EUROPA-
KOMMISSIONEN

Bruxelles, den 12.9.2018
COM(2018) 640 final

2018/0331 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om forebyggelse af udbredelsen af terrorrelateret onlineindhold

Et bidrag fra Europa-Kommissionen til ledernes møde i Salzburg den 19.-20. september 2018

{SEC(2018) 397 final} - {SWD(2018) 408 final} - {SWD(2018) 409 final}

BEGRUNDELSE

1. BAGGRUND FOR FORSLAGET

1.1. Forslagets begrundelse og formål

Internettets allestedsnærværelse gør det muligt for brugerne at kommunikere, arbejde og omgås hinanden samt skabe, indhente og dele oplysninger og indhold med flere hundrede millioner individer i hele verden. Internetplatformene øger i væsentlig grad brugernes økonomiske og sociale velfærd i og uden for Unionen. Evnen til ved minimale omkostninger at nå ud til så stort et publikum tiltrækker imidlertid også kriminelle, som misbruger internettet til ulovlige formål. Nylige terrorangreb i EU har vist, hvordan terrorister misbruger internettet til at træne og rekruttere tilhængere, forberede og fremme terroraktiviteter, forherlige deres ugerninger og tilskynde andre til at følge trop og skabe frygt blandt den almindelige befolkning.

Terrorrelateret indhold, der deles online til sådanne formål, udbredes via hostingtjenesteydere, som tillader upload af tredjepartsindhold. Terrorrelateret onlineindhold har i adskillige nyere terrorangreb i Europa vist sig at spille en stor rolle med hensyn til at radikalisere og inspirere såkaldte "ensomme ulve" til angreb. Sådant indhold har ikke blot negative virkninger for enkeltpersoner og for samfundet som helhed – det mindsker også internetbrugerens tillid og påvirker de berørte virksomheders forretningsmodeller og omdømme. Terrorister har ikke blot misbrugt store sociale medieplatforme men i stigende grad også mindre udbydere, der udbyder forskellige former for hostingtjenester på globalt plan. Dette misbrug af internettet understreger internetplatformenes særlige samfundsmæssige ansvar for at beskytte deres brugere mod eksponering for terrorrelateret indhold og de alvorlige sikkerhedsrisici, som dette indhold udgør for samfundet som helhed.

Hostingtjenesteyderne har på de offentlige myndigheders opfordring iværksat visse foranstaltninger for at tackle terrorindhold på deres tjenester. Der er gjort fremskridt gennem frivillige rammer og partnerskaber, herunder EU's internetforum, der blev lanceret i december 2015 som del af den europæiske dagsorden om sikkerhed. EU's internetforum har været med til at fremme medlemsstaternes og hostingtjenesteydernes frivillige samarbejde og tiltag for at reducere tilgængeligheden af terrorrelateret onlineindhold og styrke civilsamfundets aktører med henblik på at øge mængden af effektive, alternative budskaber på nettet. Disse bestræbelser har bidraget til at øge samarbejdet, forbedre virksomhedernes reaktion på indberetninger fra de nationale myndigheder og Europols enhed for internetindberetning, fremmet iværksættelsen af frivillige proaktive foranstaltninger til forbedring af automatiseret sporing af terrorindhold, øget samarbejdet inden for industrien – herunder udviklingen af databasen over hashkoder for at forhindre, at kendt terrorindhold bliver uploadet på forbundne platforme – og skabt øget gennemsigtighed i indsatsen. Selv om samarbejdet inden for rammerne af EU's internetforum bør fortsætte i fremtiden, har de frivillige ordninger også vist deres begrænsninger. For det første har ikke alle berørte hostingtjenesteydere engageret sig i forummet, og for det andet er omfanget og hastigheden af de fremskridt, hostingtjenesteydere generelt gør, ikke nok til at tage ordentligt hånd om problemet.

Der er pga. disse begrænsninger et klart behov for en øget indsats fra Den Europæiske Unions side for at bekæmpe terrorrelateret onlineindhold. Den 1. marts 2018 vedtog Kommissionen en henstilling om foranstaltninger til effektiv bekæmpelse af ulovligt indhold på nettet, som

bygger på Kommissionens meddelelse fra september[1] såvel som på indsatsen i EU's internetforum. Henstillingen indeholder et særligt kapitel, hvor der beskrives en række foranstaltninger, som effektivt skal dæmme op for uploading og deling af terrorpropaganda på nettet, f.eks. forbedringer af indberetningsprocessen, en frist på en time for at reagere på indberetninger, mere proaktiv sporing, effektiv fjernelse og tilstrækkelige foranstaltninger til akkurat vurdering af terrorrelateret indhold[2].

Behovet for at skærpe indsatsen med hensyn til terrorrelateret onlineindhold afspejles ligeledes i EU-medlemsstaternes opfordringer, og nogle af dem har allerede lovgivet på området eller har planer om at gøre det. Efter en række terrorangreb i EU og i betragtning af, at terrorrelateret onlineindhold fortsat er let tilgængeligt, opfordrede Det Europæiske Råd af 22.-23. juni 2017 industrien til at udvikle "nye teknologier og værktøjer til at forbedre den automatiske påvisning og fjernelse af indhold, som tilskynder til terroristiske aktiviteter. Dette bør i nødvendigt omfang suppleres af de relevante lovgivningsmæssige foranstaltninger på EU-plan." Det Europæiske Råd af 28. juni 2018 så med tilfredshed på "Kommissionens hensigt om at forelægge et lovgivningsforslag, der skal forbedre påvisning og fjernelse af indhold, som tilskynder til had og til at begå terrorhandlinger". Derudover opfordrede Europa-Parlamentet i sin beslutning om onlineplatforme og det digitale indre marked af 15. juni 2017 de pågældende platforme "til at styrke foranstaltninger til bekæmpelse af ulovligt og skadeligt indhold" og opfordrede Kommissionen til at fremlægge forslag til løsning af disse problemer.

For at tackle disse udfordringer og reagere på medlemsstaternes og Europa-Parlamentets opfordringer stræber Kommissionen med dette forslag efter at skabe en klar og harmoniseret retlig ramme til forebyggelse af misbrug af hostingtjenester til udbredelse af terrorrelateret onlineindhold med henblik på at garantere et velfungerende digitalt indre marked og sikre tillid og sikkerhed. Denne forordning har til formål at skabe klarhed med hensyn til det ansvar, der påhviler hostingtjenesteydere, for at træffe alle de passende, rimelige og forholdsmæssige foranstaltninger, som er nødvendige for at sørge for, at deres tjenester er sikre, og for hurtigt og effektivt at spore og fjerne terrorindhold på nettet under hensyntagen til den grundlæggende betydning af ytrings- og informationsfriheden i et åbent og demokratisk samfund. Med forordningen indføres der også en række nødvendige sikkerhedsforanstaltninger, som skal sikre fuld overholdelse af de grundlæggende rettigheder såsom ytrings- og informationsfriheden i et demokratisk samfund, samt retlige klagemuligheder som garanteret af den ret til adgang til effektive retsmidler, der er fastsat i artikel 19 i TEU og artikel 47 i Den Europæiske Unions charter om grundlæggende rettigheder.

Ved at fastsætte et sæt minimumskrav til den rettidige omhu, som hostingtjenesteyderne skal udvise, herunder visse specifikke regler og forpligtelser, såvel som forpligtelser for medlemsstaterne, stiler forslaget mod at øge de eksisterende foranstaltningers effektivitet med hensyn til at spore, identificere og fjerne terrorrelateret onlineindhold uden at gribe ind i grundlæggende rettigheder som ytrings- og informationsfriheden. En sådan harmoniseret retlig ramme vil fremme leveringen af onlinetjenester i det digitale indre marked, sikre lige vilkår for alle hostingtjenesteydere, som leverer tjenester i Den Europæiske Union, og udgøre en solid retlig ramme for sporing og fjernelse af terrorindhold med passende sikkerhedsforanstaltninger til beskyttelse af grundlæggende rettigheder. Især gennemsigtighedsreglerne vil øge tilliden blandt borgerne, særligt internetbrugerne, og øge

[1] Meddelelse om bekæmpelse af ulovligt indhold på nettet (COM(2017) 555 final).

[2] Henstilling af 1. marts 2018 om foranstaltninger til effektiv bekæmpelse af ulovligt indhold på nettet (C(2018)1177 final).

ansvarligheden og gennemsigtigheden i virksomhedernes handlinger, herunder hvad angår offentlige myndigheder. I forslaget er der ligeledes fastsat forpligtelser til at indføre retsmidler og klagemekanismer, der skal sikre, at brugerne kan gøre indsigelse mod fjernelsen af deres indhold. Forpligtelser for medlemsstaterne vil bidrage til at nå disse mål, ligesom det vil forbedre de relevante myndigheders evne til at træffe passende foranstaltninger mod terrorrelateret onlineindhold og til at bekæmpe kriminalitet. Hvis hostingtjenesteyderne ikke overholder bestemmelserne i forordningen, kan medlemsstaterne pålægge sanktioner.

