



JUSTITSMINISTERIET

Dato: 5. november 2018  
Kontor: Forebyggelseskontoret  
Sagsbeh: Nathalie Bidstrup Nielsen  
Sagsnr.: 2018-6100-0021  
Dok.: 897075

## GRUND- OG NÆRHEDSNOTAT

### Forslag til Europa-Parlamentets og Rådets forordning om forebyggelse af udbredelsen af terrorrelateret online-indhold.

**KOM (2018) 640**

**Nyt notat**

#### 1. Resumé

*Kommissionen har den 12. september 2018 fremsat forslag til Europa-Parlamentets og Rådets forordning om forebyggelse af udbredelsen af terrorrelateret online-indhold. Forslaget er fremsat i en samlet sikkerhedspakke bestående af tre initiativer, der har til formål at styrke de redskaber, som EU giver de nationale retshåndhævende myndigheder for at bekæmpe terrorisme og grænseoverskridende kriminalitet. Forslaget har til formål at skabe en klar og harmoniseret retlig ramme til at forebygge misbrug af hostingtjenester, herunder bl.a. online platforme, hvor udbredelse af terrorrelateret indhold på nettet finder sted med henblik på at garantere et velfungerende digitalt indre marked. Forslaget har en indre markeds hjemmel og er derfor ikke omfattet af retsforbeholdet. Det vurderes, at en vedtagelse af forslaget vil have visse økonomiske konsekvenser for Danmark. På det foreliggende grundlag vurderes forslaget at være i overensstemmelse med nærhedsprincippet. Der ses ikke at foreligge offentlige tilkendegivelser om de øvrige medlemsstaters holdninger til forslaget. Fra dansk side finder man på nuværende tidspunkt – hvor den igangsatte høring ikke er afsluttet – ikke at burde tage endelig stilling til forslaget. Fra dansk side er man dog foreløbigt overordnet set positiv over for forslaget, der har til formål at styrke og supplere den fælles og frivillige indsats, der allerede er iværksat på EU-niveau i forhold til at bekæmpe mængden af terrorindhold online.*

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)

## 2. Baggrund

Kommissionens formand præsenterede i sin State of the Union-tale den 12. september 2018 en ”sikkerhedspakke” bestående af tre initiativer til at styrke de redskaber, som EU giver de nationale retshåndhævende myndigheder for at bekæmpe terrorisme og grænseoverskridende kriminalitet. Kommissionens forslag til forordning om forebyggelse af udbredelsen af terrorrelateret online-indhold er et af initiativerne.

Forordningsforslaget er fremsat med hjemmel i TEUF artikel 114 om sikring af et velfungerende indre marked og er derfor ikke omfattet af Danmarks forbehold vedrørende retlige og indre anliggender. Forslaget skal behandles efter den almindelige lovgivningsprocedure i TEUF artikel 294, dvs. med Europa-Parlamentet som medlovgiver.

Arbejdet med at bekæmpe udbredelsen af terrorrelateret indhold online er indtil nu sket ved hjælp af frivillige ordninger mellem Kommissionen, medlemsstaterne og en række hostingtjenesteydere, herunder bl.a. Facebook, Google, Twitter og Microsoft, særligt i regi af EU’s internetforum. EU’s internetforum blev etableret af Kommissionen i december 2015 og har til formål at fremme medlemsstaternes og hostingtjenesteydernes frivillige samarbejde og tiltag for effektivt at reducere terrorrelateret onlineindhold og styrke civilsamfundets aktører med henblik på at øge mængden af effektive, alternative budskaber på nettet.

Kommissionen vedtog den 1. marts 2018 en henstilling om effektiv bekæmpelse af ulovligt indhold på internettet<sup>1</sup>, som bygger videre på Kommissionens meddelelse om bekæmpelse af ulovligt indhold på nettet fra september 2017<sup>2</sup>. Baggrunden for henstillingen var, at der ifølge Kommissionen er behov for en øget indsats fra EU’s side på området. Henstillingen indeholder konkrete anbefalinger til, hvordan udbydere af online platforme og medlemsstater kan intensivere arbejdet med bekæmpelse af ulovligt indhold på nettet, herunder særligt terrorrelateret indhold. Kommissionen tilkendegav i forbindelse med vedtagelsen af henstillingen, at man ville overveje behovet for lovgivning på området.

