



JUSTITSMINISTERIET

Dato:  
Kontor: Internationalt Politikontor  
Sagsbeh: Sofie Anne Marner  
Sagsnr.: 2018-330-0031  
Dok.: 857874

## GRUND- OG NÆRHEDSNOTAT

### **Kommissionens forslag til Europa-Parlamentets og Rådets forordning om europæiske editions- og sikringskendelser om elektronisk bevismateriale**

*Sagen er omfattet af retsforbeholdet.*

#### **KOM(2018) 225 endelig**

*Revideret udgave af grund- og nærhedsnotat af 20. juni 2018. Nye afsnit er markeret med kursiv.*

#### **1. Resumé**

*Kommissionen har den 17. april 2018 fremsat forslag til Europa-Parlamentets og Rådets forordning om europæiske editions- og sikringskendelser om elektronisk bevismateriale. Forslaget er fremsat i en samlet pakke med Kommissionens forslag til direktiv om harmoniserede regler for udpegning af retlige repræsentanter med henblik på indsamling af bevismateriale i straffesager (KOM (2018) 226 endelig) og er en del af en række tiltag fra Kommissionen som opfølgning på Kommissionens antiterrorpakke fra oktober 2017. Forslaget til forordning og forslaget til direktiv har tilsammen overordnet til formål at lette indsamlingen af elektronisk bevismateriale på tværs af landegrænser i straffesager. Forordningsforslaget er omfattet af det danske retsforbehold, og forslaget har derfor i sig selv ikke lovgivningsmæssige eller statsfinansielle konsekvenser. Det vurderes dog umiddelbart, at en vedtagelse af forordningsforslaget sammenholdt med en vedtagelse af*

Slotsholmsgade 10  
1216 København K.

T +45 7226 8400  
F +45 3393 3510

[www.justitsministeriet.dk](http://www.justitsministeriet.dk)  
[jm@jm.dk](mailto:jm@jm.dk)

*det samtidigt fremsatte direktivforslag – som ikke er omfattet af retsforbeholdet – vil have konsekvenser for Danmark. Forslaget vurderes at være i overensstemmelse med nærhedsprincippet. Der ses ikke at foreligge offentlige tilkendegivelser om de øvrige medlemsstaters holdninger til forslaget. Fra dansk side er man foreløbigt overordnet positiv over for forslaget. Fra dansk side vil der blive lagt vægt på, hvilken betydning forslaget vil have for Danmark i lyset af retsforbeholdet, herunder for danske myndigheder og tjenesteudbydere, samt for det fremtidige samarbejde med de øvrige medlemsstater.*

## **2. Baggrund**

Kommissionen fremsatte den 17. april 2018 en pakke bestående af et forslag til forordning om europæiske editions- og sikringskendelser om elektronisk bevismateriale samt et forslag til direktiv om harmoniserede regler for udpegning af retlige repræsentanter med henblik på indsamling af bevismateriale i straffesager.

Forordningsforslaget er fremsat *med hjemmel i TEUF artikel 82, stk. 1. I henhold til artikel 1 og 2 i protokollen om Danmarks stilling (forbeholdet vedrørende retlige og indre anliggender) deltager Danmark ikke i en kommende vedtagelse af det foreliggende forordningsforslag, der således ikke vil være bindende for eller finde anvendelse i Danmark.*

Direktivforslaget er fremsat *med hjemmel i TEUF artikel 53 og 62. Direktivforslaget er ikke omfattet af retsforbeholdet, og Danmark deltager derfor i en kommende vedtagelse af det foreliggende direktivforslag, der således vil være bindende for og finde anvendelse i Danmark.*

*Begge forslag skal vedtages efter den almindelige lovgivningsprocedure (TEUF artikel 294).*

Dette notat vedrører forordningsforslaget.

Forbedring af grænseoverskridende adgang til e-beviser har indgået i arbejdet med strafforfølgelse i cyberspace, der bl.a. omfatter spørgsmål vedrørende kryptering og e-beviser. Emnet har været drøftet på en række rådsmøder fra 2015-2017.

De to forslag supplerer de eksisterende regler om retligt samarbejde, herunder konventionen om gensidig retshjælp i straffesager mellem Den Europæiske Unions medlemsstater samt den europæiske efterforskningskendelse. Danmark deltager ikke i sidstnævnte på grund af retsforbeholdet.

Forordningsforslaget er oversendt til Rådet i dansk sprogversion den 24. maj 2018.

### **3. Formål og indhold**

#### **3.1. Forslaget generelt**

Forordningsforslaget bygger på princippet om gensidig anerkendelse og indfører europæiske pålæg om (1) udlevering og (2) sikring af elektronisk bevismateriale, der er lagret af en tjenesteudbyder, der udbyder sine tjenester i EU. De to typer pålæg kan kun udstedes i forbindelse med straffesager, herunder i forbindelse med efterforskning.

Begge typer pålæg vil skulle udstedes eller godkendes af en judiciel myndighed i en medlemsstat (udstedelsesstaten) og fremsendes ved brug af en særlig attest direkte til tjenesteudbyderen eller dennes retlige repræsentant, som tjenesteudbyderen – i medfør af det samtidigt fremsatte direktivforslag – har udpeget med henblik på indsamling af bevismateriale.