1.2. Sammenhæng med den gældende retlige ramme i Unionen på samme område

Nærværende forslag er i overensstemmelse med reglerne om det digitale indre marked og især e-handelsdirektivet. Enhver foranstaltning, som hostingtjenesteyderen træffer i overensstemmelse med denne forordning, herunder proaktive foranstaltninger, bør ikke i sig selv føre til, at tjenesteyderen mister den ansvarsfritagelse, der er gældende under visse betingelser, jf. artikel 14 i e-handelsdirektivet. En afgørelse truffet af nationale myndigheder om at pålægge forholdsmæssige og specifikke proaktive foranstaltninger bør i princippet ikke føre til, at medlemsstaterne pålægges en generel forpligtelse til overvågning som omhandlet i artikel 15, stk. 1, i direktiv 2000/31/EF. De særligt alvorlige risici, der er forbundet med udbredelsen af terrorindhold, taget i betragtning kan afgørelser truffet i henhold til denne forordning imidlertid undtagelsesvis fravige dette princip i en EU-kontekst. Den kompetente myndighed bør, før den træffer sådanne afgørelser, finde en rimelig balance mellem behovet for offentlig sikkerhed og de berørte interesser og de grundlæggende rettigheder, herunder især retten til ytrings- og informationsfrihed, friheden til at oprette og drive egen virksomhed og retten til beskyttelse af personoplysninger. Hostingtjenesteydernes rettidige omhu bør afspejle og respektere denne balance, som er udtykt i e-handelsdirektivet.

Forslaget er også i overensstemmelse med og afstemt efter direktiv (EU) 2017/541 om bekæmpelse af terrorisme, hvis mål er at harmonisere medlemsstaternes lovgivning om kriminalisering af terrorhandlinger. Ifølge artikel 21 i direktivet om bekæmpelse af terrorisme skal medlemsstaterne træffe de nødvendige foranstaltninger for at sikre øjeblikkelig fjernelse af onlineindhold, der udgør en offentlig opfordring til at begå en terrorhandling, Dens præventive karakter taget i betragtning omfatter denne forordning ikke blot materiale, der opfordrer til terrorisme, men også materiale til rekrutterings- og uddannelsesformål, hvilket afspejler andre strafbare handlinger relateret til terroraktiviteter, som også er omfattet af direktiv (EU) 2017/541. Med denne forordning pålægges hostingtjenesteyderne direkte en forpligtelse til at fjerne terrorindhold og harmonisere procedurerne for påbud om fjernelse med sigte på at begrænse adgangen til terrorrelateret onlineindhold.

Forordningen supplerer de regler, der er fastsat i det fremtidige direktiv om audiovisuelle medietjenester, for så vidt at det personelle og materielle anvendelsesområde er bredere. Denne forordning omfatter ikke kun videodelingsplatforme, men alle typer af hostingtjenesteydere. Derudover omfatter den ikke blot videoer, men også billeder og tekst. Nærværende forordning går videre end direktivet hvad angår materielle bestemmelser, idet den harmoniserer reglerne for anmodninger om fjernelse af terrorindhold såvel som proaktive foranstaltninger.

Den foreslåede forordning bygger på Kommissionens henstilling[3] om bekæmpelse af ulovligt indhold på nettet fra marts 2018. Henstillingen er fortsat gyldig, og alle parter, som spiller en

[3] Henstilling af 1. marts 2018 om foranstaltninger til effektiv bekæmpelse af ulovligt indhold på nettet (C(2018)1177 final).

rolle for at begrænse adgangen til ulovligt indhold, herunder terrorindhold, bør fortsætte deres indsats med de foranstaltninger, der er indkredset i henstillingen.

1.3. Resumé af forslaget til forordning

Forslagets personelle anvendelsesområde omfatter hostingtjenesteydere, som udbyder tjenester i Unionen, uanset hvor de er etableret, eller hvor store de er. Med den foreslåede lovgivning indføres der en række foranstaltninger til forebyggelse af misbrug af hostingtjenester til udbredelse af terrorrelateret onlineindhold med henblik på at garantere et velfungerende digitalt indre marked og sikre tillid og sikkerhed. Definitionen af ulovligt terrorindhold er i overensstemmelse med definitionen på terrorhandlinger som fastsat i direktiv (EU) 2017/541, og defineres som oplysninger, der bruges til at opfordre til og forherlige udførelsen af terrorhandlinger, tilskynde til at bidrage til og give instruktioner i udførelse af terrorhandlinger såvel som promovering af deltagelse i terrorgrupper.

For at sikre, at ulovligt terrorindhold bliver fjernet, indføres der med forordningen et påbud om fjernelse, der kan udstedes som en administrativ eller retlig afgørelse af en kompetent myndighed i en medlemsstat. I sådanne tilfælde er hostingstjenesteyderen forpligtet til enten at fjerne indholdet eller deaktivere adgangen hertil inden for en time. Derudover harmoniserer forordningen minimumskravene til de indberetninger, som medlemsstaternes kompetente myndigheder og Unionens organer (såsom Europol) sender til hostingtjenesteyderne, så disse kan vurdere dem i forhold til deres egne vilkår og betingelser. Endelig fastsættes det i forordningen, at hostingtjenesteyderne, hvis det er relevant, skal træffe proaktive foranstaltninger, der står i et rimeligt forhold til risikoen, og fjerne terrormateriale fra deres tjenester, herunder ved hjælp af redskaber til automatisk sporing.

Foranstaltningerne til begrænsning af mængden af terrorrelateret onlineindhold ledsages af en række vigtige sikkerhedsforanstaltninger, som skal sikre fuld beskyttelse af grundlæggende rettigheder. Som del af de foranstaltninger, der skal beskytte indhold, som ikke er terrorindhold, mod fejlagtig fjernelse, er der i forslaget ligeledes fastsat forpligtelser til at indføre retsmidler og klagemekanismer, der skal sikre, at brugerne kan gøre indsigelse mod fjernelsen af deres indhold. Dertil kommer, at der med forordningen indføres forpligtelser vedrørende gennemsigtighed for så vidt angår de foranstaltninger, som hostingtjenesteyderne træffer for at bekæmpe terrorindhold, så ansvarligheden over for brugere, borgere og offentlige myndigheder sikres.

Forordningen forpligter også medlemsstaterne til at sikre, at deres kompetente myndigheder har den fornødne kapacitet til at gribe ind over for terrorrelateret onlineindhold. Medlemsstaterne er tillige forpligtet til at informere og samarbejde med hinanden og kan gøre brug af de kanaler, som Europol har etableret, for at sikre koordinering med hensyn til påbud om fjernelse og indberetninger. Forordningen omfatter også forpligtelser for hostingtjenesteydere til mere detaljeret rapportering om de trufne foranstaltninger og til underretning af de retshåndhævende myndigheder, når de sporer indhold, som udgør en trussel mod menneskers liv eller sikkerhed. Endelig er hostingtjenesteyderne forpligtet til at opbevare det fjernede indhold, hvilket fungerer som en sikkerhedsforanstaltning mod fejlagtig fjernelse og sikrer, at potentielle beviser til brug for forebyggelse, sporing, efterforskning og retsforfølgning af terrorhandlinger ikke går tabt.

2. RETSGRUNDLAG, NÆRHEDSPRINCIPPET OG PROPORTIONALITETSPRINCIPPET

2.1. Retsgrundlag

Retsgrundlaget er artikel 114 i traktaten om Den Europæiske Unions funktionsmåde, ifølge hvilken der kan træffes foranstaltninger for at sikre et velfungerende indre marked.

Artikel 114 er det passende retsgrundlag for harmonisering af hostingtjenesteydernes betingelser for at yde grænseoverskridende tjenester i det digitale indre marked og afhjælpe de forskelle mellem medlemsstaternes bestemmelser, som ellers kan obstruere et velfungerende indre marked. Dette vil ligeledes forebygge, at der i fremtiden opstår hindringer for økonomisk aktivitet, som skyldes, at de nationale lovgivninger udvikler sig i forskellig retning.

Artikel 113 i TEUF kan ligeledes bruges til at pålægge forpligtelser for tjenesteydere, der er etableret uden for Unionen, hvis deres levering af tjenester påvirker det indre marked, eftersom dette er nødvendigt for at nå det ønskede mål for det indre marked.

2.2. Valg af retsakt

Artikel 114 i TEUF giver EU-lovgiveren mulighed for at vedtage forordninger og direktiver.

Eftersom forslaget vedrører forpligtelser for tjenesteydere, som normalt udbyder tjenester til flere medlemsstater, vil uoverensstemmelse i anvendelsen af disse regler forhindre leverandører, der opererer i flere medlemsstater, i at levere tjenester. En forordning gør det muligt at indføre den samme forpligtelse på ensartet vis i hele Unionen, er umiddelbart gældende, giver klarhed og større retssikkerhed, ligesom den forhindrer uensartet gennemførelse i medlemsstaterne. Af disse årsager anses en forordning for at være det mest passende instrument.

