

Bruxelles, den 18. maj 2018
(OR. en)

8110/18

**Interinstitutionel sag:
2018/0108 (COD)**

JAI 323
COPEN 104
CYBER 66
DROIPEN 53
JAIEX 27
ENFOPOL 171
TELECOM 94
DAPIX 106
EJUSTICE 27
MI 269
IA 101
CODEC 577

FORSLAG

fra:	Jordi AYET PUIGARNAU, direktør, på vegne af generalsekretæren for Europa-Kommissionen
modtaget:	18. maj 2018
til:	Jeppe TRANHOLM-MIKKELSEN, generalsekretær for Rådet for Den Europæiske Union
Komm. dok. nr.:	COM(2018) 225 final
Vedr.:	Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om europæiske editions- og sikringskendelser om elektronisk bevismateriale i straffesager

Hermed følger til delegationerne dokument - COM(2018) 225 final.

Bilag: COM(2018) 225 final



EUROPA-
KOMMISSIONEN

Strasbourg, den 17.4.2018
COM(2018) 225 final

2018/0108 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

**om europæiske editions- og sikringskendelser om elektronisk bevismateriale i
straffesager**

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

BEGRUNDELSE

1. BAGGRUND FOR FORSLAGET

• Forslagets begrundelse og formål

I dag er det blevet almindeligt i mange dele af verden at bruge webmail, sociale medier, beskedtjenester og applikationer ("apps") til at kommunikere, arbejde, mødes og indhente oplysninger. Disse tjenester forbinder hundredvis af millioner af brugere med hinanden. De øger i væsentlig grad brugernes økonomiske og sociale velfærd i og uden for Unionen. De kan imidlertid også misbruges som redskaber til at begå eller muliggøre kriminalitet, herunder grov kriminalitet såsom terrorangreb. Når dette sker, er disse tjenester og applikationer ofte det eneste sted, hvor efterforskere kan finde spor til at fastslå, hvem der har begået kriminalitet, og fremskaffe bevismateriale, som kan bruges i retten.

I betragtning af internettets grænseløse karakter kan sådanne tjenester leveres fra hvor som helst i verden, og det kræver ikke nødvendigvis en fysisk infrastruktur, etablering af en virksomhed eller personale i de medlemsstater, hvor tjenesterne udbydes, eller i det indre marked som helhed. Det er heller ikke en forudsætning, at oplysningerne lagres et bestemt sted, og tjenesteudbyderen vælger ofte dette sted ud fra legitime hensyn såsom datasikkerhed, stordriftsfordele og hurtig adgang. I forbindelse med et stigende antal straffesager, der involverer alle former for kriminalitet¹, skal medlemsstaternes myndigheder derfor have adgang til oplysninger, der kan tjene som bevismateriale, og som er lagret uden for deres egen medlemsstat og/eller af tjenesteudbydere i andre medlemsstater eller tredjelande.

Der er blevet indført mekanismer for samarbejde mellem landene for flere årtier siden til håndtering af de situationer, hvor bevismaterialet eller tjenesteudbyderen befinder sig et andet sted². Trods jævnlige reformer er disse samarbejdsmechanismer under stigende pres som følge af det voksende behov for rettidig, grænseoverskridende adgang til elektronisk bevismateriale. En række medlemsstater og tredjelande har i denne forbindelse udvidet deres nationale værktøjer. Den heraf følgende fragmentering skaber retsusikkerhed og modstridende forpligtelser og skaber tvivl om beskyttelsen af de grundlæggende rettigheder og retssikkerhedsgarantier for personer, der er berørt af sådanne anmodninger.

I 2016 opfordrede Rådet til konkrete foranstaltninger baseret på en fælles EU-tilgang med henblik på at gøre den gensidige retshjælp mere effektiv, at forbedre samarbejdet mellem medlemsstaternes myndigheder og tjenesteudbydere etableret i tredjelande og at foreslå løsninger på problemet med at fastlægge og håndhæve kompetencen³ i cyberspace⁴. Europa-Parlamentet fremhævede ligeledes, at de forskellige lovgivningsrammer kan skabe problemer for tjenesteudbyderne, når de forsøger at imødekomme anmodninger fra de retshåndhævende myndigheder, og opfordrede til, at der blev etableret en europæisk lovgivningsramme med tilstrækkelige garantier for alle berørte parter rettigheder og friheder⁵.

¹ Jf. afsnit 2.1.1 og 2.3 i konsekvensanalysen.

² I Unionen – aftaler om gensidig anerkendelse – i dag baseret på direktivet om den europæiske efterforskningskendelse, med tredjelande – aftaler om gensidig retshjælp.

³ I dette dokument forstås ved udtrykket "håndhævelseskompetence" de relevante myndigheders kompetence til at udføre en efterforskningsforanstaltning.

⁴ [Rådets konklusioner om styrkelse af strafferetten i cyberspace af 9. juni 2016, ST9579/16.](#)

⁵ [P8_TA\(2017\)0366.](#)

I dette forslag er der fokus på det særlige problem med elektronisk bevismateriale meget ustabile karakter og dets internationale dimension. Det har til formål at tilpasse samarbejdsmekanismerne til den digitale tidsalder, give domstolene og de retshåndhævende myndigheder redskaber til at sætte ind over for den måde, som kriminelle kommunikerer på i dag, og imødegå nye former for kriminalitet. Sådanne redskaber er betinget af, at de er omfattet af stærke mekanismer til beskyttelse af grundlæggende rettigheder. Formålet med dette forslag er at styrke myndighedernes, tjenesteudbydernes og de berørte personers retssikkerhed og at opretholde en høj standard for anmodninger fra de retshåndhævende myndigheder og således sikre beskyttelsen af grundlæggende rettigheder, gennemsigtighed og ansvarlighed. Det fremskynder endvidere processen med at sikre og indhente elektronisk bevismateriale, som lagres og/eller opbevares af tjenesteudbydere, der er etableret i en anden jurisdiktion. Dette instrument er et supplement til de nuværende instrumenter for retligt samarbejde, som stadig er relevante og kan anvendes af de kompetente myndigheder, når det er hensigtsmæssigt. Sideløbende hermed arbejder Kommissionen på at styrke de eksisterende mekanismer for retligt samarbejde gennem foranstaltninger såsom oprettelsen af en sikker platform for hurtig udveksling af anmodninger mellem judicielle myndigheder i EU og investeringer på 1 mio. EUR i efteruddannelse af fagfolk fra alle EU-medlemsstaterne på området gensidig retshjælp og samarbejde med fokus på USA, som er det tredjeland, der modtager det største antal anmodninger fra EU⁶.

For så vidt angår forkyndelse og fuldbyrdelse af kendelser i henhold til dette instrument, bør myndighederne stille kendelsen til den retlige repræsentant udpeget af tjenesteudbyderne. Kommissionen fremlægger i dag et forslag, der skal sikre, at sådanne retlige repræsentanter rent faktisk udpeges. Det sikrer en fælles, EU-dækkende løsning, hvor kendelser til tjenesteudbydere stiles til den retlige repræsentant.

- **Sammenhæng med de gældende regler på samme område og Europarådets Budapestkonvention**

Den gældende retlige ramme i EU omfatter Unionens samarbejdsinstrumenter i straffesager såsom direktiv 2014/41/EU om den europæiske efterforskningskendelse i straffesager⁷, konventionen om gensidig retshjælp i straffesager mellem Den Europæiske Unions medlemsstater⁸, Rådets afgørelse 2002/187/RIA om oprettelse af Eurojust⁹, forordning (EU) 2016/794 om Europol¹⁰, Rådets rammeafgørelse 2002/465/RIA om fælles efterforskningshold¹¹ samt bilaterale aftaler mellem Unionen og tredjelande såsom aftalen om

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

⁷ Europa-Parlamentets og Rådets [direktiv 2014/41/EU](#) af 3. april 2014 om den europæiske efterforskningskendelse i straffesager (EUT L 130 af 1.5.2014, s. 1).

⁸ [Rådets retsakt af 29. maj 2000](#) om udarbejdelse i henhold til artikel 34 i traktaten om Den Europæiske Union af konventionen om gensidig retshjælp i straffesager mellem Den Europæiske Unions medlemsstater.

⁹ [Rådets afgørelse 2002/187/RIA](#) af 28. februar 2002 om oprettelse af Eurojust for at styrke bekæmpelsen af grov kriminalitet. I 2013 vedtog Kommissionen et [forslag til forordning](#) om en reform af Eurojust (forslag til Europa-Parlamentets og Rådets forordning om Den Europæiske Unions Agentur for Strafferetligt Samarbejde (Eurojust), COM/2013/0535 final).

¹⁰ Europa-Parlamentets og Rådets [forordning \(EU\) 2016/794](#) af 11. maj 2016 om Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol) og om erstating og ophævelse af Rådets afgørelse 2009/371/RIA, 2009/934/RIA, 2009/935/RIA, 2009/936/RIA og 2009/968/RIA.

¹¹ [Rådets rammeafgørelse 2002/465/RIA](#) af 13. juni 2002 om fælles efterforskningshold.

gensidig retshjælp mellem EU og USA¹² og aftalen om gensidig retshjælp mellem EU og Japan¹³.

Ved at indføre europæiske editionskendelser og europæiske sikringskendelser gør forslaget det lettere at sikre og indhente elektronisk bevismateriale i straffesager, der lagres eller opbevares af tjenesteudbydere i en anden jurisdiktion. Direktivet om den europæiske efterforskningskendelse, som i vid udstrækning har erstattet konventionen om gensidig retshjælp i straffesager, omfatter alle efterforskningsforanstaltninger¹⁴. Det omfatter adgang til elektronisk bevismateriale, men direktivet om den europæiske efterforskningskendelse indeholder ingen specifikke bestemmelser om denne type bevismateriale¹⁵. Det nye instrument vil ikke erstatte den europæiske efterforskningskendelse til fremskaffelse af elektronisk bevismateriale, men er et yderligere redskab til myndighederne. Der kan være situationer, f.eks. når flere efterforskningsforanstaltninger skal udføres i fuldbyrdesstaten, hvor den europæiske efterforskningskendelse kan være det foretrukne valg for de offentlige myndigheder. Oprettelsen af et nyt instrument til indhentning af elektronisk bevismateriale er et bedre alternativ end at ændre direktivet om den europæiske efterforskningskendelse på grund af de særlige udfordringer, der er forbundet med at indhente elektronisk bevismateriale, som ikke berører de andre efterforskningsforanstaltninger, der er omfattet af direktivet om den europæiske efterforskningskendelse.

For at lette den grænseoverskridende indsamling af elektronisk bevismateriale er det nye instrument baseret på principperne om gensidig anerkendelse. En myndighed i det land, hvor modtageren af kendelsen er bosat eller etableret, behøver ikke at være direkte involveret i forkyndelsen og fuldbyrdelsen af kendelsen, medmindre der er tale om manglende overholdelse, hvor fuldbyrdelse i så fald vil være påkrævet, og hvor den kompetente myndighed i det land, hvor repræsentanten er bosat eller beliggende, skal gribe ind. Instrumentet skal derfor ledsages af et sæt robuste garantier og bestemmelser såsom den judicielle myndigheds godkendelse af den enkelte kendelse. Europæiske editionskendelser om fremlæggelse af transaktions- eller indholdsdata (ikke abonnent- og adgangsdata) må f.eks. kun udstedes for lovovertrædelser, der i udstedelsesstaten kan straffes med en frihedsstraf af en maksimal varighed på mindst tre år, eller for specifikke cyber- eller terrorrelaterede strafbare handlinger som omhandlet i forslaget.

Personoplysninger, der er omfattet af dette forslag, er beskyttet og kan kun behandles i overensstemmelse med den generelle forordning om databeskyttelse¹⁶ og direktivet om databeskyttelse vedrørende politi og strafferetlige myndigheder (direktivet om databeskyttelse

¹² [Rådets afgørelse 2009/820/FUSP](#) af 23. oktober 2009 om indgåelse på Den Europæiske Unions vegne af aftalen mellem Den Europæiske Union og Amerikas Forenede Stater om udlevering og aftalen mellem Den Europæiske Union og Amerikas Forenede Stater om gensidig retshjælp.

¹³ [Rådets afgørelse 2010/616/EU](#) af 7. oktober 2010 om indgåelse af aftalen mellem Den Europæiske Union og Japan om gensidig retshjælp i straffesager.

¹⁴ Undtagen for fælles efterforskningshold (jf. artikel 3 i direktivet om den europæiske efterforskningskendelse). Det er ikke alle medlemsstaterne, som deltager i direktivet om den europæiske efterforskningskendelse (Irland, Danmark).

¹⁵ Bortset fra en henvisning til identifikation af en person med en IP-adresse i artikel 10, stk. 2, litra e), hvor der ikke kan påberåbes dobbelt strafbarhed som begrundelse for ikke at anerkende og fuldbyrde anmodningen.

¹⁶ 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.

på retshåndhævelsesområdet)¹⁷. Den generelle forordning om databeskyttelse træder i kraft den 25. maj 2018, og direktivet om databeskyttelse på retshåndhævelsesområdet skal være gennemført af medlemsstaterne senest den 6. maj 2018.

I Europarådets Budapestkonvention om IT-kriminalitet (CETS nr. 185), der er ratificeret af de fleste EU-medlemsstater, er der fastsat internationale samarbejdsmekanismer til bekæmpelse af IT-kriminalitet¹⁸. Konventionen omhandler kriminalitet, der begås ved hjælp af internettet og andre edb-netværk. Den pålægger ligeledes parterne at fastsætte beføjelser og procedurer til indsamling af elektronisk bevismateriale og at yde hinanden gensidig retshjælp, ikke kun om IT-kriminalitet. Konventionen pålægger navnlig parterne at indføre bestemmelser vedrørende pålæg om udlevering af elektroniske data fra serviceudbydere på deres område og af kundeoplysninger fra serviceudbydere, der udbyder deres tjenester på deres område. Konventionen indeholder desuden bestemmelser vedrørende pålæg om udlevering af elektroniske data, hvis der er grund til at antage, at relevante data er særligt udsatte for at gå tabt eller blive ændret. Forkyndelse og fuldbyrdelse af nationale pålæg om udlevering af elektroniske data fra serviceudbydere, der er etableret uden for en part i konventionens område, giver anledning til yderligere problemer. I denne forbindelse er yderligere foranstaltninger til at forbedre den grænseoverskridende adgang til elektroniske beviser i øjeblikket under overvejelse¹⁹.

• **Resumé af forslaget til forordning**

Den foreslåede forordning indfører bindende europæiske editions- og sikringskendelser. Begge kendelser skal udstedes og godkendes af en judiciel myndighed i en medlemsstat. Der kan udstedes en kendelse om sikring eller fremlæggelse af oplysninger, som opbevares af en tjenesteudbyder, der er etableret i en anden jurisdiktion, der er nødvendige som bevismateriale i strafferetlige efterforskninger eller straffesager. Sådanne kendelser kan kun udstedes, hvis en lignende foranstaltning er tilgængelig for samme lovovertrædelse i en sammenlignelig national situation i udstedelsesstaten. Begge kendelser kan rettes til udbydere af elektroniske kommunikationstjenester, sociale netværk, onlinemarkedspladser, andre hostingtjenester og udbydere af internetinfrastruktur såsom IP-adresse- og domænenavneadministratorer eller deres eventuelle retlige repræsentanter. Den europæiske sikringskendelse rettes ligesom den europæiske editionskendelse til den retlige repræsentant uden for udstedelsesstatens jurisdiktion for at sikre, at oplysningerne bevares med henblik på en efterfølgende anmodning om at fremlægge disse oplysninger, f.eks. via kanaler for gensidig retshjælp i forbindelse med tredjelande eller via en europæisk efterforskningskendelse mellem de deltagende medlemsstater. I modsætning til overvågningsforanstaltninger eller pligt til opbevaring af data i henhold til lovgivningen, som ikke er omfattet af denne forordning, er den europæiske sikringskendelse en kendelse udstedt eller godkendt af en judiciel myndighed i forbindelse

¹⁷ Europa-Parlamentets og Rådets [direktiv \(EU\) 2016/680](#) af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA.

¹⁸ I EU-strategien for cybersikkerhed fra 2013 blev Budapestkonventionen anerkendt som den primære multilaterale ramme for bekæmpelse af IT-kriminalitet – fælles meddelelse til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget om en EU-strategi for cybersikkerhed: Et åbent, sikkert og beskyttet cyberspace (COM JOIN(2013) 1 final)).

¹⁹ På sin 17. plenarforsamling (juni 2017) vedtog komitéen om konventionen om IT-kriminalitet (T-CY) vedtaget af kommissoriet for udarbejdelsen af den anden tillægsprotokol til konventionen ("anden tillægsprotokol"), som skal udarbejdes og færdigbehandles af T-CY senest i december 2019. Formålet er at bevæge sig væk fra, at det sted, hvor oplysningerne er lagret, er en afgørende faktor.

med en konkret straffesag efter en individuel vurdering af proportionaliteten og nødvendigheden af den enkelte kendelse. Ligesom den europæiske editionskendelse vedrører den specifikke kendte eller ukendte gerningsmænd til en strafbar handling, der allerede har fundet sted. Den europæiske sikringskendelse gør det kun muligt at bevare data, der allerede er lagret på tidspunktet for modtagelsen af kendelsen, idet der ikke kan opnås adgang til data på et senere tidspunkt efter modtagelsen af den europæiske sikringskendelse.

Begge kendelser kan kun anvendes i straffesager i perioden forud for retssagen indtil sagens afslutning ved dom eller anden afgørelse. Kendelser om fremlæggelse af abonnent- og adgangsdata kan udstedes for enhver lovovertrædelse, hvorimod kendelser om fremlæggelse af transaktions- eller indholdsdata kun kan udstedes for lovovertrædelser, der i udstedelsesstaten kan straffes med en frihedsstraf af en maksimal varighed på mindst tre år, eller for specifikke forbrydelser som omhandlet i forslaget, hvor der er en specifik forbindelse til de elektroniske værktøjer og lovovertrædelser, der er omfattet af direktiv (EU) 2017/541 om bekæmpelse af terrorisme.

I betragtning af de forskellige niveauer af indgriben forbundet med de foranstaltninger, der træffes for at fremskaffe de anmodede oplysninger, indeholder forslaget en række betingelser og garantier. Disse omfatter forpligtelsen til at indhente en judiciel myndigheds forudgående godkendelse af kendelser. Forslaget finder kun anvendelse på lagrede data. Tidstro aflytning af telekommunikation er ikke omfattet af dette forslag. Foranstaltningen er begrænset til, hvad der er nødvendigt og står i rimeligt forhold til formålet med relevante straffesager. Det giver ligeledes tjenesteudbyderne mulighed for at anmode udstedelsesmyndighederne om en nærmere forklaring, hvis det er nødvendigt. Hvis disse problemer ikke kan løses, og udstedelsesmyndigheden beslutter at gennemføre fuldbyrdelsen, kan tjenesteudbyderne gøre de samme grunde gældende ved indsigelsen mod dens egne myndigheders fuldbyrdelse. Der indføres desuden en særlig procedure for situationer, hvor forpligtelsen til at fremlægge oplysninger er i strid med en forpligtelse i et tredjelandets lovgivning.

EU-lovgivningen beskytter mistænkte og tiltalte rettigheder i straffesager, og der er allerede indført bestemmelser om beskyttelse af personoplysninger. For personer, hvis oplysninger efterspørges, sikrer disse yderligere garantier i forslaget imidlertid disse personer proceduremæssige rettigheder i straffesager og andre sager. Dette omfatter muligheden for at anfægte lovligheden, nødvendigheden eller proportionaliteten af kendelsen uden at begrænse indsigelsesgrundene i overensstemmelse med national lovgivning. Rettighederne i henhold til lovgivningen i fuldbyrdelsesstaten respekteres fuldt ud ved at sikre, at immuniteter og privilegier, som beskytter de oplysninger, der anmodes om i tjenesteudbyderens medlemsstat, tages i betragtning i udstedelsesstaten. Dette er navnlig tilfældet, når de sikrer en højere beskyttelse end lovgivningen i udstedelsesstaten.

Kendelserne som omhandlet i den foreslåede forordning kan fuldbyrdes på samme måde som tilsvarende nationale kendelser i den jurisdiktion, hvor tjenesteudbyderen modtager kendelsen. Det fastslås i forordningen, at medlemsstaterne skal indføre effektive og forholdsmæssige sanktioner.

2. RETSGRUNDLAG, NÆRHEDSPRINCIPPET OG PROPORTIONALITETSPRINCIPPET

• Retsgrundlag

Retsgrundlaget for foranstaltninger på området er artikel 82, stk. 1, i traktaten om Den Europæiske Unions funktionsmåde. I henhold til artikel 82, stk. 1, kan der vedtages

foranstaltninger efter den almindelige lovgivningsprocedure til fastlæggelse af regler og procedurer, der sikrer anerkendelsen af alle former for domme og retsafgørelser i hele Unionen. Der kan ligeledes vedtages foranstaltninger for at fremme samarbejdet mellem judicielle eller tilsvarende myndigheder i medlemsstaterne i forbindelse med strafforfølgning og fuldbyrdelse af afgørelser.

Dette retsgrundlag finder anvendelse på de mekanismer, der er omfattet af denne forordning. Artikel 82, stk. 1, sikrer gensidig anerkendelse af retsafgørelser, hvorved en judiciel myndighed i udstedelsesstaten retter henvendelse til en juridisk person i en anden medlemsstat og endog pålægger denne forpligtelser uden forudgående inddragelse af en judiciel myndighed i denne anden medlemsstat. Den europæiske editions- eller sikringskendelse kan indebære, at en judiciel myndighed i fuldbyrdelsesstaten griber ind, hvis det er nødvendigt for at fuldbyrde afgørelsen.

- **Valg af retsakt**

Artikel 82, stk. 1, i TEUF giver EU-lovgiveren mulighed for at vedtage forordninger og direktiver.

Eftersom forslaget vedrører grænseoverskridende procedurer, hvor der er behov for ensartede regler, er det ikke nødvendigt at give medlemsstaterne en margin til omsætningen af disse regler. En forordning gælder umiddelbart, skaber klarhed og større retssikkerhed, og forskellige fortolkninger i medlemsstaterne og andre gennemførelsesproblemer, f.eks. som i forbindelse med rammeafgørelserne om gensidig anerkendelse af domme og retsafgørelser, undgås. Med en forordning kan den samme forpligtelse desuden pålægges på en ensartet måde i Unionen. Derfor anses den mest hensigtsmæssige form til dette instrument til gensidig anerkendelse at være en forordning.

- **Nærhedsprincippet**

I betragtning af den grænseoverskridende dimension af de pågældende problemer skal foranstaltningerne i forslaget vedtages på EU-plan for at nå de fastsatte mål. De former for kriminalitet, hvor der foreligger elektronisk bevismateriale, involverer ofte situationer, hvor den infrastruktur, som det elektroniske bevismateriale er lagret på, og tjenesteudbyderen, der driver infrastrukturen, er omfattet en anden national retlig ramme i eller uden for Unionen end den nationale retlige ramme, som ofret og gerningsmanden til den strafbare handling er omfattet af. Det kan derfor være meget tidkrævende og vanskeligt for det kompetente land at få effektiv adgang til elektronisk bevismateriale på tværs af grænserne uden fælles minimumsregler. De medlemsstater, der handler alene, ville navnlig have vanskeligt ved at håndtere følgende aspekter:

- De forskellige lovgivningsrammer i medlemsstaterne, der blev identificeret som en stor udfordring af tjenesteudbydere, når de forsøger at imødekomme anmodninger baseret på forskellige nationale lovgivninger.
- Et mere effektivt retligt samarbejde på grundlag af eksisterende EU-lovgivning, navnlig via den europæiske efterforskningskendelse.