---

<sup>1</sup> Henstilling af 1. marts 2018 om foranstaltninger til effektiv bekæmpelse af ulovligt indhold på nettet (C(2018)1177 final).

<sup>2</sup> Meddelelse af 28. september 2017 om bekæmpelse af ulovligt indhold på nettet (COM(2017) 555 final).

Den 19. juni 2018 fremlagde Frankrig og Tyskland en erklæring om fremtidige tiltag i EU, hvor de to lande bl.a. opfordrede til indførelsen af lovgivning på EU-niveau for at bekæmpe terrorrelateret indhold på nettet. Erklæringen førte til, at medlemsstaternes stats- og regeringschefer på foranledning af Frankrig i DER-konklusioner af 28. juni 2018 bød Kommissionens planer om et lovgivningsforslag om fjernelse af indhold, som tilskynder til had og til at begå terrorhandlinger, velkommen.

Derudover har Europa-Parlamentet i sin beslutning om onlineplatforme og det digitale indre marked af 15. juni 2017 opfordret de pågældende platforme "til at styrke foranstaltninger til bekæmpelse af ulovligt og skadeligt indhold" og opfordret Kommissionen til at fremlægge forslag til løsning af disse problemer.

Forordningsforslaget supplerer de eksisterende frivillige ordninger i regi af EU's internetforum og bygger videre på Kommissionens henstilling om bekæmpelse af ulovligt indhold på nettet fra marts 2018. Derudover supplerer forordningen de eksisterende regler på EU-niveau om bekæmpelse af ulovligt indhold på nettet, herunder det fremtidige direktiv om audiovisuelle medietjenester.

Forhandlingerne om forordningsforslaget blev indledt den 25. september 2018 på arbejdsgruppeniveau i Rådet. Det østrigske formandskab og Kommissionen har lagt op til en intens forhandlingsproces med henblik på, at forslaget kan vedtages inden det kommende valg til Europa-Parlamentet i maj 2019.

Forslaget er oversendt til Rådet i dansk sprogversion den 1. oktober 2018.

### **3. Formål og indhold**

#### **3.1 Forslaget generelt**

Formålet med forordningsforslaget er at skabe en klar og harmoniseret retlig ramme til at forebygge misbrug af hostingtjenester til udbredelse af terrorrelateret indhold på internettet med henblik på at garantere et velfungerende digitalt indre marked.

Forordningsforslaget omfatter alle hostingtjenesteydere, som udbyder tjenester i EU, uanset om tjenesteyderen er etableret i eller uden for EU. Baggrunden for også at omfatte hostingtjenesteydere, der er etableret uden

for Unionen, men som udbyder tjenester inden for Unionen, er, at en betydelig del af de hostingtjenesteydere, der eksponeres for terrorindhold på deres tjenester, er etableret i tredjelande.

### 3.2 Nærmere om forslaget centrale elementer

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

I forslaget kapitel 2 er der fastsat regler om rettidig omhu for hostingtjenesteydere, påbud om fjernelse af terrorrelateret indhold, indberetninger, proaktive foranstaltninger og opbevaring af indhold og dertil knyttede data.

I forslaget kapitel 3 er der fastsat regler om hostingtjenesteyderens forpligtelser til gennemsigtighed, fastsættelse af sikkerhedsforanstaltninger vedrørende brug og gennemførelse af proaktive foranstaltninger, klagemekanismer og oplysningspligt over for indholdsleverandøren.

I forslaget kapitel 4 er der fastsat regler om sikring af den eller de nationale kompetente myndigheders kapaciteter og ressourcer, samarbejdet mellem hostingtjenesteydere, nationale kompetente myndigheder og andre relevante EU-organer samt hostingtjenesteyderens etablering af et kontaktpunkt til modtagelse af påbud om fjernelse og indberetninger.