Forslaget adskiller sig fra andre retsakter, der bygger på princippet om gensidig anerkendelse, ved, at myndighederne i den medlemsstat, hvor tjenesteudbyderen er etableret eller repræsenteret (den fuldbyrdende medlemsstat), som udgangspunkt ikke inddrages, idet pålægget sendes direkte til tjenesteudbyderen eller dennes retlige repræsentant.

Myndighederne i det land, hvor tjenesteudbyderen er etableret eller repræsenteret, vil kun blive inddraget i særlige tilfælde, eller hvis tjenesteudbyderen eller repræsentanten ikke efterkommer pålægget.

Forslaget finder kun anvendelse *i grænseoverskridende situationer, det vil sige* i tilfælde, hvor tjenesteudbyderen er etableret eller repræsenteret i en anden medlemsstat end udstedelsesstaten. I de tilfælde, hvor tjenesteudbyderen er etableret eller repræsenteret i samme medlemsstat som den udstedende myndighed, vil sikringen eller udleveringen af bevismaterialet skulle ske

efter nationale regler. Forslaget finder ligeledes anvendelse, hvis tjenesteudbyderen ikke er etableret eller repræsenteret i EU, men udbyder tjenester i EU.

### 3.2. Nærmere om forslagets centrale elementer

I forslagets kapitel 1 er der fastsat regler om genstand, definitioner og anvendelsesområde.

I forslagets kapitel 2 er der fastsat regler om udstedelse og gennemførelse af pålæg, brug af attester, fortrolighed, underretning af den person, dataene vedrører, og godtgørelse af udgifter.

I forslagets kapitel 3 er der fastsat regler om sanktioner og fuldbyrdelse i tilfælde af manglende overholdelse.

I forslagets kapitel 4 er der fastsat regler om retsmidler.

I forslagets kapitel 5 er der fastsat afsluttende bestemmelser om bl.a. overvågning og rapportering, Kommissionens delegerede beføjelser, evaluering samt ikrafttræden.

#### *Omfattede tjenesteudbydere*

Forordningen gælder for alle tjenesteudbydere, der udbyder en række nærmere angivne tjenester i EU, herunder tjenesteudbydere, der ikke er etableret i EU.

Det afgørende for, om en tjenesteudbyder ”udbyder tjenester i EU”, er, om tjenesteudbyderen gør det muligt for juridiske eller fysiske personer i en eller flere medlemsstater at anvende sine tjenester. Den blotte tilgængelighed af tjenesten er dog ikke tilstrækkelig. Der stilles derfor også krav om en ”væsentlig tilknytning” til den eller de medlemsstater, hvor tjenesterne stilles til rådighed, hvilket vil skulle afgøres på grundlag af en række momenter. En sådan væsentlig tilknytning anses for at være til stede, hvis tjenesteudbyderen er etableret i en eller flere medlemsstater i EU. For tjenesteudbydere uden for EU vil det være afgørende, om der er et betydeligt antal brugere i en eller flere medlemsstater, eller om tjenesteudbyderen målretter sine tjenester en eller flere medlemsstater, f.eks. ved at markedsføre tjenesterne på det nationale sprog eller ved at udbyde app’s i lokale ”app-butikker”.

Udbydere af følgende typer af tjenester er omfattet af forslaget:

- 1) Elektroniske kommunikationstjenester som defineret i artikel 2, stk. 4, i direktivet om en europæisk kodeks for elektronisk kommunikation (forslaget til direktiv er endnu ikke vedtaget).
- 2) Informationssamfundets tjenester som defineret i artikel 1, stk. 1, litra b), i Europa-Parlamentets og Rådets direktiv (EU) 2015/1535, for hvilke lagring af data er et afgørende element i den tjeneste, der leveres til brugeren, herunder sociale netværk, onlinemarkedspladser til fremme af transaktioner mellem deres brugere samt andre udbydere af hostingtjenester.
- 3) Internetdomænenavns- og IP-nummereringstjenester, såsom udbydere af IP-adresser, domænenavnsadministratorer, domænenavnsregistratorer og hermed forbundne privatlivs- og proxytjenester.

### *Omfattede data*

Følgende typer af data er omfattet af forslaget:

- 1) Abonnementsdata, hvilket omfatter data vedrørende:
  - a) en abonnents eller en kundes identitet, herunder navn, fødselsdato, postadresse eller fysisk adresse, fakturerings- og betalingsoplysninger, telefonnummer eller e-mail
  - b) type tjeneste og dens varighed
- 2) Adgangsdata (data vedrørende påbegyndelsen og afslutningen af en brugeradgangssession til en tjeneste, som skal bruges til at identificere brugeren, f.eks. oplysninger om den IP-adresse, der anvendes under adgangssessionen)
- 3) 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, f.eks. afsender og modtager af en meddelelse eller en anden form for interaktion)
- 4) Indholdsdata (lagrede data i digitalt format, f.eks. en nedskrevet eller indtalt besked, videoer, billeder og lyd)

De omfattede typer data er nærmere beskrevet i forordningsforslaget.

Forslaget omfatter data, der allerede er lagret af eller på vegne af tjenesteudbyderen, og kan således ikke anvendes i forhold til data, der lagres efter det tidspunkt, hvor pålægget modtages.