2.3. Nærhedsprincippet

I betragtning af pågældende problemers grænseoverskridende dimension skal foranstaltningerne i forslaget vedtages på EU-plan for at nå de fastsatte mål. Internettet er i sagens natur grænseoverskridende, og indhold, der hostes i en medlemsstat, kan normalt tilgås fra enhver anden medlemsstat.

De forskellige nationale regler til bekæmpelse af terrorrelateret onlineindhold resulterer i en fragmenteret ramme, og risikoen vokser. Dette kan igen pålægge virksomhederne en byrde, fordi de skal overholde forskellige regler, ligesom det skaber ulige vilkår for virksomhederne og sikkerhedsmæssige smuthuller.

EU's tiltag skal derfor højne retssikkerheden og øge effektiviteten af hostingtjenesteydernes indsats for at bekæmpe terrorrelateret onlineindhold. Dette bør gøre det muligt for virksomhederne at skride til handling, herunder virksomheder, der er etableret uden for Den Europæiske Union, idet det digitale indre markeds integritet styrkes.

Behovet for handling fra EU's side er således berettiget, hvilket også fremgår af Det Europæiske Råds konklusioner fra juni 2018, hvor Kommissionen opfordres til at fremlægge et lovgivningsforslag på området.

2.4. Proportionalitetsprincippet

I forslaget fastsættes der regler, ifølge hvilke hostingtjenesteydere skal træffe foranstaltninger for hurtigt at fjerne terrorindhold fra deres tjenester. Centrale elementer begrænser forslaget til det, der er nødvendigt for at nå de politiske målsætninger.

Forslaget tager højde for den byrde, der pålægges hostingtjenesteydere, og for sikkerhedsforanstaltninger, herunder beskyttelsen af ytrings- og informationsfriheden og andre grundlæggende rettigheder. Fristen på en time for fjernelse gælder kun for påbud om fjernelse, hvor de kompetente myndigheder har konstateret ulovligheden i en afgørelse, der er underlagt retslig prøvelse. For så vidt angår indberetninger er der en forpligtelse til at træffe foranstaltninger, som fremmer en hurtigt vurdering af terrorindholdet, uden at der dog skabes forpligtelser til at fjerne det, ej heller inden for endelige frister. Den endelige afgørelse forbliver en frivillig afgørelse truffet af hostingtjenesteyderen. Den byrde, som virksomhederne oplever ved at skulle vurdere indholdet, lettes ved den kendsgerning, at medlemsstaternes kompetente myndigheder og EU-organerne forklarer, hvorfor et givet indhold kan betragtes som terrorindhold. Hostingtjenesteyderne træffer, hvis det er passende, proaktive foranstaltninger til beskyttelse af deres tjenester mod udbredelse af terrorrelateret indhold. Specifikke forpligtelser vedrørende proaktive foranstaltninger er begrænset til de hostingtjenesteydere, som eksponeres for terrorindhold og modtager et endeligt påbud om fjernelse. Disse forpligtelser skal stå i rimeligt forhold til risikoniveauet og virksomhedens ressourcer. Opbevaringen af det fjernede indhold og de dertil knyttede data begrænses til en periode, der står i forhold til formålet om at muliggøre sager med administrativ eller retslig prøvelse og forebyggelse, sporing, efterforskning og retsforfølgning af terrorhandlinger.

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

3.1. Høringer af interesserede parter

Som forberedelse til dette lovgivningsforslag har Kommissionen hørt alle relevante interessenter for at forstå deres synspunkter og finde en potentiel vej frem. Kommissionen foretog en åben offentlig høring om foranstaltninger til en mere effektiv bekæmpelse af ulovligt indhold og modtog 8 961 svar, hvoraf 8 749 var fra enkeltpersoner, 172 fra organisationer, 10 fra offentlige administrationer og 30 fra andre kategorier af respondenter. Sideløbende blev der foretaget en Eurobarometer-undersøgelse blandt 33 500 tilfældigt udvalgte EU-borgere om ulovligt indhold på nettet. Kommissionen hørte ligeledes medlemsstaternes myndigheder såvel som hostingtjenesteydere i løbet af maj og juni 2018 med hensyn til specifikke foranstaltninger til bekæmpelse af terrorrelateret onlineindhold.

I det store og hele gav interessenterne udtryk for, at terrorrelateret onlineindhold er et alvorligt samfundsproblem, der påvirker internetbrugerne og hostingtjenesteydernes forretningsmodeller. 65 % af respondenterne i Eurobarometer-undersøgelsen[4] svarede mere generelt, at internettet ikke er sikkert for brugerne, og ifølge 90 % af respondenterne er det vigtigt at begrænse udbredelsen af ulovligt onlineindhold. Høringerne af medlemsstaterne afslørede, at der, selv om de frivillige ordninger giver resultater, ifølge mange er behov for bindende forpligtelser for så vidt angår terrorrelateret indhold, hvilket også er afspejlet i Rådets konklusioner af juni 2018. Skønt hostingtjenesteyderne generelt gik ind for en fortsættelse af de frivillige foranstaltninger, fremhævede de potentielt negative virkninger af den begyndende juridiske fragmentering i Unionen.

Mange interessenter bemærkede desuden, at der er behov for at sikre, at lovgivningsmæssige foranstaltninger for fjernelse af indhold, navnlig proaktive foranstaltninger og strenge frister, bliver kombineret med garantier for grundlæggende rettigheder, især for ytringsfriheden. Interessenterne fremhævede en række nødvendige foranstaltninger vedrørende

[4] Eurobarometer 469 "Illegal content online", juni 2018.

gennemsigtighed og ansvarlighed såvel som behovet for menneskeligt tilsyn, når der anvendes redskaber til automatisk sporing.

3.2. Konsekvensanalyse

Udvalget for Forskriftskontrol afgav en positiv udtalelse om konsekvensanalysen med visse forbehold og fremsatte forskellige forbedringsforslag[5]. Efter denne udtalelse blev konsekvensanalysen ændret for at tage højde for udvalgets vigtigste kommentarer, så fokus blev rettet specifikt mod terrorindhold, konsekvenserne for et velfungerende digitalt indre marked blev fremhævet, og der blev foretaget en mere dybdegående analyse af virkningerne på de grundlæggende rettigheder og funktionen af de foreslåede sikkerhedsforanstaltninger.

Hvis der ikke bliver truffet yderligere foranstaltninger, forventes frivillige tiltag i basisscenariet at fortsætte og være medvirkende til at begrænse terrorrelateret onlineindhold i en vis grad. Det er dog ikke sandsynligt, at samtlige hostingtjenesteydere, der eksponeres for sådant indhold, vil træffe frivillige foranstaltninger, og der forventes videre retlig fragmentering, hvilket vil skabe yderligere barrierer for grænseoverskridende levering af tjenesteydelser. Ud over basisscenariet blev der vurderet tre primære løsningsmuligheder med stigende grader af effektivitet, når det drejer sig om at opfylde de i konsekvensanalysen fastsatte målsætninger og det overordnede politiske mål om at begrænse mængden af terrorindhold på nettet.

Anvendelsesområdet for forpligtelserne under alle tre løsninger fokuserer på samtlige hostingtjenesteydere (personelt anvendelsesområde), der er etableret i EU og i tredjelande, såfremt de udbyder tjenester i Unionen (geografisk anvendelsesområde). Problemets karakter og behovet for at undgå misbrug af mindre platforme taget i betragtning er der under ingen af løsningerne planlagt undtagelser for SMV'er. Alle løsninger vil kræve, at hostingtjenesteyderne – også virksomheder etableret uden for EU – udpeger retlige repræsentanter i EU, så det sikres, at EU-reglerne håndhæves. Medlemsstaterne skal under alle løsninger indføre sanktionsmekanismer.

Under alle løsninger er det planlagt at skabe et nyt, harmoniseret system for retlige påbud om fjernelse af terrorrelateret onlineindhold udstedt af nationale myndigheder til hostingtjenesteydere med et krav om at fjerne indholdet inden for en time. Disse påbud vil ikke nødvendigvis kræve en vurdering fra hostingtjenesteydernes side og vil være underlagt retslig prøvelse.

Sikkerhedsforanstaltninger, navnlig klageprocedurer og effektive retsmidler, herunder retslig prøvelse, såvel som andre bestemmelser, der skal forhindre fejlagtig fjernelse af indhold, som ikke er terrorindhold, i respekt for grundlæggende rettigheder, er fælles for alle tre løsninger. Desuden indeholder alle løsninger rapporteringsforpligtelser i form af offentlig gennemsigtighed og rapportering til medlemsstaterne og Kommissionen såvel som til myndigheder ved mistanke om strafbare handlinger. Derudover er der fastsat forpligtelser til samarbejde mellem nationale myndigheder, hostingtjenesteydere og, hvis det er relevant, Europol.