I forslaget kapitel 5 er der fastsat regler om jurisdiktion og udpegning af retlige repræsentanter for hostingtjenesteydere, der ikke er etableret i EU, men udbyder tjenester i EU.

I forslaget kapitel 6 er der fastsat regler om udpegning af kompetente nationale myndigheder, sanktioner samt en række afsluttende bestemmelser om bl.a. Kommissionens delegerede beføjelser, overvågning, rapportering, evaluering og ikrafttræden.

#### *Terrorrelateret indhold*

Begrebet ”terrorrelateret indhold” er i forslaget defineret som en eller flere af følgende oplysninger:

- (a) opfordring til eller slåen til lyd for, herunder forherligelse, udførelse af terrorhandlinger, hvorved der forårsages fare for, at sådanne handlinger begås
- (b) opfordring til at bidrage til terrorhandlinger

- (c) promovering af en terrorgruppes aktiviteter, navnlig ved opfordring til deltagelse i eller støtte til en terrorgruppe i den artikel 2, stk. 3, i direktiv (EU) 2017/541 fastsatte betydning
- (d) instruktioner i metoder eller teknikker til udførelse af terrorhandlinger

Terrorhandlinger er i den forbindelse defineret som handlinger omfattet af artikel 3, stk. 1, i direktiv (EU) 2017/541 af 15. marts 2017 om bekæmpelse af terrorisme.

Udbredelse af terrorrelateret indhold er i forslaget defineret som tilrådighedsstillelse af terrorrelateret indhold til tredjepart via hostingtjenesteyderes tjenester.

### *Omfattede hostingtjenesteydere*

Hostingtjenesteyder er i forslaget defineret som en udbyder af informationssamfundstjenester, som består i oplagring af information fra en tjenestemodtager på dennes anmodning og tilrådighedsstillelse af de lagrede informationer til tredjeparter, uanset om denne aktivitet udelukkende er af teknisk, automatisk eller passiv karakter. Sådanne udbydere af informationssamfundstjenester omfatter eksempelvis sociale medieplatforme, videostreamingtjenester, video-, billed- og lydudlejningstjenester, fildeling og andre cloudtjenester, i det omfang de gør informationerne tilgængelige for tredjepart, og websteder, hvor brugerne kan kommentere og poste anmeldelser.

Forordningen gælder for alle hostingtjenesteydere, som udbyder tjenester i EU, uanset om tjenesteyderen er etableret i eller uden for EU.

Det afgørende for, at der udbydes tjenester i EU, er, at hostingtjenesteyderen gør det muligt for juridiske eller fysiske personer i en eller flere medlemsstater at gøre brug af tjenester fra hostingtjenesteyderen. Den blotte kendsgerning, at en tjenesteyders websted, e-mailadresse eller andre kontaktoplysninger kan tilgås i en eller flere medlemsstater, er dog isoleret set ikke en tilstrækkeligt. Der stilles derfor 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 hostingtjenesteyderen er etableret i EU. For hostingtjenesteydere 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 og varetage kundeservicen på den pågældende medlemsstats sprog, eller ved at udbyde app's i nationale appbutikker.

Hostingtjenesteydere er forpligtet til at etablere kontaktpunkter, som gør det muligt at modtage påbud om fjernelse og indberetninger ad elektronisk vej.

Derudover er hostingtjenesteydere, som ikke er etableret i EU, men som udbyder sine tjenester i Unionen, forpligtet til skriftligt at udpege en juridisk eller fysisk person som sin retlige repræsentant i Unionen med henblik på modtagelse, overholdelse og håndhævelse af påbud om fjernelse, indberetninger, anmodninger og afgørelser udstedt af de kompetente myndigheder. Den retlige repræsentant skal være bosiddende eller etableret i en af de medlemsstater, hvor hostingtjenesteyderen udbyder tjenester, og repræsentanten kan drages til ansvar for manglende overholdelse af forordningens bestemmelser, uden at det berører hostingtjenesteyderens ansvar og de søgsmål, der vil kunne anlægges over for denne.

