DANSK ERHVERV
Børsen
DK-1217 København K

www.danskerhverv.dk
info@danskerhverv.dk
T. +45 3374 6000

DANSK ERHVERV

Justitsministeriet
Att.: Viktoria Egsgaard
Slotsholmsgade 10
1216 København K.
Sendt til jm@jm.dk cc veg@jm.dk
Ang. j.nr. 2018-330-0035.

6. juli 2018

Høring over forslag til EU-forordning om europæiske editions- og sikringskendelser om elektronisk bevismateriale (COM (2018) 225 final) og direktiv om udpegning af retlige repræsentanter (COM (2018) 226 final).

Dansk Erhverv har d. 15. juni modtaget høringsmateriale om EU-Kommissionens forslag til en forordning om editions- og sikringskendelser om elektronisk bevismateriale samt direktiv om harmoniserede regler for udpegning af retlige repræsentanter.

Generelle bemærkninger

Dansk Erhverv anerkender, at der i betragtning af internettets grænseløse karakter, hvor digitale tjenester og apps ofte gemmer oplysninger i andre lande, end de bliver anvendt, er et behov for en ny måde at behandle og fremskaffe elektronisk bevismateriale i straffesager på tværs af grænser. Behovet er skærpet af den omstændighed, at efterforskning i kriminalsager i stigende grad støtter sig til analyse af elektronisk bevismateriale.

Da flere medlemsstater har udvidet deres nationale værktøjer til 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 værktøjer til 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.

På den baggrund hilser Dansk Erhverv Europa-Kommissionens forslag om en forenklet og mere effektiv procedure for editions- og sikringskendelse varmt velkommen, forudsat at forordningen ikke generelt kommer til at svække tjenesteudbydernes mulighed for at sikre og beskytte deres

brugeres data. Det er således afgørende, at ingen af løsningerne implicerer såkaldte bagdøre, der kan omgå krypteringsteknologier og andre forsvarsmekanismer.

Dansk Erhvervs 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 udenfor de retslige instrumenter i forordningen, kan fx 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 fx 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.

Forslaget må også 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.

Specifikke bemærkninger
For så vidt angår forslaget om **forordningen** har Dansk Erhverv følgende bemærkninger:

Udstedelsesmyndighed og betingelser for udstedelse af en europæisk editionskendelse (art. 4-5)
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 betrykkende, 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.

Der gives en foreløbig liste i forbindelse med artikel 5 med eksempler på grovere kriminalitet, hvor kendelser for udlevering af transaktions- og indholdsdata er berettiget. Listen kan med fordel uddybes for at øge klarheden for berørte tjenesteudbydere og myndigheder.

Tidsfrister (art. 9)
Fristen for i nødsituationer at svare på en kendelse er i forslaget sat til seks timer. Det skal 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. For mange virksomheder, der ikke har økonomisk skala til at bemande en døgnvagtsfunktion, vil det dog være overordentlig vanskeligt administrativt og teknisk at besvare henvendelsen inden for den foreslåede tidsfristen. En tidsfrist på 24 timer, på linje med Europa-Kommissionens "Code of Conduct on countering illegal online hate speech" forekommer mere realistisk.

Prøvelsesprocedure i forbindelse med modstridende forpligtelser begrundet af tredjelands lovgivning art (15-16)
Danmark er i denne sammenhæng at betragte som tredjeland og 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.

For så vidt angår **direktivet**, der gør det obligatorisk for tjenesteudbydere at udpege en retlig repræsentant i et land i Unionen, som deltager i forordningen, har Dansk Erhverv følgende bemærkninger:

Variabel geometri (fx art. 3)
Dansk Erhverv noterer, at danske virksomheder, der udbyder tjenester i det øvrige EU, på grund af retsforbeholdet skal udpege en retslig repræsentant i et medlemsland, der deltager i forordningen. Det kan betyde en økonomisk og administrativ byrde, der gør det relativt vanskeligere at få gavn af det Digitale Indre Marked, end det er tilfældet for virksomheder i lande, der deltager i forordningen. Konsekvenserne af retsforbeholdet bør undersøges både for danske virksomheder og globale virksomheders tilskyndelse til at slå sig ned med hovedsæde i Danmark.

Dansk Erhverv ser frem til en dialog om konsekvenserne for Danmark og danske virksomheder af forslagene og står til rådighed, hvis der skulle være spørgsmål om høringssvaret.

Med venlig hilsen

Poul Noer
Chefkonsulent

Justitsministeriet
Slotsholmsgade 10
1216 København K

Sendt per email til **jm@jm.dk** med
kopi til **veg@jm.dk**

IT-Politisk Forening
c/o Jesper Lund
Carl Bernhards Vej 15, 2.tv
1817 Frederiksberg C

E-mail : bestyrelsen@itpol.dk
Web : http://www.itpol.dk

Dato : 6. juli 2018

Høringssvar vedr. EU-Kommissionens forslag til forordning om europæiske editions- og sikringskendelser samt forslag til direktiv om udpegning af retlige repræsentanter (J.nr. 2018-330-0035)

IT-Politisk Forening har følgende bemærkninger til EU-Kommissionens forslag til forordning om europæiske editions- og sikringskendelser om elektronisk bevismateriale i straffesager (2018/0108 (COD)) samt EU-Kommissionens forslag til direktiv om harmoniserede regler for udpegning af retlige repræsentanter med henblik på indsamling af bevismateriale (2018/0107 (COD)).

På grund af retsforbeholdet deltager Danmark ikke i forordningsforslaget, og dansk politi vil således ikke kunne gøre brug af den foreslåede europæiske editions- og sikringskendelse. Vores bemærkninger vedrørende forordningsforslaget tager derfor udgangspunkt i en generel vurdering af konsekvenserne for europæiske borgeres retssikkerhed. Der er dog situationer, hvor forordningsforslaget kan have umiddelbare konsekvenser for danske borgere. Dette punkt kommenteres særskilt.

