæiske Databeskyttelsesråd bemærker, at Kommissionen understreger, at en af de store ændringer som følge af disse forslag er, at lokaliseringskriterierne og muligheden for, at de kompetente myndigheder kan anmode om bevarelse og fremlæggelse af data, uanset hvor disse data faktisk lagres, forsvinder.

Ud fra et databeskyttelsesperspektiv er det ikke nyt, at EU's databeskyttelseslovgivning gælder, uanset hvor de berørte personers data er lagret. Faktisk afhænger anvendelsen af GDPR enten af, at den dataansvarlige eller databehandleren er etableret i EU, eller af, om EU-registreredes data behandles, selv når den dataansvarlige eller databehandleren ikke er etableret på EU's område[17], og i så fald skal de også udpege en juridisk repræsentant i EU[18]. Ud fra databeskyttelsesperspektivet er det vigtigt at

[13] Hof van Cassatie fra Belgien, YAHOO! Inc., nr. P.13.2082.N af 1. december 2015.
[14] Correctionele Rechtbank van Antwerpen, afdeling Mechelen i Belgien, nr. ME20.F1.105151-12 af 27. oktober 2016. (Skype har anket afgørelsen).
[15] Artikel 10-16.
[16] Se også fra et internationalt databeskyttelsesperspektiv "Arbejdspapiret om standarder for databeskyttelse og privatlivets fred i grænseoverskridende dataanmodninger med henblik på strafferetlig håndhævelse", Den Internationale Arbejdsgruppe om Databeskyttelse inden for Telekommunikation, 63. møde, 9.-10. april 2018, Budapest (Ungarn).
[17] Se artikel 3, herunder især stk. 2.
[18] Se artikel 27

bemærke, at det udvidede territoriale anvendelsesområde har til formål at give en mere fuldstændig beskyttelse til EU-registrerede, uanset hvor virksomheden, der behandler deres data, er etableret.

Selv om lokaliseringskriteriernes forsvinden måske er nyt på det strafferetlige område, er det ikke en stor ændring fra et databeskyttelsesperspektiv. Desuden bemærker det Europæiske Databeskyttelsesråd også, at der fortsat er en forbindelse til EU's territorium, da kun tjenesteydere, der tilbyder tjenester i Unionen, falder inden for rammerne af forslagene, og det forhold, at anmodninger kun kan behandles i forbindelse med strafferetlige undersøgelser, indebærer en forbindelse til EU (enten fordi forbrydelsen er begået på en medlemsstats område eller fordi offeret eller den kriminelle var statsborger i en medlemsstat).

Hvis lokaliseringskriteriernes forsvinden nu skal gøres gældende i strafferetten, er det vigtigste spørgsmål for det Europæiske Databeskyttelsesråd, hvordan man sikrer sig, at en sådan udvikling ikke er til skade for de registreredes og de anmodede tjenesteudbyderes databeskyttelse og strafferetlige processuelle rettigheder. Ud fra dette perspektiv anerkender det Europæiske Databeskyttelsesråd, at proceduremæssige garantier inden for EU i det mindste delvist er harmoniseret og skal ydes i overensstemmelse med den europæiske menneskerettighedskonvention. Det kan således hævdes, at lokaliseringskriteriernes forsvinden sandsynligvis vil have mere begrænsede konsekvenser, når bevismaterialet søges i EU, sammenlignet med den omvendte situation, hvor myndigheder fra tredjelande anmoder om data til virksomheder etableret i EU på samme betingelser som fastsat i forordningen om elektronisk bevismateriale. Faktisk er det Europæiske Databeskyttelsesråd særlig bekymret over, at dette kan resultere i mere problematiske situationer. I den sammenhæng kan myndigheder fra et tredjeland, hvor forskellige og potentielt mindre proceduremæssige garantier finder anvendelse på det strafferetlige område, have adgang til data, som ville være beskyttet af yderligere garantier i EU. Ud fra dette perspektiv minder det Europæiske Databeskyttelsesråd om sine bekymringer vedrørende en dobbelt standard og en svækkelse af de grundlæggende rettigheder, når tjenesteydere og registrerede ikke nyder godt af de proceduremæssige garantier i EU-lovgivningen, hvis anmodningen er indgivet af en tredjelandsmyndighed.

Da denne nye tildeling af kompetence "uanset dataenes geografiske placering" kombineres med en procedure, der hovedsagelig bygger på direkte anmodninger fra kompetente myndigheder til tjenesteudbydere, er det Europæiske Databeskyttelsesråd bekymret for, at databeskyttelsesgarantier ikke anvendes af private virksomheder, der modtager anmodninger og som ikke er bundet af et retligt instrument som f.eks. en MLAT, der traditionelt styrer udvekslingen af data mellem retsmyndigheder og indeholder garantier. Navnlig inden for rammerne af MLAT'er indeholder minimumsgarantier for databeskyttelse f.eks. fortrolighedsforpligtelser og specificitetsprincippet, som indebærer, at dataene ikke behandles til et andet formål.

Det Europæiske Databeskyttelsesråd minder derfor om, at man som minimum bør anvende garantierne i direktiv 2016/680, herunder med hensyn til dataoverførsler, og navnlig artikel 39, hvis tjenesteyderen er etableret i et tredjeland uden en tilstrækkelig beslutning på dette område. Det Europæiske Databeskyttelsesråd understreger især, at denne bestemmelse navnlig omfatter oplysninger fra den kompetente databeskyttelsesmyndighed i den medlemsstat, som huser den myndighed, der har udstedt kendelsen(erne), og dokumentationen for overførslen, herunder med hensyn til begrundelsen for, at en overførsel til tredjelandets kompetente myndighed var ineffektiv eller upassende.

4. Begrebet "tjenesteydere" bør begrænses eller suppleres med yderligere garantier for de registreredes rettigheder

For så vidt angår udbydere af tjenesteydelser, bifalder det Europæiske Databeskyttelsesråd den brede definition, der gør det muligt at inkludere både kommunikationstjenester og over-the-top-tjenester (OTT), da alle disse tjenester er funktionelt ækvivalente, og de påtænkte foranstaltninger kan derfor have tilsvarende indflydelse på retten til privatlivets fred og retten til hemmeligholdelse af kommunikation som anført i Artikel 29-Gruppens erklæring og tidligere i udtalelse 01/2017 om den foreslåede forordning til e-datadirektivet. Forslaget til forordning om elektronisk bevismateriale omfatter tjenesteydere, der enten leverer elektroniske kommunikationstjenester som defineret i artikel 2, stk. 4, i direktivet om oprettelse af den europæiske kodeks for elektronisk kommunikation, informationssamfundstjenester som defineret i artikel 1, stk. 1, litra b) i direktiv (EU) 2015/1535, "hvor opbevaring af data er en afgørende del af den service, der leveres til brugeren, herunder sociale netværk, online markedspladser, der letter transaktioner mellem deres brugere og andre hosting-udbydere" eller internet domænenavns- og IP-nummereringstjenester "som f.eks. IP-udbyderes domænenavnsregistre, domænenavnsregistratorer og tilhørende privatlivs- og proxy-tjenester"[19].