### *Rettidig omhu*

For at skabe klarhed over det ansvar, der påhviler hostingtjenesteydere, har alle hostingtjenesteydere pligt til at træffe passende, rimelige og forholdsmæssige foranstaltninger under hensyntagen til ytrings- og informationsfriheden med henblik på at sikre, at deres platforme ikke misbruges til at udbrede terrorrelateret indhold. Denne omhu indebærer ikke en generel forpligtelse til overvågning.

Den rettidige omhu indebærer dog, at hostingtjenesteyderne skal handle på en omhyggelig, forholdsmæssig og ikke-diskriminerende måde i respekt for det indhold, de lagrer, navnlig når de gennemfører deres egne vilkår og betingelser, med henblik på at undgå fjernelse af indhold, som ikke er terrorindhold.

### *Pålæg om fjernelse af terrorrelateret indhold*

En kompetent national myndighed, der kan være både administrativ og retlig, kan give hostingtjenesteydere påbud om at fjerne terrorrelateret indhold på deres platforme eller deaktivere adgangen til sådant materiale. Hostingtjenesteyderen skal i givet fald fjerne eller deaktivere adgangen til det pågældende materiale inden for en time efter modtagelse af et påbud om fjernelse. Et påbud skal udformes på en formular, der er indsat som bilag til forslaget, og indeholde en række nærmere definerede oplysninger, herunder

en forklaring på, hvorfor det pågældende indhold betragtes som terrorrelateret og oplysninger om hostingtjenesteyderens og den pågældende indholdsleverandørs klagemuligheder.

### *Indberetninger*

Den kompetente nationale myndighed eller det relevante EU-organ, f.eks. Europol, kan sende en indberetning til en hostingtjenesteyder om oplysninger, som efter den pågældende myndigheds vurdering kan betragtes som terrorindhold, med henblik på, at hostingtjenesteyderen på frivilligt basis overvejer, hvorvidt indholdet er i overensstemmelse med leverandørens egne vilkår og betingelser. Hostingtjenesteyderen skal hurtigt underrette den nationale kompetente myndighed eller det relevante EU-organ om resultatet af sine overvejelser, herunder eventuelle foranstaltninger der træffes som følge af indberetningen og tidsplanen herfor.

### *Proaktive foranstaltninger*

Hostingtjenesteyderne skal iværksætte passende proaktive foranstaltninger ud fra en vurdering af risici og graden af eksponering for terrorindhold samt af konsekvenserne for tredjeparts rettidighed og offentlighedens interesse i oplysningerne. Har hostingtjenesteyderen ikke modtaget påbud om fjernelse og indberetninger vil det være tegn på lav eksponering for terrorindhold. Kravet om proaktive foranstaltninger må ikke indebære en generel forpligtelse til overvågning.

Hvis en kompetent national myndighed har modtaget underretning om, at der over for en hostingtjenesteyder er udstedt påbud om fjernelse af terrorrelateret indhold, skal den anmode hostingtjenesteyderen om inden for tre måneder og derefter mindst én gang årligt at fremlægge en rapport om de specifikke proaktive foranstaltninger, som den pågældende hostingtjenesteyder har iværksat for dels at forebygge, at indhold, der er blevet fjernet, eller hvortil adgangen er blevet deaktiveret, genuploades, dels at spore, identificere og hurtigt fjerne eller deaktivere adgangen til andet terrorrelateret indhold.

Mener den kompetente myndighed, at de proaktive foranstaltninger, som hostingtjenesteyderen har iværksat, er utilstrækkelige, kan den anmode udbyderen om at træffe yderligere proaktive foranstaltninger. Hostingtjenesteyderen skal i den forbindelse samarbejde med den kompetente myndighed om at indkredse, hvilke specifikke foranstaltninger som skal iværksættes.