IT-Politisk Forening er i gang med at drøfte forordningsforslaget og direktivforslaget med vores samarbejdspartnere i organisationen European Digital Rights (EDRi). De foreløbige bemærkninger fra IT-Politisk Forening i dette høringssvar er i høj grad baseret på dette arbejde. Det er muligt, at vi på et senere tidspunkt vil

fremsende yderligere bemærkninger til Justitsministeriet og/eller Folketingets Europaudvalg og Retsudvalg.

A. Forordningsforslaget om den europæiske editions- og sikringskendelse

Hvis efterforskningsmyndigheder i en EU-medlemsstat i forbindelse med en strafferetlig efterforskning ønsker adgang til oplysninger hos en tjenesteudbyder i et andet land, kan dette i dag ske via internationale aftaler om gensidig retshjælp, direktivet om den europæiske efterforskningskendelse (som Danmark og Irland ikke deltager i) hvis der er tale om et andet EU-land, eller udlevering af oplysningerne fra tjenesteudbyderen på frivillig basis. En tjenesteudbyder i eksempelvis USA er ikke juridisk forpligtet til at efterleve en editionskendelse fra en efterforskningsmyndighed i et EU-land, men kan gøre dette på frivillig basis, hvis amerikansk lov tillader det. Den amerikanske Electronic Communications Privacy Act (ECPA) tillader udlevering af ikke-indholdsdata til udenlandske myndigheder på frivillig basis.

Forordningsforslaget giver efterforskningsmyndigheder i en EU-medlemsstat mulighed for at udstede retligt bindende editionskendelser (og sikringskendelser) til tjenesteudbydere uden for medlemsstatens eget territorium. Den formelle modtager af kendelsen er tjenesteudbyderens retlige repræsentant, og forordningsforslagets anvendelsesområde er efterforskninger, hvor den retlige repræsentant befinder sig i en anden EU-medlemsstat. Hvis den retlige repræsentant er i samme medlemsstat som efterforskningsmyndigheden, finder medlemsstatens nationale lov anvendelse. Tjenesteudbydere uden for EU, som udbyder tjenester i EU omfattet af forordningsforslaget, skal udpege en retlig repræsentant inden for EU som kan modtage europæiske editions- og sikringskendelser (jf. direktivforslaget om udpegning af retlige repræsentanter).

Modsat hvad der er gældende for den europæiske efterforskningskendelse er myndighederne i den modtagende EU-medlemsstat som udgangspunkt ikke involveret i processen. Tjenesteudbyderens retlige repræsentant modtager editionskendelsen direkte fra

efterforskningsmyndigheden i en anden EU-medlemsstat og er forpligtet til at udlevere de angivne oplysninger. Arbejdsgangen minder således om "frivillig udlevering" i den forstand at efterforskningsmyndigheden retter direkte henvendelse til tjenesteudbyderen i en andet stat uden om denne stats myndigheder.

Generelle bemærkninger til forordningsforslaget

Efter IT-Politisk Forenings opfattelse bør udlevering af personoplysninger fra tjenesteudbydere i andre stater 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 bliver overholdt. I den forbindelse er man på EU-plan nødt til at forholde sig til, at retsstaten i visse EU-lande (særligt Ungarn og Polen) har undergået en meget bekymrende udvikling i de seneste år.

Den europæiske efterforskningskendelse giver myndighederne i den modtagende stat mulighed for at afslå kendelsen under visse omstændigheder (jf. artikel 11 i direktivet om den europæiske efterforskningskendelse). For den europæiske efterforskningskendelse er den eneste kontrolforanstaltning i den modtagende stat, at tjenesteudbyderen kan afvise kendelsen, hvis "den tydeligvis er i modstrid med Den Europæiske Unions charter om grundlæggende rettigheder." Betingelserne for at afslå er meget begrænsede, og det er under alle omstændigheder ikke rimeligt over for hverken borgere eller erhvervslivet, at private virksomheder skal udføre kontrolforanstaltninger som burde være tillagt domstole eller andre uafhængige myndigheder.

Endvidere giver forordningsforslagets betragtning 46 et betydeligt incitament til altid til 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.

IT-Politisk Forening er opmærksom på, at procedurerne for aftaler om gensidig retshjælp ofte stammer fra en tid, hvor der var et mere begrænset behov for dette samarbejde på tværs af landegrænser, og hvor borgerne ikke i stor stil benyttede udenlandske tjenesteudbydere på internettet til elektronisk kommunikation, nethandel eller andre online services. Svaret på disse udfordringer bør imidlertid være en grundlæggende reform af systemet for gensidig retshjælp med henblik på at effektivisere arbejdsgangene, gerne via internationale konventioner i et forum som Europarådets Cybercrime-konvention.

Hvis man tillader efterforskningsmyndigheder at arbejde ekstraterritorialt, som forordningsforslaget gør omend begrænset til inden for den Europæiske Union, kan det have stærkt negative konsekvenser for borgernes retssikkerhed. En vigtig opgave for en stat er at beskytte dens borgere mod udenlandske stater. Den bedste måde til at sikre dette er samarbejde mellem nationale og udenlandske efterforskningsmyndigheder, når sidstnævnte vil indlede en strafferetlig efterforskning mod statens borgere, og krav om dobbelt strafbarhed.

Inden for EU giver den europæiske efterforskningskendelse mulighed for en mere effektiv procedure end aftaler gensidig retshjælp, men fuldbyrdelsesmyndigheden har stadig en væsentlig rolle for at sikre borgerens retssikkerhed. Direktivet om den europæiske efterforskningskendelse er fra 2014, og da de fleste EU-lande har gennemført direktivet inden for det seneste år (andet halvår af 2017 og frem), kan der på nuværende tidspunkt kun være begrænsede erfaringer med den europæiske efterforskningskendelse. Alene af den grund virker det forhastet, at EU-Kommissionen allerede nu fremsætter et meget vidtgående forslag, som indebærer at efterforskningsmyndigheder kan udstede editionskendelser direkte til private virksomheder i andre EU-medlemsstater.