Det fremgår af forslaget, at alle kategorier indeholder personlige data og dermed er omfattet af garantiene i EU-databeskyttelsesreglerne.

På grund af de forskellige grader af indgreb i de grundlæggende rettigheder er der i forordningsforslaget fastsat forskellige betingelser for anvendelse af editions- og sikringskendelser vedrørende abonnents- og adgangsdata på den ene side og transaktions- og indholdsdata på den anden side.

#### *Udstedende myndighed*

I alle tilfælde skal en judiciel myndighed have enten udstedt eller godkendt pålægget om udlevering eller sikring af bevismaterialet.

Et pålæg om *udlevering* af transaktions- eller indholdsdata kan kun udstedes eller godkendes af domstolene. Er der tale om udlevering af abonnements- eller adgangsdata, vil pålægget også kunne udstedes eller godkendes af anklagemyndigheden.

Et pålæg om *sikring* af data vil kunne godkendes af både domstolene og anklagemyndigheden, uanset hvilken type data, der er tale om.

#### *Betingelser for udstedelse af pålæg*

Et pålæg om udlevering af abonnentsdata og adgangsdata og et pålæg om sikring af elektronisk bevismateriale vil kunne udstedes for enhver lovovertrædelse.

Et pålæg om udlevering af transaktions- og indholdsdata forudsætter derimod, at der er tale om en af følgende typer overtrædelse:

- 1) En strafferetlig overtrædelse, der i udstedelsesstaten er undergivet en strafferamme på mindst 3 års fængsel.
- 2) En række særlige harmoniserede strafferetlige overtrædelser, hvor bevismaterialet typisk kun vil være tilgængeligt i elektronisk form. Det drejer sig om overtrædelse af en række nærmere opregnede bestemmelser i følgende retsakter:
  - a) Rådets rammeafgørelse 2001/413/RIA af 28. maj 2001 om bekæmpelse af svig og forfalskning i forbindelse med andre betalingsmidler end kontanter.
  - b) Europa-Parlamentets og Rådets direktiv 2011/92/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.
  - c) 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.

- d) 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.

Det er en betingelse, at der er tale om bevismateriale til brug for efterforskningen eller retsforfølgningen i en konkret straffesag, og at pålægget er nødvendigt og forholdsmæssigt i den enkelte sag. For pålæg om udlevering af bevismateriale er det desuden en betingelse, at et lignende retsmiddel er tilgængeligt for samme overtrædelse i en sammenlignelig national situation i udstedelsesstaten.

#### *Brug af attester*

Begge typer pålæg vil skulle fremsendes via særlige attester, der skal oversættes til et af de officielle EU-sprog i den medlemsstat, hvor den retlige repræsentant er bosiddende eller etableret, medmindre modtageren har erklæret at ville acceptere attester på et af de andre officielle EU-sprog.

#### *Tidsfrister*

For så vidt angår pålæg om udlevering af bevismateriale skal modtageren fremsende de efterspurgte oplysninger senest 10 dage efter modtagelse af pålægget, medmindre udstedelsesmyndigheden har angivet en kortere frist. I nødssituationer skal modtageren fremsende oplysningerne uden unødigt forsinkelse og senest efter 6 timer.

For så vidt angår pålæg om sikring af bevismateriale skal modtageren sikre de efterspurgte oplysninger uden unødigt forsinkelse. Modtageren vil skulle opretholde sikringen af data i 60 dage eller – hvis udstedelsesmyndigheden inden for de 60 dage over for modtageren bekræfter, at der er blevet indledt en procedure om anmodning om udlevering – så længe det er nødvendigt for, at modtageren kan efterkomme den efterfølgende anmodning om udlevering.

Forslaget fastsætter regler for de tilfælde, hvor modtageren af en række nærmere opregnede grunde ikke kan imødekomme pålægget, eller hvor modtageren vurderer, at et pålæg om udlevering af oplysninger tydeligvis er i strid med EU's charter om grundlæggende rettigheder eller åbenbart er udtryk for misbrug.

#### *Sanktioner og fuldbyrdelse*

Medlemsstaterne skal fastsætte regler om økonomiske sanktioner i tilfælde af tjenesteudbydernes manglende overholdelse af deres forpligtelser i forhold til gennemførelse af pålæg og fortrolighed.

Efterkommer modtageren ikke et pålæg om udlevering eller sikring inden for fristen, og fremkommer modtageren ikke med en begrundelse, som accepteres af udstedelsesmyndigheden, vil udstedelsesmyndigheden kunne oversende pålægget til den myndighed i fuldbyrdelsesstaten, der er kompetent til at fuldbyrde pålægget (fuldbyrdelsesmyndigheden) med henblik på fuldbyrdelse i overensstemmelse med national lovgivning i fuldbyrdelsesstaten. Fuldbyrdelsesmyndigheden vil skulle anerkende pålægget uden yderligere formaliteter inden for en frist på 5 arbejdsdage, medmindre den vurderer, at der foreligger en af en række nærmere opregnede indsigelsesgrunde. Modtageren vil også selv kunne gøre indsigelse mod fuldbyrdelsen af pålægget med henvisning til en række indsigelsesgrunde. Fuldbyrdelsesmyndigheden vil skulle inddrage den udstedende myndighed inden eventuel afgørelse om ikke at anerkende pålægget.