Lykkes det ikke inden for en periode på 3 måneder for hostingtjenesteyderen og den kompetente myndighed at nå til en aftale om, hvilke specifikke proaktive foranstaltninger, der skal iværksættes, kan den kompetente myndighed udstede en afgørelse, som pålægger hostingtjenesteyderen at træffe særlige yderligere nødvendige og forholdsmæssige proaktive foranstaltninger. I en sådan afgørelse tages der bl.a. højde for især hostingtjenesteyderens økonomiske kapacitet, antallet af påbud om fjernelse og indberetninger og virkningen af sådanne foranstaltninger for brugernes grundlæggende rettigheder og den grundlæggende betydning af ytrings- og informationsfriheden.

Hostingtjenesteyderen kan til enhver tid anmode den kompetente myndighed om at tage anmodninger eller afgørelser om foranstaltninger op til revision og, hvis det er passende, tilbagekalde dem.

#### *Sikkerhedsforanstaltninger og klagemekanismer*

Hostingtjenesteydere, som anvender automatiserede værktøjer, skal have effektive og passende beskyttelsesforanstaltninger, som sikrer, at beslutninger navnlig vedrørende fjernelse eller deaktivering af adgangen til indhold, som anses for ulovligt indhold, er korrekte og velfunderede.

Derudover har hostingtjenesteydere pligt til at indføre effektive og tilgængelige klagemekanismer, som gør det muligt for indholdsleverandører, hvis indhold er blevet fjernet, eller hvor adgangen til indholdet er blevet deaktiveret som følge af en indberetning eller proaktive foranstaltninger, at indgive en klage mod hostingtjenesteyderens handlinger.

Hostingtjenesteydere skal straks undersøge enhver klage, som modtages, og genindsætte indholdet uden unødigt forsinkelse, hvis det uberettiget er blevet fjernet eller deaktiveret og underrette klageren om udfaldet af undersøgelsen.

#### *Samarbejde og jurisdiktioner*

Den medlemsstat, hvor hostingtjenesteyderens hovedsæde befinder sig, har jurisdiktion med henblik på anmodninger og afgørelser om proaktive foranstaltninger, økonomiske sanktioner og overvågning. En hostingtjenesteyder, hvis hovedsæde ikke befinder sig i en medlemsstat, anses for at høre under den medlemsstats jurisdiktion, hvor den af hostingtjenesteyderen udpegede retlige repræsentant er bosiddende eller etableret.



I tilfælde af at en myndighed i en anden medlemsstat har udstedt et påbud om fjernelse af terrorrelateret indhold, har denne medlemsstat kompetence til at træffe tvangsforanstaltninger, f.eks. tvangsbøder, i henhold til national ret for at håndhæve påbuddet om fjernelse.

Såfremt en hostingtjenesteyder ikke udpeger en retlig repræsentant, har alle medlemsstater kompetence.

De kompetente myndigheder i medlemsstaterne skal informere, koordinere og samarbejde med hinanden og om nødvendigt med relevante EU-organer såsom Europol med hensyn til påbud om fjernelse og indberetninger for at undgå dobbeltarbejde, øge koordineringen og undgå forstyrrelser af efterforskninger i forskellige medlemsstater.

Såfremt en hostingtjenesteyder bliver bekendt med beviser for terrorhandlinger, skal de omgående informere de relevante myndigheder i den medlemsstat, hvor hostingtjenesteyderne har deres hovedsæde eller retlige repræsentant. Hostingtjenesteyderne kan i tvivlstilfælde videregive oplysningerne til Europol til opfølgning.

### *Sanktioner*

Medlemsstaterne skal fastsætte regler vedrørende økonomiske sanktioner i tilfælde af en hostingtjenesteydernes overtrædelse af forordningens bestemmelser om hostingtjenesteyderens vilkår og betingelser, gennemførelse af og feedback om påbud om fjernelse, vurdering af og feedback af indberetninger, pligt til rapportering om proaktive foranstaltninger mv., opbevaring af data, pligt til gennemsigtighed, pligt til at træffe sikkerhedsforanstaltninger vedrørende proaktive foranstaltninger og klageprocedurer, oplysninger til indholdsleverandører, oplysninger om beviser på terrorhandlinger, kravet om kontaktpunkter og udpegelse af en retlig repræsentant.