Forslaget er endvidere forhastet, fordi der i komitéen for Europarådets cybercrime-konvention (T-CY) er igangværende overvejelser om en tillægsprotokol om adgang til elektroniske oplysninger hos cloud-tjenester. Udover problemet med overlap mellem de to instrumenter, kan EU-Kommissionens forordningsforslag risikere at fremme en udvikling for den kommende T-CY tillægsprotokol, hvor efterforskningsmyndigheder får tillagt

ekstraterritoriale beføjelser over for private tjenesteudbydere ikke bare inden for den Europæiske Unions område, men for det store antal stater (mere end 50) som deltager i Cybercrime-konventionen, hvoraf flere stater må siges at have alvorlige problemer med menneskerettighederne.

Den stigende brug af elektroniske kommunikationstjenester, sociale medier og cloud-tjenester på internettet skaber givetvis et behov for at modernisere reglerne for efterforskningsmyndigheders adgang til oplysninger og "strafforfølgelse i cyberspace". Naturligvis skal kriminelle ikke kunne undslå sig straf, fordi relevant bevismateriale befinder sig på servere i en anden stats territorium, eller måske ligefrem bevidst er placeret der for at vanskeliggøre en efterforskning.

Men den stigende brug af internettet skaber samtidig en kraftigt forøget risiko for at en stats borgere uretmæssigt kan komme i søgelyset for efterforskningsmyndigheder i andre stater, og at borgerne i den forbindelse kan blive udsat for indgribende efterforskningsmetoder, for eksempel politiets adgang til deres private kommunikation. Det kan ske på grund af fejltagelser ved navnesammenfald, forskelle i retsgarantier og retsplejelov mellem stater (grundlaget for at en efterforskning kan indledes), eller fordi bestemte handlinger kan være lovlige i et land men strafbare i andre lande. Selv inden for den Europæiske Union er der ikke en fuldharmonisering af hvad der udgør strafbare forhold (eller politisk ønske om dette). Eksempelvis er ytringer om Holocaust-benægtelser lovlige i Danmark, men strafbare i visse EU-lande, i nogle tilfælde endda med en strafferamme på tre år eller mere.

Betingelser for udstedelse af editionskendelsen

Der er to parallelle sæt af krav. Det skal være muligt for efterforskningsmyndigheden at udstede en editionskendelse for en tilsvarende national efterforskning. Derudover er der et kriminalitetskrav for adgang til transaktionsdata og indholdsdata, hvor hovedreglen er en strafferamme på tre år eller mere, suppleret med en række specifikke lovovertrædelser uden krav om strafferamme på mindst tre år. For abonnement- og adgangsdata er der ikke yderligere krav udover at editionskendelsen skal være

mulig i en tilsvarende national strafferetlig efterforskning.

Der er ikke, som i direktivet om den europæiske efterforskningskendelse (for visse efterforsknings-foranstaltninger), krav om at den pågældende efterforskningsforanstaltning skal være tilladt i den modtagende medlemsstat. Borgere, der eksempelvis benytter en svensk email-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 mildere krav for adgangen til indholdet af elektronisk kommunikation.

Det skaber en betydelig usikkerhed for borgernes retssikkerhed. Det skaber også en risiko for forumshopping i forbindelse med internationale efterforskninger, hvor udstedelse af editionskendelser overlades til efterforskningsmyndigheder i den medlemsstat, som har den mest omfattende mulighed for adgang til indholdet af elektronisk kommunikation, som er lagret hos en tjenesteudbyder (forordningsforslaget omfatter ikke decideret aflytning eller fremadrettet indsamling af oplysninger, som tjenesteudbyderen ikke under normale omstændigheder ville lagre i sine systemer).

Kategorier af data og betingelser for udlevering

Forordningsforslaget introducerer et nyt begreb "adgangsdata", som har en uklar placering i forhold til den traditionelle opdeling i abonnementdata (stamdataoplysninger om brugeren/kunden), trafikdata og lokaliseringsdata (metadata for elektronisk kommunikation) og indholdsdata.

Fra Kommissionens side synes dette at være et forsøg på at udvide definitionen af abonnementdata, som der er adgang til i alle efterforskninger, men det skaber juridisk usikkerhed, fordi der er en betydelig gråzone mellem især det nye begreb "adgangsdata" og den traditionelle definition af trafikdata i Cybercrime-konventionen og e-databeskyttelsesdirektivet (samt definitionen af metadata i den foreslåede e-databeskyttelsesforordning 2017/0003 (COD)).

For abonnement- og adgangsdata fastsætter forordningsforslaget ingen materielle betingelser for udlevering. Det er tvivlsomt, om det i alle situationer er i overensstemmelse med EU-retten og retspraksis fra den Europæiske Menneskerettighedsdomstol (EMD). Identifikation af brugeren af en dynamisk IP-adresse vil generelt kræve behandling af trafikdata, og måske endda trafikdata som tjenesteudbyderen alene er i besiddelse af på grund af national lovgivning om logning. En sådan lovgivning (om logning) udgør efter præmisserne i Tele2-dommen (de forenede sager C-203/15 og C-698/15 ved EU-Domstolen) et særligt alvorligt indgreb i rettigheder sikret af e-databeskyttelsesdirektivet, og såvel lagringskravet (der ikke må være generel og udifferentieret, men skal være målrettet) som adgangen til de lagrede oplysninger skal overholde artikel 15, stk. 1 i e-databeskyttelsesdirektivet. Det indebærer blandt andet, jf. Tele2-dommens præmisser, at der kun kan gives adgang til de lagrede oplysninger i sager om alvorlig kriminalitet, og at der skal ske en forhåndsgodkendelse af en dommer eller en uafhængig administrativ myndighed.

Forordningsforslaget indebærer, at en anklager kan udstede en editionskendelse om adgang til abonnement- og adgangsdata, uden krav om forudgående kontrol af en domstol eller en uafhængig administrativ myndighed. Selv hvis der er tale om en adgang til abonnementdata, som falder uden for e-databeskyttelsesdirektivet og de skærpede betingelser i Tele2-dommens præmisser, vil denne udstedelsesbeføjelse til en anklager næppe være forenelig med præmisserne i EMD-dommen Benedik v Slovenia, sag nr. 62357/14, af 24. april 2018.