På grund af de forskellige retlige tilgange, antallet af berørte politikområder (sikkerhed, grundlæggende rettigheder, herunder proceduremæssige rettigheder og beskyttelse af personoplysninger, økonomiske aspekter) og den brede vifte af interessenter er lovgivning på EU-plan det mest hensigtsmæssige middel til at tackle de konstaterede problemer.

- **Proportionalitetsprincippet**

I forslaget fastsættes regler, hvorefter en kompetent myndighed i en medlemsstat kan pålægge en tjenesteudbyder, der udbyder tjenester i Unionen, men ikke er etableret i samme medlemsstat, at fremlægge eller bevare elektronisk bevismateriale. De vigtigste elementer i forslaget såsom det materielle anvendelsesområde for den europæiske editionskendelse, betingelser, der sikrer anerkendelse af domme, sanktionsmekanismen og garantierne og retsmidlerne begrænser forslaget til, hvad der er nødvendigt for at nå dets vigtigste mål. Forslaget er navnlig begrænset til anmodninger om lagrede data (data fra tidstro aflytning af telekommunikation er ikke omfattet) og til kendelser udstedt i straffesager for en bestemt strafbar handling, der efterforskes. Forslaget vedrører derfor ikke forebyggelse af kriminalitet eller andre typer procedurer eller overtrædelser (f.eks. administrative procedurer for overtrædelse af retsreglerne), og der stilles ikke krav til udbyderne om at indsamle eller opbevare flere personoplysninger, end de gør af forretningsmæssige årsager eller for at opfylde andre lovkrav. Kendelser om fremlæggelse af abonnent- og adgangsdata kan udstedes for enhver lovovertrædelse, hvorimod kendelser om fremlæggelse af transaktions- eller indholdsdata kun kan udstedes for lovovertrædelser, der i udstedelsesstaten kan straffes med en frihedsstraf af en maksimal varighed på mindst tre år, eller for specifikke cyberrelaterede strafbare handlinger som defineret i forslaget og terrorrelaterede strafbare handlinger. Endelig redegøres der i forslaget nærmere for de procedureregler og garantier, der gælder for grænseoverskridende adgang til elektronisk bevismateriale, men det går ikke så vidt som til at harmonisere nationale foranstaltninger. Det er begrænset til, hvad der er nødvendigt og forholdsmæssigt for at imødekomme de retshåndhævende og judicielle myndigheders behov i den digitale tidsalder.

3. RESULTATER AF EFTERFØLGENDE EVALUERINGER, HØRINGER AF INTERESSEREDE PARTER OG KONSEKVENSANALYSER

- **Høringer af interesserede parter**

Kommissionen hørte alle relevante interessenter i over halvandet år for at identificere problemer og løsninger. Dette blev gjort gennem undersøgelser, lige fra en åben offentlig høring til målrettede undersøgelser med de relevante offentlige myndigheder. Der blev ligeledes afholdt ekspertmøder og bilaterale møder for at drøfte de potentielle virkninger af EU-lovgivning. Der blev også afholdt konferencer om grænseoverskridende adgang til elektronisk bevismateriale, hvor der blev indsamlet feedback vedrørende initiativet.

Respondenterne i undersøgelserne var i det store og hele af den opfattelse, at den øgede anvendelse af informationstjenester var en udfordring for de retshåndhævende myndigheder, da de relevante myndigheder ofte er dårligt udrustet til at håndtere onlinebevismateriale. Den langvarige proces med at fremskaffe bevismateriale anerkendes også som en af de største hindringer. Andre vigtige spørgsmål, der blev fremhævet af de offentlige myndigheder, var, at der ikke var et pålideligt samarbejde med tjenesteudbydere, manglende gennemsigtighed og retsusikkerhed omkring retternes kompetence i forbindelse med efterforskningsforanstaltninger. Direkte grænseoverskridende samarbejde mellem retshåndhævende myndigheder og udbydere af digitale tjenester blev anset for at tilføre merværdi i en strafferetlig efterforskning. Tjenesteudbydere og en række civilsamsfundsorganisationer påpegede behovet for at sikre retssikkerheden i forbindelse med samarbejdet med de offentlige myndigheder og undgå lovkonflikter. Med hensyn til bekymringer over, hvordan den nye EU-lovgivning kan påvirke rettigheder, mente interessenterne, at bestemte garantier burde sikres som en nødvendig betingelse for ethvert grænseoverskridende instrument.

Feedback fra den indledende konsekvensanalyse viste, at interessenterne mente, at afhjælpning af manglerne i det nuværende system for gensidig retshjælp vil gøre det mere effektivt og forbedre retssikkerheden. Nogle civilsamfundsorganisationer var imod lovgivning på EU-plan om direkte samarbejde. De ønskede at begrænse EU's indsats til forbedring af procedurerne for gensidig retshjælp. Denne idé vil indgå i de konkrete foranstaltninger, der blev godkendt af Rådet i juni 2016.

En undersøgelse rettet mod offentlige myndigheder i medlemsstaterne viste ligeledes, at der ikke var nogen fælles tilgang til opnåelse af grænseoverskridende adgang til elektronisk bevismateriale, da de enkelte medlemsstater har deres egen nationale praksis. Tjenesteudbydere reagerer ligeledes forskelligt på anmodninger fra udenlandske retshåndhævende myndigheder, og svartiderne varierer afhængigt af den anmodende medlemsstat. Dette skaber retsusikkerhed for alle involverede interessenter.

Generelt viste høringen af interessenterne, at det nuværende retsgrundlag er fragmenteret og komplekst. Dette kan føre til forsinkelser i gennemførelsesfasen og en ineffektiv efterforskning og retsforfølgning af kriminalitet, der forudsætter grænseoverskridende adgang til elektronisk bevismateriale.

- **Konsekvensanalyse**

Udvalget for Forskriftskontrol afgav en positiv udtalelse om konsekvensanalysen, som ledsager dette forslag²⁰, og foreslog forskellige forbedringer²¹. Efter denne udtalelse blev konsekvensanalysen ændret for at sætte yderligere fokus på grundlæggende rettigheder i forbindelse med grænseoverskridende datadeling, navnlig på forbindelserne mellem de forskellige foranstaltninger, der indgår i den foretrukne løsningsmodel. Analysen blev også ændret, således at den i højere grad afspejlede interessenternes og medlemsstaternes synspunkter. Desuden blev den politiske kontekst uddybet gennem yderligere henvisninger til forskellige aspekter såsom drøftelser i ekspertgrupper, der havde bidraget til udformningen af initiativet. Komplementariteten mellem forskellige foranstaltninger (navnlig direktivet om den europæiske efterforskningskendelse, forhandlingerne om en tillægsprotokol til Budapestkonventionen og den fælles revision af aftalen om gensidig retshjælp mellem EU og USA) blev præciseret i henseende til anvendelsesområde, tidsplan og dybde, og referencescenariet blev revideret, således at det i højere grad afspejler den sandsynlige udvikling uafhængigt af vedtagelsen af de foreslåede foranstaltninger. Endelig blev der tilføjet flowdiagrammer for at præcisere arbejdsgangene for datadeling.

Fire løsningsmodeller blev overvejet ud over referencescenariet (løsningsmodel O): En række praktiske foranstaltninger, der skal forbedre de retlige samarbejdsprocedurer og det direkte samarbejde mellem offentlige myndigheder og tjenesteudbydere (løsningsmodel A: ikkelovgivningsmæssig), en løsningsmodel, som kombinerer de praktiske foranstaltninger i løsningsmodel A med internationale løsninger på bilateralt eller multilateralt plan (løsningsmodel B: lovgivningsmæssig), en løsningsmodel, som kombinerer foranstaltningerne

²⁰ Arbejdsdokument fra Kommissionens tjenestegrene – Konsekvensanalyse, der ledsager forslag til forordning om europæiske editions- og sikringskendelser om elektronisk bevismateriale i straffesager og forslag til direktiv om harmoniserede regler for udpegning af retlige repræsentanter med henblik på at indsamle bevismateriale i straffesager (SWD(2018) 118).

²¹ Kommissionens Udvalg for Forskriftskontrol – Udtalelse om konsekvensanalyse – forslag til forordning om europæiske editions- og sikringskendelser om elektronisk bevismateriale i straffesager og forslag til direktiv om harmoniserede regler for udpegning af retlige repræsentanter med henblik på at indsamle bevismateriale i straffesager (SEC(2018) 199).

i løsningsmodel B med en europæisk editionskendelse og en foranstaltning, der skal forbedre adgangen til databaser med abonnentdata på søgebasis, f.eks. Domain Name Whois (løsningsmodel C: lovgivningsmæssig), og en løsningsmodel, som kombinerer alle foranstaltningerne i løsningsmodel C med lovgivning om direkte adgang til fjernlagrede data (løsningsmodel D: lovgivningsmæssig)²².

Hvis der ikke træffes foranstaltninger (løsningsmodel O), vil et stigende antal anmodninger forværre situationen. Alle andre løsningsmodeller kan bidrage til at nå initiativets mål, men i varierende grad. Løsningsmodel A vil forbedre de nuværende processers effektivitet, f.eks. ved at forbedre anmodningernes kvalitet, men mulighederne for forbedringer vil være begrænsede på grund af det nuværende systems strukturelle mangler.

Løsningsmodel B vil føre til yderligere forbedringer gennem internationalt anerkendte løsninger, men resultatet af disse internationale løsninger vil i vid udstrækning afhænge af tredjelande. Løsningerne er derfor usikre og vil sandsynligvis ikke være lige så effektive og sikre lige så mange garantier som en EU-løsning.

Løsningsmodel C vil klart tilføre en merværdi sammenlignet med de forrige løsningsmodeller, da der ligeledes indføres et internt EU-instrument til fremme af direkte samarbejde med tjenesteudbydere, som vil løse de fleste af de identificerede problemer, når en tjenesteudbyder opbevarer de pågældende oplysninger.

Løsningsmodel D er den mest omfattende pakke af løsninger. Ud over foranstaltningerne i de andre løsningsmodeller omfatter modellen en lovgivningsforanstaltning om direkte adgang i situationer, hvor der ikke er behov for inddragelse af en tjenesteudbyder.

Dette lovgivningsinitiativ fra Kommissionen er baseret på resultaterne af konsekvensanalysen. Denne lovgivning vil blive suppleret med praktiske foranstaltninger som beskrevet i konsekvensanalysen, og der vil fortsat blive arbejdet hen imod en tillægsprotokol til Budapestkonventionen. Kommissionen vil med udgangspunkt i lovforslaget ligeledes drøfte muligheden for fremtidige bilaterale eller multilaterale aftaler om grænseoverskridende adgang til elektronisk bevismateriale med ledsagende garantier med USA og andre tredjelande. Med hensyn til foranstaltningerne om direkte adgang og adgang til databaser, der indgår i løsningsmodel D, fremsætter Kommissionen ikke lovgivning på nuværende tidspunkt, men vil gøre sig yderligere overvejelser om den bedste løsning på disse to spørgsmål.

Initiativet forventes at give mulighed for mere effektiv efterforskning og retsforfølgning og samtidig forbedre gennemsigtigheden og ansvarligheden og sikre overholdelsen af de grundlæggende rettigheder. Det forventes også at skabe tillid til det digitale indre marked ved at forbedre sikkerheden og mindske indtrykket af, at der er straffrihed for kriminalitet begået på eller gennem netværksbaserede enheder.

Initiativet forventes at medføre indledende gennemførelsesomkostninger for offentlige myndigheder, der på lang sigt vil blive udlignet af besparelser i faste omkostninger. De nationale myndigheder skal tilpasse sig nye procedurer og efteruddannes. Myndighederne vil

²² Nærmere oplysninger i arbejdsdokumentet fra Kommissionens tjenestegrene – Konsekvensanalyse, der ledsager forslaget til forordning om europæiske editions- og sikringskendelser om elektronisk bevismateriale i straffesager og forslaget til direktiv om harmoniserede regler for udpegning af retlige repræsentanter med henblik på at indsamle bevismateriale i straffesager (SWD(2018) 118).

imidlertid efterfølgende nyde godt af forenklingen og centraliseringen og de klare retlige rammer for anmodninger om adgang til oplysninger, da dette bør medføre effektivitetsgevinster. Da den foretrukne løsningsmodel vil lette presset på retlige samarbejdskanaler, vil de lande, der modtager anmodninger, sandsynligvis ligeledes modtage færre anmodninger, som skal behandles.

Tjenesteudbydere skal tilpasse sig en ny lovgivningsmæssig ramme gennem indførelse af (nye) procedurer og efteruddannelse af deres personale. En harmoniseret ramme kan til gengæld mindske byrden for disse udbydere, der i øjeblikket besvarer anmodninger om ikkeindholdsdata, som de skal vurdere i henhold til de forskellige lovgivninger i alle medlemsstaterne. Retssikkerhed og standardisering af procedurer bør ligeledes have en positiv indvirkning på små og mellemstore virksomheder, da dette vil lette den administrative byrde og fremme konkurrencen. Generelt forventes initiativet også at indebære besparelser for dem.

- **Grundlæggende rettigheder**

Forslaget kan potentielt påvirke en række grundlæggende rettigheder:

- rettigheder for den person, hvis data der gives adgang til: retten til beskyttelse af personoplysninger, retten til respekt for privatliv og familieliv, retten til ytringsfrihed, retten til forsvar, adgang til effektive retsmidler og til en upartisk domstol,
- serviceudbyderens rettigheder: friheden til at oprette og drive egen virksomhed, adgang til effektive retsmidler,
- alle borgeres rettigheder: retten til frihed og sikkerhed.

Under hensyntagen til den relevante lovgivning om databeskyttelse er der indført tilstrækkelige og vigtige garantier i forslaget til forordning for at sikre, at disse personers rettigheder er beskyttet.

Da kendelser kun kan udstedes i straffesager og i henhold til sammenlignelige nationale situationer både før og under retssagen, finder alle retssikkerhedsmæssige garantier i straffesager anvendelse. Dette omfatter navnlig retten til en retfærdig rettergang som forankret i artikel 6 i den europæiske menneskerettighedskonvention og artikel 47 og 48 i chartret om grundlæggende rettigheder. Det omfatter ligeledes den relevante lovgivning på EU-niveau om retssikkerhedsmæssige garantier i straffesager: direktiv 2010/64/EU om retten til tolke- og oversætterbistand i straffesager, direktiv 2012/13/EU om ret til information under straffesager, direktiv 2013/48/EU om ret til adgang til advokatbistand og til at kommunikere med slægtning under frihedsberøvelsen, direktiv 2016/343 om styrkelse af visse aspekter af uskyldsformodningen og retten til at være til stede under retssagen i straffesager, direktiv 2016/800 om retssikkerhedsgarantier for børn og direktiv 2016/1919 om retshjælp til mistænkte og tiltalte i straffesager og til eftersøgte i sager angående europæiske arrestordre.

En judiciel myndigheds forudgående inddragelse ved udstedelsen af kendelsen sikrer mere specifikt, at foranstaltningens lovlighed og dens nødvendighed og proportionalitet i den pågældende sag er blevet kontrolleret. Det sikrer også, at kendelsen ikke griber unødigt ind i grundlæggende rettigheder, herunder virkningerne af retsprincipper såsom retten til fortrolighed mellem advokat og klient. Udstedelsesmyndigheden er forpligtet til at sikre, at foranstaltningen er nødvendig og forholdsmæssig i den enkelte sag, bl.a. i forhold til grovheden af den lovovertrædelse, der efterforskes. Forslaget omfatter også tærskler for transaktions- og indholdsdata, der sikrer, at den europæiske editionskendelse kun vil blive udstedt i forbindelse med grovere former for kriminalitet i relation til sådanne data.

Der er ligeledes udtrykkeligt fokus på adgangen til effektive retsmidler for personer, hvis oplysninger efterspørges. Immuniteter og privilegier for visse erhverv såsom advokater samt grundlæggende interesser forbundet med statens sikkerhed eller forsvar i modtagerens medlemsstat skal ligeledes tages i betragtning under retssagen i udstedelsesstaten. Prøvelse ved en judiciel myndighed er en yderligere garanti denne forbindelse.

Da kendelsen er en bindende foranstaltning, berører den ligeledes tjenesteudbydernes rettigheder, navnlig friheden til at oprette og drive egen virksomhed. Forslaget giver tjenesteudbyderen ret til at rejse visse krav i udstedelsesstaten, f.eks. hvis kendelsen ikke er blevet udstedt eller godkendt af en judiciel myndighed. Hvis kendelsen er fremsendt til fuldbyrdelse til fuldbyrdesstaten, kan fuldbyrdesmyndigheden beslutte ikke at anerkende og fuldbyrde kendelsen efter høring af udstedelsesmyndigheden, hvis en af de begrænsede indsigelsesgrunde finder anvendelse. Hvis fuldbyrdesproceduren indledes, kan modtageren desuden selv gøre indsigelse mod kendelsen over for fuldbyrdesmyndigheden under påberåbelse af sådanne begrænsede grunde. Dette omfatter f.eks. tilfælde, hvor det er åbenlyst, at kendelsen ikke er blevet udstedt eller godkendt af en kompetent myndighed, eller hvor overholdelsen tydeligvis er i modstrid med chartret eller åbenbart urimelig. Dette berører ikke modtagerens adgang til effektive retsmidler til prøvelse af en afgørelse om pålæggelse af en sanktion.

Et potentielt problem i forbindelse med EU-foranstaltninger på dette område er muligheden for, at de kan føre til, at tredjelande indfører gensidige forpligtelser for EU-tjenesteudbydere, der ikke er i overensstemmelse med EU's grundlæggende rettigheder og forpligtelser, herunder det høje databeskyttelsesniveau, der er sikret i gældende EU-ret. I forslaget imødegås dette på to måder: for det første ved at indføre en foranstaltning, der omfatter stærke garantier og udtrykkelige henvisninger til de betingelser og garantier, der allerede er fastsat i gældende EU-ret, som således er et forbillede for udenlandske lovgivning, og for det andet ved at inkludere en specifik bestemmelse om "modstridende forpligtelser", som giver tjenesteudbydere mulighed for at identificere og påpege modstridende forpligtelser med henblik på judiciel prøvelse. Denne bestemmelse tager sigte på at sikre respekten for generelle blokadelove, f.eks. den amerikanske "Electronic Communications Privacy Act" (ECPA) (lov om beskyttelse af elektronisk kommunikation), der forbyder videregivelse af indholdsdata inden for lovens geografiske anvendelsesområde, bortset fra i ganske særlige tilfælde, samt for love, som generelt ikke forbyder videregivelse, men kan gøre det i specifikke sager. I sager vedrørende ECPA kan der på nuværende tidspunkt lægges hindringer i vejen for adgang til indholdsdata i visse situationer, og gensidig retshjælp bør derfor fortsat være det vigtigste redskab til at få adgang til sådanne data. Med ændringerne som følge af vedtagelsen af den amerikanske "Cloud Act"²³ (lov om præcisering af lovlig udenlandsk anvendelse af data) kan blokadeloven imidlertid ophæves, hvis EU indgår en aftale med USA. Yderligere internationale aftaler med andre vigtige partnere kan begrænse lovkonflikter yderligere.

På baggrund af ovenstående er foranstaltningerne i dette forslag forenelige med de grundlæggende rettigheder.

4. VIRKNINGER FOR BUDGETTET

Forslaget til forordning påvirker ikke EU-budgettet.

²³ Den 23. marts 2018 blev "Clarifying Lawful Overseas Use of Data (CLOUD) Act" vedtaget i USA. CLOUD Act findes [her](#).

5. ANDRE FORHOLD

- **Planer for gennemførelse og foranstaltninger til overvågning, evaluering og rapportering**

Forordningen finder direkte anvendelse i EU. Den vil blive anvendt umiddelbart af jurister, uden at det er nødvendigt at ændre interne retssystemer.

Forordningen vil blive evalueret, og Kommissionen vil forelægge en rapport for Europa-Parlamentet og Rådet senest fem år efter dens ikrafttræden. På grundlag af resultaterne fra denne rapport, navnlig vedrørende spørgsmålet om, hvorvidt der er huller i forordningen, som er relevante i praksis, og under hensyntagen til den teknologiske udvikling vil Kommissionen vurdere behovet for at udvide forordningens anvendelsesområde. Kommissionen vil om nødvendigt fremsætte forslag om tilpasning af denne forordning. Medlemsstaterne vil give Kommissionen de oplysninger, der er nødvendige for at udarbejde denne rapport. Medlemsstaterne vil indsamle de oplysninger, der er nødvendige for den årlige overvågning af forordningen.

Kommissionen vil om nødvendigt udstikke retningslinjer for tjenesteudbydernes opfyldelse af forpligtelserne i henhold til forordningen.

- **Nærmere redegørelse for de enkelte bestemmelser i forslaget**

	FORORDNING	
	Artikel	Betragtning
I. Emne, definitioner og anvendelsesområde	1. Emne	1-15
	2. Definitioner	16-23
	3. Anvendelsesområde	24-27
II. Europæisk editionskendelse, europæisk sikringskendelse og attester, retlig repræsentant	4. Udstedelsesmyndighed	30
	5. Betingelser for udstedelse af en europæisk editionskendelse	28-29, 31-35
	6. Betingelser for udstedelse af en europæisk sikringskendelse	36
	7. Modtageren af en europæisk editionskendelse og en europæisk sikringskendelse	37
	8. Attest for en europæisk editionskendelse og attest for en europæisk sikringskendelse	38-39
	9. Gennemførelse af en EPOC	40-41
	10. Gennemførelse af en EPOC-PR	42
	11. Fortrolighed og brugeroplysninger	43

	12. Godtgørelse af udgifter	Ingen
III. Sanktioner og håndhævelse	13. Sanktioner	Ingen
	14. Fuldbyrdelesprocedure	44-45, 55
IV. Retsmidler	15. og 16. Prøvelsesprocedure i forbindelse med modstridende forpligtelser begrundet i et tredjelands lovgivning	47-53
	17. Effektive retsmidler	54
	18. Sikring af privilegier og immuniteter i henhold til fuldbyrdelsesstatens lovgivning	35
V. Afsluttende bestemmelser	19. Overvågning og rapportering	58
	20. Ændringer af attesterne og formularerne	59-60
	21. Udøvelse af delegerede beføjelser	60
	22. Meddelelser	Ingen
	23. Forbindelsen til europæiske efterforskningskendelser	61
	24. Vurdering	62
	25. Ikrafttræden	Ingen

Kapitel 1: Emne, definitioner og anvendelsesområde

Artikel 1: Emne

I denne artikel fastlægges det generelle anvendelsesområde for og formål med forslaget, som er at fastsætte regler, hvorefter en kompetent judiciel myndighed i EU kan pålægge en tjenesteudbyder, der udbyder tjenester i Unionen, at fremlægge eller bevare elektronisk bevismateriale gennem en europæisk editions- eller sikringskendelse. Disse instrumenter kan kun anvendes i grænseoverskridende situationer, dvs. situationer, hvor tjenesteudbyderen er etableret eller repræsenteret i en anden medlemsstat.

Denne forordning sikrer efterforskningsmyndighederne yderligere værktøjer til indsamling af elektronisk bevismateriale uden at begrænse de beføjelser, der allerede er fastsat i national ret til at pålægge tjenesteudbydere, der er etableret eller repræsenteret på deres område, at overholde tilsvarende nationale foranstaltninger. Hvis tjenesteudbyderen er etableret eller repræsenteret i den samme medlemsstat, anvender myndighederne i den pågældende medlemsstat således nationale foranstaltninger til at pålægge tjenesteudbyderen at overholde tilsvarende nationale foranstaltninger.