Men da en tjenesteyder i udkastet til forordningen er "enhver fysisk eller juridisk person, der leverer en eller flere af følgende kategorier af tjenester", er det Europæiske Databeskyttelsesråd imidlertid bekymret for, at dette instrument kan omfatte både registeransvarlige og databehandlere i den forstand som omhandlet i GDPR. Eftersom "udbud af tjenesteydelser" som defineret i artikel 2, stk. 4, i udkastet til forordningen både betyder, at man gør det muligt for juridiske eller fysiske personer i en eller flere medlemsstater at anvende de nævnte tjenester og have en væsentlig forbindelse til de(n) omhandlede medlemsstat(er), omfatter disse aktiviteter de aktiviteter, en databehandler udfører for en registeransvarlig, som f.eks. lagring af data.

Det Europæiske Databeskyttelsesråd frygter derfor, at de registreredes rettigheder i en situation uden begrænsninger på tjenesteydere, der fungerer som registeransvarlige som omhandlet i GDPR, og uden nogen særlig forpligtelse for databehandleren til at underrette den registeransvarlige, når vedkommende modtager en henvendelse vedrørende en editions- og sikringskendelse, kan omgås. Dette er især tilfældet, fordi de retslige myndigheder i forbindelse med eventuelle modstridende forpligtelser, der forhindrer modtageren i at gennemføre de modtagne kendelser, også i selve forslaget til forordning opfordres til at henvende sig til den bedst egnede aktør uden hensyn til de gældende bestemmelser om beskyttelse af personoplysninger, navnlig i betragtning af, at det er muligt at anmode om alle data og ikke kun personlige data i henhold til GDPR[20].

Ifølge GDPR reagerer en databehandler kun på instruktioner fra den registeransvarlige. Det er derfor den registeransvarliges ansvar at sikre, at de registreredes rettigheder respekteres, og at give dem de relevante oplysninger, herunder med hensyn til modtagere af deres data, f.eks. i forbindelse med udøvelsen af deres ret til adgang. Databehandleren modtager ikke disse anmodninger fra registrerede og vil ikke være i stand til at svare, medmindre de udtrykkeligt bedes herom af den registeransvarlige.

Derfor understreger det Europæiske Databeskyttelsesråd, at medmindre deres rettigheder er blevet begrænset i forbindelse med anvendelsen af GDPR, kan de registrerede, der nyder godt af anvendelsen af GDPR, muligvis ikke udøve deres rettigheder effektivt, hvis den registeransvarlige ikke er i stand til at levere fuldstændige oplysninger. Det Europæiske Databeskyttelsesråd bemærker endvidere, at

[19] Artikel 2, stk. 3, litra c), i forslaget til forordning om elektronisk bevismateriale
[20] Se artikel 7, stk. 3 og 4

sandsynligheden for, at der mangler oplysninger, er endnu højere, når databehandleren ikke har nogen særlig forpligtelse til at underrette den registeransvarlige, når de ønskede oplysninger vedrører registrerede, der ikke er omfattet af den beskyttelse, som GDPR yder. De retslige myndigheder, som anmoder om oplysningerne, er i dette tilfælde ikke nødvendigvis forpligtet til at oplyse de registrerede om deres egen viderebehandling af oplysningerne. Det Europæiske Databeskyttelsesråd opfordrer derfor til at begrænse anvendelsesområdet til dataansvarlige som omhandlet i GDPR eller til at indføre en bestemmelse, der præciserer, at tjenesteudbyderen i tilfælde, hvor denne ikke er den dataansvarlige, skal de underrette den dataansvarlige.

5. Begreberne "etablering" og "juridisk repræsentant" i forbindelse med disse forslag bør klart skelnes fra disse begreber inden for rammerne af GDPR

Da lokaliseringskriterierne ikke er anvendelige med hensyn til data, er modtagerne af editions- og sikringskendelser inden for rammerne af den foreslåede forordning begrænset til tjenesteydere, der tilbyder tjenester i Unionen, uanset om de er etableret i EU eller ej, med pligt til at udpege en juridisk repræsentant i henhold til de regler, der er foreslået i udkastet til direktivet. Disse begreber for "etablering" og "juridisk repræsentant" defineres derfor i udkastet til instrumenter.

Det Europæiske Databeskyttelsesråd bemærker, at disse begreber også forekommer i sammenhæng med andre EU-instrumenter, især i forbindelse med GDPR. Derfor bør der gives præciseringer af definitionen og afgrænsningen af disse begreber inden for rammerne af udkastet til forslag og i forbindelse med GDPR.

a) Oprettelse

Det Europæiske Databeskyttelsesråd minder også om, at begrebet "etablering" i forbindelse med udkastet til forordningen ikke skal forveksles med begrebet i forbindelse med GDPR. For så vidt angår udkastet til forordning er begrebet etablering, som defineret i artikel 2, stk. 5, bredere end i GDPR, da det omfatter "enten den egentlige udøvelse af en økonomisk aktivitet på ubestemt tid gennem en stabil infrastruktur, hvorfra tjenesteydelsen udføres, eller en stabil infrastruktur, hvorfra virksomheden forvaltes", uanset om behandling af personoplysninger foregår i forbindelse med virksomhedens aktiviteter. Hvis "etablering" som omhandlet i GDPR skulle indgå uden tvivl i den etablering, der er defineret i udkastet til forordning, ville det modsatte derfor ikke være tilfældet.

Det Europæiske Databeskyttelsesråd advarer derfor om, at etablering af tjenesteydere i henhold til udkastet til forordning ikke nødvendigvis indebærer, at betingelserne for anvendelse af GDPR i henhold til artikel 3, stk. 1, er opfyldt. I den forbindelse opfordres dataansvarlige og databehandlere til at undersøge, om GDPR's anvendelighed hidrører fra artikel 3, stk. 2, hvilket ville indebære udpegelse af en juridisk repræsentant i EU og fraværet af One Stop-Shop-mekanismen.

b) Juridisk repræsentant

I sin erklæring understregede Artikel 29-Gruppen, at man bør undgå at forveksle forpligtelsen til at udpege en juridisk repræsentant i henhold til artikel 27 i GDPR og den juridiske repræsentant, der er planlagt i henhold til udkastet til forordningen om elektronisk bevismateriale.