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, og i betragtning 55 anføres det, at "fremlæggelse af indholdsdata vedrørende en udefineret gruppe af personer i et geografisk område eller uden tilknytning til en konkret straffesag" ikke er i overensstemmelse med betingelserne for en europæiske efterforskningskendelse. Men alene indholdsdata nævnes i denne sammenhæng i betragtning 55.

Hvis der er tale om trafikdata hos en tjenesteudbyder omfattet af e-databeskyttelsesdirektivet, stiller præmis 119 i Tele2-dommen mere specifikke krav for adgangen til de lagrede oplysninger. Som udgangspunkt tillader præmis 119 kun adgang til lagrede oplysninger "vedrørende personer, der er mistænkt for at planlægge, ville begå eller have begået en alvorlig lovovertrædelse eller på en eller anden måde være involveret i en sådan lovovertrædelse".

Indholdet af borgernes elektronisk kommunikation er i mange tilfælde lagret hos tjenesteudbydere, for eksempel email-tjenester. Forordningsforslaget bør fastsætte præcise betingelser (mere præcise end betragtning 55) for hvilke personers elektroniske kommunikation, som efterforskningsmyndighederne kan få udleveret. Det samme gælder metadata for denne kommunikation, som i mange tilfælde kan være lige så afslørende, eller endda mere afslørende, end selve indholdet af kommunikation.

Det er ikke tilstrækkeligt, at sådanne begrænsninger kan være fastsat i national lovgivning i den udstedende medlemsstat. Når EU-retten (som med dette forordningsforslag) giver efterforskningsmyndigheder beføjelser i andre medlemsstater, bør EU-retten også fastsætte de nødvendige begrænsninger for disse beføjelser af hensyn til borgernes grundlæggende rettigheder.

Lovkonflikter med andre stater

Fordi der via det tilhørende direktivforslag stilles krav om, at tjenesteudbydere fra tredjelande der udbyder deres tjenester i en eller flere EU-medlemsstater udnævner en retlig repræsentant inden for EU, kommer forordningsforslaget om den europæiske editionskendelse til at have virkning for tjenesteudbydere i hele verden. De europæiske efterforskningsmyndigheder kan udstede editionskendelser vedrørende alle brugere hos disse tjenesteudbydere uanset brugerens hjemland (der måske er ukendt), hvis disse brugere på en eller anden måde indgår i en strafferetlig efterforskning i det pågældende EU-land.

Det skaber en risiko for lovkonflikter, hvor en

efterforskningsmyndighed i en EU-medlemsstat kan have ret til at udstede en editionskendelse, men hvor tjenesteudbyderen efter lovgivningen i det land hvor tjenesteudbyderen er hjemhørende ikke må udlevere oplysningerne, eller mere sandsynligt ikke må udlevere oplysningerne uden en dommerkendelse fra en domstol i tjenesteudbyderens hjemland. Et eksempel på dette kunne være indholdet af elektronisk kommunikation, som opbevares af en tjenesteudbyder i USA (hvor ECPA kræver en amerikansk dommerkendelse for adgang til indholdsdata). 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, men det er uklart, om det er tilstrækkeligt. Derudover er det overladt til modtageren af editionskendelsen, altså en privat tjenesteudbyder eller dennes retlige repræsentant, at gøre indsigelse mod kendelsen for at undgå eventuelle lovkonflikter.

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 som at artikel 15 og 16 ikke vil kunne anvendes for tjenesteudbydere der er hjemhørende inden for EU, for eksempel en dansk tjenesteudbyder, der har udnævnt en retlig repræsentant i en anden EU-medlemsstat, og hvor udlevering af de pågældende oplysninger via en europæisk editionskendelse uden om danske myndigheder kunne være i strid med dansk lov. IT-Politisk Forening har ikke overblik over, om en sådan situation vil kunne opstå for Danmarks vedkommende.

Konsekvenser for danske borgere

Danmark er på grund af retsforbeholdet ikke omfattet af forordningsforslaget, og dansk politi vil således ikke få gavn af den europæiske editions- og sikringskendelse, medmindre der er tale om situationer hvor dansk politi deltager i en international efterforskning sammen med efterforskningsmyndigheder i andre EU-medlemsstater.

Danmarks retsforbehold udelukker imidlertid ikke, 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.

For det første kan danske borgere benytte tjenesteudbydere uden for Danmark. I dag kan disse borgeres oplysninger udleveres efter lovgivningen i det land, hvor tjenesteudbyderen er hjemhørende eller via den europæiske efterforskningskendelse. Fremover vil efterforskningsmyndigheder i alle EU-medlemsstater (som deltager i det retlige samarbejde) kunne få adgang uden at involvere myndighederne i den medlemsstat, hvor tjenesteudbyderens er hjemhørende.

For det andet kan en tjenesteudbyder, som er hjemhørende 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. Det fremgår af direktivforslaget vedrørende retlige repræsentanter. 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, inklusiv 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.

B. Direktivforslaget om udpegning af retlige repræsentanter

Efter direktivforslaget skal medlemstaterne sikre, at tjenesteudbydere som er etableret i medlemsstaten og udbyder tjenester i EU, udpeger mindst én retlig repræsentant i EU til modtagelse, overholdelse og håndhævelse af afgørelser og kendelser udstedt af medlemsstaternes kompetente myndigheder med henblik på indsamling af bevismateriale i straffesager (artikel 3, stk. 1).

For tjenesteudbydere, som ikke er etableret i EU, skal medlemsstaterne sikre, at der udpeges en retlig repræsentant inden for EU, hvis tjenesteudbyderen udbyder tjenester i EU (artikel 3, stk. 2).