De oplysninger, der anmodes om gennem en europæisk editionskendelse, bør fremsendes direkte til myndighederne uden inddragelse af myndighederne i den medlemsstat, hvor tjenesteudbyderen er etableret eller repræsenteret. Forordningen bevæger sig også væk fra, at det sted, hvor oplysningerne er lagret, er en afgørende tilknytningsfaktor, da datalagring normalt ikke indebærer, at den medlemsstat, på hvis område oplysningerne er lagret, kontrollerer disse. En sådan oplagring er i de fleste tilfælde bestemt af udbyderen alene ud fra forretningsmæssige hensyn²⁴.

Endvidere finder forordningen også anvendelse, hvis tjenesteudbydere ikke er etableret eller repræsenteret i Unionen, men udbyder tjenester i Unionen, jf. artikel 3, stk. 1.

Da forslaget omhandler tjenesteudbydere, der er etableret eller repræsenteret i en medlemsstat ved en udpeget retlig repræsentant, indebærer udpegningen af en retlig repræsentant ikke i sig selv, at tjenesteudbyderen har et etableringssted med henblik på anvendelsen af denne forordning.

Det understreges i artikel 1, stk. 2, at denne forordning ikke indebærer nogen ændring af pligten til at respektere de grundlæggende rettigheder og retsprincipper som fastsat i artikel 6 i TEU.

Artikel 2: Definitioner

I denne artikel fastsættes de definitioner, der anvendes i hele retsaksen.

Følgende typer tjenesteudbydere falder ind under forordningens anvendelsesområde: udbydere af elektroniske kommunikationstjenester, udbydere af informationssamfundstjenester, hvor lagring af data er et afgørende element i den tjeneste, der leveres til brugeren, herunder sociale netværk i det omfang de ikke betragtes som elektroniske kommunikationstjenester, onlinemarkedspladser til fremme af transaktioner mellem deres brugere (såsom forbrugere eller virksomheder) og andre udbydere af hostingtjenester og udbydere af internetdomænenavne og nummereringstjenester.

Forordningens anvendelsesområde omfatter udbydere af elektroniske kommunikationstjenester som defineret i [direktivet om en europæisk kodeks for elektronisk kommunikation]. Traditionelle telekommunikationstjenester, forbrugere og virksomheder er i stigende grad afhængige af nye internetbaserede tjenester, der muliggør interpersonel kommunikation såsom internettelefoni, instant messaging og e-mailtjenester i stedet for traditionelle kommunikationstjenester. Disse tjenester bør sammen med sociale netværk såsom Twitter og Facebook, der gør det muligt for brugerne at dele indhold, således være omfattet af dette forslag.

I mange tilfælde er oplysningerne ikke længere lagret på en brugers enhed, men tilgængelige på en skybaseret infrastruktur, og der er i princippet adgang hertil fra et hvilket som helst sted. Tjenesteudbydere behøver ikke at være etableret eller at have servere i alle jurisdiktioner, men har oftere en centraliseret administration og decentraliserede systemer til lagring af data og levering af deres tjenester. Formålet hermed er at optimere belastningen og afkorte svartiden på brugernes anmodninger om data. Netværk til levering af indhold (CDN'er) anvendes normalt til at fremskynde levering af indhold ved at kopiere indholdet på flere servere i hele verden. Dette gør det muligt for virksomhederne at levere indhold fra servere,

²⁴ Konsekvensanalysen indeholder yderligere forklaringer.

der er tættest på brugeren, eller som kan route kommunikation gennem et mindre overbelastet net. Under hensyntagen til denne udvikling dækker definitionen cloud- og andre hostingtjenester, som omfatter en bred vifte af ressourcer såsom netværk, servere eller anden infrastruktur, lagring, apps og tjenester, der gør det muligt at lagre data til forskellige formål. Retsakten finder ligeledes anvendelse på digitale markeder, som gør det muligt for forbrugere og/eller virksomheder til at indgå transaktioner via onlinekøbs- eller tjenesteydelsesaftaler. Sådanne transaktioner foretages enten på onlinemarkedspladsens websted eller på webstedet for en erhvervsdrivende, som anvender databehandlingstjenester, der udbydes på onlinemarkedspladsen. Det er derfor denne markedsplads, der er i besiddelse af det elektronisk bevismateriale, der måtte være behov for i løbet af en straffesag.

Tjenester, hvor lagring af data ikke er et afgørende element, er ikke omfattet af forslaget. Selv om de fleste tjenester, der leveres af udbydere, indebærer en eller anden form for lagring af data, især når de leveres ad elektronisk vej, kan der være tjenester, hvor lagring af data ikke er et afgørende element og derfor kun er af accessorisk karakter, herunder juridiske rådgivnings-, arkitekt-, ingeniør- og regnskabs tjenester leveret ad elektronisk vej.

Data, der lagres af udbydere af internetinfrastruktur tjenester, såsom domænenavneadministratorer og -registratorer og privatlivs- og proxytjenester eller regionale onlineregistre for IP-adresser kan være af relevans i straffesager, da de kan give spor, der gør det muligt at identificere en person eller enhed, som er involveret i kriminelle aktiviteter.

De kategorier af data, som kan indhentes gennem en europæisk editionskendelse udstedt af de kompetente myndigheder, omfatter abonnentdata adgangsdata, transaktionsdata (tre kategorier, der samlet benævnes "ikkeindholdsdata") og lagrede indholdsdata. Denne sondring findes i mange medlemsstaters retsorden. også uden for EU's retlige rammer, dog ikke for adgangsdata.

Alle kategorier indeholder personoplysninger og er dermed omfattet af garantierne i EU-databeskyttelsesreglerne. Indvirkningen på de grundlæggende rettigheder er forskellig, alt efter om der er tale om abonnentdata eller transaktions- og indholdsdata. Det er afgørende, at alle disse kategorier er omfattet af instrumentet, da abonnent- og adgangsdata ofte er udgangspunktet for at finde spor i en efterforskning vedrørende den mistænkte identitet, hvorimod transaktions- og indholdsdata kan være mest relevant som bevismateriale. På grund af de forskellige grader af indgriben i de grundlæggende rettigheder er det berettiget at knytte forskellige betingelser til indhentning af abonnentdata og transaktions- og indholdsdata i en række bestemmelser i forordningen.

Det er hensigtsmæssigt at adskille adgangsdata som en særlig datakategori i denne forordning. Adgangsdata som defineret i forordningen anvendes til samme formål som abonnentdata, dvs. til at identificere brugeren, og graden af indgriben i de grundlæggende rettigheder er den samme. De bør derfor være underlagt de samme betingelser som abonnentdata. Dette forslag indfører derfor en ny kategori af data, der skal behandles som abonnentdata, hvis formålet er det samme.

I artikel 2 defineres de medlemsstater og myndigheder, der kan blive inddraget i proceduren. Udstedelsesmyndigheden er defineret i artikel 4.

Nødsituationer er ekstraordinære situationer, der ofte kræver, at tjenesteudbydere griber rettidigt ind, og der gælder særlige betingelser i disse situationer. De defineres derfor særskilt i denne artikel.

Artikel 3: Anvendelsesområde

I denne artikel fastsættes forslagets anvendelsesområde. Forordningen finder anvendelse på alle tjenesteudbydere, der udbyder tjenester i Unionen, herunder tjenesteudbydere, der ikke er etableret i Unionen. Aktiv udbydelse af tjenester i Unionen med alle de fordele, der følger heraf, berettiger, at disse tjenesteudbydere også omfattes af forordningen, hvilket sikrer lige vilkår mellem deltagere på de samme markeder. Hvis disse tjenesteudbydere ikke blev omfattet, ville der desuden blive skabt en kløft, og det ville gøre det let for kriminelle at omgå forordningens anvendelsesområde.

For at fastslå, om der udbydes tjenester, skal myndighederne vurdere, om tjenesteudbyderen gør det muligt for juridiske eller fysiske personer i en eller flere medlemsstater at gøre brug af udbyderens tjenester. Adgang til tjenesten (der også kan bestå i adgang til udbyderens eller en mellemmands websted eller en e-mailadresse og andre kontaktoplysninger) bør imidlertid ikke i sig selv være en tilstrækkelig betingelse for anvendelsen af denne forordning. Der skal derfor være en væsentlig tilknytning til de pågældende medlemsstater for at fastslå, at der er en tilstrækkelig tilknytning mellem udbyderen og område, hvor denne udbyder sine tjenester. En sådan væsentlig tilknytning foreligger, når en tjenesteudbyder er etableret i en eller flere medlemsstater. Hvis tjenesteudbyderen ikke er etableret i Unionen, bør kriteriet om en væsentlig tilknytning til Unionen vurderes på grundlag af, om der er et betydeligt antal brugere i en eller flere medlemsstater, eller om tjenesteudbyderen retter sin virksomhed mod en eller flere medlemsstater. Målretning af virksomheden mod en eller flere medlemsstater kan fastslås på grundlag af alle relevante omstændigheder, herunder faktorer såsom anvendelsen af et sprog eller en valuta, der almindeligvis anvendes i en medlemsstat. Målretningen af virksomheden mod en medlemsstat kan ligeledes udledes af tilgængeligheden af en app i den relevante nationale app-butik, af lokal annoncering eller annoncering på det sprog, der anvendes i en medlemsstat, anvendelsen af oplysninger fra personer i medlemsstaterne i forbindelse med virksomheden eller håndteringen af kunderelationer, f.eks. ved at yde kundeservice på det sprog, der normalt anvendes i en medlemsstat. Det må endvidere antages, at der er en væsentlig tilknytning, hvis tjenesteudbyderen retter sin virksomhed mod en eller flere medlemsstater, jf. artikel 17, stk. 1, litra c), i forordning (EU) nr. 1215/2012 om retternes kompetence og om anerkendelse og fuldbyrdelse af retsafgørelser på det civil- og handelsretlige område.

Den europæiske editionskendelse og den europæiske sikringskendelse er efterforskningsforanstaltninger, som kun kan udstedes i strafferetlige efterforskninger eller straffesager i forbindelse med konkrete strafbare handlinger. Tilknytningen til en konkret efterforskning adskiller kendelsen fra forebyggende foranstaltninger eller pligt til opbevaring af data i henhold til lovgivningen og sikrer anvendelsen af de proceduremæssige rettigheder, der finder anvendelse i straffesager. Kompetencen til at indlede en efterforskning af en konkret lovovertrædelse er derfor en forudsætning for anvendelsen af forordningen.

Som et yderligere krav skal de oplysninger, der anmodes om, være knyttet til de tjenester, der udbydes af tjenesteudbyderen i Unionen.

Kapitel 2: Europæisk editionskendelse, europæisk sikringskendelse og attester

Artikel 4: Udstedelsesmyndighed

Ved udstedelse af en europæisk editions- eller sikringskendelse skal en judiciel myndighed altid inddrages enten som udstedelses- eller godkendelsesmyndighed. Kendelser om

fremlæggelse transaktions- eller indholdsdata skal udstedes og godkendes af en dommer eller domstol. Kendelser om fremlæggelse af abonnent- og adgangsdata kan også udstedes og godkendes af en anklager.

Artikel 5: Betingelser for udstedelse af en europæisk editionskendelse

I artikel 5 fastsættes betingelserne for udstedelse af europæiske editionskendelser. De skal vurderes af den judicielle udstedelsesmyndighed.

Den europæiske editionskendelse kan kun udstedes, hvis dette er nødvendigt og forholdsmæssigt i den enkelte sag. Den kan desuden kun udstedes, hvis en lignende foranstaltning er tilgængelig i en sammenlignelig national situation i udstedelsesstaten.

Kendelser om fremlæggelse af abonnentdata og adgangsdata kan udstedes for alle lovovertrædelser. Transaktions- og indholdsdata bør være underlagt strengere krav for at tage højde for den mere følsomme karakter af disse oplysninger og den tilsvarende større indgriben af kendelser om sådanne oplysninger i forhold til abonnent- og adgangsdata. Kendelser kan derfor kun udstedes for lovovertrædelser, der kan straffes med en frihedsstraf af en maksimal varighed på mindst tre år. Fastsættelsen af en tærskel baseret på en maksimal frihedsstraf gør det muligt at anlægge en mere forholdsmæssig tilgang, og dette sikrer sammen med en række andre forudgående og efterfølgende betingelser og garantier, at proportionalitetsprincippet og de berørte personers rettigheder overholdes.

Tærsklen bør samtidig ikke underminere instrumentets effektivitet og de retshåndhævende myndigheders brug heraf. Medlemsstaterne anvender forskellige maksimumsgrænser for domme, der vedrører deres nationale system. De nationale strafferetsbestemmelser er forskellige og er ikke harmoniseret. Dette er tilfældet for lovovertrædelser og sanktionerne herfor. Tærsklerne i de nationale retsplejebestemmelser for indhentning af transaktionsdata eller indholdsdata er ligeledes forskellige, idet nogle medlemsstater ikke har fastsat specifikke tærskler, mens andre har udarbejdet en liste over lovovertrædelser. En treårig tærskel begrænser instrumentets anvendelsesområde til grovere former for kriminalitet, men begrænser ikke i for høj grad de retshåndhævende myndigheders muligheder for at anvende det. Denne tærskel udelukker en lang række strafbare handlinger fra anvendelsesområdet afhængigt af medlemsstatens straffelov (i nogle medlemsstater f.eks. deltagelse i en organiseret kriminel gruppes aktiviteter og bortførelse, men også lovovertrædelser såsom småtyveri, bedrageri og overfald, hvor anvendelsen af en grænseoverskridende editionskendelse om fremlæggelse af mere følsomme oplysninger kan blive betragtet som uforholdsmæssig). En treårig tærskel omfatter derimod kriminalitet, der kræver en mere effektiv tilgang, f.eks. medlemskab af en kriminel organisation, finansiering af terrorgrupper, støtte til og markedsføring af en kriminel organisation, træning i udførelse af terrorhandlinger, visse lovovertrædelser med terrorforsæt og forberedelse af en lovovertrædelse med terrorforsæt eller forberedelse af gidseltagning, som ellers ville være udelukket, hvis tærsklen var højere, afhængigt af medlemsstaten. Denne tærskel er blevet valgt for at sikre en balance i alle medlemsstaterne mellem effektive strafferetlige efterforskninger og beskyttelse af rettigheder og proportionalitetsprincippet. En tærskel har ligeledes den fordel, at den er let at anvende i praksis.

Kendelser om fremlæggelse transaktions- eller indholdsdata kan desuden også udstedes for de i bestemmelsen omhandlede specifikke harmoniserede lovovertrædelser, hvor bevismaterialet for det meste typisk kun vil være tilgængeligt i elektronisk form. Dette berettiger ligeledes anvendelsen af forordningen, når den maksimale frihedsstraf ligger under ovennævnte

tærskel, da disse lovovertrædelser i modsat fald ikke kan efterforskes ordentligt, hvilket kan føre til straffrihed. Lovovertrædelserne er nævnt i specifikke bestemmelser i: i) Rådets rammeafgørelse 2001/413/RIA om bekæmpelse af svig og forfalskning i forbindelse med andre betalingsmidler end kontanter, direktiv 2011/93/EU om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og børnepornografi og om erstatning af Rådets rammeafgørelse 2004/68/RIA og ii) direktiv 2013/40/EU om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA. Der kan ligeledes udstedes kendelser for de lovovertrædelser, der er nævnt i direktiv (EU) 2017/541 om bekæmpelse af terrorisme og om erstatning af Rådets rammeafgørelse 2002/475/RIA og ændring af Rådets afgørelse 2005/671/RIA. Nogle af disse lovovertrædelser har en maksimumstærskel på mindst et år, andre på to år, men ingen har en maksimumstærskel på under et år.

I artiklen fastsættes desuden obligatoriske oplysninger, som skal anføres i den europæiske editionskendelse, således at tjenesteudbyderen kan identificere og fremlægge de oplysninger, der anmodes om. Begrundelsen for denne foranstaltnings proportionalitet og nødvendighed anføres ligeledes i den europæiske editionskendelse.

Den europæiske editionskendelse gennemføres ved at udstede en attest for den europæiske editionskendelse (EPOC) (jf. artikel 8), der oversættes og fremsendes til tjenesteudbyderen. EPOC'en indeholder de samme obligatoriske oplysninger som kendelsen bortset fra begrundelsen for foranstaltningens proportionalitet og nødvendighed og yderligere oplysninger om sagen.

Hvis de oplysninger, der anmodes om, opbevares eller behandles som en del af en tjenesteudbyders infrastruktur, der stilles til rådighed for en virksomhed, typisk i forbindelse med hosting- eller softwaretjenester, bør virksomheden selv være den primære modtager af en anmodning fra efterforskningsmyndighederne. Dette kan nødvendiggøre udstedelsen af en europæisk efterforskningskendelse eller en procedure for gensidig retshjælp, når virksomheden ikke er en tjenesteudbyder, der er omfattet af denne forordnings anvendelsesområde. Den europæiske editionskendelse kan udelukkende rettes til tjenesteudbyderen, hvis det ikke er hensigtsmæssigt at rette kendelsen til virksomheden, navnlig hvis det kan bringe efterforskningen i fare, f.eks. hvis det er virksomheden selv, der efterforskes.

Inden udstedelsen af en europæisk editionskendelse skal udstedelsesmyndigheden ligeledes tage hensyn til eventuelle immuniteter og privilegier i henhold til lovgivningen i tjenesteudbyderens medlemsstat eller til enhver indvirkning på den pågældende medlemsstats grundlæggende interesser såsom statens sikkerhed og forsvar. Formålet med denne bestemmelse er at sikre, at immuniteter og privilegier, som beskytter de oplysninger, der anmodes om i tjenesteudbyderens medlemsstat, tages i betragtning i udstedelsesstaten, navnlig når de sikrer en højere beskyttelse end lovgivningen i udstedelsesstaten.

Artikel 6: Betingelser for udstedelse af en europæisk sikringskendelse

En europæisk sikringskendelse er underlagt de samme betingelser som den europæiske editionskendelse. Den kan udstedes for alle lovovertrædelser i overensstemmelse med de øvrige betingelser, der er fastsat i artikel 6. Formålet er at forhindre fjernelse, sletning eller ændring af relevante oplysninger i situationer, hvor det kan tage længere tid at få indhentet disse oplysninger, f.eks. fordi der anvendes retlige samarbejdskanaler. Da den europæiske efterforskningskendelse f.eks. kan udstedes generelt for alle lovovertrædelser uden at være begrænset af tærskler, er den europæiske sikringskendelse heller ikke pålagt begrænsninger. I

modsat fald ville instrumentet ikke være effektivt. Europæiske sikringskendelser kan ligeledes udstedes eller godkendes af en anklager for at give efterforskningsmyndighederne mulighed for at handle hurtigt, da den relevante anmodning om fremlæggelse af oplysningerne er den efterfølgende anmodning, hvor alle betingelserne vil blive kontrolleret på ny.

Artikel 7: Modtageren af en europæisk editionskendelse eller en europæisk sikringskendelse

Europæiske editionskendelser og europæiske sikringskendelser bør rettes til en retlig repræsentant, der er udpeget af tjenesteudbyderen med henblik på at indsamle bevismateriale i straffesager i overensstemmelse med direktivet om harmoniserede regler for udpegning af retlige repræsentanter med henblik på at indsamle bevismateriale i straffesager. Kendelsen fremsendes i form af en attest for den europæiske editionskendelse ("EPOC") eller en attest for den europæiske sikringskendelse ("EPOC-PR") som omhandlet i artikel 8. Den retlige repræsentant er ansvarlig for modtagelsen og den rettidige og fuldstændige gennemførelse af kendelsen. Tjenesteudbyderne kan således selv vælge, hvordan de vil organisere sig til for at fremlægge de oplysninger, som medlemsstaternes myndigheder har anmodet om.

Hvis der ikke er udpeget en retlig repræsentant, kan kendelser rettes til ethvert af tjenesteudbyderens etableringssteder i Unionen. Dette alternativ har til formål at sikre, at systemet er effektivt, hvis tjenesteudbyderen (endnu) ikke har udpeget en særlig repræsentant, f.eks. hvis der ikke er nogen forpligtelse til at udpege en retlig repræsentant i henhold til direktivet, da udbyderne kun er etableret og aktive i en medlemsstat, eller hvis en forpligtelse til at udpege en retlig repræsentant endnu ikke er trådt i kraft før fristen for direktivets gennemførelse.

I tilfælde af den retlige repræsentants manglende overholdelse kan udstedelsesmyndigheden rette kendelsen til ethvert af tjenesteudbyderens etableringssteder i Unionen i to situationer, nemlig i nødsituationer som defineret i artikel 9, stk. 2, og hvis den retlige repræsentant ikke overholder sine forpligtelser i henhold til stk. 9 eller 10, og udstedelsesmyndigheden skønner, at der er en klar risiko for tab af data.

Artikel 8: Attest for en europæisk editions- og sikringskendelse

EPOC'en og EPOC-PR'en anvendes til at fremsende kendelser til den modtager, der er defineret i artikel 7. Modeller for begge attester findes i bilag I og II til forordningen. De skal oversættes til et af de officielle sprog i den medlemsstat, hvor modtageren er bosiddende eller etableret. Tjenesteudbyderen kan meddele, at kendelser ligeledes vil blive accepteret på andre officielle EU-sprog. Formålet med attesterne er at angive alle de nødvendige oplysninger, som skal fremsendes til modtageren, i et standardiseret format, at minimere fejlkilder og gøre det let at identificere oplysningerne og i videst muligt omfang undgå fritekst og dermed reducere oversættelsesomkostningerne. Den fuldstændige begrundelse for nødvendigheden og proportionaliteten eller yderligere oplysninger om sagen angives ikke i attesten for at undgå at bringe efterforskningen i fare. Den er derfor kun nødvendig som en del af selve kendelsen, således at den mistænkte kan gøre indsigelse mod den på et senere tidspunkt under straffesager.

Nogle tjenesteudbydere har allerede etableret platforme til indgivelse af de retshåndhævende myndigheders anmodninger. Anvendelsen af disse platforme er i overensstemmelse med forordningen, da de har mange fordele, herunder muligheden for en nem autentifikation og sikker overførsel af oplysningerne. Disse platforme skal imidlertid gøre det muligt at

fremsende EPOC'en og EPOC-PR'en i det format, der er fastsat i bilag I og II, uden at anmode om yderligere oplysninger vedrørende kendelsen.

Platforme, der er etableret af medlemsstaterne eller EU-organer, kan ligeledes tilvejebringe et sikkert fremsendelsesmiddel og lette autentifikationen af kendelserne og indsamlingen af statistikker. Det bør overvejes at udvide eCodex- og SIRIUS-platformene til at omfatte en sikker forbindelse til tjenesteudbydere med henblik på fremsendelse af EPOC'en og EPOC-PR'en og, hvor det er relevant, tjenesteudbyderes svar.

Artikel 9: Gennemførelse af en EPOC

Artikel 9 pålægger modtagerne at besvare EPOC'er, og der indføres obligatoriske frister. Den normale frist er 10 dage, men myndighederne kan fastsætte en kortere frist, hvis det er berettiget. I nødsituationer, der er defineret som en situation, hvor der er en overhængende fare for en persons liv eller fysiske integritet eller for kritisk infrastruktur, er fristen seks timer.