De største forskelle mellem de tre løsninger vedrører anvendelsesområdet for definitionen af terrorindhold, omfanget af harmonisering af indberetninger, anvendelsesområdet for proaktive foranstaltninger, forpligtelser for medlemsstaterne til at koordinere såvel som krav til opbevaring af data. Løsning 1 vil med en meget snæver definition begrænse det materielle

[5] Link til Udvalget for Forskriftskontrols udtalelse om forordningen.

anvendelsesområde til indhold, som udbredes for direkte at opfordre til at begå en terrorhandling, mens løsning 2 og 3 indebærer en mere omfattende tilgang, der også dækker materiale vedrørende rekruttering og uddannelse. For så vidt angår proaktive foranstaltninger vil hostingtjenesteydere, som eksponeres for terrorindhold, under løsning 1 skulle foretage en risikovurdering, mens proaktive foranstaltninger til afbødning af risikoen vil forblive frivillige. Under løsning 2 vil hostingtjenesteyderne skulle udarbejde en handlingsplan, som kan omfatte anvendelse af redskaber til automatisk forebyggelse af genupload af indhold, der tidligere er blevet fjernet. Løsning 3 indebærer mere omfattende proaktive foranstaltninger, der kræver, at tjenesteydere eksponeret for terrorindhold ligeledes identificerer nyt materiale. Under alle løsninger til kravene i forbindelse med proaktive foranstaltninger stå i forhold til graden af eksponering for terrormateriale såvel som til tjenesteyderens økonomiske kapacitet. Hvad angår indberetninger vil løsning 1 ikke harmonisere tilgangen til indberetninger, hvilket er tilfældet for løsning 2 for så vidt angår Europol, ligesom løsning 3 vil inkludere medlemsstaternes indberetninger. Medlemsstaterne vil under løsning 2 og 3 være forpligtet til at informere, koordinere og samarbejde med hinanden, og under løsning 3 vil de ligeledes skulle sikre, at de kompetente myndigheder har kapacitet til at spore og indberette terrorindhold. Endelig indeholder løsning 3 også et krav om opbevaring af data som en sikkerhedsforanstaltning i tilfælde af fejlagtig fjernelse og for at lette strafferetlige efterforskninger.

Foruden de retlige bestemmelser skal alle de lovgivningsmæssige løsninger efter planen ledsages af en række støtteforanstaltninger, som især skal øge samarbejdet mellem de nationale myndigheder og Europol såvel som samarbejdet med hostingtjenesteyderne, samt støtte til forskning, udvikling og innovation inden for udvikling og ibrugtagning af teknologiske løsninger. Yderligere oplysnings- og støtteinstrumenter for SMV'er vil ligeledes kunne anvendes efter vedtagelsen af retsakten.

Det konkluderes i konsekvensanalysen, at en række foranstaltninger er påkrævet for at nå den politiske målsætning. Den omfattende definition af terrorindhold, som omfatter det mest skadelige materiale, vil være at foretrække frem for en snæver definition af indholdet (løsning 1). Proaktive foranstaltninger, der er begrænset til forebyggelse af genupload af terrorindhold (løsning 2), vil være mindre virkningsfuld sammenlignet med forpligtelserne til sporing af nyt terrorindhold (løsning 3). Bestemmelserne om indberetninger bør omfatte indberetninger fra både Europol og medlemsstaterne (løsning 3) og ikke kun begrænses til indberetninger fra Europol (løsning 2), da indberetninger fra medlemsstaterne er et vigtigt bidrag til den overordnede indsats for at begrænse adgangen til terrorrelateret onlineindhold. Sådanne foranstaltninger vil skulle gennemføres som supplement til de foranstaltninger, der er fælles for alle tre løsninger, herunder solide sikkerhedsforanstaltninger mod fejlagtig fjernelse af indhold.

3.3. Grundlæggende rettigheder

Terroristers onlinepropaganda har til formål at tilskynde enkeltpersoner til at udføre terrorangreb, herunder ved at give dem detaljerede instruktioner i, hvordan der gøres størst mulig skade. Yderligere propaganda offentliggøres typisk efter sådanne ugerninger med henblik på at forherlige handlingerne og opfordre andre til at følge trop. Denne forordning bidrager til beskyttelsen af den offentlige sikkerhed ved at begrænse adgangen til terrorindhold, som promoverer og opfordrer til overtrædelse af grundlæggende rettigheder.

Forslaget kan potentielt påvirke en række grundlæggende rettigheder:

(a) indholdsleverandørens rettigheder: retten til ytringsfrihed, retten til beskyttelse af personoplysninger, retten til respekt for privatliv og familieliv, princippet om ikkeforskelsbehandling og retten til effektive retsmidler

(b) tjenesteyderens rettigheder: friheden til at oprette og drive egen virksomhed, adgangen til effektive retsmidler,

(c) alle borgeres rettigheder: ytrings- og informationsfriheden.

Passende og solide sikkerhedsforanstaltninger er under hensyntagen til relevant gældende EU-ret inkluderet i den foreslåede forordning for at sikre beskyttelse af disse personers rettigheder.

Det første element i den forbindelse er, at der med forordningen fastsættes en definition af terrorrelateret onlineindhold, som er i overensstemmelse med definitionen på terrorhandlinger i direktiv (EU) 2017/541. Definitionen gælder for påbud om fjernelse og indberetninger såvel som for proaktive foranstaltninger. Denne definition sikrer, at det kun er ulovligt indhold svarende til en EU-dækkende definition af relaterede strafbare handlinger, som fjernes. Dertil kommer, at forordningen indeholder bestemmelser om, at hostingtjenesteyderne generelt skal udvise rettidig omhu og 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.

Forordningen er mere specifikt blevet udarbejdet for at sikre foranstaltningernes proportionalitet med hensyn til grundlæggende rettigheder. Hvad angår påbud om fjernelse retfærdiggør en kompetent myndigheds vurdering af indholdet (herunder eventuel juridisk kontrol) fristen på en time for fjernelse for denne foranstaltning. Desuden er denne forordnings bestemmelser vedrørende indberetninger begrænset til de indberetninger, der sendes af kompetente myndigheder og EU-organer, og som indeholder forklaringer af, hvorfor indholdet kan betragtes som værende terrorindhold. Om end ansvaret for at fjerne det indhold, der er identificeret i en indberetning, ligger hos hostingtjenesteyderen, fremmes afgørelsen af førnævnte vurdering.

Hvad angår proaktive foranstaltninger ligger ansvaret for at identificere, vurdere og fjerne indholdet hos hostingtjenesteyderne, og disse er forpligtet til at træffe sikkerhedsforanstaltninger, herunder menneskeligt tilsyn, for at sikre, at indholdet ikke fjernes fejlagtigt, navnlig hvis der er brug for yderligere forklaringer af konteksten. Ulig basisscenariet, hvor de fleste berørte virksomheder anvender automatiserede værktøjer uden offentligt tilsyn, vil udformningen af foranstaltningerne og deres gennemførelse være underlagt krav om rapportering til de kompetente myndigheder i medlemsstaterne. Forpligtelsen reducerer risikoen for fejlagtig fjernelse – både for virksomheder, der er ved at tage nye redskaber i brug, og for dem, der allerede bruger dem. Derudover kræves det, at hostingtjenesteyderne stiller brugervenlige klagemekanismer til rådighed for indholdsleverandørerne, så disse kan gøre indsigelse mod fjernelsen af deres indhold, lige så vel som de skal offentliggøre gennemsigtighedsrapporter til den brede offentlighed.

Hvis indhold og dertil knyttede data bliver fejlagtigt fjernet til trods for disse sikkerhedsforanstaltninger, skal hostingtjenesteyderne opbevare det i en periode på seks måneder for at kunne genindsætte det og dermed sikre effektive klageprocedurer med henblik på at beskytte ytrings- og informationsfriheden. Samtidig tjener opbevaringen også retshåndhævelsesformål. Hostingtjenesteyderne skal iværksætte tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre, at dataene ikke anvendes til andre formål.

De foreslåede foranstaltninger, navnlig de, som vedrører påbud om fjernelse, indberetninger, proaktive foranstaltninger og opbevaring af data, skal ikke kun beskytte internetbrugerne mod terrorindhold, men også bidrage til at beskytte borgernes ret til livet ved at begrænse adgangen til terrorrelateret onlineindhold.

4. VIRKNINGER FOR BUDGETTET

Forslaget til forordning påvirker ikke EU-budgettet.

5. ANDRE FORHOLD

5.1. Planer for gennemførelsen og foranstaltninger til overvågning, evaluering og rapportering

Kommissionen vil inden [et år efter denne forordnings ikrafttrædelsesdato] fastsætte et detaljeret program for overvågning af forordningens output, resultater og virkninger. Overvågningsprogrammet skal fastlægge metoderne til samt indikatorerne og intervallerne for indsamling af data og anden nødvendig dokumentation. Det skal specificere de tiltag, Kommissionen og medlemsstaterne skal gøre med hensyn til indsamling og analyse af data og andre beviser med henblik på at overvåge fremskridtene og evaluere denne forordning.