Med det foreliggende udkast til forslag ønsker det Europæiske Databeskyttelsesråd at minde om disse henstillinger og især at understrege, at der efter rådets opfattelse under alle omstændigheder skal udpeges en juridisk repræsentant som omhandlet i udkastet til direktiv om udnævnelse af en juridisk repræsentant inden for rammerne af forslaget om elektronisk bevismateriale, vedkommende skal tillægges specifikke funktioner, have beføjelse til uafhængigt af bemyndigelse fra tjenesteudbyderen at besvare anmodninger og handle på vegne af tjenesteudbyderen og et større ansvar end den juridiske repræsentant i GDPR.

Desuden understreger det Europæiske Databeskyttelsesråd, at forpligtelsen i henhold til udkastene til forslag om elektronisk bevismateriale til at udpege en juridisk repræsentant under alle omstændigheder, uanset om tjenesteudbyderen er etableret i EU eller ej, muligheden i henhold til direktivet om elektronisk bevismateriale for at udpege flere juridiske repræsentanter for samme tjenesteudbyder og forpligtelsen til at meddele udpegelsen af den juridiske repræsentant til medlemsstaternes myndigheder adskiller sig fra GDPR, som ikke indeholder en sådan forpligtelse til at underrette den udpegede juridiske repræsentant, undtagelser for udpegelsen og begrænset ansvar for den juridiske repræsentant.

I betragtning af de vigtige forskelle med hensyn til rolle, ansvar og forhold til tjenesteudbyderens øvrige filialer i det ene tilfælde og den dataansvarlige eller databehandleren i det andet, anbefaler det Europæiske Databeskyttelsesråd, at der i tilfælde, hvor en tjenesteudbyder ikke er etableret i EU, men er underlagt både GDPR i henhold til artikel 3, stk. 2, og forordningen om elektronisk bevismateriale, bør udpeges to forskellige juridiske repræsentanter, som hver har klare særskilte funktioner i henhold til det instrument, på grundlag af hvilket de er udpeget.

6. Nye datakategorier

Den foreslåede forordning definerer forskellige datakategorier i henhold til artikel 2: abonnentdata, adgangsdata, transaktionsdata og indholdsdata. I betragtning 20 i Kommissionens forslag specificeres det endvidere, at "*de kategorier af data, som denne forordning dækker, omfatter abonnentdata, adgangsdata, transaktionsdata (disse tre kategorier kaldes "ikke-indholdsdata") og indholdsdata. Denne sondring findes, undtagen for adgangsdata, i lovgivningen i mange medlemsstater og også i USA's gældende retlige ramme, der gør det muligt for tjenesteudbydere at dele ikke-indholdsdata med udenlandske retshåndhævende myndigheder på frivillig basis.*"

I denne forbindelse fremhæver det Europæiske Databeskyttelsesråd først og fremmest, at alle fire ovennævnte datakategorier skal betragtes som personoplysninger i henhold til EU's databeskyttelseslovgivning, da de indeholder oplysninger vedrørende en identificeret eller identificerbar fysisk person, uanset om den registrerede er benævnt "abonnent" eller "bruger" i den foreslåede forordning. Det skal ligeledes bemærkes, at "elektronisk bevismateriale" som defineret i artikel 2, stk. 6, i Kommissionens forslag omfatter alle fire datakategorier og derfor vedrører personoplysninger. Derfor, snarere end at fastsætte reglerne for adgang til bevismateriale, der er defineret og kvalificeret i henhold til national lovgivning og retslige procedurer, giver de foreslåede forordninger nye materielle og proceduremæssige forhold vedrørende adgang til personoplysninger.

Selv om den foreslåede forordning indeholder nye underkategorier af personoplysninger, for hvilke der gælder forskellige proceduremæssige betingelser for adgang, gør det Europæiske Databeskyttelsesråd opmærksom på, at det i overensstemmelse med EU-Domstolens relevante retspraksis, i forbindelse med undersøgelsen af, om der foreligger et indgreb i den grundlæggende ret

til privatlivets fred, er uden betydning, om de pågældende oplysninger vedrørende privatlivet er følsomme oplysninger, eller om indgrebet har medført eventuelle ubehageligheder for de berørte

Det Europæiske Databeskyttelsesråd minder endvidere om, at EU-Domstolen hvad angår "ikke-indholdsdata", som omfatter abonnentdata, adgangsdata og transaktionsdata, i sin dom i de forenede sager C-203/15 og C-698/15 Tele*2 Sverige AB har* afgjort, at metadata såsom trafikdata og lokaliseringsdata giver mulighed for at lave en profil af de berørte personer, oplysninger, der under hensyntagen til retten til privatlivets fred ikke er mindre følsomme, end selve indholdet af meddelelserne[21].

Som allerede nævnt i Artikel 29-Gruppens erklæring af 29. november 2017 om databeskyttelse og elementer i forbindelse med grænseoverskridende adgang til elektronisk bevismateriale, der vedrører privatlivets fred, fastholder det Europæiske Databeskyttelsesråd sine tvivl og bekymringer med hensyn til den nuværende afgrænsning af "ikke-indhold" og indholdsdata, såvel som til de fire kategorier af personoplysninger, der er fastsat i den foreslåede forordning. Faktisk synes de fire foreslåede kategorier ikke at være klart afgrænset, og definitionen af "adgangsdata" er stadig vag i forhold til de andre kategorier. Det Europæiske Databeskyttelsesråd beklager derfor, at Kommissionens konsekvensanalyse og forslag ikke yderligere underbyggede begrundelsen for at oprette disse nye underkategorier af personoplysninger, og giver udtryk for sin bekymring med hensyn til det anderledes garantiniveau i forbindelse med de materielle og proceduremæssige betingelser for adgang til kategorierne af personoplysninger, især i betragtning af de praktiske vanskeligheder, der i nogle tilfælde gør sig gældende i forbindelse med en vurdering af, hvilken datakategori de ønskede data tilhører. F.eks. IP adresser kan både betegnes som transaktionsdata og abonnentdata.

I denne forbindelse minder det Europæiske Databeskyttelsesråd ligeledes om, det i betragtning 14 i Kommissionens forslag til forordning om respekt for privatlivet og beskyttelsen af personoplysninger i elektronisk kommunikation (ePrivacy) er Kommissionens holdning, at "elektroniske kommunikationsdata bør defineres på en så tilstrækkeligt bred og teknologineutral måde, at enhver oplysning om sendt eller udvekslet indhold (elektronisk kommunikationsindhold) og oplysninger om en slutbruger af elektroniske kommunikationstjenester, der behandles med henblik på at videresende, distribuere eller muliggøre udveksling af elektronisk kommunikationsindhold, herunder data til at spore og identificere kilden til og modtageren af en meddelelse, geografisk placering og dato, tid, varighed og kommunikationstypen". Da den nuværende og fremtidige ramme for e-databeskyttelse og de hermed forbundne begrænsninger af retten til privatlivets fred gælder for reglerne for retshåndhævende personales adgang til elektronisk bevismateriale, anbefaler det Europæiske Databeskyttelsesråd, at der medtages en bredere definition af elektronisk kommunikation i forslaget til forordningen for at sikre, at de relevante garantier og adgangsbetingelser, som skal etableres, konsekvent dækker både "ikke-indholdsdata" og "indholdsdata".