Artiklen sikrer ligeledes mulighed for en dialog mellem modtageren og udstedelsesmyndigheden. Hvis EPOC'en er ufuldstændig, indeholder åbenbare fejl eller ikke indeholder tilstrækkelige oplysninger til, at tjenesteudbyderen kan gennemføre EPOC'en, retter modtageren henvendelse til udstedelsesmyndigheden med anmodning om en nærmere forklaring ved brug af formularen i bilag III. Modtageren underretter ligeledes udstedelsesmyndigheden, hvis modtageren ikke kan fremlægge oplysningerne på grund af force majeure, eller da det er de facto umuligt. Dette er f.eks. tilfældet, hvis den person, hvis oplysninger efterspørges, hverken var en kunde hos denne tjeneste eller – f.eks. i henhold til andre forpligtelser til at sikre privatlivets fred – oplysningerne er blevet slettet lovligt af tjenesteudbyderen eller dennes retlige repræsentant, der modtog kendelsen. Udstedelsesmyndigheden skal være bekendt med disse forhold for at reagere hurtigt, for eventuelt at indsamle elektronisk bevismateriale fra en anden tjenesteudbyder og for at forhindre udstedelsesmyndigheden i at indlede en fuldbyrdelsesprocedure, hvis det ikke giver nogen mening.

Hvis modtageren slet ikke fremlægger oplysningerne, ikke fremlægger fyldestgørende oplysninger eller ikke fremlægger oplysningerne rettidigt af andre grunde end ovennævnte, skal modtageren underrette udstedelsesmyndigheden om grundene hertil ved brug af formularen i bilag III. Modtageren kan således rejse ethvert spørgsmål vedrørende gennemførelsen af EPOC'en over for udstedelsesmyndigheden. Dette giver udstedelsesmyndigheden mulighed for at korrigere eller genoverveje EPOC'en på et tidligt tidspunkt inden fuldbyrdelsesfasen.

Hvis oplysningerne ikke fremlægges omgående, navnlig hvis modtageren og udstedelsesmyndigheden indleder en dialog, der indebærer, at fristerne i artikel 9, stk. 1, ikke længere overholdes, har tjenesteudbyderen pligt til at bevare oplysningerne for at undgå at miste dem efter modtagelsen af EPOC'en, forudsat at oplysningerne kan identificeres. Sikringen kan vedrøre den præciserede EPOC eller en efterfølgende anmodning om gensidig retshjælp eller en europæisk efterforskningskendelse, der fremsendes i stedet for den oprindelige EPOC.

Artikel 10: Gennemførelse af en EPOC-PR

Gennemførelsen af en EPOC-PR indebærer, at de oplysninger, der er lagret på tidspunktet for modtagelsen af kendelsen, skal bevares. Tjenesteudbyderne bør bevare oplysningerne, så

længe det er nødvendigt for at fremlægge oplysningerne på anmodning, forudsat at udstedelsesmyndigheden senest 60 dage efter udstedelsen af kendelsen bekræfter, at den har indledt proceduren for den efterfølgende anmodning om fremlæggelse af oplysninger. Dette kræver, at der som minimum er truffet en række formelle foranstaltninger, f.eks. fremsendelse af en anmodning om gensidig retshjælp til oversættelse.

Anmodninger om sikring bør derimod kun udstedes eller opretholdes, så længe det er nødvendigt med henblik på en efterfølgende anmodning om fremlæggelse af disse oplysninger. For at undgå en unødvendig eller for lang sikring underretter den myndighed, som udstedte den europæiske sikringskendelse, modtageren, så snart der er truffet en afgørelse om at undlade at udstede eller ophæve en editionskendelse eller en anmodning om retligt samarbejde.

Denne bestemmelse sikrer ligeledes mulighed for en dialog mellem modtageren og udstedelsesmyndigheden på samme måde som bestemmelserne i artikel 9. Hvis EPOC-PR'en er ufuldstændig, indeholder åbenbare fejl eller ikke indeholder tilstrækkelige oplysninger til, at tjenesteudbyderen kan gennemføre EPOC-PR'en, retter modtageren henvendelse til udstedelsesmyndigheden med anmodning om en nærmere forklaring ved brug af formularen i bilag III. Modtageren underretter ligeledes udstedelsesmyndigheden, hvis modtageren ikke kan fremlægge oplysningerne på grund af omstændigheder, der betragtes som force majeure, eller hvis det er de facto umuligt, eller af andre grunde.

Artikel 11: Fortrolighed og brugeroplysninger

Fortroligheden af den igangværende efterforskning, herunder det forhold, at der er udstedt en kendelse for at indhente relevante oplysninger, skal beskyttes. Denne artikel er inspireret af artikel 19 i direktivet om den europæiske efterforskningskendelse. Den pålægger modtageren eller – hvis denne er en anden – tjenesteudbyderen at sikre fortroligheden af EPOC'en eller EPOC-PR'en, navnlig ved ikke at underrette den person, hvis oplysninger efterspørges, når udstedelsesmyndigheden anmoder herom for at beskytte efterforskningen af lovovertrædelser i overensstemmelse med artikel 23 i den generelle forordning om databeskyttelse.

Det er imidlertid vigtigt, herunder for udøvelsen af retsmidler, at den person, hvis oplysninger efterspørges, underrettes. Hvis tjenesteudbyderen ikke gør dette på udstedelsesmyndighedens anmodning, underretter udstedelsesmyndigheden den pågældende i overensstemmelse med artikel 13 i direktivet om databeskyttelse på retshåndhævelsesområdet, når der ikke længere er nogen risiko for at bringe efterforskningen i fare, herunder om de retsmidler, der er til rådighed. På grund af den mindre indgriben i de pågældende rettigheder foretages denne underretning ikke i forbindelse med en europæisk sikringskendelse, men kun i forbindelse med europæiske editionskendelser.

Artikel 12: Godtgørelse af udgifter

Hvis det er fastsat i national lovgivning i udstedelsesstaten for nationale kendelser i lignende nationale sager, kan tjenesteudbyderen ligeledes kræve, at udstedelsesstaten godtgør udbyderens udgifter i overensstemmelse med national lovgivning i udstedelsesstaten. Dette sikrer lige behandling af tjenesteudbydere, der har modtaget en national kendelse og de udbydere, der har modtaget en EPOC fra den samme medlemsstat, hvis denne medlemsstat har valgt at godtgøre visse tjenesteudbydere. Den foreslåede forordning harmoniserer derimod ikke godtgørelsen af udgifter, da medlemsstaterne har truffet forskellige valg i denne henseende.

Udgifterne kan kræves godtgjort enten direkte af tjenesteudbyderen eller via dennes retlige repræsentant. De kan kun godtgøres én gang.

Kapitel 3: Sanktioner og fuldbyrdelse

Artikel 13: Sanktioner

Medlemsstaterne sikrer, at der er indført effektive, forholdsmæssige og afskrækkende bøder, når tjenesteudbydere ikke opfylder deres forpligtelser i henhold til artikel 9, 10 eller 11. Dette berører ikke nationale love med bestemmelser om pålæggelse af strafferetlige sanktioner i sådanne situationer.

Artikel 14: Fuldbyrdesprocedure

Artikel 14 indeholder bestemmelser om en procedure til fuldbyrdelse af kendelser i tilfælde af manglende overholdelse med hjælp fra den medlemsstat, hvor modtageren af den fremsendte attest er bosiddende eller etableret. Afhængigt af den oprindelige modtager er det enten tjenesteudbyderens eller den retlige repræsentants medlemsstat. Udstedelsesmyndigheden fremsender hele kendelsen, herunder begrundelsen for nødvendigheden og proportionaliteten, ledsaget af attesten til den kompetente myndighed i fuldbyrdesstaten, der fuldbyrder den i overensstemmelse med sin nationale lovgivning, om nødvendigt ved pålæggelse af de sanktioner, der er nævnt i artikel 13. Hvis kendelsen er fremsendt til fuldbyrdelse til fuldbyrdesstaten, kan fuldbyrdesmyndigheden beslutte ikke at anerkende og fuldbyrde kendelsen efter høring af udstedelsesmyndigheden, hvis myndigheden finder, at en af de modtagne begrænsede indsigelsesgrunde finder anvendelse. Hvis fuldbyrdesproceduren indledes, kan modtageren desuden selv gøre indsigelse mod kendelsen over for fuldbyrdesmyndigheden. Modtageren kan gøre dette under påberåbelse af enhver af disse grunde med undtagelse af immuniteter og privilegier, også hvor det er åbenlyst, at kendelsen ikke er blevet udstedt eller godkendt af en kompetent myndighed, eller hvor overholdelsen tydeligvis er i modstrid med Den Europæiske Unions charter om grundlæggende rettigheder eller åbenbart urimelig. En kendelse om fremlæggelse af indholdsdata vedrørende en udefineret gruppe af personer i et geografisk område eller uden tilknytning til en konkret straffesag er tydeligvis ikke i overensstemmelse med betingelserne for udstedelse af en europæisk editionskendelse som fastsat i denne forordning, og det vil allerede være klart ud fra indholdet i selve attesten. Andre grunde kan kun påberåbes af den person, hvis oplysninger efterspørges, inden for rammerne af deres egne retsmidler i udstedelsesstaten (jf. artikel 17 nedenfor). Tjenesteudbyderen har desuden adgang til retsmidler til prøvelse af en afgørelse om bødepålæg truffet af fuldbyrdesmyndigheden.

Fuldbyrdesproceduren indeholder flere frister for fuldbyrdes- og udstedelsesmyndigheden for at undgå yderligere forsinkelser i denne procedure.

Kapitel 4: Retsmidler

Artikel 15 og 16: Prøvelsesprocedure i forbindelse med modstridende forpligtelser begrundet i et tredjeland's lovgivning

I artikel 15 og 16 fastsættes en prøvelsesprocedure, der kan anvendes, hvis tjenesteudbydere med hovedsæde i tredjelande står over for modstridende forpligtelser. Disse bestemmelser er også af stor betydning for at sikre beskyttelsen af individuelle rettigheder og international anerkendelse af domme. Formålet med bestemmelserne er at tilskynde tredjelande til at sikre et tilsvarende beskyttelsesniveau ved at fastsætte en høj standard. I den omvendte situation,

hvor myndighederne i et tredjeland ønsker at indhente oplysninger om en EU-borger fra en EU-tjenesteudbyder, kan EU-lovgivningen eller medlemsstaternes lovgivning til beskyttelse af grundlæggende rettigheder såsom databeskyttelsesreglerne ligeledes forhindre videregivelse. EU forventer, at tredjelande overholder disse forbud, der overholdes i dette forslag.

Proceduren i artikel 15 kan indledes af modtageren, hvis overholdelsen af en europæisk editionskendelse vil medføre en overtrædelse af lovgivningen i et tredjeland, som forbyder videregivelse af oplysningerne, med den begrundelse, at det er nødvendigt for at beskytte de berørte personers grundlæggende rettigheder eller tredjelandets grundlæggende rettigheder forbundet med statens sikkerhed eller forsvar. Modtageren er forpligtet til at underrette udstedelsesmyndigheden ved at rejse en begrundet indsigelse om grundene til konklusionen om, at der er modstridende forpligtelser. Denne begrundede indsigelse kan ikke baseres alene på det forhold, at der ikke findes tilsvarende bestemmelser i tredjelandets lovgivning, eller alene på det forhold, at oplysningerne er lagret i et tredjeland. Den begrundede indsigelse skal rejses i henhold til den procedure, der er fastsat i artikel 9, stk. 5, for meddelelse om, at modtageren ikke agter at overholde kendelsen, ved brug af formularen i bilag III.

Udstedelsesmyndigheden kontrollerer sin egen kendelse på grundlag af denne begrundede indsigelse. Hvis udstedelsesmyndigheden vælger at trække kendelsen tilbage, afsluttes proceduren. Hvis udstedelsesmyndigheden ønsker kendelsen stadfæstet, overdrages sagen til den kompetente ret i myndighedens medlemsstat. Retten vurderer herefter på grundlag af den begrundede indsigelse og under hensyntagen til alle sagens relevante omstændigheder, om tredjelandets lovgivning finder anvendelse på den konkrete sag og – hvis den anvendes – om der er en konflikt i den foreliggende sag. I forbindelse med denne vurdering bør retten tage højde for, om tredjelandets lovgivning i stedet for at beskytte tredjelandets grundlæggende rettigheder eller grundlæggende interesser forbundet med statens sikkerhed eller forsvar åbenlyst har til formål at beskytte andre interesser eller ulovlige aktiviteter mod anmodninger fra de retshåndhævende myndigheder i forbindelse med strafferetlige efterforskninger.

Hvis retten fastslår, at der rent faktisk er modstridende forpligter begrundet i lovgivningen til beskyttelse af den enkeltes grundlæggende rettigheder eller tredjelandets grundlæggende rettigheder forbundet med statens sikkerhed eller forsvar, skal retten anmode om en udtalelse fra det relevante tredjeland via de nationale centrale myndigheder i tredjelandet. Hvis det konsulterede tredjeland bekræfter, at der er en konflikt, og gør indsigelse mod fuldbyrdelsen af kendelsen, skal retten ophæve kendelsen.

Hvis der opstår en konflikt på grundlag af anden lovgivning i tredjelande, som ikke har til formål at beskytte den enkeltes grundlæggende rettigheder eller tredjelandets grundlæggende rettigheder forbundet med statens sikkerhed eller forsvar, træffer retten sin afgørelse på grundlag af en afvejning af interesserne for og imod en stadfæstelse af kendelsen.

De betingelser, der er fastsat i artikel 9, især de sikringsforpligtelser, der er omhandlet i artikel 9, stk. 6, finder ligeledes anvendelse i tilfælde af modstridende forpligtelser begrundet i lovgivningen i et tredjeland. Hvis retten finder, at kendelsen skal stadfæstes, underrettes udstedelsesmyndigheden og tjenesteudbyderen med henblik på fuldbyrdelse. Hvis kendelsen ophæves, kan der udstedes en særskilt europæisk sikringskendelse for at sikre, at oplysningerne er tilgængelige, hvis de kan opnås på grundlag af en anmodning om gensidig retshjælp.

Da den europæiske sikringskendelse ikke i sig selv indebærer videregivelse af oplysninger og derfor ikke giver anledning til de samme problemer, er prøvelsesproceduren begrænset til den europæiske editionskendelse.

Artikel 17: Effektive retsmidler

Denne bestemmelse sikrer, at personer, der er berørt af den europæiske editionskendelse, har adgang til effektive retsmidler. Disse retsmidler udøves i udstedelsesstaten i overensstemmelse med national lovgivning. For mistænkte og tiltalte vedkommende udøves retsmidlerne normalt under straffesagen. Der er ingen specifikke retsmidler over for den europæiske sikringskendelse, som ikke i sig selv indebærer videregivelse af oplysninger, bortset fra i de tilfælde, hvor den efterfølges af en europæisk editionskendelse eller et andet instrument, der indebærer videregivelse, som derefter giver adgang til specifikke retsmidler.

Personer, hvis oplysninger er blevet efterspurgt, og som ikke er mistænkte eller tiltalte i straffesager, har også ret til retsmidler i udstedelsesstaten. Alle disse rettigheder berører ikke tilgængelige retsmidler i henhold til direktivet om databeskyttelse på retshåndhævelsesområdet og den generelle forordning om databeskyttelse.

I modsætning til, hvad der er gældende for tjenesteudbydere, begrænser forordningen ikke alle disse personers mulige grunde til at anfægte kendelsens lovlighed. Disse grunde omfatter kendelsens nødvendighed og proportionalitet.

Udøvelsen af retsmidler i udstedelsesstaten belaster ikke de berørte personer på en uforholdsmæssig måde. Som det er tilfældet med kendelser, der fuldbyrdes gennem andre former for retligt samarbejde, har retterne i udstedelsesstaten de bedste forudsætninger for at prøve lovligheden af europæiske editionskendelser udstedt af deres egne myndigheder og for at vurdere foreneligheden med deres nationale lovgivning. I fuldbyrdelsesfasen kan modtagerne desuden særskilt gøre indsigelse mod fuldbyrdelsen af EPOC'en eller EPOC-PR'en i værtsmedlemsstaten på grundlag af den liste over grunde, som er opstillet i forordningen (jf. artikel 14 ovenfor).

Artikel 18: Sikring af privilegier og immuniteter i henhold til den modtagende stats lovgivning

Denne bestemmelse har samme formål som artikel 5, stk. 7, nemlig at sikre, at udstedelsesstaten tager hensyn til immuniteter og privilegier, som beskytter de oplysninger, der anmodes om i tjenesteudbyderens medlemsstat, navnlig når der er forskelle mellem disse medlemsstater, og til den pågældende medlemsstats grundlæggende interesser såsom statens sikkerhed og forsvar. Artikel 18 bestemmer, at retten i udstedelsesstaten skal tage hensyn til dem på samme måde, som hvis de var omfattet af national lovgivning. På grund af medlemsstaternes forskellige vurdering af relevansen og antageligheden af bevismateriale giver bestemmelsen retterne en vis grad af fleksibilitet til at tage hensyn til dem.

Kapitel 5: Afsluttende bestemmelser

Artikel 19: Overvågning og rapportering

I denne artikel pålægges medlemsstaterne at indberette specifikke oplysninger om anvendelsen af forordningen med henblik på at bistå Kommissionen i udøvelsen af dennes opgaver i henhold til artikel 24. Kommissionen fastlægger et detaljeret program for overvågning af forordningens resultater og virkninger.

Artikel 20: Ændringer af attesterne og formularerne

Attesterne og formularerne i bilag I, II og III i dette forslag vil gøre det lettere at gennemføre en EPOC og en EPOC-PR. Derfor er det nødvendigt fremover at kunne afhjælpe et muligt

behov for at forbedre attestens og formularens indhold så hurtigt som mulig. Hvis de tre bilag skal ændres inden for rammerne af den almindelige lovgivningsprocedure, er dette krav ikke opfyldt, og de udgør ikkevæsentlige elementer i de lovgivningsmæssige retsakter, og hovedelementerne er defineret i artikel 8. Derfor fastsættes der en hurtigere og mere fleksibel procedure for ændringer gennem delegerede retsakter i artikel 20.

Artikel 21: Udøvelse af delegerede beføjelser

Denne artikel indeholder betingelserne for, hvornår Kommissionen har beføjelse til at vedtage delegerede retsakter for at indføre nødvendige ændringer af attesten og formularerne, der er vedlagt forslaget. Der fastlægges en standardprocedure for vedtagelse af sådanne delegerede retsakter.

Artikel 22: Meddelelser

Medlemsstaterne skal give Kommissionen meddelelse om, hvem de kompetente udstedelses- og fuldbyrdelsesmyndigheder er, og hvilke retter der er kompetente til at behandle tjenesteudbydernes begrundede indsigelser i tilfælde af en lovkonflikt.

Artikel 23: Forbindelsen til europæiske efterforskningskendelser

Det præciseres i denne bestemmelse, at forordningen ikke forhindrer medlemsstaternes myndigheder i at udstede europæiske efterforskningskendelser i henhold til direktiv 2014/41/EU med henblik på fremskaffelse af elektronisk bevismateriale.

Artikel 24: Vurdering

Det fastsættes i bestemmelsen, at Kommissionen foretager en evaluering af denne forordning i overensstemmelse med Kommissionens retningslinjer for bedre lovgivning og i henhold til punkt 22 i den interinstitutionelle aftale af 13. april 2016²⁵. Kommissionen skal forelægge en rapport for Europa-Parlamentet og Rådet om resultaterne af evalueringen, herunder en vurdering af behovet for at udvide forordningens anvendelsesområde til tjenester, der endnu ikke er omfattet, men som kan blive mere relevante for efterforskninger, fem år efter den foreslåede forordnings ikrafttræden.

Artikel 25: Ikrafttræden

Dette forslag til forordning træder i kraft på tyvendedagen efter offentliggørelsen i Den Europæiske Unions Tidende. Forordningen anvendes seks måneder efter datoen for ikrafttrædelsen.

²⁵ Interinstitutionel aftale mellem Europa-Parlamentet, Rådet for Den Europæiske Union og Europa-Kommissionen om bedre lovgivning af 13. april 2016 (EUT L 123 af 12.5. 2016, s. 1).

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING**om europæiske editions- og sikringskendelser om elektronisk bevismateriale i straffesager**

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 82, stk. 1,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg²⁶,

efter den almindelige lovgivningsprocedure, og

ud fra følgende betragtninger:

- (1) Unionen har sat sig som mål at bevare og udbygge et område med frihed, sikkerhed og retfærdighed. Med henblik på gradvis at indføre et sådant område skal Unionen vedtage foranstaltninger vedrørende retligt samarbejde i straffesager baseret på princippet om gensidig anerkendelse af domme og retsafgørelser, som normalt er blevet betegnet som en hovedhjørnesten i det retlige samarbejde i straffesager i Unionen siden Det Europæiske Råd i Tammerfors den 15. og 16. oktober 1999.
- (2) Foranstaltninger til at indhente og bevare elektronisk bevismateriale får stadig større betydning for strafferetlige efterforskninger og retsforfølgelser i hele EU. Effektive mekanismer til at indhente elektronisk bevismateriale er afgørende for at bekæmpe kriminalitet på betingelser, der sikrer fuld overensstemmelse med de grundlæggende rettigheder og principper, der er anerkendt i Den Europæiske Unions charter om grundlæggende rettigheder som forankret i traktaterne, navnlig principperne om nødvendighed og proportionalitet, retfærdig rettergang, databaseskyttelse, brevhemmelighed og privatlivets fred.
- (3) I den fælles erklæring fra EU's justits- og indenrigsministre og EU-institutionernes repræsentanter om terrorangrebene den 22. marts 2016 i Bruxelles understreges behovet for som en prioritet at finde metoder til hurtigere og mere effektivt at sikre og indhente digitalt bevismateriale og for at fastlægge konkrete foranstaltninger til håndtering af dette spørgsmål.
- (4) Rådet understregede i sine konklusioner af 9. juni 2016 den stigende betydning af elektronisk bevismateriale i straffesager og af beskyttelsen af cyberspace mod misbrug og kriminelle aktiviteter til gavn for økonomier og samfund og således behovet for, at de retshåndhævende og judicielle myndigheder har effektive redskaber til at efterforske og retsforfølge kriminelle aktiviteter i cyberspace.

²⁶ EUT C [...] af [...], s. [...].