Kommissionen vil inden for to år efter denne forordnings ikrafttræden og på grundlag af det fastsatte overvågningsprogram rapportere om gennemførelsen af forordningen ud fra de gennemsigtighedsrapporter, som virksomhederne offentliggør, såvel som oplysninger tilvejebragt af medlemsstaterne. Kommissionen vil tidligst fire år efter forordningens ikrafttræden foretage en evaluering.

Kommissionen vil baseret på evalueringens konklusioner, herunder om hvorvidt der fortsat er visse huller eller sårbarheder, og under hensyntagen til den teknologiske udvikling, vurdere behovet for at udvide forordningens anvendelsesområde. Kommissionen vil om nødvendigt fremsætte forslag om tilpasning af denne forordning.

Kommissionen vil støtte gennemførelsen, overvågningen og evalueringen af forordningen via en ekspertgruppe under Kommissionen. Gruppen vil også fremme samarbejdet mellem hostingtjenesteyderne, de retshåndhævende myndigheder og Europol, fremme udveksling af praksis vedrørende sporing og fjernelse af terrorindhold, tilbyde sin ekspertise inden for udviklingen af terroristernes modus operandi på nettet såvel som yde rådgivning og vejledning, hvis det er passende, med henblik på gennemførelse af bestemmelserne.

Gennemførelsen af den foreslåede forordning kan fremmes ved hjælp af en række støtteforanstaltninger. Disse omfatter den mulige udvikling af en platform inden for rammerne af Europol, hvis formål vil være at bistå i koordineringen af indberetninger og påbud om fjernelse. EU-finansieret forskning i udviklingen inden for terroristernes modus operandi øger forståelsen og bevidstheden hos alle relevante interessenter. Dertil kommer, at Horisont 2020 støtter forskning med henblik på udvikling af nye teknologier, herunder automatisk forebyggelse af, at terrorindhold bliver uploadet. Endelig vil Kommissionen fortsat analysere, hvordan de kompetente myndigheder og hostingtjenesteyderne kan støttes i gennemførelsen af denne forordning via EU's finansielle instrumenter.

5.2. Nærmere redegørelse for de enkelte bestemmelser i forslaget

I artikel 1 fastsættes forordningens genstand, idet det anføres, at der med forordningen fastsættes regler, som skal forhindre misbrug af hostingtjenester til udbredelse af terrorrelateret onlineindhold, herunder hostingtjenesteydernes forpligtelse til at udvise rettidig omhu og foranstaltninger, som medlemsstaterne skal iværksætte. Desuden fastsættes det geografiske anvendelsesområde, som omfatter hostingtjenesteydere, der udbyder tjenester i Unionen, uanset hvor deres hovedsæde ligger.

Artikel 2 indeholder definitioner af de udtryk, der bruges i forslaget. Der fastsættes ligeledes en definition på terrorindhold til præventive formål med udgangspunkt i direktivet om bekæmpelse af terrorisme med det formål at inkludere materiale og informationer, som tilskynder til, opfordrer til eller slår til lyd for udførelse af eller bidrag til terrorhandlinger, giver instruktioner i udførelsen af sådanne handlinger eller promoverer deltagelsen i en terrorgruppes aktiviteter.

I artikel 3 fastsættes bestemmelser om den rettidige omhu, som hostingtjenesteyderne skal udvise, når de skrider til handling i henhold til denne forordning og navnlig under behørig hensyntagen til de berørte grundlæggende rettigheder. Det fastlægges, at der i hostingtjenesteydernes vilkår og betingelser skal fastsættes passende bestemmelser, og at det skal sikres, at disse anvendes.

I artikel 4 fastsættes det, at medlemsstaterne skal tillægge de kompetente myndigheder beføjelser til at udstede påbud om fjernelse, og det kræves, at hostingtjenesteyderne fjerner indholdet inden for en time efter modtagelse af et påbud om fjernelse. Der fastsættes ligeledes en række elementer, som påbud om fjernelse som minimum skal indeholde, og procedurer for hostingtjenesteydernes feedback til den udstedende myndighed, ligesom det fastsættes, at sidstnævnte skal underrettes, hvis det ikke er muligt at efterkomme påbuddet, eller hvis der er behov for yderligere præciseringer. Det kræves ligeså, at den udstedende myndighed underretter den myndighed, der fører tilsyn med gennemførelsen af proaktive foranstaltninger i den medlemsstat, som har jurisdiktion over hostingtjenesteyderen.

I artikel 5 fastsættes et krav til hostingtjenesteyderne om at træffe foranstaltninger til hurtigt at vurdere det indhold, som er fremlagt i en indberetning fra enten en kompetent myndighed i en medlemsstat eller et EU-organ, uden at der dog pålægges et krav om at fjerne det indberettede indhold eller fastsættes en specifik frist for handling. Det fastsættes ligeledes, hvilke elementer, indberetninger som minimum skal indeholde, og hvordan hostingtjenesteyderne skal give feedback til den udstedende myndighed og anmode om præciseringer hos den myndighed, som har indberettet indholdet.

I artikel 6 fastsættes det, at hostingtjenesteyderne, hvis det er relevant, skal træffe proaktive foranstaltninger. Der fastsættes en procedure, som sikrer, at visse hostingtjenesteydere (dvs. de, som har modtaget et påbud om fjernelse, der er blevet endeligt) træffer yderligere proaktive foranstaltninger, hvis det er nødvendigt for at afbøde risiciene og i overensstemmelse med graden af eksponering for terrorindhold på deres tjenester. Hostingtjenesteyderen skal samarbejde med den kompetente myndighed om de fornødne foranstaltninger, og hvis der ikke kan nås til enighed, kan myndigheden pålægge hostingtjenesteyderen foranstaltninger. I artiklen fastsættes der ligeledes en procedure for klager over myndighedens afgørelse.

I artikel 7 kræves det, at hostingtjenesteyderne opbevarer det fjernede indhold og de dertil knyttede data i seks måneder med henblik på klagesager og til efterforskningsformål. Denne periode kan forlænges for at muliggøre afslutning af klagesagen. Det kræves endvidere i artiklen, at tjenesteyderne skal indføre sikkerhedsforanstaltninger, som skal sikre, at det opbevarede indhold og de dertil knyttede data ikke kan tilgås eller behandles til andre formål.

I artikel 8 fastsættes en forpligtelse for hostingtjenesteyderne til at redegøre for deres politik over for terrorindhold og til at offentliggøre årlige gennemsigtighedsrapporter om de foranstaltninger, der er truffet i den forbindelse.

I artikel 9 fastsættes specifikke sikkerhedsforanstaltninger vedrørende brug og gennemførelse af proaktive foranstaltninger ved brug af automatiserede værktøjer, som skal sikre, at afgørelserne er korrekte og velfunderede.

I artikel 10 kræves det, at hostingtjenesteyderne indfører klagemekanismer i forbindelse med fjernelser, indberetninger og proaktive foranstaltninger, og at de nøje gennemgår hver eneste klage.

I artikel 11 fastsættes der en forpligtelse for hostingtjenesteyderne til at stille oplysninger om fjernelsen til rådighed for indholdsleverandøren, medmindre den kompetente myndighed kræver, at videregivelse af oplysninger ikke må finde sted af hensyn til den offentlige sikkerhed.

I artikel 12 kræves det, at medlemsstaterne sikrer, at de kompetente myndigheder har tilstrækkelig kapacitet og ressourcer til at opfylde deres forpligtelser i henhold til denne forordning.

I artikel 13 kræves det, at medlemsstaterne samarbejder med hinanden og, hvis det er passende, med Europol for at undgå dobbeltarbejde og forstyrrelser af efterforskninger. Artiklen giver også mulighed for, at medlemsstaterne og hostingtjenesteyderne kan gøre brug af særlige værktøjer, herunder Europols værktøjer, til behandling af og feedback på påbud om fjernelse og indberetninger, og for at de kan samarbejde om proaktive foranstaltninger. Det kræves også, at medlemsstaterne har passende kommunikationskanaler på plads, så de sikrer rettidig udveksling af oplysninger i gennemførelsen og håndhævelsen af denne forordnings bestemmelser. Artiklen pålægger desuden hostingtjenesteyderne at underrette de relevante myndigheder, når de bliver bekendt med beviser for terrorhandlinger som omhandlet i artikel 3 i direktiv (EU) 2017/541 om bekæmpelse af terrorisme.

I artikel 14 fastsættes det, at både hostingtjenesteyderne og medlemsstaterne skal etablere kontaktpunkter, der skal fremme kommunikationen imellem dem, navnlig hvad angår indberetninger og påbud om fjernelse.

I artikel 15 fastlægges medlemsstaternes jurisdiktion med henblik på kontrol med proaktive foranstaltninger, fastsættelse af sanktioner og overvågningsindsats.