For de fleste tjenesteudbydere vil det være tilstrækkeligt med én retlig repræsentant i EU, og tjenesteudbydere hjemhørende i EU kan normalt opfylde direktivets krav ved at udpege en retlig repræsentant i deres hjemland. Det gælder imidlertid ikke for Danmarks vedkommende på grund af retsforholdet.

For så vidt angår modtagelse m.v. af afgørelser og kendelser vedrørende indsamling af bevismateriale i straffesager under instrumenter, som er vedtaget i henhold til afsnit V, kapitel 4 i traktaten om Den Europæiske Unions funktionsmåde (TEUF), skal medlemsstater som deltager i disse retlige instrumenter sikre, at tjenesteudbydere som udbyder tjenester på deres område udpeger en retlig repræsentant i en af de medlemsstater, som deltager i de pågældende retlige instrumenter (direktivforslagets artikel 3, stk. 3).

Dette krav vil ramme tjenesteudbydere med hjemsted i Danmark i forhold til den europæiske editionskendelse (hvor hjemlen er artikel 82 i TEUF afsnit V, kapitel 4), hvis den danske tjenesteudbyder udbyder tjenester i EU-lande som deltager i det retlige samarbejde. Den danske tjenesteudbyder vil i henhold til direktivforslaget (mere præcist den lovmæssige gennemførelse i de EU-lande, hvor der udbydes tjenester) være forpligtet til at udnævne en retlig repræsentant uden for Danmark.

Det fremgår af de indledende bemærkninger til direktivforslaget (side 7 om byrder og rettigheder for virksomheder og 10 om den "variable geometri" for det strafferetlige område i EU) at formålet med disse krav er at sikre, at efterforskningsmyndigheder i EU-medlemsstater som deltager i det retlige samarbejde (instrumenter under TEUF afsnit V, kapitel 4) vil kunne udstede europæiske editionskendelser m.v. til alle tjenesteudbydere, der udbyder tjenester på deres område, uanset hvor disse tjenesteudbydere er etableret.

I forhold til det indre marked giver dette krav danske

tjenesteudbydere en vis konkurrencemæssig ulempe, da de modsat tjenesteudbydere i andre EU-lande ikke nødvendigvis kan nøjes med at udpege en retlig repræsentant i deres hjemland (i dette tilfælde Danmark). Særligt for mindre danske tjenesteudbydere, der opererer i det digitale indre marked, kan det være en væsentlig administrativ ulempe. Det ligger dog uden for IT-Politisk Forenings naturlige arbejdsområde at vurdere omfanget af denne ulempe.

Derudover betyder kravet i direktivforslagets artikel 3, stk. 3, at efterforskningsmyndigheder i andre EU-lande vil kunne få adgang til personoplysninger og lagret indhold af elektronisk kommunikation for danske borgere der er kunder hos danske tjenesteudbydere uden at involvere danske myndigheder. Den mulighed vil foreligge, hvis den danske tjenesteudbyder udbyder tjenester i andre EU-lande end Danmark, hvilket generelt må forventes i mange tilfælde.

Definitionen af "udbyder tjenester" i direktivforslaget kræver dog en "væsentlig tilknytning" til de øvrige EU-lande, hvilket nærmere uddybes i direktivforslagets præambelbetragtninger (målrettet markedsføring mod et bestemt EU-land vil bl.a. udgøre en væsentlig tilknytning til dette EU-land). Det vil næppe ramme danske teleselskaber, der må antages kun at udbyde tjenester i Danmark, men for mange andre udbydere af elektroniske kommunikationstjenester og informationssamfunds-tjenester er EU, ikke Danmark, det naturlige marked.

Efter artikel 3, stk. 7 i direktivforslaget skal dansk lov sikre, at tjenesteudbydere i Danmark giver deres retlige repræsentanter de nødvendige ressourcer og beføjelser til at efterleve afgørelser og kendelser. IT-Politisk Forening fortolker dette som et krav om, at dansk lov trods retsforbeholdet skal sikre, at en dansk tjenesteudbyder kan udlevere de nødvendige oplysninger om danske borgere til en retlig repræsentant uden for Danmark med henblik på at den retlige repræsentant kan efterleve eksempelvis en europæisk editionskendelse fra efterforskningsmyndigheder i en EU-medlemsstat, der deltager i det retlige samarbejde (altså alle øvrige EU-lande undtagen muligvis Storbritannien og Irland).

Hvis en dansk tjenesteudbyder begynder at udbyde

tjenester i Tyskland og udpeger en retlig repræsentant i eksempelvis Tyskland (det mest logiske i situationen), vil konsekvensen af samspillet mellem forordningsforslaget og direktivforslaget være, at efterforskningsmyndigheder i bl.a. Polen og Ungarn kan udstede editionskendelser vedrørende danske borgere, som den danske tjenesteudbyder via den retlige repræsentant i Tyskland er forpligtet til at efterleve. Med den aktuelle retsstats-situation i Polen og Ungarn vil mange formentlig anse dette scenarie som stærkt uønsket.

Det grundlæggende problem er at forordningsforslaget om den europæiske editionskendelse giver efterforskningsmyndigheder mulighed for at operere direkte i andre EU-lande ved at udstede bindende editionskendelser til tjenesteudbydere uden at involvere myndighederne i modtagerlandet.

Hvis der var en automatisk involvering af myndighederne i tjenesteudbyderens hjemland, som hvis den europæiske efterforskningskendelse blev benyttet som instrumentet til at sikre adgang til de ønskede oplysninger i forbindelse med efterforskningen, ville det være muligt at fastsætte passende bestemmelser i lovgivningen for at beskytte borgernes retssikkerhed og grundlæggende rettigheder. Der vil også kunne indbygges passende "sikkerhedsventiler", som tager højde for den aktuelle situation vedrørende Polen og Ungarn, og eventuelle lignende problemer som måtte opstå i fremtiden for andre EU-medlemsstater. Sådanne retsgarantier kan i sagens natur ikke være til stede, når det som med forordningsforslaget om den europæiske editions- og sikringskendelse overlades til private tjenesteudbydere at værne om borgernes retssikkerhed og grundlæggende rettigheder.