7. Analyse af procedurerne for europæiske editions- og sikringskendelser

Generelt synes proceduren for håndtering af en editions- eller sikringskendelse at være følgende:

[21] EU-Domstolens dom af 21. december 2016, præmis 99.

- Den kompetente retsmyndighed — den udstedende myndighed — udsteder alt efter hvilken type data, der anmodes om, og typen af kendelse, kendelsen i henhold til de (stramme) betingelser, der er nævnt i artikel 5 og 6, sender den ved at anvende et harmoniseret certifikat til den lovlige repræsentant for tjenesteudbyderen eller til en af dennes filialer i EU — modtageren.
- Ved modtagelse af certifikatet skal modtageren fuldbyrde kendelsen — det vil sige overføre dataene inden 10 dage eller 6 timer i nødstilfælde, eller bevare dem i op til 60 dage — medmindre dette er umuligt, fordi certifikatet er ufuldstændigt, på grund af *force majeure* eller fordi det er de facto umuligt for modtageren eller fordi modtageren nægter på grund af modstridende forpligtelser, som enten vedrører de grundlæggende rettigheder eller grundlæggende interesser i et tredjeland eller af andre grunde.
- Hvis modtageren ikke har opfyldt den modtagne kendelse uden at angive en grund, der kan accepteres af den udstedende myndighed, fuldbyrdes kendelsen i henhold til de planlagte procedurer af en kompetent fuldbyrdelsesmyndighed i den medlemsstat, hvor tjenesteyderen er repræsenteret eller etableret, medmindre der gælder begrænsede grunde til at nægte fuldbyrdelse og den fuldbyrdende myndighed gør indsigelse mod anerkendelsen eller fuldbyrdelsen af kendelsen.
- Hvis modtageren udstedte en begrundet indsigelse mod kendelsen på grundlag af modstridende forpligtelser, skal den udstedende myndighed henvise sagen til den kompetente domstol i sin medlemsstat, som derefter bliver ansvarlig for at vurdere den eventuelle konflikt og opretholde kendelsen, hvis der ikke er en konflikt. I tilfælde af en konflikt skal den kompetente domstol enten henvende sig til de centrale myndigheder i tredjelandet via sine nationale centralmyndigheder inden for en svarfrist på 15 dage, som kan forlænges med 30 dage efter begrundet anmodning i tilfælde af modstridende forpligtelser med hensyn til et tredjelands grundlæggende rettigheder eller grundlæggende interesser, eller afgøre, om den skal opretholde eller trække kendelsen tilbage på grund af andre grunde til afslag anført af modtageren.
- Uden forbehold for retsmidler, der er tilgængelige under GDPR og LED'en, har personer, hvis data er indhentet via en editionskendelse, også ret til effektive retsmidler mod denne kendelse.

Det Europæiske Databeskyttelsesråd vurderede de i udkastet til forordning planlagte procedurer og stillede garantier, som skal knyttes til de forskellige trin, og anbefaler følgende garantier og ændringer for hvert af de aspekter, der lægges frem i det efterfølgende.

a) Tærsklerne for udstedelse af kendelser bør hæves og kendelser skal udstedes eller godkendes af domstole

Hvad angår betingelserne for udstedelse af kendelser, bifalder det Europæiske Databeskyttelsesråd princippet om højere garantier for at få adgang til transaktions- eller indholdsdata. Det bemærkes dog, at henvisningen til "strafbare handlinger i udstedelsesstaten med en frihedsstraf på mindst 3 år"[22] på grund af manglen på fuldstændig harmonisering af strafferetlige sanktioner mellem medlemsstaterne

[22] Se artikel 5, stk. 3, litra a)

stadigvæk indebærer divergerende tærskler og uoverensstemmelser i beskyttelsen af registreredes data i EU.

Desuden understreger det Europæiske Databeskyttelsesråd, at tærsklen i udkastet, navnlig i betragtning af den brede definition af abonnentdata, synes ret lav for sikringskendelser og editionskendelser vedrørende abonnents- eller adgangsdata, eftersom alle strafbare handlinger i princippet kan begrunde udstedelsen af sådanne kendelser. På sammen måde er de myndigheder, der har tilladelse til at udstede sådanne kendelser, mere begrænsede i forbindelse med editionskendelser vedrørende transaktions- eller indholdsdata end i forbindelse med udstedelse af sikringskendelser eller editionskendelser om fremlæggelse af abonnents- eller adgangsdata, da anklagere kun kan udstede eller godkende sidstnævnte kendelser, mens enhver dommer, domstol eller undersøgelsesdommer kan udstede eller godkende alle kendelser.

Det Europæiske Databeskyttelsesråd beklager især, at den laveste tærskel, der giver de retshåndhævende myndigheder mulighed for at anmode om adgang til abonnents- og adgangsdata i forbindelse med en lovovertrædelse, bygger på en modsætningsslutning fra EU-Domstolens retspraksis (som fokuserer på de andre data) med henblik på at skelne mellem de garantier, der skal ydes. Faktisk understregede EU-Domstolen specifikt, at kompetente myndigheders adgang til trafik- og lokaliseringsdata skal begrænses til udelukkende at gælde i forbindelse med bekæmpelse af grov kriminalitet[23]. Det Europæiske Databeskyttelsesråd forstod, at forslaget ville give mulighed for uden forudgående tilladelse fra en domstol at anmode om adgang til meget grundlæggende oplysninger, som kun ville give mulighed for at identificere en person uden at afsløre nogen kommunikationsdata. Det beklager imidlertid den brede modsætningsslutning af denne afgørelse fra Kommissionen og opfordrer til, at der indføres højere garantier for at begrænse grundlaget for adgang til andre abonnent- og adgangsdata. Det Europæiske Databeskyttelsesråd foreslår, at man enten begrænser adgangen til disse data til en liste over forbrydelser i udkastet til forordning, eller i det mindste til "alvorlige lovovertrædelser", især i betragtning af den lavere tærskel for forhåndsgodkendelse, der er planlagt for disse data.