I artikel 16 kræves det, at hostingtjenesteydere, som ikke er etableret i en medlemsstat, men som udbyder tjenester i Unionen, skal udpege en retlig repræsentant i Unionen.

I artikel 17 fastsættes det, at medlemsstaterne skal udpege de myndigheder, der skal udstede påbud om fjernelse og indberette terrorindhold samt føre tilsyn med gennemførelsen af proaktive foranstaltninger og håndhævelsen af denne forordning.

Af artikel 18 fremgår det, at medlemsstaterne skal fastsætte regler for sanktioner for manglende overholdelse, og der opstilles kriterier, som medlemsstaterne skal tage højde for, når de fastsætter sanktionernes art og størrelse. I betragtning af vigtigheden af hurtigt at fjerne det terrorindhold, der er identificeret i et påbud om fjernelse, bør der fastsættes specifikke regler for økonomiske sanktioner for systematiske krænkelser af dette krav.

I artikel 19 fastlægges en hurtigere og mere fleksibel procedure for, hvordan der via delegerede retsakter kan foretages ændringer af formularerne til brug ved påbud om fjernelse og autentificerede transmissionskanaler.

I artikel 20 fastsættes de betingelser, på hvilke Kommissionen har beføjelser til at vedtage delegerede retsakter med henblik på at foretage de nødvendige ændringer af formularerne og af de tekniske krav til påbud om fjernelse.

I artikel 21 pålægges medlemsstaterne at indsamle og indberette specifikke oplysninger om anvendelsen af forordningen med henblik på at bistå Kommissionen i udøvelsen af dennes opgaver i henhold til artikel 23. Kommissionen fastlægger et detaljeret program for overvågning af forordningens resultater og virkninger.

I artikel 22 fastsættes det, at Kommissionen to år efter forordningens ikrafttræden skal rapportere om dens gennemførelse.

I artikel 23 fastsættes det, at Kommissionen tidligst tre år efter forordningens ikrafttræden skal rapportere om dens evaluering.

I artikel 24 fastsættes det, at den foreslåede forordning vil træde i kraft på tyvendedagen efter offentliggørelsen i Den Europæiske Unions Tidende, og at den anvendes seks måneder efter dens ikrafttræden. Denne frist foreslås i betragtning af behovet for gennemførelsesforanstaltninger og i erkendelse af, at det haster med at anvende reglerne i den foreslåede forordning fuldt ud. Denne frist for gennemførelse på seks måneder er fastsat ud fra den antagelse, at forhandlingerne forløber hurtigt.

2018/0331 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om forebyggelse af udbredelsen af terrorrelateret onlineindhold

Et bidrag fra Europa-Kommissionen til ledernes møde i Salzburg den 19.-20. september 2018

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 114,

under henvisning til forslag fra Europa-Kommissionen,

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

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg[6],

efter den almindelige lovgivningsprocedure, og

ud fra følgende betragtninger:

(1) Denne forordning stiler mod at sikre et velfungerende digitalt indre marked i et åbent og demokratisk samfund ved at forebygge misbrug af hostingtjenester til terrorformål. Det digitale indre markeds funktion bør forbedres ved at højne hostingtjenesteydernes retssikkerhed, øge brugernes tillid til onlinemiljøet og styrke beskyttelsen af ytrings- og informationsfriheden.

(2) Hostingtjenesteydere, som er aktive på internettet, spiller en afgørende rolle i den digitale økonomi ved at skabe forbindelse mellem erhvervslivet og borgerne og ved at lette offentlig debat samt formidling og modtagelse af oplysninger, synspunkter og idéer, hvorved de bidrager betydeligt til innovation, økonomisk vækst og jobskabelse i Unionen. Imidlertid misbruges deres tjenester i visse tilfælde af tredjepart til at udføre ulovlige aktiviteter på nettet. Særligt bekymrende er det, at terrorgrupper og deres tilhængere misbruger hostingtjenester til at sprede terrorrelateret indhold på nettet og dermed udbrede deres budskab, radikalisere og rekruttere samt fremme og styre terroraktiviteter.

(3) Tilstedeværelsen af terrorrelateret indhold på nettet har alvorlige negative konsekvenser for brugerne, borgerne og samfundet som helhed såvel som for udbydere af onlinetjenester, der hoster sådant indhold, eftersom det underminerer brugernes tillid og skader udbydernes forretningsmodeller. I betragtning af deres centrale rolle og de teknologiske midler og kapaciteter, der er forbundet med de tjenester, som de leverer, har udbydere af onlinetjenester et særligt samfundsmæssigt ansvar for at

[6] EUT C […] af […], s. […].

beskytte deres tjenester mod terroristernes misbrug og hjælpe med at bekæmpe terrorrelateret indhold, som udbredes via deres tjenester.

(4) De bestræbelser på EU-niveau for at bekæmpe terrorrelateret onlineindhold, som blev påbegyndt i 2015 via en ramme for frivilligt samarbejde mellem medlemsstater og hostingtjenesteydere, skal suppleres af en klar retlig ramme for yderligere at begrænse adgangen til terrorrelateret onlineindhold og på passende vis håndtere et voksende problem. Denne retlige ramme stiler mod at bygge på den frivillige indsats, som blev styrket med Kommissionens henstilling (EU) 2018/334[7], og kommer som reaktion på opfordringer fra Europa-Parlamentet om at styrke foranstaltningerne til bekæmpelse af ulovligt og skadeligt indhold, og fra Rådet om at forbedre den automatiske sporing og fjernelse af indhold, der tilskynder til terrorhandlinger.

(5) Anvendelsen af denne forordning bør ikke påvirke anvendelsen af artikel 14 i direktiv 2000/31/EF[8]. Især bør enhver foranstaltning, som hostingtjenesteyderen træffer i overensstemmelse med denne forordning, herunder proaktive foranstaltninger, ikke i sig selv føre til, at tjenesteyderen mister den ansvarsfritagelse, som er fastsat i nævnte artikel. Denne forordning påvirker ikke de nationale myndigheder og domstoles beføjelser til at fastslå hostingtjenesteyders ansvar i specifikke sager, hvis betingelserne i artikel 14 i direktiv 2000/31/EF for ansvarsfritagelse ikke er opfyldt.

(6) I denne forordning er der fastsat regler, som skal forebygge misbrug af hostingtjenester til udbredelse af terrorrelateret onlineindhold og således garantere et velfungerende indre marked, under fuld overholdelse af de grundlæggende rettigheder, der er beskyttet i Unionens retsorden, og navnlig dem, der er sikret i Den Europæiske Unions charter om grundlæggende rettigheder.

(7) Denne forordning bidrager til beskyttelsen af den offentlige sikkerhed, idet den fastsætter passende og solide beskyttelsesforanstaltninger, som skal sørge for beskyttelse af de grundlæggende rettigheder, der er på spil. Dette omfatter retten til respekt for privatlivets fred og beskyttelse af personoplysninger, retten til effektiv retsbeskyttelse, ytringsfriheden, herunder retten til frit at modtage og videregive information, friheden til at oprette og drive egen virksomhed og princippet om ikkeforskelsbehandling. Kompetente myndigheder og hostingtjenesteydere bør kun træffe foranstaltninger, som er nødvendige, passende og forholdsmæssige i et demokratisk samfund, idet der tages hensyn til den særlige betydning, der tillægges ytrings- og informationsfriheden, som er en af de hjørnestenene i et pluralistisk, demokratisk samfund og en af de værdier, som Unionen bygger på. Foranstaltninger, som forstyrrer ytrings- og informationsfriheden, bør være yderst målrettede i den forstand, at de skal tjene til forebyggelse af udbredelsen af terrorindhold uden dermed dog at påvirke retten til lovligt at modtage og videregive information, under hensyntagen til den centrale rolle, som hostingtjenesteydere spiller for den offentlige debat samt formidling og modtagelse af oplysninger, synspunkter og idéer i overensstemmelse med lovgivningen.

(8) Retten til adgang til effektive retsmidler er fastlagt i artikel 19 i TEU og artikel 47 i Den Europæiske Unions charter om grundlæggende rettigheder. Enhver fysisk eller

---

[7] Kommissionens henstilling (EU) 2018/334 af 1.3.2018 om foranstaltninger til effektiv bekæmpelse af ulovligt indhold på nettet (EUT L 63 af 6.3.2018, s. 50).

[8] Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked ("direktivet om elektronisk handel") (EFT L 178 af 17.7.2000, s. 1).

juridisk person har ret til effektive retsmidler ved den kompetente nationale domstol til prøvelse af de foranstaltninger, som træffes i henhold til denne forordning, og som kan have negativ indvirkning på denne person. Denne ret omfatter navnlig muligheden for, at hostingstjenesteydere og indholdsleverandører reelt kan gøre indsigelse mod påbud om fjernelse ved retten i den medlemsstat, hvis myndigheder har udstedt påbuddet.