Sanktionerne skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning. I den forbindelse skal medlemsstaterne sikre, at de kompetente myndigheder ved fastsættelse af sanktionernes art og størrelse tager hensyn til følgende relevante omstændigheder:

- (a) overtrædelsens art, grovhed og varighed
- (b) hvorvidt overtrædelsen blev begået forsætligt eller uagtsomt
- (c) overtrædelser, som den juridiske person, der er ansvarlig for overtrædelsen, tidligere har begået
- (d) den ansvarlige juridiske persons finansielle styrke

- (e) hostingtjenesteyderens grad af samarbejde med de kompetente myndigheder.

Derudover skal medlemstaterne sikre, at systematisk mangel på overholdelse af forpligtelsen til at fjerne eller deaktivere terrorelateret indhold inden for en time efter at have modtaget påbuddet om fjernelse af en kompetent national myndighed, medfører økonomiske sanktioner på op til 4 pct. af hostingtjenesteyderens samlede omsætning for det seneste regnskabsår.

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

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

#### **5. Nærhedsprincippet**

Kommissionen har anført, at internettet i sagens natur er grænseoverskridende, og at indhold, der hostes i en medlemsstat, normalt kan tilgås fra enhver anden medlemsstat. Kommissionen anfører, at denne grænseoverskridende dimension nødvendiggør tiltag på EU-niveau for at opnå de fastsatte mål.

Kommissionen har i den forbindelse anført, at forskellige nationale regler til bekæmpelse af terrorrelateret onlineindhold resulterer i en fragmenteret ramme, som kan pålægge virksomhederne en byrde, fordi de skal overholde forskellige regler, ligesom det skaber ulige vilkår for virksomhederne og sikkerhedsmæssige smuthuller.

Kommissionen anfører derfor, at forslaget skal højne retssikkerheden og øge effektiviteten af hostingtjenesteydernes indsats for at bekæmpe terrorrelateret onlineindhold.

På baggrund af det grænseoverskridende element, de forskellige nationale regler i medlemstaterne til bekæmpelse af terrorrelateret onlineindhold og hensynet til de berørte virksomheders retssikkerhed, vurderer Kommissionen således, at det er berettiget med lovgivning på EU-niveau for at kunne adresse de angivne problemer.

Kommissionens vurdering støttes ligeledes af DER-konklusioner af 28. juni 2018, hvor Kommissionen opfordredes til at fremlægge et lovgivningsforslag på området.

Forslaget vurderes – af de af Kommissionen anførte grunde – at være i overensstemmelse med nærhedsprincippet.

## **6. Gældende dansk ret**

Det følger af grundlovens § 77, at enhver er berettiget til på tryk, i skrift og tale at offentliggøre sine tanker, dog under ansvar for domstolene, og at censur og andre forebyggende foranstaltninger ingensinde på ny kan indføres.

Danmark har i regi af den nationale handlingsplan om forebyggelse og bekæmpelse af ekstremisme og radikaliserings fra oktober 2016 gennemført en række tiltag, der har til formål at bekæmpe ekstremistisk propaganda og forebygge online-radikalisering, bl.a. ved at fjerne og blokere terrorrelateret indhold på internettet.

Der blev således i sommeren 2017 på initiativ fra regeringen indsat en ny bestemmelse i retsplejelovens § 791 d, der giver hjemmel til at blokere en hjemmeside, hvis der er rimelig grund til at antage, at der fra hjemmesiden begås en overtrædelse af bl.a. straffelovens §§ 114-114 i om terrorisme. Afgørelser om blokering af en hjemmeside træffes ved retskendelse efter begæring fra politiet.

Derudover har Danmark ligesom en række andre medlemsstater i regi af EU's Internetforum etableret en såkaldt *internet referral unit* (IRU-enhed), der er forankret i Politiets Efterretningstjeneste (PET). Enheden har til formål at identificere voldeligt ekstremistisk indhold på nettet, herunder terrorrelateret indhold, og indberette indholdet til hostingtjenesteydere med henblik på hurtig fjernelse. Enheden indgår ligeledes i et samarbejde med Europol med henblik på at koordinere bortfjernelse af terrorrelateret materiale.