- (5) I den fælles meddelelse om modstandsdygtighed, afskrækkelse og forsvar af 13. september 2017²⁷ understregede Kommissionen, at effektiv efterforskning og retsforfølgning af cyberkriminalitet er et centralt afskrækkelsesmiddel over for cyberangreb, og at de aktuelle proceduremæssige rammer skal tilpasses bedre til internettets tidsalder. Hastigheden af cyberangreb kan være for høj for de aktuelle procedurer og skabe særlige behov for samarbejde på tværs af grænserne.
- (6) Europa-Parlamentet understregede ligeledes disse bekymringer i sin beslutning af 3. oktober 2017²⁸ om bekæmpelse af IT-kriminalitet og fremhævede ligeledes, at de forskellige lovgivningsrammer kan skabe problemer for tjenesteudbydere, når de forsøger at imødekomme anmodninger fra de retshåndhævende myndigheder, og opfordrede Kommissionen til at etablere EU-lovgivningsrammer for elektronisk bevismateriale med tilstrækkelige garantier for alle berørte parter rettigheder og friheder.
- (7) Nettjenester kan leveres fra hvor som helst og kræver ikke en fysisk infrastruktur, lokaler eller personale i det pågældende land. Relevant bevismateriale opbevares derfor ofte uden for efterforskningsstaten eller af en tjenesteudbyder, der er etableret uden for denne stat. Der er ofte ingen tilknytning mellem den sag, der efterforskes i den pågældende stat, og den stat, hvor oplysningerne er lagret, eller hvor tjenesteudbyderen har sit hjemsted.
- (8) På grund af denne manglende tilknytning fremsendes anmodninger om retligt samarbejde ofte til stater, der er værtsstater for et stort antal tjenesteudbydere, men som ikke har anden tilknytning til den foreliggende sag. Desuden er antallet af anmodninger mangedoblet på grund af den stigende brug af nettjenester, der i sagens natur er grænseløse. Fremskaffelse af elektronisk bevismateriale gennem retlige samarbejdskanaler tager derfor ofte lang tid – muligvis så lang tid, at efterfølgende spor ikke længere er tilgængelige. Der er desuden ingen klar ramme for samarbejdet med tjenesteudbydere, men visse udbydere fra tredjelande accepterer direkte anmodninger om ikkeindholdsdata, i den udstrækning gældende national lovgivning gør det muligt. Alle medlemsstaterne anvender således kanaler for samarbejde med tjenesteudbydere, hvis de findes, ved brug af forskellige nationale værktøjer, betingelser og procedurer. For så vidt angår indholdsdata, har nogle medlemsstater desuden truffet ensidige foranstaltninger, mens andre fortsat gør brug af det retlige samarbejde.
- (9) De forskellige lovgivningsrammer skaber problemer for tjenesteudbydere, når de forsøger at imødekomme anmodninger fra de retshåndhævende myndigheder. Det er derfor nødvendigt at indføre en europæisk retlig ramme for elektronisk bevismateriale for at pålægge tjenesteudbydere, der er omfattet af instrumentets anvendelsesområde, en forpligtelse til at reagere direkte i forhold til myndigheder uden inddragelse af en judiciel myndighed i tjenesteudbyderens medlemsstat.
- (10) Kendelser i henhold til denne forordning bør rettes til tjenesteudbyderens retlige repræsentanter, der er udpeget med henblik herpå. Hvis en tjenesteudbyder, der er etableret i Unionen, ikke har udpeget en retlig repræsentant, kan kendelsen rettes til ethvert af tjenesteudbyderens etableringssteder i Unionen. Dette alternativ har til formål at sikre, at systemet er effektivt, hvis tjenesteudbyderen (endnu) ikke har udpeget en særlig repræsentant.

²⁷ JOIN(2017) 450 final.

²⁸ 2017/2068(INI).

- (11) Ordningen med den europæiske editionskendelse og den europæiske sikringskendelse for elektronisk bevismateriale i straffesager kan kun fungere på grundlag af en høj grad af gensidig tillid mellem medlemsstaterne, hvilket er en afgørende forudsætning for, at dette instrument fungerer tilfredsstillende.
- (12) I denne forordning overholdes de grundlæggende rettigheder og de principper, som er anerkendt i bl.a. Den Europæiske Unions charter om grundlæggende rettigheder. Disse omfatter retten til frihed og sikkerhed, respekten for privatliv og familieliv, beskyttelse af personoplysninger, friheden til at oprette og drive egen virksomhed, ejendomsretten, adgang til effektive retsmidler og til en upartisk domstol, uskyldsformodningen og retten til forsvar, legalitetsprincippet og princippet om proportionalitet samt retten til ikke at blive retsforfulgt eller straffet to gange for samme lovovertrædelse. Hvis udstedelsesstaten ser visse tegn på, at der muligvis føres parallelle straffesager i en anden medlemsstat, skal den høre myndighederne i denne medlemsstat i overensstemmelse med Rådets rammeafgørelse 2009/948/RIA²⁹.
- (13) For at sikre, at de grundlæggende rettigheder respekteres fuldt ud, henvises der i denne forordning udtrykkeligt til de nødvendige standarder for indsamling af personoplysninger, behandlingen af sådanne oplysninger, den judicielle prøvelse af anvendelsen af efterforskningsforanstaltningen som omhandlet i denne retsakt og de retsmidler, som står til rådighed.
- (14) Denne forordning bør anvendes, uden at det berører de proceduremæssige rettigheder i straffesager, der er fastsat i Europa-Parlamentets og Rådets direktiv 2010/64/EU³⁰, 2012/13/EU³¹, 2013/48/EU³², 2016/343³³, 2016/800³⁴ og 2016/1919³⁵.
- (15) I denne retsakt fastlægges de generelle regler, hvorefter en kompetent judiciel myndighed i EU kan pålægge en tjenesteudbyder, der udbyder tjenester i Unionen, at fremlægge eller bevare elektronisk bevismateriale gennem en europæisk editions- eller sikringskendelse. Denne forordning finder anvendelse i alle tilfælde, hvor tjenesteudbyderen er etableret eller repræsenteret i en anden medlemsstat. I en national kontekst, hvor de instrumenter, der er fastsat i denne forordning, ikke kan anvendes, bør forordningen ikke begrænse de nationale kompetente myndigheders beføjelser, der allerede er fastsat i national ret, til at pålægge tjenesteudbydere, der er etableret eller repræsenteret på deres område, at overholde tilsvarende nationale foranstaltninger.

²⁹ [Rådets rammeafgørelse 2009/948/RIA](#) af 30. november 2009 om forebyggelse og bilæggelse af konflikter om udøvelse af jurisdiktion i straffesager (EUT L 328 af 15.12.2009, s. 42).

³⁰ Europa-Parlamentets og Rådets [direktiv 2010/64/EU](#) af 20. oktober 2010 om retten til tolke- og oversætterbistand i straffesager (EUT L 280 af 26.10.2010, s. 1).

³¹ Europa-Parlamentets og Rådets [direktiv 2012/13/EU](#) af 22. maj 2012 om ret til information under straffesager (EUT L 142 af 1.6.2012, s. 1).

³² Europa-Parlamentets og Rådets [direktiv 2013/48/EU](#) af 22. oktober 2013 om ret til adgang til advokatbistand i straffesager og i sager angående europæiske arrestordre og om ret til at få en tredjemand underrettet ved frihedsberøvelse og til at kommunikere med tredjemand og med konsulære myndigheder under frihedsberøvelsen (EUT L 294 af 6.11.2013, s. 1).

³³ Europa-Parlamentets og Rådets [direktiv \(EU\) 2016/343](#) af 9. marts 2016 om styrkelse af visse aspekter af uskyldsformodningen og retten til at være til stede under retssagen i straffesager (EUT L 65 af 11.3.2016, s. 1).

³⁴ Europa-Parlamentets og Rådets [direktiv \(EU\) 2016/800](#) af 11. maj 2016 om retssikkerhedsgarantier for børn, der er mistænkte eller tiltalte i straffesager (EUT L 132 af 21.5.2016, s. 1).

³⁵ Europa-Parlamentets og Rådets [direktiv \(EU\) 2016/1919](#) af 26. oktober 2016 om retshjælp til mistænkte og tiltalte i straffesager og til eftersøgte i sager angående europæiske arrestordre (EUT L 297 af 4.11.2016, s. 1).

- (16) De tjenesteudbydere, der er mest relevante i straffesager, er udbydere af elektroniske kommunikationstjenester og udbydere af informationssamfundstjenester, som letter interaktionen mellem brugerne. Begge grupper bør således være omfattet af denne forordning. Udbydere af elektroniske kommunikationstjenester er defineret i forslaget til direktiv om en europæisk kodeks for elektronisk kommunikation. De omfatter interpersonel kommunikation såsom internettelefoni, instant messaging og e-mailtjenester. De kategorier af informationssamfundstjenester, der er omfattet her, er de tjenester, hvor lagring af data er et afgørende element i den tjeneste, der leveres til brugeren, navnlig sociale netværk i det omfang de ikke betragtes som elektroniske kommunikationstjenester, onlinemarkedspladser til fremme af transaktioner mellem deres brugere (såsom forbrugere eller virksomheder) og andre hostingtjenester, herunder hvor tjenesten leveres via cloudcomputing. Informationssamfundets tjenester, hvor lagring af data ikke er et afgørende element i den tjeneste, der leveres til brugeren, og derfor kun er af accessorisk karakter, f.eks. juridiske rådgivnings-, arkitekt-, ingeniør- og regnskabstjenester leveret ad elektronisk vej, bør udelukkes fra denne forordnings anvendelsesområde, også selv om de falder ind under definitionen af informationssamfundets tjenester i direktiv (EU) 2015/1535.
- (17) I mange tilfælde lagres eller behandles oplysningerne ikke længere på en brugers enhed, men er tilgængelige på en skybaseret infrastruktur, der er adgang til fra et hvilket som helst sted. Tjenesteudbyderne behøver ikke at være etableret eller at have servere i en specifik jurisdiktion for at drive disse tjenester. Anvendelsen af denne forordning bør således ikke afhænge af tjenesteudbyderens faktiske etableringssted eller af databehandlings- eller lagerfacilitetens faktiske beliggenhed.
- (18) Udbydere af internetinfrastruktur-tjenester vedrørende tildeling af navne og numre, f.eks. domænenavneadministratorer og -registratorer og privatlivs- og proxytjenester eller regionale onlineregistre for IP-adresser, er af særlig relevans i forbindelse med identifikation af aktører bag ondsindede eller kompromitterede websteder. De opbevarer oplysninger, der er af særlig relevans for straffesager, da de kan gøre det muligt at identificere en enkeltperson eller enhed bag et websted, der anvendes til kriminelle aktiviteter, eller ofret for kriminelle handlinger i tilfælde af et kompromitteret websted, der er blevet overtaget af kriminelle.
- (19) Denne forordning regulerer kun indsamling af lagrede data, dvs. de data, som en tjenesteudbyder ligger inde med på tidspunktet for modtagelsen af en attest for en europæisk editions- eller sikringskendelse. Forordningen indfører ikke en generel pligt til opbevaring af data og tillader heller ikke aflytning eller indhentning af data, der lagres på et senere tidspunkt efter modtagelsen af en attest for en editions- eller sikringskendelse. Dataene bør fremlægges, uanset om de er krypteret eller ej.
- (20) Datakategorierne i denne forordning omfatter abonnentdata, adgangsdata, transaktionsdata (tre kategorier, der samlet benævnes "ikkeindholdsdata") og indholdsdata. Denne sondring findes i mange medlemsstaters retsorden, også i den gældende lovgivningsramme i USA, der giver tjenesteudbyderne mulighed for at udveksle ikkeindholdsdata med udenlandske retshåndhævende myndigheder på frivillig basis.
- (21) Det er hensigtsmæssigt at adskille adgangsdata som en særlig datakategori i denne forordning. Adgangsdata anvendes til samme formål som abonnentdata, med andre ord til at identificere brugeren, og graden af indgriben i de grundlæggende rettigheder er den samme. Adgangsdata registreres typisk i forbindelse med registreringen af hændelser (med andre ord en serverlog) for at angive påbegyndelsen og afslutningen

af en brugeradgangssession til en tjeneste. Det er ofte en individuel IP-adresse (statisk eller dynamisk) eller en anden identifikator for den netgrænseflade, der anvendes under adgangssessionen. Hvis brugeren er ukendt, skal den ofte indhentes, inden tjenesteudbyderen kan pålægges at fremlægge abonnentdata vedrørende denne identifikator.

- (22) Der anmodes derimod generelt om transaktionsdata for at få oplysninger om brugerens kontakter og færden, og der kan udstedes en kendelse for at fastlægge den pågældendes profil. Når dette er sagt, kan adgangsdata ikke i sig selv bruges til at fastslå, om formålet er det samme, da de f.eks. ikke indeholder oplysninger om brugerens kontakter. Dette forslag indfører derfor en ny kategori af data, der skal behandles som abonnentdata, hvis formålet med fremskaffelsen af dataene er det samme.
- (23) Alle datakategorier indeholder personoplysninger og er dermed omfattet af garantiene i EU-databeskyttelsesreglerne, men indvirkningen på de grundlæggende rettigheder er forskellig, alt efter om der er tale om abonnent- og adgangsdata eller transaktions- og indholdsdata. Abonnent- og adgangsdata er nyttige til at finde de første spor i en efterforskning vedrørende den mistænkte identitet, og transaktions- og indholdsdata er mest relevante som bevismateriale. Det er derfor afgørende, at alle disse datakategorier er omfattet af instrumentet. På grund af den forskellige grad af indgriben i de grundlæggende rettigheder er der knyttet forskellige betingelser til indhentning af abonnentdata og transaktions- og indholdsdata.
- (24) Den europæiske editionskendelse og den europæiske sikringskendelse er efterforskningsforanstaltninger, som kun bør udstedes i straffesager mod bestemte kendte eller stadig ukendte gerningsmænd til en konkret strafbar handling, der allerede har fundet sted, efter en individuel vurdering af proportionaliteten og nødvendigheden af den enkelte kendelse.
- (25) Denne forordning berører ikke myndighedernes undersøgelsesbeføjelser i civile og administrative sager, herunder når disse sager kan føre til pålæggelse af sanktioner.
- (26) Denne forordning bør finde anvendelse på tjenesteudbydere, der udbyder tjenester i Unionen, og de kendelser, der er omhandlet i denne forordning, må kun udstedes for data vedrørende tjenester, der udbydes i Unionen. Tjenester, der udelukkende udbydes uden for Unionen, er ikke omfattet af denne forordning, selv om tjenesteudbyderen er etableret i Unionen.
- (27) For at fastslå, om en tjenesteudbyder udbyder tjenester i Unionen, skal det vurderes, om tjenesteudbyderen gør det muligt for juridiske eller fysiske personer i en eller flere medlemsstater at gøre brug af udbyderens tjenester. Adgangen til en onlinegrænseflade, f.eks. adgang til tjenesteudbyderens eller en mellemmands websted eller til en e-mailadresse og andre kontaktoplysninger i en eller flere medlemsstater, bør imidlertid ikke i sig selv være en tilstrækkelig betingelse for anvendelsen af denne forordning.
- (28) En væsentlig tilknytning til Unionen bør også være relevant for at fastslå denne forordnings anvendelsesområde. En sådan væsentlig tilknytning til Unionen bør anses for at være til stede, hvis tjenesteudbyderen er etableret i Unionen. Hvis tjenesteudbyderen ikke er etableret i Unionen, bør kriteriet om en væsentlig tilknytning vurderes på grundlag af, om der er et betydeligt antal brugere i en eller flere medlemsstater, eller om tjenesteudbyderen retter sin virksomhed mod en eller flere medlemsstater. Målretning af virksomheden mod en eller flere medlemsstater kan

fastslås på grundlag af alle relevante omstændigheder, herunder faktorer såsom anvendelsen af et sprog eller en valuta, der almindeligvis anvendes i en medlemsstat, eller muligheden for at bestille varer eller tjenesteydelser. Måretningen af virksomheden mod en medlemsstat kan ligeledes udledes af tilgængeligheden af en applikation ("app") i den relevante nationale app-butik, af lokal annoncering eller annoncering på det sprog, der anvendes i den pågældende medlemsstat, eller håndteringen af kunderelationer, f.eks. ved at yde kundeservice på det sprog, der normalt anvendes i den pågældende medlemsstat. Det må endvidere antages, at der er en væsentlig tilknytning, hvis tjenesteudbyderen retter sin virksomhed mod en eller flere medlemsstater, jf. artikel 17, stk. 1, litra c), i forordning (EU) nr. 1215/2012 om retternes kompetence og om anerkendelse og fuldbyrdelse af retsafgørelser på det civil- og handelsretlige område³⁶. Levering af tjenesten alene med det formål at overholde det forbud mod forskelsbehandling, der er fastsat i forordning (EU) 2018/302³⁷, kan ikke i sig selv betragtes som tegn på, at den erhvervsdrivende retter virksomhed mod et bestemt område i Unionen.

- (29) En europæisk editionskendelse bør kun udstedes, hvis dette er nødvendigt og forholdsmæssigt. Ved vurderingen bør der tages hensyn til, om kendelsen er begrænset til, hvad der er nødvendigt for at nå det legitime mål om at indhente de relevante og nødvendige oplysninger, der udelukkende skal tjene som bevismateriale i den konkrete sag.
- (30) En judiciel myndighed bør altid være involveret i udstedelsen af en europæiske editions- eller sikringskendelse, enten i selve udstedelsen eller i godkendelsen af kendelsen. I betragtning af den mere følsomme karakter af transaktions- og indholdsdata skal udstedelsen eller godkendelsen af europæiske editionskendelser om fremlæggelse af disse datakategorier undergives domstolsprøvelse. Da abonnement- og adgangsdata er mindre følsomme, kan europæiske editionskendelser om fremlæggelse af disse oplysninger desuden udstedes eller godkendes af kompetente anklagere.
- (31) Der skal af samme grund sondres med hensyn til det materielle anvendelsesområde for denne forordning: Kendelser om fremlæggelse af abonnement- og adgangsdata kan udstedes for enhver lovovertrædelse, hvorimod adgang til transaktions- og indholdsdata bør være underlagt strengere krav for at tage højde for den mere følsomme karakter af sådanne oplysninger. En tærskel gør det muligt at anlægge en mere forholdsmæssig tilgang, og dette sikrer sammen med en række andre forudgående og efterfølgende betingelser og garantier i forslaget, at proportionalitetsprincippet og de berørte personers rettigheder overholdes. Tærsklen bør samtidig ikke begrænse instrumentets effektivitet og de retshåndhævende myndigheders brug heraf. Muligheden for at udstede efterforskningskendelser i forbindelse med lovovertrædelser, der kan straffes med en frihedsstraf af en maksimal varighed på mindst tre år, begrænser instrumentets anvendelsesområde til grovere former for kriminalitet, men begrænser ikke i for høj grad de retshåndhævende

³⁶ Europa-Parlamentets og Rådets [forordning \(EU\) nr. 1215/2012](#) af 12. december 2012 om retternes kompetence og om anerkendelse og fuldbyrdelse af retsafgørelser på det civil- og handelsretlige område (EUT L 351 af 20.12.2012, s. 1).

³⁷ Europa-Parlamentets og Rådets [forordning \(EU\) 2018/302](#) af 28. februar 2018 om imødegåelse af uberettiget geoblokering og andre former for forskelsbehandling på grundlag af kundernes nationalitet, bopæl eller hjemsted i det indre marked og om ændring af forordning (EF) nr. 2006/2004 og (EU) 2017/2394 og af direktiv 2009/22/EF (EUT L 601 af 2.3.2018, s. 1).

myndigheders muligheder for at anvende det. Det udelukker en lang række forbrydelser, der betragtes som mindre alvorlige af medlemsstaterne som udtrykt i en lavere maksimal straf, fra anvendelsesområdet. En tærskel har ligeledes den fordel, at den er let at anvende i praksis.

- (32) Der findes særlige lovovertrædelser, hvor bevismaterialet typisk er tilgængeligt i elektronisk form og af meget flygtig karakter. Dette er tilfældet for cyberrelaterede strafbare handlinger, endog handlinger, som muligvis ikke anses for alvorlige i sig selv, men som kan forårsage omfattende eller betydelige skader, herunder navnlig handlinger, der har en begrænset indvirkning på den enkelte, men begås i et stort antal og forårsager omfattende skader samlet set. I de fleste tilfælde, hvor lovovertrædelsen er begået ved brug af et informationssystem, ville anvendelsen af den samme tærskel som for andre typer lovovertrædelser primært føre til straffrihed. Dette berettiger ligeledes anvendelsen af forordningen i forbindelse med disse overtrædelser, hvor strafferammen er under tre års fængsel. I forbindelse med andre terrorhandling som omhandlet i direktiv (EU) 2017/541 stilles der ikke krav om en maksimumstærskel på mindst tre år.
- (33) Det er desuden nødvendigt at sikre, at den europæiske editionskendelse kun kan udstedes, hvis en lignende kendelse kan udstedes for samme lovovertrædelse i en sammenlignelig national situation i udstedelsesstaten.
- (34) Hvis de oplysninger, der anmodes om, opbevares eller behandles som en del af en tjenesteudbyders infrastruktur, der stilles til rådighed for en virksomhed eller en anden enhed, der ikke er en fysisk person, typisk i forbindelse med hostingtjenester, bør den europæiske editionskendelse udelukkende anvendes, når det ikke er hensigtsmæssigt at træffe efterforskningsforanstaltninger over for den pågældende virksomhed eller enhed, navnlig hvis det kan bringe efterforskningen i fare. Dette gælder navnlig for større enheder såsom selskaber eller offentlige enheder, der benytter sig af tjenester fra tjenesteudbydere, der leverer deres IT-infrastruktur eller -tjenester eller begge dele. Den første modtager af en europæisk editionskendelse bør i dette tilfælde være virksomheden eller en anden enhed. Denne virksomhed eller anden enhed må ikke være en tjenesteudbyder, der er omfattet af denne forordnings anvendelsesområde. I sager, hvor det ikke er hensigtsmæssigt at anmode den pågældende enhed om oplysninger, f.eks. fordi enheden mistænkes for at være involveret i den pågældende sag, eller fordi der er tegn på aftalt spil med den, der efterforskes, bør de kompetente myndigheder imidlertid kunne anmode tjenesteudbyderen af den pågældende infrastruktur om at fremlægge de anmodede oplysninger. Denne bestemmelse berører ikke retten til at pålægge tjenesteudbyderen at bevare oplysningerne.
- (35) Privilegier og immuniteter for personkategorier (f.eks. diplomater) eller særligt beskyttede forhold (f.eks. retten til fortrolighed mellem advokat og klient) er omfattet af andre instrumenter til gensidig anerkendelse såsom den europæiske efterforskningskendelse. Deres rækkevidde og indvirkning er forskellig afhængigt af den gældende nationale lovgivning, der skal tages i betragtning i forbindelse med udstedelsen af kendelsen, da udstedelsesmyndigheden kun kan udstede en kendelse, hvis en lignende kendelse kan udstedes i en sammenlignelig national situation. Ud over dette grundlæggende princip bør der i udstedelsesstaten i videst muligt omfang tages hensyn til immuniteter og privilegier, der beskytter adgangs-, transaktions- eller indholdsdata i tjenesteudbyderens medlemsstat, på samme måde, som hvis de var omfattet af national lovgivning i udstedelsesstaten. Dette er navnlig relevant, hvis lovgivningen i tjenesteudbyderens eller dennes retlige repræsentants medlemsstat sikrer en højere beskyttelse end lovgivningen i udstedelsesstaten. Bestemmelsen sikrer

ligeledes, at der tages hensyn til tilfælde, hvor videregivelsen af oplysningerne kan berøre den pågældende medlemsstats grundlæggende interesser såsom statens sikkerhed og forsvar. Som en yderligere garanti bør disse aspekter tages i betragtning, ikke kun når kendelsen udstedes, men også senere i forbindelse med vurderingen af relevansen af de pågældende oplysninger i den relevante fase af straffesagen, og i forbindelse med en fuldbyrdelsesprocedure af fuldbyrdelsesmyndigheden.