#### *Retsmidler*

Hvis modtageren af et pålæg om udlevering af bevismateriale vurderer, at efterkommelse af pålægget vil være i strid med lovgivningen i et tredjeland, der forbyder udlevering af de pågældende oplysninger under henvisning til, at det er nødvendigt for at beskytte de berørte personers grundlæggende rettigheder eller tredjelandets grundlæggende rettigheder forbundet med statens sikkerhed eller forsvar, giver forslaget mulighed for en fornyet prøvelse af pålægget. Den fornyede prøvelse vil skulle ske under inddragelse af den udstedende myndighed, en domstol i udstedelsesstaten og den centrale myndighed i tredjelandet.

Forslaget giver også mulighed for fornyet prøvelse i tilfælde, hvor modtageren vurderer, at efterkommelse af et pålæg om udlevering af bevismateriale vil være i strid med lovgivningen i tredjelandet af andre grunde.

Herudover fastsætter forslaget regler om effektive retsmidler for mistænkte og tiltalte samt de personer, hvis oplysninger udleveres. Disse retsmidler vil skulle udøves af en judiciel myndighed i udstedelsesstaten i henhold til dens nationale lovgivning.

Endelig fastsætter forslaget regler om sikring af privilegier og immuniteter i henhold til lovgivningen i fuldbyrdelsesstaten.



#### **4. Europa-Parlamentets udtalelser**

Der foreligger på nuværende tidspunkt ikke udtalelser eller andre tilkendegivelser fra Europa-Parlamentet.

#### **5. Nærhedsprincippet**

Kommissionen har anført, at den grænseoverskridende dimension af de identificerede problemer betyder, at det er nødvendigt med tiltag på EU-niveau. Kommissionen har anført bl.a., at de kriminalitetstyper, som der findes elektroniske beviser for, ofte vedrører situationer, hvor den infrastruktur, de elektroniske beviser lagres på, samt tjenesteudbyderen, der driver infrastrukturen, er omfattet af en anden national retlig ramme – inden for eller uden for EU – end den retlige ramme, som ofret og gerningsmanden er omfattet af. Som følge heraf kan det være meget tidskrævende og vanskeligt for det kompetente land at få effektiv adgang til elektroniske beviser på tværs af grænserne uden fælles minimumsregler.

Kommissionen har anført, at medlemsstaterne hver for sig vil have særligt svært ved at tage højde for den forskelligartede regulering i medlemsstaterne og ved at forbedre samarbejdet efter den nuværende EU-lovgivning, navnlig via den europæiske efterforskningskendelse.

På baggrund af de forskellige retlige tilgange, antallet af berørte politikområder (sikkerhed, grundlæggende rettigheder, herunder proceduremæssige rettigheder og beskyttelsen af personoplysninger, samt økonomiske aspekter) samt den brede vifte af interessenter vurderer Kommissionen således, at det er mest hensigtsmæssigt med lovgivning på EU-niveau for at kunne adressere problemerne.

Det er – af de af Kommissionen anførte grunde – regeringens vurdering, at forslaget er i overensstemmelse med nærhedsprincippet.

#### **6. Gældende dansk ret**

Danmark har – med enkelte undtagelser – ikke gennemført særlig lovgivning om gensidig retshjælp i straffesager. Det antages imidlertid med støtte i retspraksis, at udenlandske begæringer om efterforskningskridt i Danmark kan imødekommes, uanset om fremsættelsen og behandlingen af retsanmodninger er reguleret i en aftale, der finder anvendelse mellem Danmark og den anmodende stat. De relevante efterforskningskridt gennemføres i

givet fald på grundlag af en analogisk anvendelse af de relevante bestemmelser i retsplejeloven, idet en udenlandsk anmodning om efterforskning, herunder ransagning, beslaglæggelse samt edition, kan imødekommes, hvis det pågældende efterforskningsskridt kunne gennemføres i forbindelse med en tilsvarende national strafferetlig efterforskning.

Lov om fuldbyrdelse af visse strafferetlige afgørelser i Den Europæiske Union indeholder en række særlige regler og procedurer for retshjælp til andre medlemsstater for så vidt angår fuldbyrdelse af visse strafferetlige afgørelser.

Princippet efter reglerne om gensidig retshjælp er, at anmodninger om retshjælp fremsendes mellem de relevante myndigheder i medlemsstaterne.

Der findes ikke regler om fremsendelse af pålæg om udlevering af bevismateriale i straffesager direkte til en tjenesteudbyder på tværs af landegrænserne.

Forslaget supplerer således de eksisterende regler om retligt samarbejde, herunder konventionen om gensidig retshjælp i straffesager mellem Den Europæiske Unions medlemsstater.

## **7. Konsekvenser**

Forslaget er som nævnt fremsat med hjemmel i TEUF artikel 82, stk. 1, der er omfattet af det danske retsforbehold. Danmark deltager således ikke i vedtagelsen af forordningsforslaget, ligesom forslaget ikke vil være bindende for eller finde anvendelse i Danmark.

Forslaget har derfor i sig selv ikke lovgivningsmæssige, *økonomiske eller øvrige* konsekvenser for Danmark.