Derudover vil der inden udgangen af 2018 blive indført et internetblokeringsfilter, som skal begrænse adgangen til udenlandske internetsider, der spreder terrorpropaganda eller andet voldeligt, ekstremistisk materiale.

## **7. Konsekvenser**

### 7.1. Lovgivningsmæssige konsekvenser

En forordning er umiddelbart bindende i alle enkeltheder og gælder umiddelbart i hvert EU-medlemsland.

Forslaget forventes dog alligevel at have lovgivningsmæssige konsekvenser, da det bl.a. vil være nødvendigt at fastsætte regler om, hvilken national myndighed, der skal kunne udstede påbud til hostingtjenesteydere om fjernelse af terrorrelateret indhold, og hvilken myndighed, der skal kunne pålægge en hostingtjenesteyder at iværksætte proaktive foranstaltninger.

## 7.2. Økonomiske konsekvenser

Vurderingen af, hvorvidt forslaget vil have statsfinansielle konsekvenser er endnu ikke afsluttet. Det vurderes dog ikke umiddelbart, at forslaget vil have statsfinansielle konsekvenser af betydning.

Det vurderes umiddelbart, at forslaget kan medføre administrative byrder under 4 mio. kr. årligt, som følge af krav til hostingtjenesteyderne om oplysninger til brugere, samt fjernelse eller deaktivering af terrorrelateret onlineindhold. Ud over de administrative konsekvenser kan forslaget medføre væsentlige erhvervsøkonomiske konsekvenser, som følge af forslagets bestemmelser om pligt for hostingtjenesteydere til efter påbud at fjerne terrorrelateret indhold inden for en time, indberetning og proaktive foranstaltninger. Den endelige vurdering heraf er dog endnu ikke afsluttet.

## 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, Den Danske Dommerforening, Dommerfuldmægtigforeningen, Domstolsstyrelsen, Dansk Erhverv, Dansk Industri, Danske Medier, Datatilsynet, DK Hostmaster, Fiberby, Institut for Menneskerettigheder, IT-Politisk Forening, Justitia Kriminalpolitisk Forening (KRIM), Rigsadvokaten, Teleindustrien, Telia Danmark, Københavns Universitet, Syddansk Universitet (Juridisk Institut), Aalborg Universitet (Juridisk Institut), Aarhus Universitet (Juridisk Institut).

Høringsfristen er fastsat til den 21. november 2018. Høringssvarene vil blive oversendt, så snart de foreligger enten ved et revideret grund- og nærhedsnotat eller et samlenotat.

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

Som det fremgår af pkt. 2 oven for, fremlagde Frankrig og Tyskland den 19. juni 2018 en erklæring om fremtidige tiltag i EU, hvori de to lande bl.a. opfordrede til indførelse af lovgivning på EU-niveau for at bekæmpe terrorrelateret indhold på nettet.

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

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

Fra dansk side finder man på nuværende tidspunkt, hvor den igangsatte høring ikke er afsluttet, ikke at burde tage endelig stilling til forslaget.

Man er fra dansk side overordnet set positivt indstillet over for forslaget, der har til formål at styrke og supplere den fælles og frivillige indsats, der allerede er iværksat på EU-niveau i forhold til at bekæmpe mængden af terrorindhold online.

Man vil fra dansk side under forhandlingerne have fokus på at sikre, at forslaget holder sig inden for rammerne af grundlovens § 77.

Man vil fra dansk side endvidere arbejde for, at forslaget ikke skaber urimelige eller uproportionelle byder for erhvervslivet, herunder navnlig små- og mellemstore virksomheder, eller opstiller unødige barrierer for innovation og vækst i det digitale indre marked, ligesom der skal tages højde for eksisterende krav i de gældende regler, så der sikres en klar, enkel og sammenhængende ramme for virksomhederne.

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

Sagen har ikke tidligere været forelagt Folketingets Europaudvalg.