- (36) Den europæiske sikringskendelse kan udstedes for alle lovovertrædelser. Formålet er at forhindre fjernelse, sletning eller ændring af relevante oplysninger i situationer, hvor det kan tage længere tid at få indhentet disse oplysninger, f.eks. fordi der anvendes retlige samarbejdskanaler.
- (37) Europæiske editions- og sikringskendelser bør rettes til den retlige repræsentant, der er udpeget af tjenesteudbyderen. Hvis der ikke er udpeget en retlig repræsentant, kan kendelsen rettes til ethvert af tjenesteudbyderens etableringssteder i Unionen. Dette kan være tilfældet, hvis tjenesteudbyderen ikke har nogen retlig forpligtelse til at udpege en retlig repræsentant. I tilfælde af den retlige repræsentants manglende overholdelse i nødsituationer kan den europæiske editions- eller sikringskendelse ligeledes rettes til tjenesteudbyderen sideløbende med eller i stedet for at søge fuldbyrdelse af den oprindelige kendelse i henhold til artikel 14. I tilfælde af den retlige repræsentants manglende overholdelse i ikke-nødsituationer, hvor der er en klar risiko for tab af data, kan den europæiske editionskendelse eller den europæiske sikringskendelse rettes til ethvert af tjenesteudbyderens etableringssteder i Unionen. På grund af disse forskellige mulige scenarier anvendes den generelle betegnelse "modtager" i bestemmelserne. Hvis en forpligtelse, f.eks. vedrørende fortrolighed, ikke kun gælder for modtageren, men ligeledes for tjenesteudbyderen, hvis denne ikke er modtageren, er dette anført i den pågældende bestemmelse.
- (38) De europæiske editions- eller sikringskendelser bør fremsendes til tjenesteudbyderen i form af en attest for den europæiske editionskendelse (EPOC) eller en attest for den europæiske sikringskendelse (EPOC-PR), der bør oversættes. Attesterne bør indeholde de samme obligatoriske oplysninger som kendelserne bortset fra begrundelsen for foranstaltningens proportionalitet og nødvendighed og yderligere oplysninger om sagen for at undgå at bringe efterforskningen i fare. Da de er en del af selve kendelsen, giver de den mistænkte mulighed for at gøre indsigelse mod den på et senere tidspunkt under straffesagen. Om nødvendigt skal attesten oversættes til (et af) de officielle sprog i modtagerens medlemsstat eller til et andet officielt sprog, som tjenesteudbyderen har erklæret at ville acceptere.
- (39) Den kompetente udstedelsesmyndighed bør fremsende EPOC'en eller EPOC-PR'en direkte til modtageren ved hjælp af ethvert middel, som kan efterlade et skriftligt spor, og som giver tjenesteudbyderen mulighed for at fastslå ægtheden, f.eks. pr. anbefalet brev, sikker e-mail og platforme eller andre sikre kanaler, herunder dem, der stilles til rådighed af tjenesteudbyderen, i overensstemmelse med reglerne om beskyttelse af personoplysninger.
- (40) De anmodede oplysninger bør fremsendes til myndighederne senest 10 dage efter modtagelsen af EPOC'en. Kortere frister skal overholdes af tjenesteudbyderen i nødsituationer, og hvis udstedelsesmyndigheden anfører andre grunde til at afvige fra fristen på 10 dage. Ud over den overhængende fare for sletning af de anmodede oplysninger kan sådanne grunde omfatte forhold vedrørende en igangværende efterforskning, f.eks. hvis de anmodede oplysninger er knyttet til andre hastende

efterforskningsforanstaltninger, som ikke kan gennemføres uden de manglende oplysninger eller på anden vis er afhængige af dem.

- (41) For at gøre det muligt for tjenesteudbydere at løse formelle problemer er det nødvendigt at fastlægge en procedure for kommunikation mellem tjenesteudbyderen og den judicielle udstedelsesmyndighed, hvis EPOC'en er ufuldstændig eller indeholder åbenbare fejl eller ikke indeholder tilstrækkelige oplysninger. Hvis tjenesteudbyderen ikke fremlægger fyldestgørende eller rettidige oplysninger af andre grunde, f.eks. fordi udbyderen mener, at der er en modstridende forpligtelse begrundet i et tredjelands lovgivning, eller fordi udbyderen mener, at den europæiske editionskendelse ikke er blevet udstedt i overensstemmelse med de betingelser, der er fastsat i denne forordning, bør udbyderen desuden rette henvendelse til udstedelsesmyndigheden med en passende begrundelse. Kommunikationsproceduren bør generelt give udstedelsesmyndigheden mulighed for at korrigere eller genoverveje EPOC'en på et tidligt tidspunkt. For at sikre adgangen til oplysningerne bør tjenesteudbyderen bevare oplysningerne, hvis denne kan identificere de oplysninger, der anmodes om.
- (42) Efter modtagelsen af attesten for den europæiske sikringskendelse ("EPOC-PR") bør tjenesteudbyderen bevare de anmodede oplysninger i højst 60 dage, medmindre udstedelsesmyndigheden meddeler tjenesteudbyderen, at den har indledt proceduren for den efterfølgende anmodning om fremlæggelse af oplysninger, i hvilket tilfælde oplysningerne fortsat bør bevares. Fristen på 60 dage beregnes med henblik indledning af proceduren for den officielle anmodning. Dette kræver, at der som minimum er truffet en række formelle foranstaltninger, f.eks. fremsendelse af en anmodning om gensidig retshjælp til oversættelse. Efter modtagelsen af denne information bør oplysningerne bevares, så længe det er nødvendigt for at fremlægge oplysningerne i forbindelse med en efterfølgende anmodning om fremlæggelse af oplysninger.
- (43) Tjenesteudbydere og deres retlige repræsentanter bør sikre fortroligheden og undlade at underrette den person, hvis oplysninger efterspørges, når udstedelsesmyndigheden anmoder herom, for at beskytte efterforskningen af lovovertrædelser i overensstemmelse med artikel 23 i forordning (EU) 2016/679³⁸. Brugeroplysninger er imidlertid et afgørende element i revisionen og domstolsprøvelsen, og myndigheden bør tilvejebringe disse, hvis tjenesteudbyderen er blevet anmodet om ikke at underrette brugeren, når der ikke er nogen risiko for at bringe igangværende efterforskninger i fare, i overensstemmelse med de nationale foranstaltninger til gennemførelse af artikel 13 i direktiv (EU) 2016/680³⁹.
- (44) I tilfælde af modtagerens manglende overholdelse kan udstedelsesmyndigheden fremsende hele kendelsen, herunder begrundelsen for nødvendigheden og proportionaliteten, ledsaget af attesten til den kompetente myndighed i den medlemsstat, hvor modtageren af attesten er bosiddende eller etableret. Denne

³⁸ 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 (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

³⁹ Europa-Parlamentets og Rådets [direktiv \(EU\) 2016/680](#) af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (EUT L 119 af 4.5.2016, s. 89).

medlemsstat bør fuldbyrde kendelsen i overensstemmelse med national lovgivning. Medlemsstaterne bør pålægge effektive, forholdsmæssige og afskrækkende økonomiske sanktioner i tilfælde af overtrædelser af de forpligtelser, der er fastsat i denne forordning.

- (45) Fuldbyrdeproceduren er en procedure, hvor modtageren kan gøre indsigelse mod fuldbyrdelsen på grundlag af visse begrænsede grunde. Fuldbyrdeproceduren kan nægte at anerkende og fuldbyrde en kendelse med samme begrundelse, eller hvis privilegier og immuniteter i henhold til den nationale lovgivning finder anvendelse, eller hvis videregivelsen kan berøre nationale grundlæggende interesser såsom statens sikkerhed og forsvar. Fuldbyrdeproceduren bør høre udstedelsesmyndigheden, inden den nægter at anerkende eller fuldbyrde kendelsen med denne begrundelse. I tilfælde af manglende overholdelse kan myndighederne pålægge sanktioner. Disse sanktioner bør stå i et rimeligt forhold til den manglende overholdelse, herunder særlige omstændigheder såsom gentagen eller systematisk manglende overholdelse.
- (46) Uanset deres databeskyttelsesforpligtelser bør tjenesteudbydere ikke holdes ansvarlige i medlemsstaterne for skade på deres brugere eller tredjeparter, der udelukkende kan tilskrives overholdelse i god tro af en EPOC eller en EPOC-PR.
- (47) Ud over de personer, hvis oplysninger efterspørges, kan tjenesteudbydere og tredjelande blive berørt af efterforskningsforanstaltningen. For at sikre international anerkendelse af domme i forhold til tredjelands suveræne interesser, beskytte den pågældende person og håndtere tjenesteudbyderes modstridende forpligtelser indføres der med dette instrument en særlig ordning for juridisk prøvelse, hvis overholdelsen af en europæisk editionskendelse vil forhindre tjenesteudbydere i at opfylde retlige forpligtelser i henhold til et tredjelands lovgivning.
- (48) Når modtageren mener, at den europæiske editionskendelse i det konkrete tilfælde vil indebære en overtrædelse af en retlig forpligtelse i henhold til lovgivningen i et tredjeland, bør modtageren således underrette udstedelsesmyndigheden ved at rejse en begrundet indsigelse ved brug af formularerne i bilaget. Udstedelsesmyndigheden bør derefter kontrollere den europæiske editionskendelse på grundlag af den begrundede indsigelse under hensyntagen til de samme kriterier som den kompetente ret. Når myndigheden beslutter at opretholde kendelsen, bør proceduren henvises til den kompetente ret som meddelt af den pågældende medlemsstat, der herefter foretager en prøvelse af kendelsen.
- (49) Ved afgørelsen af, om der foreligger en modstridende forpligtelse under de særlige omstændigheder i den foreliggende sag, bør den kompetente ret benytte sig af passende eksternt ekspertise efter behov, f.eks. hvis prøvelsen rejser spørgsmål om fortolkning af lovgivningen i det pågældende tredjeland. Dette kan omfatte høring af de centrale myndigheder i det pågældende tredjeland.
- (50) Ekspertviden om fortolkningen kan ligeledes indhentes i eventuelle ekspertudtalelser. Der bør være adgang til oplysninger og retspraksis vedrørende fortolkningen af tredjelands lovgivning om modstridende procedurer i medlemsstaterne på en central platform såsom SIRIUS-projektet og/eller det europæiske retlige netværk. Dette bør gøre det muligt for retterne at drage fordel af erfaringer og ekspertviden, der er indsamlet af andre retter om samme eller lignende spørgsmål. Dette bør ikke være til hinder for en fornyet høring af det pågældende tredjeland, hvis det er relevant.
- (51) Hvis der er modstridende forpligtelser bør retten afgøre, om de modstridende bestemmelser i tredjelandet forbyder videregivelse af de pågældende oplysninger med

den begrundelse, at det er nødvendigt for at beskytte de berørte personers grundlæggende rettigheder eller tredjelandets grundlæggende rettigheder forbundet med statens sikkerhed eller forsvar. I forbindelse med denne vurdering bør retten tage højde for, om tredjelandets lovgivning i stedet for at beskytte tredjelandets grundlæggende rettigheder eller grundlæggende interesser forbundet med statens sikkerhed eller forsvar åbenlyst har til formål at beskytte andre interesser eller ulovlige aktiviteter mod anmodninger fra de retshåndhævende myndigheder i forbindelse med strafferetlige efterforskninger. Hvis retten fastslår, at modstridende bestemmelser i tredjelandet forbyder videregivelse af de pågældende oplysninger med den begrundelse, at det er nødvendigt for at beskytte de berørte personers grundlæggende rettigheder eller tredjelandets grundlæggende rettigheder forbundet med statens sikkerhed eller forsvar, bør den høre det pågældende tredjeland gennem dets centrale myndigheder for gensidig retshjælp, der findes de fleste dele af verden. Retten bør fastsætte en frist for det pågældende tredjelandets indsigelse mod gennemførelsen af den europæiske editionskendelse, og hvis myndighederne i tredjelandet ikke reagerer inden for den (udvidede) frist på trods af en påmindelse om konsekvenserne af at undlade at svare, stadfæster retten kendelsen. Hvis myndighederne i tredjelandet modsætter sig videregivelse, bør retten ophæve kendelsen.

- (52) I forbindelse med alle andre modstridende forpligtelser, der ikke vedrører den enkeltes grundlæggende rettigheder eller tredjelandets grundlæggende rettigheder forbundet med statens sikkerhed eller forsvar, bør retten træffe afgørelse om, hvorvidt den europæiske editionskendelse skal stadfæstes, ved at afveje en række elementer, der kan bruges til at vurdere styrken af tilknytningen til de to jurisdiktioner, de respektive interesser i at opnå eller forhindre videregivelse af oplysningerne og de eventuelle konsekvenser for tjenesteudbyderen forbundet med efterlevelsen af kendelsen. For cyberrelaterede strafbare handlinger omfatter det sted, hvor handlingen blev begået, både det eller de steder, hvor foranstaltningen blev truffet, og det eller de steder, hvor den strafbare handling fik konsekvenser.
- (53) De betingelser, der er fastsat i artikel 9, finder ligeledes anvendelse i tilfælde af modstridende forpligtelser begrundet i lovgivningen i et tredjeland. Oplysningerne bør bevares under denne procedure. Hvis kendelsen ophæves, kan der udstedes en ny sikringskendelse, således at udstedelsesmyndigheden kan anmode om at få oplysningerne fremlagt gennem andre kanaler såsom gensidig retshjælp.
- (54) Det er vigtigt, at alle personer, hvis oplysninger efterspørges i forbindelse med en strafferetlig efterforskning eller retsforfølgning, har adgang til effektive retsmidler i overensstemmelse med artikel 47 i Den Europæiske Unions charter om grundlæggende rettigheder. For mistænkte og tiltalte vedkommende bør adgangen til effektive retsmidler udøves under straffesagen. Dette kan påvirke antageligheden eller eventuelt den vægt, som bevismaterialet fremskaffet ved brug af sådanne retsmidler tillægges under retssagen. De drager desuden fordel af alle de proceduremæssige garantier, der gælder for dem, såsom retten til information. Andre personer, der ikke er mistænkte eller tiltalte, bør også have adgang til effektive retsmidler. Der bør derfor som minimum være mulighed for at anfægte lovligheden af en europæisk editionskendelse, herunder kendelsens nødvendighed og proportionalitet. Denne forordning bør ikke begrænse de mulige grunde til at anfægte kendelsens lovlighed. Disse retsmidler bør udøves i udstedelsesstaten i overensstemmelse med national lovgivning. Reglerne om foreløbige forholdsregler bør reguleres af national lovgivning.

- (55) Under fuldbyrdelsesproceduren og de efterfølgende retsmidler kan modtageren desuden gøre indsigelse mod fuldbyrdelsen af en europæisk editions- eller sikringskendelse med påberåbelse af en række begrænsede grunde, herunder at kendelsen ikke er udstedt eller godkendt af en kompetent myndighed, eller at den tydeligvis er i modstrid med Den Europæiske Unions charter om grundlæggende rettigheder eller er åbenbart urimelig. En kendelse om fremlæggelse af indholdsdata vedrørende en udefineret gruppe af personer i et geografisk område eller uden tilknytning til en konkret straffesag er tydeligvis ikke i overensstemmelse med betingelserne for udstedelse af en europæisk editionskendelse.
- (56) Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger er en grundlæggende rettighed. I overensstemmelse med artikel 8, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder og artikel 16, stk. 1, i TEUF har enhver ret til beskyttelse af personoplysninger, der vedrører den pågældende. I forbindelse med gennemførelsen af denne forordning bør medlemsstaterne sikre, at personoplysninger beskyttes og kun behandles i overensstemmelse med forordning (EU) 2016/679 og direktiv (EU) 2016/680.
- (57) Personoplysninger, der tilvejebringes i henhold til denne forordning, bør kun behandles, når det er nødvendigt og står i et rimeligt forhold til formålene om forebyggelse, efterforskning, opdagelse eller retsforfølgelse af kriminalitet eller fuldbyrdelse af strafferetlige sanktioner samt udøvelse af retten til et forsvar. Medlemsstaterne bør navnlig sikre, at relevante databeskyttelsespolitikker og -foranstaltninger finder anvendelse på videregivelse af personoplysninger fra relevante myndigheder til tjenesteudbydere med henblik på denne forordning, herunder foranstaltninger, der skal sikre oplysningernes sikkerhed. Tjenesteudbydere bør sikre det samme for videregivelse af personoplysninger til relevante myndigheder. Kun autoriserede personer bør have adgang til oplysninger, der indeholder personoplysninger, som kan opnås gennem kontrolprocesser. Det bør overvejes at anvende mekanismer til sikring af ægthed, f.eks. anmeldte nationale elektroniske identifikationssystemer eller tillidstjenester som omhandlet i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.
- (58) Kommissionen bør foretage en evaluering af denne forordning, som bør være baseret på de fem kriterier, nemlig effektivitet, virkningsgrad, relevans, sammenhæng og merværdi for EU, og som bør danne grundlag for konsekvensanalyser af mulige yderligere foranstaltninger. Der bør regelmæssigt indsamles oplysninger til brug for evaluering af denne forordning.
- (59) Anvendelsen af oversatte standardformularer letter samarbejdet og udvekslingen af oplysninger mellem judicielle myndigheder og tjenesteudbydere, således at de kan sikre og videreende elektronisk bevismateriale hurtigere og mere effektivt og samtidigt opfylde de nødvendige sikkerhedskrav på en brugervenlig måde. De mindsker udgifterne til oversættelse og bidrager til en høj kvalitetsstandard. Svarformularerne bør ligeledes give mulighed for en standardiseret informationsudveksling, navnlig når tjenesteudbydere ikke kan efterleve kendelsen, fordi kontoen ikke findes, eller fordi der ikke foreligger nogen oplysninger. Formularerne bør også lette indsamlingen af statistikker.
- (60) For effektivt at imødegå et eventuelt behov for forbedringer af indholdet af EPOC'erne og EPOC-PR'erne og af de formularer, der skal anvendes til at oplyse om, hvorfor det

ikke er muligt at gennemføre EPOC'en eller EPOC-PR'en, bør beføjelsen til at vedtage retsakter i overensstemmelse med artikel 290 i traktaten om Den Europæiske Unions funktionsmåde uddelegeres til Kommissionen med henblik på at ændre bilag I, II og III til denne forordning. Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning⁴⁰. For at sikre lige deltagelse i forberedelsen af delegerede retsakter modtager Europa-Parlamentet og Rådet navnlig alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter har systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.

- (61) Foranstaltningerne baseret på denne forordning bør ikke have forrang for europæiske efterforskningskendelser i overensstemmelse med Europa-Parlamentets og Rådets direktiv 2014/41/EU⁴¹ med henblik på fremskaffelse af elektronisk bevismateriale. Medlemsstaternes myndigheder bør vælge det redskab, der passer bedst til deres situation. De foretrækker måske at anvende den europæiske efterforskningskendelse, når de anmoder om alternative efterforskningsforanstaltninger, herunder men ikke begrænset til fremlæggelse af elektronisk bevismateriale fra en anden medlemsstat.
- (62) På grund af den teknologiske udvikling kan nye former for kommunikationsmidler være fremherskende om nogle få år, eller der kan opstå huller i anvendelsen af denne forordning. Det er derfor vigtigt at sikre, at forordningens anvendelse kontrolleres.
- (63) Eftersom målene med denne forordning, nemlig at forbedre sikringen og fremskaffelsen af elektronisk bevismateriale på tværs af grænserne, ikke i tilstrækkelig grad kan opfyldes af medlemsstaterne på grund af forordningens grænseoverskridende karakter, men bedre kan nås på EU-plan, kan Unionen vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke videre, end hvad der er nødvendigt for at nå disse mål.
- (64) I medfør af artikel 3 i protokollen om Det Forenede Kongeriges og Irlands stilling for så vidt angår området med frihed, sikkerhed og retfærdighed, der er knyttet som bilag til traktaten om Den Europæiske Union og til traktaten om Den Europæiske Unions funktionsmåde, [har Det Forenede Kongerige og Irland meddelt, at de ønsker at deltage i vedtagelsen og anvendelsen af denne forordning]/[og med forbehold af samme protokols artikel 4 deltager Det Forenede Kongerige/Irland ikke i vedtagelsen af denne forordning, som ikke er bindende for og ikke finder anvendelse i Det Forenede Kongerige/Irland].
- (65) I medfør af artikel 1 og 2 i protokol nr. 22 om Danmarks stilling, der er knyttet som bilag til traktaten om Den Europæiske Union og til traktaten om Den Europæiske Unions funktionsmåde, deltager Danmark ikke i vedtagelsen af denne forordning, som ikke er bindende for og ikke finder anvendelse i Danmark.

⁴⁰ EUT L 123 af 12.5. 2016, s. 1.

⁴¹ Europa-Parlamentets og Rådets [direktiv 2014/41/EU](#) af 3. april 2014 om den europæiske efterforskningskendelse i straffesager (EUT L 130 af 1.5.2014, s. 1).

- (66) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 28, stk. 2, i Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001⁴² og har afgivet en udtalelse den (...) ⁴³ —

VEDTAGET DENNE FORORDNING:

Kapitel 1: Emne, definitioner og anvendelsesområde

Artikel 1

Emne

1. I denne forordning fastsættes regler, hvorefter en myndighed i en medlemsstat kan pålægge en tjenesteudbyder, der udbyder tjenester i Unionen, at fremlægge eller sikre elektronisk bevismateriale, uanset hvor dataene befinder sig. Denne forordning berører ikke de nationale myndigheders beføjelser til at pålægge tjenesteudbydere, der er etableret eller repræsenteret på deres område, at overholde tilsvarende nationale foranstaltninger.
2. Denne forordning indebærer ikke nogen ændring af pligten til at respektere de grundlæggende rettigheder og retsprincipper som fastsat i artikel 6 i TEU, herunder retten til et forsvar for personer, der er anklaget i en straffesag, og eventuelle forpligtelser, der påhviler de retshåndhævende og judicielle myndigheder i denne henseende, berøres ikke.

Artikel 2

Definitioner

I denne forordning forstås ved:

- (1) "europæisk editionskendelse": en bindende afgørelse truffet af en udstedelsesmyndighed i en medlemsstat, der pålægger en tjenesteudbyder, der udbyder tjenester i Unionen og er etableret eller repræsenteret i en anden medlemsstat, at fremlægge elektronisk bevismateriale
- (2) "europæisk sikringskendelse": en bindende afgørelse truffet af en udstedelsesmyndighed i en medlemsstat, der pålægger en tjenesteudbyder, der udbyder tjenester i Unionen og er etableret eller repræsenteret i en anden medlemsstat, at bevare elektronisk bevismateriale med henblik på en efterfølgende anmodning om fremlæggelse af bevismaterialet
- (3) "tjenesteudbyder": enhver fysisk eller juridisk person, der udbyder en eller flere af følgende kategorier af tjenester:
 - (a) elektroniske kommunikationstjenester som defineret i artikel 2, stk. 4, i [direktivet om en europæisk kodeks for elektronisk kommunikation]
 - (b) informationssamfundets tjenester som defineret i artikel 1, stk. 1, litra b), i Europa-Parlamentets og Rådets direktiv (EU) 2015/1535⁴⁴, hvor lagring af data

⁴² Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger (EFT L 8 af 12.1.2001, s. 1).