Det bemærkes imidlertid, at forordningsforslaget skal ses i sammenhæng med det samtidig fremsatte direktivforslag, som ikke er omfattet af retsforbeholdet, hvorfor det umiddelbart vurderes, at en vedtagelse af forordningsforslaget sammenholdt med en vedtagelse af det samtidigt fremsatte direktivforslag vil have konsekvenser for Danmark, herunder for erhvervslivet. *Danmarks stilling i relation til forordningsforslaget er i øjeblikket ved at blive nærmere afdækket i samarbejde med Kommissionen i lyset af Dan-*

*marks tilknytning til direktivforslaget. De mulige konsekvenser af forordningsforslaget i lyset af direktivforslaget vil på baggrund af resultatet af denne undersøgelse kunne fastlægges nærmere.*

## **8. Høring**

Kommissionens forslag er sendt i høring hos følgende myndigheder og organisationer mv.:

Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Præsidenten for Sø- og Handelsretten, Præsidenterne for byretterne, Advokatrådet, Amnesty International, Dansk Erhverv, Danske Advokater, Datatilsynet, Den Danske Dommerforening, Dommerfuldmægtigforeningen, Domstolsstyrelsen, Foreningen af Advokater og Advokatfuldmægtige, Foreningen af Offentlige Anklagere, Handelshøjskolen i København (Juridisk Institut), Handelshøjskolen i Aarhus (Juridisk Institut), Institut for Menneskerettigheder, Kriminalpolitisk Forening (KRIM), Københavns Universitet, Landsforeningen af Forsvarsadvokater, Politiforbundet, Retspolitisk Forening, Rigsadvokaten, Rigspolitiet, Syddansk Universitet (Juridisk Institut), Aalborg Universitet (Juridisk Institut), Aarhus Universitet (Juridisk Institut)

*Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Præsidenten for Sø- og Handelsretten, Præsidenterne for byretterne, Institut for Menneskerettigheder, Rigspolitiet, Politiforbundet, Datatilsynet og Domstolsstyrelsen har afgivet høringssvar, men har ikke haft bemærkninger til forslaget.*

*Advokatrådet, IT-Politisk Forening, Erhvervsstyrelsen og Dansk Erhverv har afgivet høringssvar med bemærkninger til forslaget.*

### 8.1. Advokatrådets høringssvar

*Advokatrådet har henvist til en udtalelse om forslaget fra the Council of Bars and Law Societies of Europe (CCBE), som Advokatrådet henholder sig til. Der lægges i udtalelsen særligt vægt på tre forskellige problemstillinger.*

*Den første problemstilling omhandler oplysninger, som er fortrolige som følge af, at de udgør kommunikationen mellem en advokat og dennes klient. CCBE understreger bl.a., at når en europæisk editionskendelse fuldbyrdes, skal den pågældende organisation, som dataene stammer fra, gives mulig-*

*hed for at vurdere sine juridiske rettigheder og pligter og hvis muligt få adgang til at udfordre anmodningen, inden dataene bliver udleveret. Det er på den baggrund CCBE's opfattelse, at en anmodning om adgang til data altid skal rettes til den dataansvarlige og ikke til databehandleren, således at den dataansvarlige kan vurdere, om dataene udgør fortrolig korrespondance mellem en advokat og dennes klient. Bestemmelsen herom i forslagets artikel 5, stk. 6, er efter CCBE's opfattelse for bred og vil ikke omfatte alle typer af advokatkontorer. CCBE foreslår videre, at i tilfælde hvor der er risiko for destruktion af data, hvis udleveringen ikke foretages med det samme, kan der indføres en to-trinsproces, hvor den anmodende medlemsstat først udsteder en sikringskendelse og dermed giver den dataansvarlige mulighed for at gennemse oplysningerne, før der eventuelt efterfølgende udstedes en editionskendelse.*

*Endvidere er det CCBE's opfattelse, at det skal specificeres i forslagets artikel 9, at det faktum, at de pågældende data udgør fortrolige oplysninger mellem en advokat og dennes klient, skal udgøre et gyldigt grundlag for at afvise at fuldbyrde editionskendelsen.*

*Den anden problemstilling, som CCBE lægger vægt på, vedrører princippet om "equality of arms", som indebærer, at begge parter i en retssag skal gives lige adgang til at gøre sig bekendt med dokumenter, afhøre vidner mv. Det er således CCBE's opfattelse, at en tiltalt i en straffesag og dennes advokat skal have adgang til at anmode om, at der udstedes en europæisk editions- eller sikringskendelse på lige fod med politi og anklagemyndighed.*

*Endelig skal der ifølge CCBE lægges vægt på en bestemmelse vedrørende adgang til effektive retsmidler i overensstemmelse med den mekanisme, der er lagt op til i artikel 42 i forordningen om den Europæiske Anklagemyndighed (EPPO), særligt i relation til EU-domstolens jurisdiktion.*