Desuden understreger det Europæiske Databeskyttelsesråd, at denne modsætningsslutning også medfører, at forslaget giver anklagere mulighed for at udstede eller godkende udstedelse af kendelser. Det Europæiske Databeskyttelsesråd er af den opfattelse, at dette med undtagelse af tilfælde vedrørende anmodninger om meget grundlæggende oplysninger, der kun vil kunne identificere en person uden at afsløre nogen kommunikationsdata, udgør et skridt tilbage i forhold til EU-Domstolens retspraksis vedrørende adgang til kommunikationsdata. I sin retspraksis vedrørende adgang til kommunikationsdata med henblik på retshåndhævelse har EU-Domstolen begrænset muligheden for at give denne type adgang, blandt andre kriterier og "*undtagen i tilfælde af gyldigt fastslået påtrængende nødvendighed*"[24], til en "*forudgående gennemgang foretaget af en domstol eller en uafhængig administrativ myndighed*", "*efter en begrundet anmodning fra kompetente nationale myndigheder, der er indgivet inden for rammerne af procedurer for forebyggelse, opklaring eller kriminel retsforfølgning*." [25]

Det Europæiske Databeskyttelsesråd minder om, at begrebet "domstol" er et selvstændigt begreb i EU-lovgivningen, og at EU-Domstolen konstant har understreget og mindet om de kriterier, der skal opfyldes for at blive betragtet som en domstol, herunder kriterierne for uafhængighed,[26] hvilket ikke

[23] Se sag 203/15 - præmis (125)
[24] Se sag 203/15 — præmis (120)
[25] Se forenede sager C 293/12 og C 594/12 — præmis (62)
[26] Se f.eks. sag C 203/14

synes at være tilfældet for anklagere, hvilket Den Europæiske Menneskerettighedsdomstol også har mindet om i sin retspraksis[27].

Derfor resulterer artikel 4, stk. 1, litra a) og b), og stk. 3, litra a) og b) i procedurer, hvor der gælder væsentligt færre garantier for abonnent- og adgangsdata, fordi en anklager på egen hånd vil være i stand til at anmode om data uden nogen yderligere kontrol fra myndigheden i den stat, hvor de ønskede data opbevares, eller fra myndigheden på det sted, hvor den juridiske repræsentant for det anmodede selskab befinder sig, og uden nogen form for kontrol fra en uafhængig administrativ myndighed.

Desuden bemærker det Europæiske Databeskyttelsesråd den såkaldte ekstra garanti i henhold til artikel 5, stk. 2, som begrænser muligheden for at udstede en editionskendelse i tilfælde, hvor en lignende foranstaltning er tilgængelig for samme forbrydelse i en sammenlignelig national situation. Databeskyttelsesrådet advarer mod en sådan bestemmelses kontraproduktive virkning: Det forekommer i højere grad som en opfordring til medlemsstaterne om at udvide deres nationale muligheder for at anmode om fremlæggelse af abonnents- eller adgangsdata med henblik på at sikre, at det er muligt at udstede editionskendelser i henhold til denne forordning, end et forsøg på at sørge for yderligere garantier.

b) Frister for tilvejebringelse af data bør være berettigede

Det Europæiske Databeskyttelsesråd bemærker, at europæiske editionskendelser skal besvares senest 10 dage efter modtagelsen af certifikatet, medmindre udstedelsesmyndigheden begrunder en tidligere videregivelse, og senest inden for 6 timer i nødsituationer, som fastsat i artikel 9, stk. 1 og 2.

Det Europæiske Databeskyttelsesråd har imidlertid ikke set nogen kriterier for fastlæggelse af myndighedernes forpligtelse til at dokumentere den nødsituation, som nødvendiggør fremlæggelse af data, heller ikke *efterfølgende*, med det formål at muliggøre en eventuel kontrol med anvendelsen af denne meget hurtige procedure, selv om en frist på seks timer sandsynligvis vil betyde en meget let kontrol, før dataene fremlægges, eller måske endda fraværet af nogen form for kontrol fra tjenesteyderens side. I konsekvensanalysen understreges nødvendigheden af, at de kompetente myndigheder har adgang til data i tide. Eksemplerne i konsekvensanalysen vedrører dog alle bevismateriale, som der er behov for i tilfælde af alvorlige forbrydelser (terrorhandlinger som involverer gidsler, vedvarende situationer med seksuelt misbrug af børn), men det forekommer ikke at være tilstrækkeligt at begrunde med bevismaterialets ustabile karakter, når der ikke er anden anledning til hastværket, end netop dataenes ustabile karakter. Derudover giver dataenes ustabile karakter ingen yderligere begrundelse for proportionaliteten med hensyn til at få adgang til data med færre garantier i disse situationer, hvor der ikke er anden anledning til hastværket, end netop dataenes ustabile karakter.

Desuden tvivler det Europæiske Databeskyttelsesråd på nødvendigheden af at fastsætte en frist på seks timer, når denne frist ikke finder anvendelse, før den udstedende myndighed giver yderligere præciseringer "inden for fem dage", i tilfælde af, at tjenesteyderen ikke kan overholde sin forpligtelse.

Det Europæiske Databeskyttelsesråd opfordrer derfor til at føje flere elementer til konsekvensanalysen med henblik på at begrunde nødvendigheden af disse frister i tilfælde, hvor forbrydelsen der begås eller retsforfølges ikke er alvorlig, og medmindre sådanne detaljerede elementer er angivet, at nødsituationen begrundes med eksplicitte kriterier, hvis der udstedes EPOC'er. Man kunne eksempelvis overveje samme model som i EIO-direktivet. EIO-direktivet indeholder en kortere frist, når det er berettiget på grundlag af "proceduremæssige frister, lovovertrædelsens grovhed eller andre

[27] Se f.eks. Moulin c/ Frankrig 23/11/2010

særligt presserende omstændigheder" (se artikel 12, stk. 2), eller en frist på 24 timer til at træffe afgørelse om midlertidige foranstaltninger (se artikel 32, stk. 2). Konsekvensanalysen af udkastet til forordningen indeholder ikke detaljerede elementer, som begrunder, hvorfor disse frister ikke er effektive, og de eneste understregede elementer er, at antallet af anmodninger, der sendes, overbelaster de modtagende retslige myndigheder, som ikke kan overholde fristerne.

c) Europæiske editions- og sikringskendelser må ikke anvendes til at anmode om data fra registrerede i en anden medlemsstat, uden som minimum at underrette de kompetente myndigheder i den pågældende medlemsstat, navnlig med hensyn til indholdsdata

Det Europæiske Databeskyttelsesråd minder om, at eksisterende instrumenter omfatter retsligt samarbejde og dermed supplerende sikkerhedsforanstaltninger, især med henblik på at kontrollere anmodningernes nødvendighed og proportionalitet, og understreger, at disse garantier er så meget desto mere berettiget i tilfælde, hvor de ønskede data er indholdsdata, som indebærer flere begrænsninger af de registreredes rettigheder med hensyn til at beskytte deres personlige oplysninger og privatliv. I den henseende minder det Europæiske Databeskyttelsesråd om, at EIO-direktivet også giver mulighed for at opfange telekommunikation med teknisk bistand fra en anden medlemsstat (se artikel 30) og for forpligtelsen til at underrette den kompetente myndighed i en anden medlemsstat om enhver form for opfangning af data, når der ikke er behov for assistance, når den berørte person er eller vil være på denne medlemsstats område (se artikel 31).