Advokatrådet

ADVOKAT SAMFUNDET

Justitsministeriet
Slotsholmsgade 10
1216 København K

KRONPRINSESSEGADE 28
1306 KØBENHAVN K
TLF. 33 96 97 98

DATO: 4. juli 2018
SAGSNR.: 2018 - 1596
ID NR.: 535104

e-mail: jm@jm.dk + veg@jm.dk

Høring over Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om europæiske editions- og sikringskendelser om elektronisk bevismateriale i straffesager samt Europa-Kommissionens forslag til Europa-Parlamentets og Rådets direktiv om harmoniserede regler for udpegning af retlige repræsentanter med henblik på indsamling af bevismateriale

Ved e-mail af 15. juni 2018 har Justitsministeriet anmodet om Advokatrådets bemærkninger til ovennævnte forslag.

The Council of Bars and Law Societies of Europe (CCBE), som er sammenslutningen af advokatråd i Europa, har afgivet vedlagte høringssvar vedrørende forslagene, som Advokatrådet kan henholde sig til.

Med venlig hilsen

Torben Jensen

CCBE Preliminary comments on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters

The Council of Bars and Law Societies of Europe (CCBE) represents the bars and law societies of 45 countries, and through them more than 1 million European lawyers. The CCBE regularly responds on behalf of its members on policy issues which affect European citizens and lawyers.

On 14 April 2018, the European Commission published a proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters.

The CCBE welcomes that the Commission took into account various aspects which the CCBE suggested during the preceding consultation process. With this paper, the CCBE wishes to share its initial observations in relation to a number of aspects of the proposal. A more detailed position paper will follow in due course.

The key question arising from this legislative initiative is whether the proposal to enhance the powers to access electronic evidence across national borders by investigating authorities is coupled with sufficient procedural safeguards and due process procedures. In other words, are there any aspects that could undermine fair trial rights, and, if so, how might these aspects be addressed?

There are three core issues within which most of the detailed observations sit:

1. The provision of an effective mechanism which ensures the protection of lawyer-client communications. This raises in particular the following issues:
   (a) Upon which persons should the Orders be served?
   (b) How far is judicial scrutiny of applications necessary?
   (c) How can the effectiveness of such scrutiny be secured?
   (d) Do the proposed grounds for refusal need to be supplemented?
   (e) Do the provisions for notification require to be supplemented?
2. Ensuring equality of arms between the prosecution and the defence.
3. Provision of effective judicial review

The discussion below contains certain preliminary observations on these and other matters. It is accepted that these observations are likely to be the first step in a dynamic and collaborative process in addressing the text of the Proposal in the course of the legislative process, and should be seen as a preliminary document. The CCBE will present fuller and more detailed observations as the legislative process proceeds.

1. Protection of confidentiality of lawyer-client communication

For lawyers to be effective in defending their clients' rights, there must be confidence that communications between a client and their lawyer are kept confidential. This principle – usually referred to as 'professional secrecy' or 'legal professional privilege' – is recognised by all EU countries and has been upheld by the European Court of Justice and the European Court of Human Rights in numerous cases. The violation of professional secrecy constitutes in some EU Member States not only a violation of a professional duty, but also a criminal offence.

Material which is potentially privileged will enjoy the heightened protection of article 8 of the European Convention on Human Rights (ECHR). Additionally, lawyer-client communications in relation to

contentious proceedings (criminal or civil litigation) also enjoy protection under Article 6 ECHR concerning the right to a fair trial. Article 6 rights (unlike article 8 rights) are absolute in the sense that limitations or derogations cannot be applied.

Addressees of European Production Orders

When responding to the public consultation on e-evidence, the CCBE stressed that when a production order is enforced, an organisation should be notified, allowed to assess its legal rights and obligations, and if possible, be able to challenge the request before any data can be seized.

This entails that requests for access to digital evidence should, whenever possible, always be addressed to the data controllers, rather than the data processors, which, especially when the data is controlled by a law firm, would provide better safeguards against any unlawful sharing of privileged information. Data processors, or other intermediaries, would have no information on many important aspects of the context of the data which has been sought, and therefore would not always be in a position to assess the lawfulness of the request, or any further legal requirements that would need to be fulfilled.

The proposed Regulation makes clear in **Article 5(6)** that, where a European Production Order (EPO) targets the data of an enterprise, the data should be sought in the first instance from that enterprise, unless doing so would undermine the investigation.

This safeguard is important since data controllers are generally in the best position to review and assert any rights that attach to the electronic evidence they are requested to hand over.

Law firms are covered by this provision and should therefore be directly addressed so that they are in a position to assess the legal requirements for fulfilling such data requests, including the fact whether the data requested is subject to professional secrecy/legal professional privilege. This exemption is therefore especially critical in cases where the requested data is held by a law firm.

The CCBE is however concerned about the very general wording, which provides law enforcement authorities with a very wide leeway to still circumvent data controllers. Furthermore, this article only applies to enterprises, whereas in most jurisdictions sole practitioners (who make up the vast majority of European law practices) are not considered legal persons. Sole practitioner lawyers who are natural persons would thus not be subject to the same protection as law firms. The term 'regulated professionals' should therefore be added. Regardless of how a practice is organised (single practitioner or law firm), professional secrecy must always be protected and all safeguards have to be fulfilled to this effect,

European Production Orders covering privileged information must not be issued nor executed

Another key issue is that data of which the requesting authority knows, or ought to have known, is protected by obligations of professional secrecy/legal professional privilege under the law of the issuing and/or executing State is exempted from the scope of the legislative instrument.

Article 5(7) sets out that in case there are reasons to believe that the requested data is covered by professional secrecy, clarification has to be sought by contacting the relevant authorities before proceeding with the request. If it is covered by professional secrecy obligations, the EPO must not be issued.