⁴³ EUT C [...] af [...], s. [...].

er et afgørende element i den tjeneste, der leveres til brugeren, herunder sociale netværk, onlinemarkedspladser til fremme af transaktioner mellem deres brugere og andre udbydere af hostingtjenester

- (c) internetdomænenavne og IP-nummereringstjenester såsom udbydere af IP-adresser, domænenavneadministratorer, domænenavnregistratorer og hermed forbundne privatlivs- og proxytjenester
- (4) "der udbyder tjenester i Unionen":
 - (a) der giver juridiske eller fysiske personer i en eller flere medlemsstater mulighed for at anvende de tjenester, der er opstillet i stk. 3 ovenfor, og
 - (b) som har en væsentlig tilknytning til den eller de medlemsstater, der er nævnt i litra a)
- (5) "etablering": enten faktisk udøvelse af erhvervsvirksomhed i et ikke nærmere angivet tidsrum og ved hjælp af en fast infrastruktur, hvorfra aktiviteten med levering af tjenester rent faktisk udføres, eller en fast infrastruktur, hvorfra forretningen drives
- (6) "elektronisk bevismateriale": bevismateriale, der er lagret i elektronisk form af eller på vegne af en tjenesteudbyder på tidspunktet for modtagelsen af en attest for en sikrings- eller editionskendelse, og som omfatter lagrede abonnentdata, adgangsdata, transaktionsdata og indholdsdata
- (7) "abonnentdata": data vedrørende:
 - (a) en abonnents eller en kundes identitet såsom navn, fødselsdato, postadresse eller fysisk adresse, fakturerings- og betalingsoplysninger, telefon eller e-mail
 - (b) type tjeneste og dens varighed, herunder tekniske data og data til identifikation af tilknyttede tekniske foranstaltninger eller grænseflader, der anvendes af eller leveres til abonnenten eller kunden, og data vedrørende validering af brugen af tjenesten, bortset fra password eller andre autentifikationsmidler, der anvendes i stedet for et password, som leveres af en bruger eller oprettes efter anmodning fra en bruger
- (8) "adgangsdata": data vedrørende påbegyndelsen og afslutningen af en brugeradgangssession til en tjeneste, som er strengt nødvendige alene med det formål at identificere brugeren af tjenesten, f.eks. dato og tidspunkt for brug eller log-in og log-off sammen med den IP-adresse, som internetudbyderen tildeler brugeren af en tjeneste, data, der identificerer den anvendte grænseflade og bruger-ID. Dette omfatter elektroniske kommunikationsmetadata som defineret i artikel 4, stk. 3, litra g), i [forordning om respekt for privatliv og beskyttelse af personoplysninger i forbindelse med elektroniske kommunikation]
- (9) "transaktionsdata": data vedrørende leveringen af en tjeneste, der udbydes af en tjenesteudbyder, som tilvejebringer en kontekst eller yderligere oplysninger om en sådan tjeneste og er genereret eller behandlet af tjenesteudbyderens informationssystem, såsom afsender og modtager af en meddelelse eller en anden form for interaktion, data om enhedens placering, dato, tidspunkt, varighed, størrelse, routing, format, den anvendte protokol og kompressionstypen, medmindre sådanne

⁴⁴ Europa-Parlamentets og Rådets [direktiv \(EU\) 2015/1535](#) af 9. september 2015 om en informationsprocedure med hensyn til tekniske forskrifter samt forskrifter for informationssamfundets tjenester (EUT L 241 af 17.9.2015, s. 1).

oplysninger er adgangsdata. Dette omfatter elektroniske kommunikationsmetadata som defineret i artikel 4, stk. 3, litra g), i [forordning om respekt for privatliv og beskyttelse af personoplysninger i forbindelse med elektronisk kommunikation]

- (10) "indholdsdata": lagrede data i digitalt format såsom nedskrevne eller talte beskeder, videoer, billeder og lyd, bortset fra abonnent-, adgangs- eller transaktionsdata
- (11) "informationssystem": en tjeneste som defineret i artikel 2, litra a), i Europa-Parlamentets og Rådets direktiv 2013/40/EU⁴⁵
- (12) "udstedelsesstat": den medlemsstat, hvor den europæiske editionskendelse eller den europæiske sikringskendelse er udstedt
- (13) "fuldbyrdesstat": den medlemsstat, hvor modtageren af den europæiske editionskendelse eller den europæiske sikringskendelse er bosat eller etableret, og til hvilken den europæiske editionskendelse og attesten for den europæiske editionskendelse eller den europæiske sikringskendelse og attesten for den europæiske sikringskendelse fremsendes til fuldbyrdelse
- (14) "fuldbyrdesmyndighed": den kompetente myndighed i fuldbyrdesstaten til hvilken den europæiske editionskendelse og attesten for den europæiske editionskendelse eller den europæiske sikringskendelse og attesten for den europæiske sikringskendelse fremsendes af udstedelsesmyndigheden til fuldbyrdelse
- (15) "nødsituationer": situationer, hvor der er en overhængende fare for en persons liv eller fysiske integritet eller for kritisk infrastruktur som defineret i artikel 2, litra a), i Rådets direktiv 2008/114/EF⁴⁶.

Artikel 3 *Anvendelsesområde*

- 1. Denne forordning finder anvendelse på tjenesteudbydere, der udbyder tjenester i Unionen.
- 2. Den europæiske editionskendelse og den europæiske sikringskendelse kan kun udstedes i forbindelse med straffesager, både før og under retssagen. Kendelserne kan også udstedes i sager vedrørende en lovovertrædelse, som en juridisk person kan drages til ansvar eller straffes for i udstedelsesstaten.
- 3. De kendelser, der er omhandlet i denne forordning, må kun udstedes for data vedrørende tjenester som defineret i artikel 2, stk. 3, der udbydes i Unionen.

Kapitel 2: Europæisk editionskendelse, europæisk sikringskendelse og attester

Artikel 4 *Udstedelsesmyndighed*

- 1. En europæisk editionskendelse om abonnentdata og adgangsdata kan udstedes af:

⁴⁵ Europa-Parlamentets og Rådets [direktiv 2013/40/EU](#) af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA (EUT L 218 af 14.8.2013, s. 8).

⁴⁶ Rådets [direktiv 2008/114/EF](#) af 8. december 2008 om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre (EUT L 345 af 23.12.2008, s. 75).

- (a) en dommer, domstol, undersøgelsesdommer eller anklager, der er kompetent i den pågældende sag, eller
 - (b) enhver anden kompetent myndighed som defineret af udstedelsesstaten, der i den pågældende sag handler i sin egenskab af efterforskningsmyndighed i straffesager med kompetence til at indsamle bevismateriale i henhold til national ret. Denne europæiske editionskendelse godkendes efter en undersøgelse af dens overensstemmelse med betingelserne for udstedelse af en europæisk editionskendelse i henhold til denne forordning af en dommer, domstol, undersøgelsesdommer eller offentlig anklager i udstedelsesstaten.
2. En europæisk editionskendelse om transaktions- og indholdsdata kan kun udstedes af:
- (a) en dommer, domstol eller undersøgelsesdommer, der er kompetent i den pågældende sag, eller
 - (b) enhver anden kompetent myndighed som defineret af udstedelsesstaten, der i den pågældende sag handler i sin egenskab af efterforskningsmyndighed i straffesager med kompetence til at indsamle bevismateriale i henhold til national ret. Denne europæiske editionskendelse godkendes efter en undersøgelse af dens overensstemmelse med betingelserne for udstedelse af en europæisk editionskendelse i henhold til denne forordning af en dommer, domstol eller undersøgelsesdommer i udstedelsesstaten.
3. En europæisk sikringskendelse kan udstedes af:
- (a) en dommer, domstol, undersøgelsesdommer eller anklager, der er kompetent i den pågældende sag, eller
 - (b) enhver anden kompetent myndighed som defineret af udstedelsesstaten, der i den pågældende sag handler i sin egenskab af efterforskningsmyndighed i straffesager med kompetence til at indsamle bevismateriale i henhold til national ret. Denne europæisk sikringskendelse godkendes efter en undersøgelse af dens overensstemmelse med betingelserne for udstedelse af en europæisk sikringskendelse i henhold til denne forordning af en dommer, domstol, undersøgelsesdommer eller offentlig anklager i udstedelsesstaten.
4. Når kendelsen er blevet godkendt af en judiciel myndighed i henhold til stk. 1, litra b), stk. 2, litra b), og stk. 3, litra b), kan denne myndighed også betragtes som en udstedelsesmyndighed i forbindelse med fremsendelse af atesten for den europæiske editionskendelse og atesten for den europæiske sikringskendelse.

Artikel 5

Betingelser for udstedelse af en europæisk editionskendelse

- 1. En udstedelsesmyndighed kan kun udstede en europæisk editionskendelse, hvis betingelserne i denne artikel er opfyldt.
- 2. Den europæiske editionskendelse skal være nødvendig og stå i et rimeligt forhold til de i artikel 3, stk. 2, omhandlede formål med retssagen og kan kun udstedes, hvis en lignende foranstaltning er tilgængelig for samme lovovertrædelse i en sammenlignelig national situation i udstedelsesstaten.
- 3. Europæiske editionskendelser om fremlæggelse af abonnentdata eller adgangsdata kan udstedes for alle lovovertrædelser.

4. Europæiske editionskendelser om fremlæggelse af transaktionsdata eller indholdsdata kan kun udstedes for:
- (a) lovovertrædelser, der i udstedelsesstaten kan straffes med en frihedsstraf af en maksimal varighed på mindst tre år, eller
 - (b) for følgende lovovertrædelser, hvis de helt eller delvis er begået ved brug af et informationssystem:
 - lovovertrædelser som defineret i artikel 3, 4 og 5 i Rådets rammeafgørelse 2001/413/RIA⁴⁷
 - lovovertrædelser som defineret i artikel 3-7 i Europa-Parlamentets og Rådets direktiv 2011/93/EU⁴⁸
 - lovovertrædelser som defineret i artikel 3-8 i Europa-Parlamentets og Rådets direktiv 2013/40/EU
 - (c) lovovertrædelser som defineret i artikel 3-12 og 14 i Europa-Parlamentets og Rådets direktiv (EU) 2017/541⁴⁹.
5. Den europæiske editionskendelse skal indeholde følgende oplysninger:
- (a) udstedelsesmyndigheden og eventuelt godkendelsesmyndigheden
 - (b) modtageren af den europæiske editionskendelse som omhandlet i artikel 7
 - (c) de personer, hvis oplysninger efterspørges, undtagen hvis det eneste formål med kendelsen er at identificere en person
 - (d) den ønskede datakategori (abonnentdata, adgangsdata, transaktionsdata eller indholdsdata)
 - (e) hvis relevant, tidsintervallet for fremlæggelsen
 - (f) de gældende strafferetlige bestemmelser i udstedelsesstaten
 - (g) i nødsituationer eller i tilfælde af en anmodning om tidligere videregivelse, begrundelsen herfor
 - (h) hvis de oplysninger, der anmodes om, opbevares eller behandles som en del af en tjenesteudbyders infrastruktur, der stilles til rådighed for en virksomhed eller en anden enhed, der ikke er en fysisk person, en bekræftelse på, at kendelsen er udstedt i overensstemmelse med stk. 6
 - (i) begrundelsen for nødvendigheden og proportionaliteten af den pågældende foranstaltning.
6. Hvis de oplysninger, der anmodes om, opbevares eller behandles som en del af en tjenesteudbyders infrastruktur, der stilles til rådighed for en virksomhed eller en

⁴⁷ [Rådets rammeafgørelse 2001/413/RIA](#) af 28. maj 2001 om bekæmpelse af svig og forfalskning i forbindelse med andre betalingsmidler end kontanter (EFT L 149 af 2.6.2001, s. 1).

⁴⁸ Europa-Parlamentets og Rådets [direktiv 2011/93/EU](#) af 13. december 2011 om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og børnepornografi og om erstatning af Rådets rammeafgørelse 2004/68/RIA (EUT L 335 af 17.12.2011, s. 1).

⁴⁹ Europa-Parlamentets og Rådets [direktiv \(EU\) 2017/541](#) af 15. marts 2017 om bekæmpelse af terrorisme og om erstatning af Rådets rammeafgørelse 2002/475/RIA og ændring af Rådets afgørelse 2005/671/RIA (EUT L 88 af 31.3.2017, s. 6).

anden enhed, der ikke er en fysisk person, kan den europæiske editionskendelse udelukkende rettes til tjenesteudbyderen, hvis det ikke er hensigtsmæssigt at træffe efterforskningsforanstaltninger over for den pågældende virksomhed eller enhed, navnlig fordi de kan bringe efterforskningen i fare.

7. Hvis udstedelsesmyndigheden har grund til at antage, at transaktions- eller indholdsdata er beskyttet af immuniteter og privilegier i henhold til lovgivningen i den medlemsstat, hvor tjenesteudbyderen er etableret, eller hvis videregivelsen heraf kan berøre den pågældende medlemsstats grundlæggende interesser såsom statens sikkerhed og forsvar, skal udstedelsesmyndigheden anmode om yderligere oplysninger inden udstedelsen af den europæiske editionskendelse, herunder ved høring af de kompetente myndigheder i den pågældende medlemsstat, enten direkte eller via Eurojust eller det europæiske retlige netværk. Hvis udstedelsesmyndigheden finder, at de ønskede adgangs-, transaktions- eller indholdsdata er beskyttet af sådanne immuniteter eller privilegier eller videregivelsen heraf vil berøre en anden medlemsstats grundlæggende interesser, udsteder den ikke den europæiske editionskendelse.

Artikel 6

Betingelser for udstedelse af en europæisk sikringskendelse

1. En udstedelsesmyndighed kan kun udstede en europæisk sikringskendelse, hvis betingelserne i denne artikel er opfyldt.
2. Den kan udstedes, hvis dette er nødvendigt og forholdsmæssigt for at forhindre fjernelse, sletning eller ændring af relevante oplysninger med henblik på en efterfølgende anmodning om fremlæggelse af disse oplysninger via gensidig retlig bistand, en europæisk efterforskningskendelse eller en europæisk editionskendelse. Europæiske sikringskendelser om sikring af data kan udstedes for alle lovovertrædelser.
3. Den europæiske sikringskendelse skal indeholde følgende oplysninger:
 - (a) udstedelsesmyndigheden og eventuelt godkendelsesmyndigheden
 - (b) modtageren af den europæiske sikringskendelse som omhandlet i artikel 7
 - (c) de personer, hvis oplysninger bevares, undtagen hvis det eneste formål med kendelsen er at identificere en person
 - (d) den datakategori, der skal bevares (abonntdata, adgangsdata, transaktionsdata eller indholdsdata)
 - (e) hvis relevant, det tidsinterval, inden for hvilket oplysningerne skal bevares
 - (f) de gældende strafferetlige bestemmelser i udstedelsesstaten
 - (g) begrundelsen for nødvendigheden og proportionaliteten af den pågældende foranstaltning.

Artikel 7

Modtageren af en europæisk editionskendelse og en europæisk sikringskendelse

1. Den europæiske editionskendelse og den europæiske sikringskendelse rettes direkte til en retlig repræsentant, der er udpeget tjenesteudbyderen med henblik på at indsamle bevismateriale i straffesager.
2. Hvis der ikke er udpeget en særlig retlig repræsentant, kan den europæiske editionskendelse og den europæiske sikringskendelse rettes til ethvert af tjenesteudbyderens etableringssteder i Unionen.
3. Hvis den retlige repræsentant ikke overholder en EPOC i nødsituationer i henhold til artikel 9, stk. 2, kan EPOC'en rettes til ethvert af tjenesteudbyderens etableringssteder i Unionen.
4. Hvis den retlige repræsentant ikke overholder sine forpligtelser i henhold til stk. 9 eller 10, og udstedelsesmyndigheden skønner, at der er en alvorlig risiko for tab af data, kan den europæiske editionskendelse eller den europæiske sikringskendelse rettes til ethvert af tjenesteudbyderens etableringssteder i Unionen.

Artikel 8

Attest for en europæisk editions- og sikringskendelse

1. En europæisk editions- eller sikringskendelse fremsendes til modtageren som defineret i artikel 7 i form af en attest for den europæiske editionskendelse (EPOC) eller en attest for den europæiske sikringskendelse (EPOC-PR).

Udstedelses- eller godkendelsesmyndigheden udfylder EPOC'en i bilag I eller EPOC-PR'en i bilag II, underskriver den og bekræfter indholdets nøjagtighed og rigtighed.

2. EPOC'en eller EPOC-PR'en fremsendes direkte ved hjælp af ethvert middel, som kan efterlade et skriftligt spor, og som giver modtageren mulighed for at fastslå dens ægthed.

Hvis tjenesteudbyderne, medlemsstaterne eller EU-organerne har etableret særlige platforme eller andre sikre kanaler til håndtering af anmodninger om oplysninger mellem de retshåndhævende og judicielle myndigheder, kan udstedelsesmyndigheden også vælge at fremsende attesten via disse kanaler.

3. EPOC'en skal indeholde de oplysninger, der er anført i artikel 5, stk. 5, litra a)-h), herunder fyldestgørende oplysninger, der gør det muligt for modtageren at identificere og rette henvendelse til udstedelsesmyndigheden. Begrundelsen for nødvendigheden og proportionaliteten af den pågældende foranstaltning eller yderligere oplysninger om efterforskninger medtages ikke.
4. EPOC-PR'en skal indeholde de oplysninger, der er anført i artikel 6, stk. 3, litra a)-f), herunder fyldestgørende oplysninger, der gør det muligt for modtageren at identificere og rette henvendelse til udstedelsesmyndigheden. Begrundelsen for nødvendigheden og proportionaliteten af den pågældende foranstaltning eller yderligere oplysninger om efterforskninger medtages ikke.
5. Hvis det er nødvendigt, oversættes EPOC'en eller EPOC-PR'en til et officielt EU-sprog, der accepteres af modtageren. Hvis der ikke er angivet et sprog, oversættes EPOC-PR'en eller EPOC'en til et af de officielle sprog i den medlemsstat, hvor den retlige repræsentant er bosiddende eller etableret.

Artikel 9
Gennemførelse af en EPOC

1. Efter modtagelsen af EPOC'en sikrer modtageren, at de oplysninger, der anmodes om, fremsendes direkte til den udstedelsesmyndighed eller fuldbyrdelsesmyndighed, der er anført i EPOC'en, senest 10 dage efter modtagelse af EPOC'en, medmindre udstedelsesmyndigheden begrundet en tidligere videregivelse.
2. I nødsituationer fremsender modtageren de anmodede oplysninger uden unødigt forsinkelse senest seks timer efter modtagelse af EPOC'en.
3. Hvis modtageren ikke kan opfylde sine forpligtelser, fordi EPOC'en er ufuldstændig, indeholder åbenbare fejl eller ikke indeholder tilstrækkelige oplysninger til at gennemføre EPOC'en, underretter modtageren uden unødigt forsinkelse den udstedelsesmyndighed, der er anført i EPOC'en, og anmoder om en nærmere forklaring ved brug af formularen i bilag III. Modtageren meddeler udstedelsesmyndigheden, om det var muligt at identificere og bevare oplysningerne om fastsat i stk. 6. Udstedelsesmyndigheden skal svare hurtigst muligt og senest inden for fem dage. De frister, der er fastsat i stk. 1 og 2, finder først anvendelse ved modtagelsen af den nærmere forklaring.
4. Hvis modtageren ikke kan opfylde sine forpligtelser på grund af force majeure, eller da det de facto er umuligt, uden at dette kan tilskrives modtageren eller – hvis denne er en anden – tjenesteudbyderen, navnlig fordi den person, hvis oplysninger efterspørges, ikke er dennes kunde, eller hvis oplysningerne er blevet slettet inden modtagelsen af EPOC'en, underretter modtageren uden unødigt forsinkelse den udstedelsesmyndighed, der er anført i EPOC'en, og redegør for grundene hertil ved brug af formularen i bilag III. Hvis de relevante betingelser er opfyldt, trækker udstedelsesmyndigheden EPOC'en tilbage.
5. Hvis modtageren ikke fremlægger de anmodede oplysninger, ikke fremlægger fyldestgørende oplysninger eller ikke fremlægger dem inden for den fastsatte frist af andre grunde, skal modtageren altid uden unødigt forsinkelse og senest inden for den frist, der er fastsat i stk. 1 og 2, underrette udstedelsesmyndigheden og redegøre for grundene hertil ved brug af formularen i bilag III. Udstedelsesmyndigheden kontrollerer kendelsen på grundlag af de oplysninger, som tjenesteudbyderen har fremlagt, og fastsætter om nødvendigt en ny frist for tjenesteudbyderens fremlæggelse af de pågældende oplysninger.

Hvis modtageren ikke mener, at EPOC'en kan gennemføres, da det alene ud fra oplysningerne i EPOC'en fremgår, at den tydeligvis er i modstrid med Den Europæiske Unions charter om grundlæggende rettigheder, eller at den er åbenbart urimelig, sender modtageren ligeledes formularen i bilag III til den kompetente fuldbyrdelsesmyndighed i modtagerens medlemsstat. I sådanne tilfælde kan den kompetente fuldbyrdelsesmyndighed anmode udstedelsesmyndigheden om at redegøre nærmere for den europæiske editionskendelse, enten direkte eller via Eurojust eller det europæiske retlige netværk.
6. Modtageren bevarer de anmodede oplysninger, hvis de ikke fremlægges straks, medmindre oplysningerne i EPOC'en ikke gør det muligt at identificere de anmodede oplysninger, i hvilket tilfælde modtageren anmoder om en nærmere forklaring i overensstemmelse med stk. 3. Oplysningerne bevares, indtil de er fremlagt, uanset om det er på grundlag af den afklarede europæiske editionskendelse og attesten eller gennem andre kanaler såsom gensidig retshjælp. Hvis det ikke længere er nødvendigt

at fremlægge og bevare oplysninger, underretter udstedelsesmyndigheden og, hvor det er relevant i henhold til artikel 14, stk. 8, fuldbyrdelsesmyndigheden, uden unødigt forsinkelse modtageren herom.

Artikel 10 *Gennemførelse af en EPOC-PR*

1. Efter modtagelsen af EPOC-PR'en bevarer modtageren uden unødigt forsinkelse de anmodede oplysninger. Sikringen ophører efter 60 dage, medmindre udstedelsesmyndigheden bekræfter, at proceduren for den efterfølgende anmodning om fremlæggelse af oplysninger er blevet indledt.
2. Hvis udstedelsesmyndigheden inden for den frist, der er fastsat i stk. 1, bekræfter indledningen af proceduren for den efterfølgende anmodning om fremlæggelse af oplysninger, bevarer modtageren oplysningerne, så længe det er nødvendigt for at fremlægge oplysningerne efter modtagelsen af den efterfølgende anmodning om fremlæggelse.
3. Hvis sikringen ikke længere er nødvendig, underretter udstedelsesmyndigheden uden unødigt forsinkelse modtageren herom.
4. Hvis modtageren ikke kan opfylde sine forpligtelser, fordi attesten er ufuldstændig, indeholder åbenbare fejl eller ikke indeholder tilstrækkelige oplysninger til at gennemføre EPOC-PR'en, underretter modtageren uden unødigt forsinkelse den udstedelsesmyndighed, der er anført i EPOC-PR'en, og anmoder om en nærmere forklaring ved brug af formularen i bilag III. Udstedelsesmyndigheden skal svare hurtigst muligt og senest inden for fem dage. Modtageren sikrer, at den nødvendige nærmere forklaring kan modtages, således at modtageren kan opfylde de forpligtelser, der er fastsat i stk. 1.
5. Hvis modtageren ikke kan opfylde sine forpligtelser på grund af force majeure, eller da det de facto er umuligt, uden at dette kan tilskrives modtageren eller – hvis denne er en anden – tjenesteudbyderen, navnlig fordi den person, hvis oplysninger efterspørges, ikke er dennes kunde, eller hvis oplysningerne er blevet slettet inden modtagelsen af kendelsen, kontakter modtageren uden unødigt forsinkelse den udstedelsesmyndighed, der er anført i EPOC-PR'en, og redegør for grundene hertil ved brug af formularen i bilag III. Hvis disse betingelser er opfyldt, trækker udstedelsesmyndigheden EPOC-PR'en tilbage.
6. Hvis modtageren ikke bevarer de anmodede oplysninger af andre grunde som anført i formularen i bilag III, skal modtageren altid uden unødigt forsinkelse underrette udstedelsesmyndigheden og redegøre for grundene hertil ved brug af formularen i bilag III. Udstedelsesmyndigheden kontrollerer kendelsen på grundlag af tjenesteudbyderens begrundelse.