Det Europæiske Databeskyttelsesråd finder ingen begrundelse for den procedure, der er planlagt i udkastet til regulering af elektronisk bevismateriale, for at muliggøre udlevering af indholdsdata uden inddragelse af som minimum de kompetente myndigheder i den medlemsstat, hvor den registrerede befinder sig.

d) Europæiske sikringskendelser må ikke bruges til at omgå databehandlingsforpligtelserne hos tjenesteudbyderne

Det Europæiske Databeskyttelsesråd bemærker, at hovedformålet med europæiske sikringskendelser er at forhindre, at data slettes.

Selv om det Europæiske Databeskyttelsesråd erkender, at det kan være nødvendigt og forholdsmæssigt i nogle tilfælde, beklager det de manglende garantier vedrørende udstedelsen af sådanne kendelser. Det Europæiske Databeskyttelsesråd anbefaler navnlig, at når sikringskendelser er adresseret udelukkende vedrørende specifikke data, hvor udkastet tilsyneladende tillader brede anmodninger, og at når sådanne kendelser udstedes for data, der skal slettes i overensstemmelse med datalagringsprincippet, så skal kendelsen aldrig tjene som grundlag for tjenesteudbyderen til at behandle dataene efter den oprindelige sletningsdato. Med andre ord skal dataene være "spærret".

Derudover bør forbindelsen mellem sikringskendelser og den efterfølgende anmodning om fremlæggelse af data, uanset om den modtages via en europæisk sikringskendelse, en EIO-anmodning eller en anmodning om gensidig retshjælp, styrkes for at sikre, at en europæisk sikringskendelse kun udstedes, når den anden anmodning er sikker (og ikke kun tænkt som en mulighed), og at når den anden anmodning afvises, så udløber sikringskendelsen også, uden at det bliver nødvendigt at vente i 60 dage[28], hvis den efterfølgende anmodning afvises tidligere.

[28] Se artikel 10, stk. 1

e) Fortrolighed og brugeroplysninger

Det Europæiske Databeskyttelsesråd bemærker, at en specifik artikel[29] vedrørende fortroligheden af de adresserede kendelser er blevet indført i udkastet til forordningen. For at undgå enhver forvirring og misforståelse vedrørende retten til databeskyttelse minder det Europæiske Databeskyttelsesråd om, at selv om det er fastsat i GDPR, at begrænsninger af de registreredes rettigheder med hensyn til at sikre forebyggelse, efterforskning, opklaring eller retsforfølgning af straffelovsovertrædelser bør fastsættes ved lov og derfor være offentligt tilgængelige[30], og at disse lovgivningsmæssige foranstaltninger skal indeholde særlige bestemmelser om registreredes ret til at blive informeret om begrænsningen, medmindre det er til skade for formålet med begrænsningen[31], er der ikke fastsat nogen forpligtelse til at oplyse individuelle registrerede om hver adgangsanmodning fra de retshåndhævende myndigheder.

Det Europæiske Databeskyttelsesråd minder imidlertid om, at databeskyttelsesdirektivet indeholder bestemmelser om denne ret til information for de registrerede fra de kompetente myndigheder, medmindre denne ret er blevet begrænset, til alle registrerede uden at denne ret er begrænset til de registrerede, der er bosat på EU's område.

f) Procedure for fuldbyrdelse af en kendelse, når tjenesteudbyderen nægter at fuldbyrde den

Det Europæiske Databeskyttelsesråd bemærker, at artikel 14 i udkastet til forordning indeholder bestemmelser om en procedure, som har til formål at sikre fuldbyrdelsen af en kendelse, når modtageren ikke overholder den, med henvisning til et retsligt samarbejde mellem den udstedende myndighed og en kompetent myndighed i fuldbyrdelsesstaten.

Det lader dog til, at denne procedure ikke giver fuldbyrdelsesmyndigheden mulighed for at nægte at fuldbyrde kendelsen af andre grunde end rent proceduremæssige (de samme grunde som modtageren, som hovedsagelig vedrører manglende oplysninger eller at det er faktuelt umuligt at skaffe dataene), fordi de pågældende data er beskyttet af en immunitet eller et privilegium i henhold til den nationale lovgivning, eller fordi offentliggørelsen heraf kan påvirke myndighedens grundlæggende interesser, såsom national sikkerhed og forsvar[32].

Det Europæiske Databeskyttelsesråd gentager derfor sine bekymringer med hensyn til fjernelsen af enhver dobbeltkontrol foretaget af den modtagne kompetente myndighed af den fremsendte kendelse, i forhold til de øvrige instrumenter. Selv grunden til at nægte at fuldbyrde en kendelse med den begrundelse, at den ville krænke chartret, synes at være højere end den klassiske tærskel for overtrædelse af den pågældende persons grundlæggende rettigheder. Som følge af eksemplerne i den europæiske arrestordre, som indeholder obligatoriske og valgfrie grunde til afslag, eller i det mindste i EIO-direktivet, som generelt fastsætter, at formodningen om, at "oprettelsen af et område med frihed, sikkerhed og retfærdighed inden for Unionen er baseret på gensidig tillid og en formodning om, at andre medlemsstater overholder EU-lovgivningen og især de grundlæggende rettigheder" kan genfremsættes[33], bør udkastet til forordning i det mindste indeholde den mindste klassiske undtagelse, at hvis der er væsentlige grunde til at tro, at fuldbyrdelsen af en kendelse ville resultere i en krænkelse af en persons grundlæggende ret og at fuldbyrdelsesstaten ville tilsidesætte sine

[29] Se artikel 11
[30] Se artikel 23, stk. 1, litra d)
[31] Se artikel 23, stk. 2, litra h)
[32] Se artikel 14, stk. 2
[33] Se betragtning 19 i EIO-direktivet

forpligtelser vedrørende beskyttelse af de grundlæggende rettigheder, der er anerkendt i chartret, bør fuldbyrdelsen af kendelsen nægtes.

g) Fuldbyrdelse af kendelser og modstridende forpligtelser i henhold til lovgivning i et tredjeland (artikel 15-16)

Det Europæiske Databeskyttelsesråd glæder sig over modtageres mulighed i udkastet til forordning for at nægte at fuldbyrde en kendelse med den begrundelse, at det ville være i strid med de grundlæggende rettigheder, da den har til formål at yde garantier i tilfælde af modstridende juridiske forpligtelser. Databeskyttelsesrådet anser det også for afgørende, at forslaget indeholder bestemmelser om høring af myndigheder i tredjelande, i hvert fald hvor en konflikt opstår, samt en forpligtelse til at ophæve kendelsen, når et tredjelands myndighed gør indsigelse.