*Ud over disse tre hovedpunkter påpeges det endvidere i CCBE's udtalelse, at det for alle typer af data i forordningsforslaget bør være en domstol, der udsteder editions- eller sikringskendelsen, således at en kendelse efter forslaget ikke kan udstedes af anklagemyndigheden i en medlemsstat. CCBE efterspørger videre en regel i forslagets artikel 5, hvorefter der skal være overbevisende begrundet mistanke, før den grænseoverskridende dataudveksling kan foretages. Det påpeges videre, at der bør være et bredere grundlag for at afvise en kendelse, og at en eventuel beslutning om ikke at notificere datasubjektet om indsamling af personens oplysninger skal godkendes af en uafhængig retslig myndighed.*

## 8.2. IT-Politisk Forenings hørings svar

*IT-Politisk Forening anfører i sit hørings svar, at udlevering af personoplysninger fra tjenesteudbydere i andre stater bør ske via aftaler om gensidig retshjælp eller den europæiske efterforskningskendelse, da begge instrumenter sikrer en involvering af myndighederne i den modtagende stat. Det er vigtigt af hensyn til borgernes retssikkerhed og for at sikre, at grundlæggende rettigheder overholdes.*

*Det anføres bl.a., at forordningsforslagets muligheder for at afslå en kendelse er meget begrænsede, og at det under alle omstændigheder ikke er rimeligt over for hverken borgere eller erhvervslivet, at private virksomheder skal udføre kontrolforanstaltninger, som burde være tillagt domstole eller andre uafhængige myndigheder.*

*IT-Politisk Forening anfører endvidere, at forordningsforslagets betragtning 46 udgør et betydeligt incitament til altid at efterleve editionskendelsen, idet tjenesteudbyderen ikke kan holdes ansvarlig for i god tro at udlevere personoplysninger i henhold til en europæisk editionskendelse. Derimod fastsætter forordningsforslaget bøder for manglende overholdelse, og tjenesteudbyderen har en meget kort frist (10 dage eller i visse tilfælde endda 6 timer) til at efterleve kendelsen.*

*Det fremgår af hørings svaret, at det fremsatte forordningsforslag virker forhastet. Dette begrundes bl.a. med, at direktivet om den europæiske efterforskningskendelse fra 2014 er blevet gennemført i de fleste medlemsstater inden for det seneste år, og at der derfor på nuværende tidspunkt kun er begrænsede erfaringer med instrumentet. Synspunktet begrundes endvidere med, at der i komitéen for Europarådets cybercrime-konvention (T-CY) er igangværende overvejelser om en tillægsprotokol om adgang til elektroniske oplysninger hos cloud-tjenester.*

*Ud over problemet med overlap mellem de to instrumenter påpeger IT-Politisk Forening, at forordningsforslaget kan risikere at fremme en udvikling for den kommende T-CY tillægsprotokol, hvor efterforskningsmyndigheder får tillagt ekstraterritoriale beføjelser over for private tjenesteudbydere, ikke kun inden for den EU, men for det store antal stater (mere end 50), som deltager i Cybercrime-konventionen.*

*Det påpeges endvidere, at den stigende brug af elektroniske kommunikationstjenester, sociale medier og cloudtjenester på internettet givetvis skaber et behov for at modernisere reglerne for efterforskningsmyndigheders adgang til oplysninger, men samtidig en kraftigt forøget risiko for, at borgere uretmæssigt kommer i søgelyset for efterforskningsmyndigheder i andre stater og i den forbindelse kan blive udsat for indgribende efterforskningsmetoder.*

*Vedrørende betingelserne for udstedelse af editionskendelsen anføres det bl.a. i høringsvaret, at der ikke i forordningsforslaget er et krav om, at den pågældende efterforskningsforanstaltning skal være tilladt i den modtagende medlemsstat. Borgere, der eksempelvis benytter en svensk e-mail-tjeneste, kan således ikke længere gå ud fra, at det er svensk lov, som bestemmer mulighederne for, at efterforskningsmyndigheder kan få adgang til indholdet af deres elektroniske kommunikation. Der kan være andre EU-medlemsstater med lavere krav for adgangen til indholdet af elektronisk kommunikation. Det skaber bl.a. en betydelig usikkerhed for borgernes retssikkerhed.*

*Vedrørende kategorier af data og betingelser for udlevering anfører IT-Politisk Forening bl.a., at forordningsforslaget ikke fastsætter materielle betingelser for udlevering af abonnements- og adgangsdata, og at det er tvivlsomt, om det i alle situationer er i overensstemmelse med EU-retten og retspraksis fra den Europæiske Menneskerettighedsdomstol (EMD).*

*IT-Politisk Forening anfører endvidere, at forordningsforslaget indebærer, at en anklager kan udstede en editionskendelse om adgang til abonnements- og adgangsdata, uden krav om forudgående kontrol af en domstol eller en uafhængig administrativ myndighed. Det anføres, at denne udstedelsesbeføjelse til en anklager næppe vil være forenelig med retspraksis fra EMD.*

*Forordningsforslaget giver mulighed for, at efterforskningsmyndigheden kan få adgang til transaktionsdata og indholdsdata for personer, som ikke er mistænkt i den pågældende strafferetlige efterforskning. Forordningsforslagets artikel 5, stk. 2, stiller alene det krav, at efterforskningskendelsen skal være nødvendig og proportional. IT-Politisk Forening anfører, at forordningsforslaget bør fastsætte præcise betingelser for, hvilke personers elektroniske kommunikation, efterforskningsmyndighederne kan få udleveret.*