The question however arises how law enforcement authorities (LEAs) can determine who is a lawyer, especially if it is a lawyer in another Member State. Some technical measures seem to be required to ensure that both LEAs and service providers know that data is held by lawyers (as well as some verification of lawyers' identity). A pragmatic way would be to require service providers to offer lawyers an option for indicating such information – of course, only after careful verification as to whether that user is indeed a lawyer, as claimed.

In this respect, the CCBE could assist in creating a mechanism to identify lawyers on the basis of the prototype tool developed under the FAL2 project for the identification of lawyers. This tool (which is also being used in the context of the e-CODEX system) could be tailored for this specific purpose.

Furthermore, although professional secrecy/legal professional privilege is a ground to refuse judicial validation (and has to be taken into account during a criminal trial – see Article 18), it is not an explicit ground for refusal to execute an EPO. It needs therefore to be specified in Article 9 that the fact that the requested data is covered by professional secrecy/legal professional privilege constitutes a valid ground to refuse the execution of an EPO. Also, on the form (in the Annex), an additional box should be added on professional secrecy as a reason to refuse the execution of an EPO.

2. Judicial validation

According to the CCBE, judicial validation by the requesting state is the minimum protection that needs to be ensured, especially given the fact that the order will no longer be cross-checked by the authority in the requested country (as is the case with mutual legal assistance (MLA) procedures).

There appears to be no proper justification why EPO's for subscriber and access data in general do not require judicial validation. It needs to be set out more clearly what type of data is considered 'subscriber or access data' in order to avoid the seizure of information which would normally require independent judicial oversight in accordance with national rules, MLA procedures, or the European Investigation Order (EIO). For example, IP addresses or interfaces do fall into more than one category, i.e. access data and subscriber data (**Article 2 (7) (b)**). Also, the definition of subscriber data includes not only what is usually understood under subscriber data (see Article 2 (7)(a)), but also very generic terms such as "the type of service [...] including technical data and data identifying related technical measures or interfaces [...] and data related to the validation of the use of service" (Article 2 (7) (b)). These wide terms could even include data that is not related to the usual meaning of the term "type of service", like any technical characteristics of the service provided, thus blurring the distinction between access data and subscriber data. Considering also that the new proposed e-Privacy regulation[1] uses yet another type of classification (electronic communications content and metadata), and also considering that the currently effective e-Privacy Directive[2] uses yet another definition of traffic data for roughly the same purposes, it would be very important to limit the number of such terms to the minimum necessary.

It is important to clarify that professional secrecy/legal professional privilege can cover not only content data, but also other types of data, e.g. access data, and in such cases, judicial validation and oversight is required.

If the Regulation does not provide absolute certainty about what types of data fall into the various data categories, LEAs will not know whether they need judicial validation, and addressees will not be able to assess whether EPOs have been lawfully issued.

3. Sufficient degree of suspicion

The conditions for issuing a European Production or Preservation Order do not include any threshold of a sufficient degree of suspicion (Article 5). **In order to avoid abuses, EPO's must only be validated by the relevant authorities if there are compelling reasons giving rise to a sufficient degree of suspicion to justify the cross-border seizure of data.**

4. Effective mechanism for ensuring approval

[1] Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.
[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

If the rules for approval are to be effective, there is a need for the opportunity, where appropriate, for there to be participation in the proceedings of a person who is aware of matters such as whether the evidence is likely to be covered by lawyer-client confidentiality. Normally that would be the data controller (in line with the above observations). It is appreciated that this might not always be appropriate, especially where there is a risk of destruction of the evidence. **In such cases, consideration should be given to having a two-stage process where a European Preservation Order might be used to secure the evidence before any contested application for a Production Order.**

5. Grounds for refusal to execute

The CCBE considers that the grounds for refusal to execute an EPO set out in **Article 9(5)** are too restrictive. Apart from technical or practical reasons (e.g. the EPO Certificate (EPOC) is incomplete or the addressee cannot comply because of *force majeur*), the only substantive ground for non-execution that may be invoked by the addressee is that if it considers that "based on the sole information contained in the EPOC it is apparent that it *manifestly* violates the Charter of Fundamental Rights of the European Union or that it is *manifestly* abusive". **There should be more broader grounds to refuse the execution of an EPO, including the absence of double criminality or, as pointed out above, the fact that the requested data is covered by professional secrecy/legal professional privilege. As to contentious proceedings (criminal or civil litigation) *any* violation of professional secrecy/legal professional privilege is per se a violation of the right to a fair trial according to Article 6 ECHR and should as such be recognised as a sole and sufficient ground to refuse the execution of an EPO.**

6. Notification of the data subject

Article 11(2) specifies that the person whose data is being sought needs to be informed "without undue delay about the data production". However, this "may be delayed as long as necessary and proportionate to avoid obstruction of the criminal proceeding". The notification requirement can therefore very easily be ignored by authorities since there is always a reason to find why it could jeopardise the investigation.

This severely undermines people's fair trial rights because as long as they are not aware that their data has been taken, they cannot assert their rights. **The imposition of confidentiality restrictions on EPOs must therefore be subject to the approval of an independent judicial authority and in each case be duly motivated and justified by the issuing authority on the basis of meaningful and documented assessments.**

7. The rights of the defence

Any proposal for the recovery of electronic evidence should not be seen as solely concerned with prosecution. Rights of defence should be given proper regard. The proposal does not take properly into account the requirement for equality of arms in criminal proceedings, which is a concept recognised by the European Court of Human Rights in the context of the right to a fair trial. Whereas prosecutors can issue production and preservation orders, no provisions exist enabling defendants or their representatives to access or request electronic evidence.

The CCBE therefore considers that, as with the EIO, suspected or accused persons, or their lawyers should be able to request the issuing of a European Production or Preservation Order in an equally efficient way as prosecutors can. If not, the proposal undermines the principle of equality of arms between the prosecution and defence, placing the defendant at a significant disadvantage.