Derfor bør proceduren for at nægte at fuldbyrde en kendelse på grund af modstridende forpligtelser i henhold til lovgivning i tredjelande forbedres væsentligt.

For det første bemærker det Europæiske Databeskyttelsesråd, at udkastet til forordningen overlader det til en privat virksomhed, som modtager af en editionskendelse, at vurdere, om denne kendelse er i strid med gældende lovgivning i et tredjeland, der forbyder offentliggørelse af de ønskede data. Virksomheden skal fremlægge en begrundet indsigelse, herunder alle relevante oplysninger om tredjelandets lovgivning, dens anvendelighed i den foreliggende sag og arten af de modstridende forpligtelser.

Det Europæiske Databeskyttelsesråd er først og fremmest bekymret over, at det når en sådan indsigelse er rejst, alene er den kompetente domstol i udstedelsesmyndighedens medlemsstat, der vurderer, om der er en konflikt eller ej, da det kun er når domstolen konstaterer en konflikt, at den tager kontakt til myndighederne i tredjelande. Den kompetente EU-domstol er derfor tildelt kompetence til at fortolke tredjelandes lovgivning i denne sammenhæng, uden at være en specialist på området. Det er Det Europæiske Databeskyttelsesråds holdning, at forpligtelsen til at konsultere de kompetente myndigheder i tredjelandet derfor er for begrænset i det foreliggende forslag. Hvad angår databeskyttelse henleder det Europæiske Databeskyttelsesråd lovgiverens opmærksomhed på, at hvis en kompetent domstol i et tredjeland fortolker GDPR for at vurdere, om ordningen er i modstrid med dens egne krav, skal EU's databeskyttelsesmyndigheder og de kompetente domstole fortsat være kompetente til at vurdere lovligheden af overførslen på grundlag af en dom fra en domstol eller en afgørelse truffet af en administrativ myndighed i et tredjeland, der kræver overførsel eller offentliggørelse af personoplysninger inden for rammerne af GDPR[34].

Desuden understreger det Europæiske Databeskyttelsesråd, at vurderingen af lovgivningen i tredjelandet foretaget af den kompetente domstol i EU's anmodende stat skal baseres på objektive elementer, og er bekymret over de kriterier, der skal tages i betragtning af den kompetente domstol ved vurderingen af lovgivningen i tredjelandet i henhold til artikel 15, stk. 4, og artikel 16, stk. 5, litra a), i udkastet til forordningen. Domstolen skal vurdere det faktum, at tredjelandets lov "i stedet for at beskytte de grundlæggende rettigheder eller grundlæggende interesser i tredjelandet i forbindelse med national sikkerhed eller forsvar" snarere "åbenlyst søger at beskytte andre interesser eller sigter mod at beskytte ulovlige aktiviteter mod retshåndhævelsesanmodninger i forbindelse med strafferetlige undersøgelser" eller "interesser, der beskyttes af tredjelandets relevante lovgivning, herunder tredjelandets interesse i at forhindre offentliggørelse af data". Selv om denne vurdering eksempelvis i princippet bør kræve en evidensbaseret vurdering på baggrund af al tilgængelig

[34] Se artikel 48, GDPR

information i betragtning af en sådan beslutnings potentielle indvirkning, synes som minimum formuleringen ("sigter mod") at være uklar og bør tilpasses til ("har til formål/som mål at").

Det Europæiske Databeskyttelsesråd beklager, at det eneste tilfælde, hvor myndighederne i et tredjeland ville blive hørt og kunne modsætte sig fuldbyrdelsen af en editionskendelse, ville være, hvis denne kompetente EU-domstol finder, at der er en relevant konflikt, overfører alle elementer til de centrale myndigheder i det pågældende tredjeland og den centrale myndighed i det pågældende tredjeland gør indsigelse inden for de stramme frister på højst 50 dage (15 dage, eventuelt forlænget med 30 dage og efter en sidste påmindelse, der giver yderligere 5 dage). I alle andre tilfælde vil den kompetente domstol være i stand til at opretholde editionskendelser og udstede en økonomisk sanktion mod den tjenesteudbyder, der nægter at fuldbyrde kendelsen. Det Europæiske Databeskyttelsesråd er derfor bekymret over, at de kompetente EU-domstole ikke vil have en mere vidtrækkende forpligtelse til at høre de kompetente myndigheder i de pågældende tredjelande for at sikre, at proceduren mere systematisk sikrer, at begge parters argumenter tages i betragtning og til at udvise en højere grad af respekt for tredjelandes lovgivning.

Som allerede understreget i erklæringen fra Artikel 29-Gruppen og ovenstående, minder det Europæiske Databeskyttelsesråd om, at der bør lægges særlig vægt på tredjelandes vedtagelse af lignende instrumenter, der potentielt kan påvirke de registreredes rettigheder og deres ret til privatlivets fred i EU, især risikoen for lignende instrumenter, der ville komme i direkte konflikt med EU's databeskyttelseslovgivning.

Desuden understreger det Europæiske Databeskyttelsesråd, at det ikke engang nødvendigvis er den kompetente domstol i udstedelsesmyndighedens medlemsstat, der skal fuldbyrde den kendelse, der er omhandlet i artikel 14 i udkastet til forordningen, hvilket endda øger risikoen for modstridende procedurer og mangel på krydstjek i tilfælde af modstridende love. Dette skyldes, at der i nogle tilfælde kan være tre stater involveret: den, som huser den myndighed, der udsteder kendelsen, tjenesteyderens tredjeland og den medlemsstat, hvor tjenesteyderens juridiske repræsentant befinder sig, og hvor kendelsen skal fuldbyrdes. Efter den procedure, der på nuværende tidspunkt er foreslået, kan den anmodende myndigheds domstol i medlemsstat A derfor foretage sin egen fortolkning af loven i tjenesteyderens tredjeland B uden at skulle tage hensyn til myndighederne i dette tredjelands synspunkter (selv om de ville have anfægtet kendelsen) og bede en domstol i en anden EU-medlemsstat C om at fuldbyrde sin afgørelse uden at der er mulighed for at gøre indsigelse.