*I relation til lovkonflikter med andre stater anfører IT-Politisk Forening, at forordningsforslaget vil få virkning for tjenesteudbydere i hele verden. Det skaber en risiko for lovkonflikter, hvis en efterforskningsmyndighed i en EU-medlemsstat kan have ret til at udstede en editionskendelse til en tjenesteudbyder, der er hjemmehørende i et land, hvor oplysningerne ikke må udleveres, eller mere sandsynligt ikke må udleveres uden en dommerkendelse fra en domstol i tjenesteudbyderens hjemland.*

*Det er ikke utænkeligt, at der kan være tilsvarende lovkonflikter inden for EU, herunder for de EU-medlemsstater (Danmark, Storbritannien og Irland), der har (forskellige) EU-forbehold på det retlige område. Artikel 15 og 16 i forordningsforslaget har visse undtagelser fra gennemførelsen af den europæiske editionskendelse for at imødekomme sådanne situationer. Prøvelsesproceduren og undtagelserne i artikel 15 og 16 gælder kun, hvis udlevering af oplysningerne vil være i strid med lovgivningen i et tredjeland. IT-Politisk Forening fortolker dette således, at artikel 15 og 16 ikke vil kunne anvendes for tjenesteudbydere, der er hjemmehørende inden for EU, for eksempel en dansk tjenesteudbyder.*

*Vedrørende konsekvenser for danske borgere bemærker IT-Politisk Forening, at Danmarks retsforbehold ikke udelukker, at forordningsforslaget kan få umiddelbare konsekvenser for danske borgere i den forstand, at efterforskningsmyndigheder i andre EU-medlemsstater kan få adgang til danske borgeres personoplysninger i videre omfang end efter den gældende lovgivning.*

*Fremover vil efterforskningsmyndigheder i alle EU-medlemsstater (som deltager i det retlige samarbejde) kunne få adgang til data uden at involvere myndighederne i den medlemsstat, hvor tjenesteudbyderen er hjemmehørende. Endvidere kan en tjenesteudbyder, som er hjemmehørende i Danmark, være forpligtet til at udnævne en retlig repræsentant i en anden EU-medlemsstat, hvis den danske tjenesteudbyder udbyder tjenester i andre EU-lande. Hvis den danske tjenesteudbyder har udnævnt en retlig repræsentant i et andet EU-land, vil efterforskningsmyndigheder i alle EU-lande (der deltager i det retlige samarbejde) kunne få adgang til oplysninger om danske borgere hos den danske tjenesteudbyder, herunder indholdet af deres elektroniske kommunikation, via den europæiske editionskendelse. Selv om der er tale om danske borgere, der er kunder hos en dansk tjenesteudbyder, vil dette trods retsforbeholdet kunne ske uden at involvere danske myndigheder og domstole.*

### 8.3. Erhvervsstyrelsens hørings svar

*Erhvervsstyrelsen bemærker i sit hørings svar, at forordningsforslaget er omfattet af det danske retsforbehold og derfor ikke i sig selv har lovgivningsmæssige eller statsfinansielle konsekvenser for Danmark. Forslaget skal dog ses i sammenhæng med det samtidig fremsatte direktivforslag, hvoraf det fremgår, at en retlig repræsentant vil skulle udpeges i en af de medlemsstater, hvor tjenesteudbyderen udbyder sine ydelser eller er etableret. Repræsentanten kan således udpeges i andre medlemsstater end Danmark, hvor forordningen er gældende. Erhvervsstyrelsen vurderer på den baggrund, at en vedtagelse af forordningsforslaget sammenholdt med en vedtagelse af direktivforslaget kan medføre administrative byrder for erhvervslivet. Erhvervsstyrelsen bemærker endelig, at det ikke har været muligt at fremskaffe oplysninger, som kan bidrage til at præcisere omfanget af de potentielle administrative byrder.*

### 8.4. Dansk Erhvervs hørings svar

*Dansk Erhverv bemærker i sit hørings svar, at der på tværs af grænser er behov for en ny måde at behandle og fremskaffe elektronisk bevismateriale i straffesager på. Behovet er skærpet af den omstændighed, at efterforskning i kriminalsager i stigende grad støtter sig på analyse af elektronisk bevismateriale. Da flere medlemsstater har udvidet deres nationale muligheder for at fremskaffe elektronisk bevismateriale i straffesager, er der tendens til en fragmentering af procedurerne i de grænseoverskridende sager, hvilket skaber usikkerhed som følge af modstridende forpligtelser til skade for de berørte personers retssikkerhed. Procedurerne er samtidig ineffektive og til skade for opklarings- og efterforskningsarbejdet.*

*For virksomhederne medfører fragmenteringen en betydelig byrde, når de skal være klar til at håndtere en mangfoldighed af nationale regelsæt vedrørende editions- og sikringskendelser. Det er ofte unødigt komplekst og omkostningsfuldt, hvilket især kan være en belastning for de små og mellemstore virksomheder med begrænsede juridiske ressourcer, der ønsker at udbyde tjenester i og på tværs af EU's Digitale Indre Marked.*