(9) For at skabe klarhed om de foranstaltninger, som både hostingtjenesteydere og kompetente myndigheder bør træffe for at forhindre udbredelse af terrorrelateret onlineindhold, bør der i denne forordning af forebyggelseshensyn fastsættes en definition af terrorindhold, der bygger på definitionen af terrorhandlinger som fastsat i Europa-Parlamentets og Rådets direktiv (EU) 2017/541[9]. I betragtning af behovet for at bekæmpe den mest skadelige terrorpropaganda på nettet bør definitionen omfatte materiale og informationer, som tilskynder til, opfordrer til eller slår til lyd for udførelse af eller bidrag til terrorhandlinger, giver instruktioner i udførelsen af sådanne handlinger eller promoverer deltagelsen i en terrorgruppes aktiviteter. Sådanne oplysninger omfatter især tekst, billeder, lydoptagelser og videoer. Når det vurderes, hvorvidt indholdet udgør terrorindhold som defineret i denne forordning, bør de kompetente myndigheder såvel som hostingtjenesteyderne tage højde for faktorer såsom udsagnenes art og ordlyd, den kontekst, de indgår i, og deres potentiale for at føre til skadelige konsekvenser for menneskers sikkerhed. Det faktum, at materialet er produceret af, kan tilskrives eller udbredes på vegne af en terrororganisation eller person, der er opført på EU's liste, spiller en stor rolle for vurderingen. Indhold, som udbredes til uddannelsesmæssige, journalistiske eller forskningsmæssige formål, bør beskyttes tilstrækkeligt. Fremsættelse af radikale, polemiske eller kontroversielle holdninger i den offentlige debat om følsomme politiske spørgsmål bør desuden ikke betragtes som terrorindhold.

(10) For at omfatte de hostingtjenester online, hvor terrorindholdet udbredes, bør denne forordning finde anvendelse på informationssamfundstjenester, som lagrer information fra en tjenestemodtager på dennes anmodning, og som gør de lagrede informationer tilgængelige for tredjepart, uanset om denne aktivitet udelukkende er af teknisk, automatisk eller passiv karakter. Sådanne udbydere af informationssamfundstjenester omfatter eksempelvis sociale medieplatforme, videostreamingtjenester, video-, billed- og lyddelingtjenester, fildeling og andre cloudtjenester, i det omfang de gør informationerne tilgængelige for tredjepart, og websteder, hvor brugerne kan kommentere og poste anmeldelser. Denne forordning bør også gælde for hostingtjenesteydere, der er etableret uden for Unionen, men som udbyder tjenester inden for Unionen, eftersom en betydelig del af de hostingtjenesteydere, der eksponeres for terrorindhold på deres tjenester, er etableret i tredjelande. Dette bør sikre, at alle virksomheder, som opererer i det digitale indre marked overholder samme krav, uanset hvor de er etableret. For at fastslå, om en tjenesteudbyder udbyder tjenester i Unionen, skal det vurderes, om tjenesteudbyderen gør det muligt for juridiske eller fysiske personer i en eller flere medlemsstater at gøre brug af udbyderens tjenester. 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 tilstrækkelig betingelse for, at denne forordning finder anvendelse.

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

(11) En væsentlig tilknytning til Unionen bør være relevant for bestemmelsen af denne forordnings anvendelsesområde. En sådan væsentlig tilknytning til Unionen anses for at eksistere, hvis en hostingtjenesteyder er etableret i Unionen, eller hvis dette ikke er tilfældet, hvis den har et betydeligt antal brugere i en eller flere medlemsstater eller målrettede aktiviteter mod en eller flere medlemsstater. Målretningen af aktiviteter mod en eller flere medlemsstater kan bestemmes på baggrund af alle relevante omstændigheder, herunder faktorer som anvendelse af et sprog eller en valuta, der normalt benyttes i den pågældende medlemsstat, eller muligheden for at bestille varer eller tjenesteydelser. Målretningen af aktiviteter mod en medlemsstat kan også udledes af, at en applikation er tilgængelig i den pågældende nationale appbutik, at der annonceres lokalt eller reklameres på en medlemsstats sprog, eller at kunderelationer håndteres, f.eks. at kundeservicen varetages, på det sprog, der normalt tales i denne medlemsstat. Der må også antages, at der findes en væsentlig tilknytning, hvis en tjenesteyder retter sine aktiviteter mod mere end én medlemsstat, jf. artikel 17, stk. 1, litra c), i Europa-Parlamentets og Rådets forordning (EU) nr. 1215/2012[10]. På den anden side kan leveringen af tjenesten alene med henblik på overholdelse af forbuddet mod forskelsbehandling som fastsat i Europa-Parlamentets og Rådets forordning (EU) 2018/302[11] ikke i sig selv anses for at udgøre målretning af aktiviteter mod et givet område inden for Unionen.

(12) Hostingtjenesteyderne skal udvise rettidig omhu for at forebygge udbredelse af terrorrelateret onlineindhold via deres tjenester. Denne omhu bør ikke indebære en generel forpligtelse til overvågning. Den rettidige omhu skal indebære, at hostingtjenesteyderne, når de anvender bestemmelserne i denne forordning, handler 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. Fjernelse eller deaktivering af adgangen skal foretages under overholdelse af ytrings- og informationsfriheden.

(13) De procedurer og forpligtelser i retssystemer, der kræver, at hostingtjenesteydere fjerner terrorindhold eller deaktiverer adgangen hertil, efter at de kompetente myndigheder har foretaget en vurdering, bør harmoniseres. Medlemsstaterne skal frit kunne vælge de kompetente myndigheder og således udpege de administrative, retshåndhævende eller retlige myndigheder, de ønsker skal varetage opgaven. Eftersom terrorindhold hastigt udbredes via onlinetjenester, pålægges hostingtjenesteyderne med denne bestemmelse at sikre, at det terrorindhold, der er identificeret i påbuddet om fjernelse, fjernes eller deaktiveres inden for en time efter modtagelse af påbuddet. Det er op til hostingtjenesteyderne at beslutte, hvorvidt indholdet skal fjernes, eller adgangen til det skal deaktiveres for brugere i Unionen.

(14) Den kompetente myndighed skal fremsende påbuddet om fjernelse direkte til modtageren og kontaktpunktet ved hjælp af enhver form for elektronisk middel, som kan efterlade et skriftligt spor, og som giver tjenesteyderen mulighed for at fastslå

---

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

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

ægtheden, herunder nøjagtigheden af datoen og tidspunktet for afsendelse og modtagelse af påbuddet, f.eks. sikker e-mail og platforme eller andre sikre kanaler, herunder dem, der stilles til rådighed af tjenesteyderen, i overensstemmelse med reglerne om beskyttelse af personoplysninger. Dette krav kan navnlig opfyldes ved brug af kvalificerede elektroniske registrerede leveringstjenester som defineret i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014[12].

(15) Indberetninger foretaget af kompetente myndigheder eller Europol er en hurtig og effektiv måde at gøre hostingtjenesteyderne opmærksomme på særligt indhold på deres tjenester. Denne mekanisme, hvor hostingtjenesteydere gøres bekendt med oplysninger, der kan betragtes som terrorindhold, og hvor hostingtjenesteyderne frivilligt vurderer, hvorvidt indholdet er i overensstemmelse med deres egne vilkår og betingelser, bør forblive tilgængelig som supplement til påbud om fjernelse. Det er vigtigt, at hostingtjenesteyderne prioriterer en vurdering af sådanne indberetninger, og at de hurtigt meddeler, hvilke foranstaltninger de har truffet. Den endelige afgørelse om, hvorvidt indholdet skal fjernes, fordi det ikke er foreneligt med deres vilkår og betingelser, eller hvorvidt det ikke skal, ligger hos hostingtjenesteyderne. Ved gennemførelse af denne forordning forbliver Europols mandat for så vidt angår indberetninger, jf. forordning (EU) 2016/794[13], uberørt.

(16) I betragtning af omfanget og den nødvendige hastighed for effektiv identifikation og fjernelse af terrorindhold er proaktive foranstaltninger, herunder i visse tilfælde brug af automatiserede værktøjer, et afgørende element i bekæmpelsen af terrorrelateret onlineindhold. Med henblik på at begrænse adgangen til terrorindhold via deres tjenester bør hostingtjenesteyderne vurdere, hvorvidt det er hensigtsmæssigt at træffe proaktive foranstaltninger afhængig af risiciene og graden af eksponering for terrorindhold samt af konsekvenserne for tredjeparts rettighed og offentlighedens interesse i oplysninger. Hostingstjenesteyderne bør derfor beslutte, hvilke passende, effektive og forholdsmæssige proaktive foranstaltninger, der bør iværksættes. Dette krav bør ikke indebære en generel forpligtelse til overvågning. I forbindelse med denne vurdering er manglende påbud om fjernelse og indberetninger stilet til en hostingtjenesteyder tegn på lav eksponering for terrorindhold.