Desuden bifalder det Europæiske Databeskyttelsesråd også indførelsen af specifikke retsmidler mod editionskendelser, ud over de retsmidler, der er fastsat i GDPR og i LED'en. Artikel 29-Gruppen krævede allerede sådanne garantier i sin tidligere erklæring. Det Europæiske Databeskyttelsesråd beklager imidlertid, at sådanne retsmidler ikke også er planlagt i forbindelse med sikringskendelser, da disse kendelser også kan resultere i begrænsninger af de grundlæggende rettigheder for de personer, hvis oplysninger tilbageholdes. Sikringskendelser kan medføre, at oplysninger tilbageholdes i længere tid, end de ville være blevet i henhold til databeskyttelsesreglerne. Derfor indebærer sikringskendelser en begrænsning af de berørte registrerede personers grundlæggende rettigheder, hvis berettigelse skal underkastes en undersøgelse og gøres til genstand for specifikke afhjælpende foranstaltninger, især i tilfælde, hvor sikringskendelsen er blevet udstedt sammen med en editionskendelse for at få dataene. Som i Artikel 29-Gruppens erklæring, bør der fastsættes retsmidler, der mindst svarer til dem, der er tilgængelige i en national sag.

h) Sikkerheden i forbindelse med videregivelse af oplysninger, når der reageres på en kendelse

Det Europæiske Databeskyttelsesråd bemærker, at udkastet til forordningen kun fastsætter, at kendelser skal rettes til modtagere inden for EU og derfor ikke indeholder nogen særlig kanal til overførsel af data mellem de modtagere og tjenesteydere, der er beliggende uden for EU.

Selv om det Europæiske Databeskyttelsesråd bifalder, at udkastet ikke indeholder yderligere undtagelser fra EU's generelle rammebestemmelser for databeskyttelse, minder det om, at enhver kendelse, der sendes til en modtager, som indebærer en overførsel uden for EU, skal overholde de juridiske rammer i GDPR. Omgåelse af den juridiske ramme for det retslige samarbejde, som foreskriver, at databeskyttelsesgarantier skal respekteres, bør ikke også resultere i, at modtagere af editions- og sikringskendelser omgår dataoverførselskravene om at overholde sådanne kendelser.

Hertil kommer, at mens det Europæiske Databeskyttelsesråd bifalder manglen på bestemmelser om forpligtelse til at dekryptere krypterede data[35], er det bekymret for, at udkastet til forslaget ikke indeholder et specifikt krav til modtagere om at vurdere ægtheden af de fremlagte data og understreger, at denne vurdering også er tilføjet værdi for traditionelle instrumenter baseret på retsligt samarbejde og advarer mod de øgede risici for de berørte registrerede i mangel af en sådan vurdering.

Konklusioner

På baggrund af denne vurdering ønsker det Europæiske Databeskyttelsesråd at pege på følgende lovgivningsmæssige henstillinger:

1) Forordningens retsgrundlag bør ikke være artikel 82, stk. 1, TEUF.
2) Nødvendigheden af et nyt instrument i forhold til det eksisterende EIO-direktiv eller MLAT bør bedre demonstreres, herunder med en detaljeret analyse af mindre indgribende midler med hensyn til grundlæggende rettigheder, såsom ændringer af disse eksisterende instrumenter eller begrænsning af anvendelsesområdet for dette instrument for sikringskendelser i kombination med andre eksisterende procedurer for at anmode om adgang til dataene.
3) Forordningen bør fastsætte en længere frist for at gøre det muligt for den udførende tjenesteudbyder at sikre, at garantier med hensyn til beskyttelse af grundlæggende rettigheder, kan respekteres.
4) Princippet om dobbelt strafbarhed bør opretholdes, især hvis lokaliseringskriterier for dataene opgives for at opretholde forpligtelsen til at tage hensyn til de garantier, der ydes i begge berørte stater (den anmodende myndigheds stat og den stat, hvor tjenesteyderen befinder sig).
5) Forordningens anvendelsesområde bør begrænses til registeransvarlige som omhandlet i GDPR, eller den bør indeholde en bestemmelse om, at sidstnævnte er forpligtet til at underrette den dataansvarlige i tilfælde af, at tjenesteudbyderen ikke er den registeransvarlige, men databehandleren.
6) Forordningen bør omfatte garantier vedrørende dataoverførsler, hvis tjenesteudbyderen er etableret i et tredjeland, uden at der er truffet en tilstrækkelig afgørelse på dette område, eller henvise til direktiv 2016/680, da disse garantier vil finde anvendelse.
7) Da den obligatoriske udpegelse af en juridisk repræsentant afviger fra GDPR, bør forordningen præcisere, at den juridiske repræsentant, der er udpeget i henhold til forordningen om elektronisk bevismateriale, skal være forskellig fra den, der er udpeget i henhold til artikel 3, stk. 2, i GDPR.

[35] Se betragtning 19 og side 240 af konsekvensanalysen

8) Forordningen bør indeholde en bredere definition af elektroniske kommunikationsdata for at sikre, at de relevante etablerede garantier og betingelser for adgang, dækker både ikke-indholds- og indholdsdata.
9) Forordningen bør hæve tærsklerne for udstedelse af kendelser, og kendelser skal udstedes eller godkendes af domstole med undtagelse af abonnentdata, forudsat at definitionen af denne kategori af data reduceres drastisk til meget grundlæggende oplysninger, der kun tillader at identificere en person uden at inddrage adgang til nogen kommunikationsdata.
10) Forordningen bør begrænse adgangen til abonnents- og adgangsdata til en liste over forbrydelser, der er strengt fastlagt eller i det mindste til "alvorlige lovovertrædelser".
11) Fristen for at levere data, især i tilfælde af nødsituationer, bør være bedre begrundet i forordningen, og muligheden for at anvende en hurtig 6-timers procedure bør omfatte en forpligtelse til at anmode myndighederne om at dokumentere nødsituationen, der udløser brugen af denne procedure, selv efterfølgende, for at gøre det muligt at kontrollere brugen af sådanne ekstraordinære beføjelser.
12) Den procedure, der tillader fremlæggelse af indholdsdata uden involvering af de kompetente myndigheder i den medlemsstat, hvor den registrerede er, bør opgives.
13) Garantier i forbindelse med udstedelse af europæiske sikringskendelser bør forbedres i forordningen.
14) Forordningen bør i det mindste indeholde den minimale klassiske undtagelse, at hvis der er væsentlige grunde til at antage, at fuldbyrdelsen af en kendelse ville medføre en krænkelse af en grundlæggende ret for den pågældende person, der fører fuldbyrdelsesstaten til at tilsidesætte sine forpligtelser vedrørende beskyttelse af grundlæggende rettigheder anerkendt i chartret, bør fuldbyrdelsen af kendelsen nægtes.
15) Forordningen bør indeholde en bredere forpligtelse til at konsultere de kompetente myndigheder i et tredjeland, hvor tjenesteyderen, der er blevet anmodet om at levere data, er placeret, i tilfælde af lovgivningskonflikt, for at undgå subjektive fortolkninger fra en enkelt domstol.
16) Gyldighedsperioden og varigheden af sikringskendelser skal være bedre knyttet til de editionskendelser, der følger med dem.
17) Sikkerheden ved dataoverførsler bør sikres bedre.
18) Kontrollen med dataenes ægthed bør overvejes, især hvor krypterede data kunne leveres.

For Det Europæiske Databeskyttelsesråd

Formanden

(Andrea Jelinek)