*Det bemærkes i hørings svaret, at Dansk Erhverv på den baggrund hilser Europa-Kommissionens forslag om en forenklet og mere effektiv procedure for editions- og sikringskendelser varmt velkommen, forudsat at forordningen ikke generelt kommer til at svække tjenesteudbydernes mulighed for at sikre og beskytte deres brugeres data.*



*Dansk Erhverv ser dog med bekymring på den situation, der er opstået på grund af EU's variable geometri på det retslige område med bl.a. det danske retsforbehold. Danske tjenesteudbydere, der udbyder tjenester i EU, skal som følge af direktivet udpege en retslig repræsentant. Da Danmark står uden for de retslige instrumenter i forordningen, kan f.eks. et hovedkvarter i Danmark ikke optræde som retslig repræsentant i de lande, hvor forordningen gælder. Virksomheden skal således udpege en retslig repræsentant i et af de af forordningen omfattede EU-lande. Det kan betyde omkostninger for de danske virksomheder, som deres konkurrenter i de øvrige EU-lande ikke er pålagt.*

*I forlængelse heraf er Dansk Erhverv bekymret for, at retsforbeholdet i den henseende kan gøre det mindre attraktivt for eksempelvis globale virksomheder at placere deres hovedkvarter for EU i Danmark, da de samtidig skal udpege en retslig repræsentant i et andet EU-land. Det kan også berøre de selskabskonstruktioner, som globale selskaber vælger i forbindelse med eventuel placering af datacentre i Danmark.*

*Dansk Erhverv angiver i sit høringssvar, at forslaget må formodes at svække de danske myndigheders mulighed for effektivt at få adgang til elektronisk bevismateriale fra tjenesteudbydere, der er etableret eller repræsenteret i EU under forordningen og udbyder tjenester i Danmark, i forhold til en situation, hvor Danmark var omfattet af forordningen. Samlet er der således en pris at betale på flere områder for opretholdelse af det danske retsforbehold.*

*For så vidt angår forslaget om forordningen anfører Dansk Erhverv, at det er oplagt og positivt, at der altid skal inddrages en judiciel myndighed i udstedelse af en europæisk editions- eller sikringskendelse. Desuden er det positivt, at kendelser om transaktions og indholdsdata, der kan betragtes som mere følsomme end abonnements- og adgangsdata, skal udstedes og godkendes af en dommer eller domstol. Det er derimod ikke betryggende, at udlevering af oplysninger om abonnements- og adgangsdata således skal kunne udleveres på en anklagers foranledning uden prøvelse ved en domstol. Der bør altid stå en dommer eller domstol bag en kendelse.*

*Vedrørende tidsfrister fremgår det af Dansk Erhvervs høringssvar, at fristen for i nødsituationer at svare på en kendelse er sat til seks timer. Det anerkendes, at der kan være et behov for at have en kortere frist end den obligatoriske frist på 10 dage for at fremskynde en efterforskning i nødsituationer.*

*Det anføres, at for mange virksomheder, der ikke har økonomisk skala til at bemande en døgnvagtst funktion, vil det dog være overordentlig vanskeligt administrativt og teknisk at besvare henvendelsen inden for den foreslåede tidsfrist. En tidsfrist på 24 timer på linje med Europa-Kommissionens "Code of Conduct on Countering Illegal Online Hate Speech" forekommer mere realistisk.*

*I relation til prøvelsesproceduren i forbindelse med modstridende forpligtelser begrundet af tredjelandes lovgivning i forslaget artikel 15-16 anføres det i høringssvaret, at Danmark i denne sammenhæng er at betragte som tredjeland og dermed kan komme i en situation, hvor der er modstridende forpligtelser begrundet i dansk lovgivning. I den situation kan prøvelsesproceduren være relevant. Dansk Erhverv opfordrer dog til, at der iværksættes en analyse af eventuelle modstridende forpligtelser og en mulig justering af dansk lovgivning, så den bringes i overensstemmelse med forordningen for at undgå, at der opstår situationer med modstridende forpligtelser.*

## **9. Andre landes kendte holdninger**

Der ses ikke at foreligge offentlige tilkendegivelser om de øvrige medlemsstaters holdninger til forslaget.

## **10. Regeringens foreløbige generelle holdning**

Fra dansk side er man foreløbigt overordnet positivt indstillet over for forslaget, der har til formål at lette det retlige samarbejde i straffesager.

*Det bemærkes, at Danmark, som følge af retsforbeholdet i relation til forordningsforslaget ikke fuldt ud vil kunne deltage i de fordele, forslagene medfører. Som følge af det samtidigt fremsatte direktivforslag, som ikke er omfattet af retsforbeholdet, vil forslagene dog medføre visse konsekvenser for Danmark, jf. pkt. 7.*

*Fra dansk side vil der blive lagt vægt på, hvilken betydning forslaget vil have for Danmark i lyset af retsforbeholdet, herunder for danske myndigheder og tjenesteudbydere, samt for det fremtidige samarbejde med de øvrige medlemsstater.*

## **11. Tidligere forelæggelse for Folketingets Europaudvalg**

Forslaget har senest været forelagt for Folketingets Europaudvalg på mødet den 1. juni 2018 til orientering i forbindelse med rådsmødet (retlige og indre anliggender) den 4.-5. juni 2018.