Artikel 11 *Fortrolighed og brugeroplysninger*

1. Modtagen eller – hvis denne er en anden – tjenesteudbyderen træffer de nødvendige foranstaltninger for at sikre fortroligheden af EPOC'en eller EPOC-PR'en og af de fremlagte eller bevarede oplysninger, og hvis udstedelsesmyndigheden anmoder derom, må modtageren ikke underrette den person, hvis oplysninger efterspørges, for at undgå at lægge hindringer i vejen for den pågældende straffesag.

2. Hvis udstedelsesmyndigheden har anmodet modtageren om ikke at underrette den person, hvis oplysninger efterspørges, underretter udstedelsesmyndigheden uden unødigt forsinkelse den person, hvis oplysninger efterspørges i EPOC'en, om fremlæggelsen af oplysninger. Fremlæggelsen af disse oplysninger kan udsættes, så længe det er nødvendigt og forholdsmæssigt for at undgå at lægge hindringer i vejen for den pågældende straffesag.
3. I forbindelse med underretningen informerer udstedelsesmyndigheden modtageren om tilgængelige retsmidler som omhandlet i artikel 17.

Artikel 12

Godtgørelse af udgifter

Tjenesteudbyderen kan kræve, at udstedelsesstaten godtgør udbyderens udgifter, hvis dette er fastsat i national lovgivning i udstedelsesstaten for nationale kendelser i lignende situationer, i overensstemmelse med disse nationale bestemmelser.

Kapitel 3: Sanktioner og fuldbyrdelse

Artikel 13

Sanktioner

Med forbehold af nationale love om pålæggelse af strafferetlige sanktioner fastsætter medlemsstaterne reglerne vedrørende økonomiske sanktioner for overtrædelse af forpligtelserne i henhold til artikel 9, 10 og 11 i denne forordning og træffer alle nødvendige foranstaltninger til at sikre, at de gennemføres. De fastsatte økonomiske sanktioner skal være effektive, stå i et rimeligt forhold til overtrædelsen og have en afskrækkende virkning. Medlemsstaterne giver straks Kommissionen meddelelse om disse regler og foranstaltninger og underretter den straks om senere ændringer, der berører dem.

Artikel 14

Fuldbyrdsprocedure

1. Hvis modtageren ikke fuldbyrder en EPOC inden for fristen eller en EPOC-PR uden at give en begrundelse, der godtages af udstedelsesmyndigheden, kan udstedelsesmyndigheden videresende den europæiske editionskendelse med EPOC'en eller den europæiske sikringskendelse med EPOC-PR'en samt formularen i bilag III udfyldt af modtageren og ethvert andet relevant dokument til den kompetente myndighed i fuldbyrdsstaten med henblik på fuldbyrdelse ved hjælp af ethvert middel, som kan efterlade et skriftligt spor, og som giver fuldbyrdsmyndigheden mulighed for at fastslå ægtheden. Udstedelsesmyndigheden oversætter i denne forbindelse kendelsen, formularen og eventuelle andre ledsagende dokumenter til et af de officielle sprog i denne medlemsstat og underretter modtageren om videresendelsen.
2. Efter modtagelsen anerkender fuldbyrdsmyndigheden uden yderligere formaliteter en europæisk editionskendelse eller europæisk sikringskendelse, der er videresendt i henhold til stk. 1, og træffer de nødvendige foranstaltninger med henblik på dens fuldbyrdelse, medmindre fuldbyrdsmyndigheden mener, at en af de grunde, der er omhandlet i stk. 4 eller 5, finder anvendelse, at de pågældende oplysninger er beskyttet af en immunitet eller et privilegium i henhold til national lovgivning, eller at videregivelsen kan berøre nationale grundlæggende interesser

såsom statens sikkerhed og forsvar. Fuldbyrldelsesmyndigheden træffer beslutning om at anerkende kendelsen uden unødigt forsinkelse og senest fem arbejdsdage efter modtagelsen af kendelsen.

3. Hvis fuldbyrldelsesmyndigheden anerkender kendelsen, anmoder den formelt modtageren om at opfylde den relevante forpligtelse og oplyser modtageren om muligheden for at gøre indsigelse mod fuldbyrldelsen under påberåbelse af de grunde, der er nævnt i stk. 4 og 5, samt om de gældende sanktioner for manglende overholdelse og fastsætter en frist for overholdelse eller indsigelse.
4. Modtageren kan kun gøre indsigelse mod fuldbyrldelsen af den europæiske editionskendelse af følgende grunde:
 - (a) den europæiske editionskendelse er ikke blevet udstedt eller godkendt af en udstedelsesmyndighed, jf. artikel 4
 - (b) den europæiske editionskendelse er ikke blevet udstedt for en lovovertrædelse som omhandlet i artikel 5, stk. 4
 - (c) modtageren kunne ikke gennemføre EPOC'en, da det de facto er umuligt, på grund af force majeure, eller fordi EPOC'en indeholder åbenbare fejl.
 - (d) den europæiske editionskendelse vedrører ikke oplysninger, der lagres af eller på vegne af tjenesteudbyderen på tidspunktet for modtagelsen af EPOC'en
 - (e) tjenesten er ikke omfattet af denne forordning
 - (f) det fremgår alene ud fra oplysningerne i EPOC'en, at den tydeligvis er i modstrid med chartret eller er åbenbart urimelig.
5. Modtageren kan kun gøre indsigelse mod fuldbyrldelsen af den europæiske sikringskendelse af følgende grunde:
 - (a) den europæiske sikringskendelse er ikke blevet udstedt eller godkendt af en udstedelsesmyndighed som omhandlet i artikel 4
 - (b) tjenesteudbyderen kunne ikke gennemføre EPOC-PR'en, da det de facto er umuligt, på grund af force majeure, eller fordi EPOC-PR'en indeholder åbenbare fejl
 - (c) den europæiske sikringskendelse vedrører ikke oplysninger, der lagres af eller på vegne af tjenesteudbyderen på tidspunktet for modtagelsen af EPOC-PR'en
 - (d) tjenesten er ikke omfattet af anvendelsesområdet for nærværende forordning
 - (e) det fremgår alene ud fra oplysningerne i EPOC-PR'en, at EPOC-PR'en tydeligvis er i modstrid med chartret eller er åbenbart urimelig
6. Hvis modtageren gør indsigelse, træffer fuldbyrldelsesmyndigheden afgørelse om fuldbyrldelsen af kendelsen på grundlag af oplysningerne fra modtageren og, om nødvendigt, supplerende oplysninger fra udstedelsesmyndigheden i overensstemmelse med stk. 7.
7. Inden fuldbyrldelsesmyndigheden beslutter ikke at anerkende eller fuldbyrde kendelsen i henhold til stk. 2 og 6, hører den udstedelsesmyndigheden med alle passende midler. Hvis det er hensigtsmæssigt, anmoder den udstedelsesmyndigheden om supplerende oplysninger. Udstedelsesmyndigheden besvarer sådanne anmodninger inden for fem arbejdsdage.

8. Udstedelsesmyndigheden og modtageren underrettes straks om alle afgørelser ved hjælp af ethvert middel, som kan efterlade et skriftligt spor.
9. Hvis fuldbyrdelsesmyndigheden modtager oplysninger fra modtageren, fremsender den disse til udstedelsesmyndigheden senest inden for to arbejdsdage, medmindre de pågældende oplysninger er beskyttet af en immunitet eller et privilegium i henhold til national lovgivning, eller videregivelsen kan berøre nationale grundlæggende interesser såsom statens sikkerhed og forsvar. I så fald oplyser myndigheden udstedelsesmyndigheden om begrundelsen for ikke at videregive oplysningerne.
10. Hvis modtageren ikke opfylder sine forpligtelser i henhold til en anerkendt kendelse, hvis eksigibilitet er blevet bekræftet af fuldbyrdelsesmyndigheden, pålægger denne myndighed en økonomisk sanktion i overensstemmelse med national lovgivning. Der er adgang til effektive retsmidler til prøvelse af en afgørelse om bødepålæg.

Kapitel 4: Retsmidler

Artikel 15

Prøvelsesprocedure i tilfælde af modstridende forpligtelser begrundet i grundlæggende rettigheder eller grundlæggende interesser i et tredjeland

1. Hvis modtageren mener, at overholdelsen af den europæiske editionskendelse vil være i strid med gældende lovgivning i et tredjeland, som forbyder videregivelse af de pågældende oplysninger med den begrundelse, at det er nødvendigt for at beskytte de berørte personers grundlæggende rettigheder eller tredjelandets grundlæggende rettigheder forbundet med statens sikkerhed eller forsvar, underretter modtageren udstedelsesmyndigheden om sin begrundelse for ikke at gennemføre den europæiske editionskendelse i overensstemmelse med den procedure, der er omhandlet i artikel 9, stk. 5.
2. Den begrundede indsigelse skal indeholde alle relevante oplysninger om det pågældende tredjelandets lovgivning, om dens anvendelse i den foreliggende sag, og om karakteren af den modstridende forpligtelse. Den kan ikke være baseret på det forhold, at der ikke findes tilsvarende bestemmelser vedrørende betingelserne, formaliteterne og procedurerne for udstedelse af en editionskendelse i den gældende lovgivning i det pågældende tredjeland, eller alene på det forhold, som dataene er lagret i et tredjeland.
3. Udstedelsesmyndigheden kontrollerer den europæiske editionskendelse på baggrund af den begrundede indsigelse. Hvis udstedelsesmyndigheden agter at opretholde den europæiske editionskendelse, begærer den domstolsprøvelse ved den kompetente ret i sin medlemsstat. Gennemførelsen af kendelsen suspenderes, indtil prøvelsesproceduren er afsluttet.

Den kompetente ret vurderer først, hvorvidt der foreligger en konflikt, på grundlag af en undersøgelse af:

 - (a) om tredjelandets lovgivning finder anvendelse på de særlige omstændigheder i den pågældende sag, og i så fald
 - (b) om tredjelandets lovgivning anvendt på de særlige omstændigheder i den foreliggende sag forbyder videregivelse af de pågældende oplysninger.
4. I forbindelse med denne vurdering bør retten tage højde for, om tredjelandets lovgivning i stedet for at beskytte tredjelandets grundlæggende rettigheder eller grundlæggende interesser forbundet med statens sikkerhed eller forsvar åbenlyst har

til formål at beskytte andre interesser eller ulovlige aktiviteter mod anmodninger fra de retshåndhævende myndigheder i forbindelse med strafferetlige efterforskninger.

5. Hvis den kompetente ret finder, at der ikke er nogen relevant konflikt som omhandlet i stk. 1 og 4, stadfæster den kendelsen. Hvis den kompetente ret fastslår, at der er en relevant konflikt som omhandlet i stk. 1 og 4, videregiver den kompetente ret via sin nationale centrale myndighed alle relevante faktiske og retlige oplysninger om sagen, herunder sin vurdering, til de centrale myndigheder i det pågældende tredjeland, med en svarfrist på 15 dage. Fristen kan forlænges med 30 dage, hvis tredjelandets centrale myndighed indgiver en begrundet anmodning.
6. Hvis tredjelandets centrale myndighed inden for den fastsatte frist meddeler den kompetente ret, at den gør indsigelse mod gennemførelsen af den europæiske editionskendelse i dette tilfælde, ophæver den kompetente ret kendelsen og underretter udstedelsesmyndigheden og modtageren herom. Hvis der ikke gøres indsigelse inden for den (udvidede) frist, fremsender den kompetente ret en påmindelse og giver tredjelandets centrale myndighed yderligere fem dage til at svare og informerer myndigheden om konsekvenserne af at undlade at svare. Hvis der ikke gøres indsigelse inden for denne yderligere frist, stadfæster den kompetente ret kendelsen.
7. Hvis den kompetente ret beslutter at stadfæste kendelsen, underretter den udstedelsesmyndigheden og modtageren, der skal fortsætte gennemførelsen af kendelsen.

Artikel 16

Prøvelsesprocedure i tilfælde af modstridende forpligtelser af andre grunde

1. Hvis modtageren mener, at overholdelsen af den europæiske editionskendelse vil være i strid med gældende lovgivning i et tredjeland, som forbyder videregivelse af de pågældende oplysninger af andre grunde end dem, der er nævnt i artikel 15, underretter modtageren udstedelsesmyndigheden om sin begrundelse for ikke at gennemføre den europæiske editionskendelse i overensstemmelse med den procedure, der er omhandlet i artikel 9, stk. 5.
2. Den begrundede indsigelse skal indeholde alle relevante oplysninger om det pågældende tredjlands lovgivning, om dens anvendelse i den foreliggende sag, og om karakteren af den modstridende forpligtelse. Den kan ikke være baseret på det forhold, at der ikke findes tilsvarende bestemmelser vedrørende betingelserne, formaliteterne og procedurerne for udstedelse af en editionskendelse i den gældende lovgivning i det pågældende tredjeland, eller alene på det forhold, som dataene er lagret i et tredjeland.
3. Udstedelsesmyndigheden kontrollerer den europæiske editionskendelse på baggrund af den begrundede indsigelse. Hvis udstedelsesmyndigheden agter at opretholde den europæiske editionskendelse, begærer den domstolsprøvelse ved den kompetente ret i sin medlemsstat. Gennemførelsen af kendelsen suspenderes, indtil prøvelsesproceduren er afsluttet.
4. Den kompetente ret vurderer først, hvorvidt der foreligger en konflikt, på grundlag af en undersøgelse af:
 - (a) om tredjelandets lovgivning finder anvendelse på de særlige omstændigheder i den pågældende sag, og i så fald

- (b) om tredjelandets lovgivning anvendt på de særlige omstændigheder i den foreliggende sag forbyder videregivelse af de pågældende oplysninger.
5. Hvis den kompetente ret finder, at der ikke er nogen relevant konflikt som omhandlet i stk. 1 og 4, stadfæster den kendelsen. Hvis den kompetente ret fastslår, at tredjelandets lovgivning anvendt på de særlige omstændigheder i den foreliggende sag forbyder videregivelse af de pågældende oplysninger, afgør den kompetente ret, om kendelsen skal stadfæstes eller ophæves, navnlig på grundlag af følgende faktorer:
- (a) den interesse, der er beskyttet af tredjelandets relevante lovgivning, herunder tredjelandes interesse i at forhindre videregivelse af oplysningerne
- (b) graden af tilknytning af den straffesag, i forbindelse med hvilken kendelsen er udstedt, til de to jurisdiktioner, bl.a. på grundlag af:
- beliggenhed, nationalitet og bopæl for den person, hvis oplysninger efterspørges, og/eller for ofret/ofrene
- det sted, hvor den pågældende lovovertrædelse blev begået
- (c) graden af tilknytning mellem tjenesteudbyderen og det pågældende tredjeland, og i denne forbindelse er det sted, hvor oplysningerne er lagret, ikke i sig selv tilstrækkeligt til at fastslå, at der er en væsentlig tilknytning
- (d) efterforskningsstatens interesse i fremskaffelsen af det pågældende bevismateriale ud fra, hvor alvorlig lovovertrædelsen er, og hvor vigtigt det er at fremskaffe bevismaterialet hurtigt
- (e) eventuelle konsekvenser for modtageren eller tjenesteudbyderen af efterlevelsen af den europæiske editionskendelse, herunder eventuelle sanktioner.
6. Hvis den kompetente ret beslutter at ophæve kendelse, underretter den udstedelsesmyndigheden og modtageren herom. Hvis den kompetente ret beslutter at stadfæste kendelsen, underretter den udstedelsesmyndigheden og modtageren, der skal fortsætte gennemførelsen af kendelsen.

Artikel 17 *Effektive retsmidler*

1. Mistænkte og tiltalte, hvis oplysninger er indsamlet gennem en europæisk editionskendelse, har adgang til effektive retsmidler mod den europæiske editionskendelse under den straffesag, i forbindelse med hvilken kendelsen er udstedt, uden at dette berører de retsmidler, der er til rådighed i henhold til direktiv (EU) 2016/680 og forordning (EU) 2016/679.
2. Hvis den person, hvis oplysninger er indsamlet, ikke er mistænkt eller tiltalt i en straffesag, i forbindelse med hvilken kendelsen er udstedt, har den pågældende adgang til effektive retsmidler mod en europæisk editionskendelse i udstedelsesstaten, uden at dette berører de retsmidler, der er til rådighed i henhold til direktiv (EU) 2016/680 og forordning (EU) 2016/679.
3. Denne adgang til effektive retsmidler udøves af en judiciel myndighed i udstedelsesstaten i overensstemmelse med dens nationale lovgivning og omfatter muligheden for at anfægte foranstaltningens lovlighed, herunder dens nødvendighed og proportionalitet.

4. Med forbehold af artikel 11 træffer udstedelsesmyndigheden passende foranstaltninger til at sikre, at der oplyses om mulighederne i national lovgivning for at få adgang til retsmidler, og sikre, at de kan udøves effektivt.
5. De samme tidsfrister og andre betingelser for adgang til retsmidler i lignende nationale sager finder anvendelse her, og således at det sikres, at de pågældende personer kan anvende disse retsmidler effektivt.
6. Uden at dette berører nationale procedureregler sikrer medlemsstaterne, at retten til et forsvar og en retfærdig behandling af sagen respekteres i straffesager i udstedelsesstaten i forbindelse med vurderingen af det bevismateriale, der er fremskaffet gennem den europæiske editionskendelse.

Artikel 18

Sikring af privilegier og immuniteter i henhold til fuldbyrdesstatens lovgivning

Hvis transaktions- eller indholdsdata fremskaffet gennem den europæiske editionskendelse er beskyttet af immuniteter eller privilegier i henhold til lovgivningen i modtagerens medlemsstat eller berører den pågældende medlemsstats grundlæggende interesser såsom statens sikkerhed og forsvar, sikrer retten i udstedelsesstaten under den straffesag, i forbindelse med hvilken kendelsen er udstedt, at disse grunde tages i betragtning på samme måde, som hvis de var omfattet af national lovgivning, ved vurderingen relevansen og antageligheden af det omhandlede bevismateriale. Retten kan høre myndighederne i den relevante medlemsstat, det europæiske strafferetlige netværk eller Eurojust.

Kapitel 5: Afsluttende bestemmelser

Artikel 19

Overvågning og rapportering

1. Senest den [datoen for denne forordnings anvendelse] fastlægger Kommissionen et detaljeret program for overvågning af forordningens resultater og virkninger. I overvågningsprogrammet fastlægges metoderne til samt intervallerne for indsamling af oplysninger og anden nødvendig dokumentation. Det præciserer, hvilke foranstaltninger Kommissionen og medlemsstaterne skal træffe med hensyn til indsamling og analyse af oplysningerne og den øvrige dokumentation.
2. Medlemsstaterne indsamler og vedligeholder under alle omstændigheder samlede statistikker fra de relevante myndigheder. De indsamlede oplysninger fremsendes til Kommissionen senest den 31. marts hvert år for det foregående kalenderår og skal omfatte:
 - (a) antallet af EPOC'er og EPOC-PR'er udstedt pr. type oplysninger, der anmodes om, berørte tjenesteudbydere og situationen (nødsituation eller ej)
 - (b) antallet af efterlevede eller ikkeefterlevede EPOC'er og EPOC-PR'er udstedt pr. type oplysninger, der anmodes om, berørte tjenesteudbydere og situationen (nødsituation eller ej)
 - (c) for efterlevede EPOC'er – den gennemsnitlige varighed for tilvejebringelsen af de anmodede oplysninger fra tidspunktet for udstedelse af EPOC'en til tidspunktet for tilvejebringelse, pr. type oplysninger, der anmodes om, berørte tjenesteudbydere og situationen (nødsituation eller ej)

- (d) antallet af europæiske editionskendelser fremsendt eller modtaget med henblik på fuldbyrdelse til en fuldbyrdesstat pr. type oplysninger, der anmodes om, berørte tjenesteudbydere og situationen (nødsituation eller ej) og antallet af efterlevede kendelser
- (e) antallet af retsmidler mod europæiske editionskendelser i udstedelsesstaten og i fuldbyrdesstaten pr. type oplysninger, der anmodes om.

Artikel 20

Ændringer af attesterne og formularerne

Kommissionen vedtager delegerede retsakter i overensstemmelse med artikel 21 med henblik på at ændre bilag I, II og III for effektivt at imødegå et eventuelt behov for forbedringer af indholdet af EPOC- og EPOC-PR-formularerne og af de formularer, der skal anvendes til at oplyse om, hvorfor det ikke er muligt at gennemføre EPOC'en eller EPOC-PR'en.

Artikel 21

Udøvelse af delegerede beføjelser

1. Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastlagte betingelser.
2. Den delegation af beføjelser, der er omhandlet i artikel 20, indrømmes på ubestemt tid fra den *[datoen for denne forordnings anvendelse]*.
3. Den i artikel 20 omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i *Den Europæiske Unions Tidende* eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.
4. Inden vedtagelsen af en delegeret retsakt hører Kommissionen eksperter, som er udpeget af hver enkelt medlemsstat, i overensstemmelse med principperne i den interinstitutionelle aftale om bedre lovgivning af 13. april 2016⁵⁰.
5. Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidigt Europa-Parlamentet og Rådet meddelelse herom.
6. En delegeret retsakt vedtaget i henhold til artikel 20 træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på to måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har underrettet Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med to måneder på Europa-Parlamentets eller Rådets initiativ.

Artikel 22

Meddelelser

1. Senest den *[datoen for denne forordnings anvendelse]* giver hver medlemsstat Kommissionen oplysninger om følgende:

⁵⁰ EUT L 123 af 12.5. 2016, s. 13.

- (a) de myndigheder, der i overensstemmelse med national ret er kompetente i henhold til artikel 4 til at udstede og/eller godkende europæiske editionskendelser og europæiske sikringskendelser
 - (b) den eller de fuldbyrdelsesmyndigheder, der er kompetente til at fuldbyrde europæiske editionskendelser og europæiske sikringskendelser på en anden medlemsstats vegne
 - (c) de retter, der er kompetente til at behandle begrundede indsigelser fra modtagerne i overensstemmelse med artikel 15 og 16.
2. Kommissionen stiller de i henhold til denne artikel modtagne oplysninger til rådighed for offentligheden, enten på et særligt websted eller på webstedet for det europæiske retlige netværk, der er nævnt i artikel 9 i Rådets afgørelse 2008/976/RIA⁵¹.

Artikel 23

Forbindelsen til europæiske efterforskningskendelser

Medlemsstaternes myndigheder kan fortsat udstede europæiske efterforskningskendelser i overensstemmelse med direktiv 2014/41/EU i forbindelse med indsamling af bevismateriale, der også er omfattet af denne forordnings anvendelsesområde.

Artikel 24

Vurdering

Senest den [*fem år efter datoen denne forordnings anvendelse*] foretager Kommissionen en evaluering af forordningen og forelægger en rapport for Europa-Parlamentet og Rådet om denne forordnings virkemåde, herunder en vurdering af behovet for at udvide dens anvendelsesområde. Om nødvendigt ledsages rapporten af forslag til retsakter. Evalueringen foretages i overensstemmelse med Kommissionens retningslinjer for bedre lovgivning. Medlemsstaterne giver Kommissionen alle de oplysninger, der er nødvendige for udarbejdelsen af denne rapport.

Artikel 25

Ikrafttræden

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Den anvendes fra den [seks måneder efter ikrafttrædelsen].

⁵¹ Rådets afgørelse 2008/976/RIA af 16. december 2008 om det europæiske retlige netværk (EUT L 348 af 24.12.2008, s. 130).

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i medlemsstaterne i overensstemmelse med traktaterne.

Udfærdiget i Bruxelles, den .

På Europa-Parlamentets vegne
Formand

På Rådets vegne
Formand