Moreover, the proposal does not provide any requirement or guidance for addressees to limit the transmission of e-evidence to data that is relevant for the purposes of the criminal investigation. As a result, LEAs could be overwhelmed with data. There is also no provision to ensure that defendants do not in turn become over-burdened under the weight of the e-evidence, or that such e-evidence will get

appropriate metadata such as an index and table of contents. Without the help of such metadata, it is very difficult or even impossible for lawyers to assert effectively their clients' rights.

8. **Judicial Review**

Consideration should be given to the provision of an effective means of judicial review analogous to the mechanism foreseen in article 42 of the Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office, particularly in relation to the jurisdiction of the Court of Justice in accordance with Article 267 of the Treaty on the Functioning of the European Union.

Sofie Anne Marner

Fra:	1 - ERST EU-høringer <eu-hoering@erst.dk>
Sendt:	9. juli 2018 16:57
Til:	Viktoria Egsgaard
Cc:	FP Let byrder i EU; Cagdas Citirikkaya; Bjarke Thorbjørn Petersen; Morten Vestergaard Hansen; Caroline Møller Nielsen; Ida Kirstine Andersen Boe; Sara Marie Larsen; Marie Agerbæk Iversen
Emne:	Høringssvar - udkast til grund- og nærhedsnotat om EU-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om europæiske editions- og sikringskendelser om elektronisk bevismateriale (KOM(2018) 225 endelig) og udkast til (KOM(2018) 226

Høringssvar vedrørende udkast til grund- og nærhedsnotat om EU-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om europæiske editions- og sikringskendelser om elektronisk bevismateriale (KOM(2018) 225 endelig) og udkast til direktiv (KOM(2018) 226

Erhvervsstyrelsens Team Effektiv Regulering (TER) har modtaget ovennævnte forordningsforslag og direktivforslag med dertilhørende grund- og nærhedsnotat i høring.

TER har følgende bemærkninger om de administrative konsekvenser.

Udkast til grund- og nærhedsnotat om EU-Kommissionens forslag til Europa-Parlamentets og Rådets direktiv om harmoniserede regler for udpegning af retlige repræsentanter med henblik på indsamling af bevismateriale i straffesager (KOM(2018) 226 endelig).

TER vurderer, at direktivforslaget potentielt medfører væsentlige administrative byrder for erhvervslivet. De administrative byrder består i, at medlemsstaterne skal forpligte udbydere af visse elektroniske tjenester, som udbyder tjenester i EU, til at udpege en retlig repræsentant, som skal *modtage*, *overholde* og *håndhæve* afgørelser fra kompetente myndigheder om indsamling af bevismateriale i straffesager på vegne af den pågældende tjenesteudbyder. Udbydere, som er etableret inden for EU og udbyder sine tjenester i EU, vil skulle udpege mindst én retlig repræsentant inden for EU. Repræsentanten vil skulle udpeges i en af de medlemsstater, hvor tjenesteudbyderen udbyder sine ydelser eller er etableret.

Det har ikke været mulig at fremskaffe oplysninger, som kan bidrage til at præcisere omfanget af de administrative byrder, herunder oplysninger om antal omfattede virksomheder (tjenesteudbydere) samt omfanget af krav til den retlige repræsentant. Det er derfor ikke muligt at kvantificere byrderne yderligere.

TER vil i forbindelse med implementering af direktivet foretage nærmere vurdering af de administrative konsekvenser.

Udkast til grund- og nærhedsnotat om EU-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om europæiske editions- og sikringskendelser om elektronisk bevismateriale (KOM(2018) 225 endelig)

Forordningsforslaget indfører pålæg om udlevering og sikring af elektronisk bevismateriale, der er lagret af en tjenesteudbyder, der udbyder sine tjenester i EU.

Forordningsforslaget er omfattet af det danske retsforbehold og har derfor i sig selv ikke 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. TER vurderer på den baggrund, at en vedtagelse af forordningsforslaget sammenholdt med en vedtagelse af direktivforslaget kan medføre administrative byrder for

erhvervslivet. Det har ikke været mulig at fremskaffe oplysninger, som kan bidrage til at præcisere omfanget af de potentielle administrative byrder.

Kontakt
Marie Agerbæk Iversen
Specialkonsulent
Tlf. direkte 35291053
E-post MarAge@erst.dk

Erhvervsstyrelsen har ikke yderligere bemærkninger.

Mvh
Mette Godiksen,
Erhvervsstyrelsens EU-Koordination

Fra: FP Let byrder i EU
Sendt: 6. juli 2018 13:51
Til: veg@jm.dk
Cc: Marie Agerbæk Iversen <MarIve@erst.dk>; Cagdas Citirikkaya <CagCit@erst.dk>; Malene Loftager Mundt <MalMun@erst.dk>; FP Let byrder i EU <Letbyrder-i-EU@erst.dk>
Emne: TER vurdering af adm. konsekvenser - Forordningsforslag om europæiske editions- og sikringskendelser om elektronisk bevismateriale i straffesager, COM(2018) 225, og direktivforslag om harmoniserede regler for udpegning af retlige repræsentanter, COM(2018)

Kære Viktoria,

TER vil gerne bidrage med vurdering. Jeg har bemærket den oprindelige frist på forslagene d. 6. juli, hvilket er i dag. Da det ikke er muligt for os at afgive svar i dag, håber jeg, at det går an, at vi for så vidt muligt afgiver høringssvar mandag.

Såfremt anden tidsfrist er aktuel, må du endelig lade os det vide via letbyrder-i-eu@erst.dk med Marie Agerbæk Iversen CC.

Med venlig hilsen

Ida Kirstine Andersen Boe
Student

ERHVERVSSTYRELSEN
Effektiv regulering

Dahlerups Pakhus
Langelinie Allé 17
2100 København Ø
Telefon: +45 35291000
Direkte: +45 35291983
E-mail: IdaBoe@erst.dk
www.erhvervsstyrelsen.dk

ERHVERVSMINISTERIET

Fra: Cagdas Citirikkaya
Sendt: 6. juli 2018 08:58
Til: Martin Riis Hansen <MarHan@erst.dk>; FP Let byrder i EU <Letbyrder-i-EU@erst.dk>