(17) Hostingtjenesteyderne skal, når de iværksætter proaktive foranstaltninger, sikre, at brugernes ytrings- og informationsfrihed, herunder retten til frit at modtage og videregive information, bevares. Udover at opfylde de krav, der er fastsat i lovgivningen, herunder lovgivningen om beskyttelse af personoplysninger, bør hostingtjenesteyderne handle med behørig omhu og gennemføre sikkerhedsforanstaltninger, herunder især menneskeligt tilsyn og kontrol, hvis det er passende, med henblik på at undgå utilsigtede og fejlagtige beslutninger, der fører til fjernelse af indhold, som ikke er terrorindhold. Dette er særlig relevant, hvis hostingtjenesteyderne bruger automatiserede værktøjer til at spore terrorindhold. Enhver beslutning om at anvende automatiserede værktøjer, hvad enten den træffes på hostingtjenesteyderens eget initiativ eller på den kompetente myndigheds anmodning,

---

12 Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73).

13 Europa-Parlamentets og Rådets forordning (EU) 2016/794 af 11. maj 2016 om Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol) og om erstatning og ophævelse af Rådets afgørelse 2009/371/RIA, 2009/934/RIA, 2009/935/RIA, 2009/936/RIA og 2009/968/RIA (EUT L 135 af 24.5.2016, s. 53).

bør vurderes med hensyn til underliggende teknologis pålidelighed og de dermed forbundne konsekvenser for de grundlæggende rettigheder.

(18) For at sikre, at hostingtjenesteydere, der eksponeres for terrorindhold, træffer passende foranstaltninger for at forebygge misbrug af deres tjenester, bør de kompetente myndigheder anmode hostingtjenesteydere, som har modtaget et påbud om fjernelse, der er blevet endeligt, om at rapportere om de trufne proaktive foranstaltninger. Disse kan bestå af foranstaltninger til forebyggelse af genupload af terrorindhold, der er blevet fjernet eller deaktiveret som følge af et påbud eller en indberetning, som de har modtaget, og hvor der foretages kontrol ved hjælp af offentlige eller private værktøjer, som indeholder kendt terrorindhold. De kan ligeledes gøre brug af pålidelige tekniske værktøjer til identifikation af nyt terrorindhold; enten de værktøjer, der allerede er tilgængelige på markedet, eller de, som hostingtjenesteyderen selv udvikler. Hostingtjenesteyderen bør rapportere om de specifikke proaktive foranstaltninger, der er truffet, for at gøre det muligt for den kompetente myndighed at bedømme, om foranstaltningerne er effektive og forholdsmæssige, og om – hvis der bruges automatiserede værktøjer – hostingtjenesteyderen har den fornødne kapacitet til menneskeligt tilsyn og kontrol. De kompetente myndigheder bør i deres vurdering af foranstaltningernes effektivitet og forholdsmæssighed tage højde for relevante parametre, herunder antallet af påbud om fjernelse og indberetninger, der er udstedt til hostingtjenesteyderen, dennes økonomiske kapacitet og betydningen af dens tjenester for udbredelsen af terrorindhold (f.eks. under hensyntagen til antallet af brugere i Unionen).

(19) Efter anmodningen bør den kompetente myndighed gå i dialog med hostingtjenesteyderen om de fornødne proaktive foranstaltninger, der skal træffes. Hvis det er nødvendigt, bør den kompetente myndighed pålægge hostingtjenesteyderen at træffe passende, effektive og forholdsmæssige proaktive foranstaltninger, hvis den vurderer, at de trufne foranstaltninger er utilstrækkelige til at afbøde risiciene. En afgørelse om at pålægge sådanne specifikke proaktive foranstaltninger bør i princippet ikke føre til en generel forpligtelse til overvågning som omhandlet i artikel 15, stk. 1, i direktiv 2000/31/EF. I betragtning af de særligt alvorlige risici, der er forbundet med udbredelse af terrorindhold, kan de afgørelser, som de kompetente myndigheder træffer på grundlag af forordningen, afvige fra den tilgang, der er fastsat i artikel 15, stk. 1, i direktiv 2000/31/EF, med hensyn til visse specifikke, målrettede foranstaltninger, som det er nødvendigt at træffe af tvingende hensyn til den offentlige sikkerhed. Den kompetente myndighed bør, før den træffer sådanne afgørelser, finde en rimelig balance mellem de berørte offentlige interesser og de grundlæggende rettigheder, herunder især retten til ytrings- og informationsfrihed og retten til at oprette og drive egen virksomhed, og give en behørig begrundelse.

(20) Forpligtelsen for hostingtjenesteydere til at opbevare fjernet indhold og dertil knyttede data bør fastsættes til specifikke formål og være tidsbegrænset til den periode, der er nødvendig. Der er behov for at udvide kravet om opbevaring af data, da sådanne data ellers ville gå tabt som konsekvens af fjernelsen af det pågældende indhold. Dertil knyttede data omfatter data som eksempelvis "abonnentdata", herunder navnlig data vedrørende indholdsleverandørens identitet såvel som "adgangsdata", herunder f.eks. dato og tidspunkt for indholdsleverandørens brug eller log-in og log-off fra tjenesten sammen med den IP-adresse, som internetudbyderen har tildelt indholdsleverandøren.

(21) Forpligtelsen til at opbevare indholdet til brug i sager med administrativ eller retslig prøvelse er nødvendig og berettiget for at sikre effektive klagemuligheder for den indholdsleverandør, hvis indhold er blevet fjernet eller deaktiveret, og for at sikre, at

indholdet genindsættes, som det var, før det blev fjernet, alt afhængig af udfaldet af prøvelsen. Forpligtelsen til at opbevare indhold til efterforsknings- og retsforfølgningsformål er berettiget og nødvendigt i betragtning af den værdi, dette materiale kan tilføre med hensyn til at forstyrre eller forbygge terroraktiviteter. Hvis virksomheder fjerner indhold eller deaktiverer adgangen hertil, navnlig via deres egne proaktive foranstaltninger, og ikke underretter de relevante myndigheder, fordi de vurderer, at det ikke falder inden for anvendelsesområdet for artikel 13, stk. 4, i denne forordning, kan de retshåndhævende myndigheder være uvidende om indholdets eksistens. Derfor er opbevaring af indholdet til brug for forebyggelse, sporing, efterforskning og retsforfølgning af terrorhandlinger også berettiget. Med henblik herpå er den påkrævede opbevaring af data begrænset til data, som sandsynligvis er knyttet til terrorhandlinger, og som derfor kan bidrage til retsforfølgningen af terrorhandlinger eller til at forebygge alvorlige risici for den offentlige sikkerhed.

(22) For at sikre proportionalitet bør opbevaringsperioden være begrænset til seks måneder for at give indholdsleverandørerne tilstrækkelig tid til at indlede en klageproces og gøre det muligt for de retshåndhævende myndigheder at tilgå relevante data til brug for efterforskning og retsforfølgning af terrorhandlinger. På anmodning fra den myndighed, som foretager prøvelsen, kan denne periode imidlertid forlænges til den tid, der er nødvendig i tilfælde, hvor der er indledt en klagesag, men denne ikke er afsluttet inden udløbet af perioden på seks måneder. Denne varighed bør være tilstrækkelig til at gøre det muligt for de retshåndhævende myndigheder at bevare de nødvendige beviser til brug for efterforskninger, idet balancen i forhold til de grundlæggende rettigheder sikres.

(23) Denne forordning påvirker ikke de proceduremæssige garantier og de proceduremæssige efterforskningsforanstaltninger vedrørende adgangen til indholdet og de dertil knyttede data, der opbevares med henblik på efterforskning og retsforfølgning i terrorsager, som reguleret under medlemsstaternes nationale lovgivning og EU-retten.

(24) Gennemsigtighed i hostingtjenesteydernes politikker med hensyn til terrorindhold er afgørende for at øge tjenesteydernes ansvarlighed over for brugerne og styrke borgernes tillid til det digitale indre marked. Hostingtjenesteyderne bør offentliggøre årlige gennemsigtighedsrapporter med meningsfulde oplysninger om de foranstaltninger, der er truffet med hensyn til sporing, identifikation og fjernelse af terrorindhold.

(25) Klageprocedurer udgør en nødvendig sikkerhedsforanstaltning mod fejlagtig fjernelse af indhold, som er beskyttet under ytrings- og informationsfriheden. Hostingtjenesteydere bør derfor etablere brugervenlige klagemekanismer og sikre, at klager håndteres omgående og i fuld gennemsigtighed over for indholdsleverandøren. Kravet om, at hostingtjenesteyderen skal genindsætte indholdet, hvis det er blevet fjernet ved en fejl, påvirker ikke hostingtjenesteydernes mulighed for at håndhæve deres vilkår og betingelser af andre årsager.

(26) Effektiv retsbeskyttelse i henhold til artikel 19 i TEU og artikel 47 i Den Europæiske Unions charter om grundlæggende rettigheder kræver, at de berørte personer kan få kendskab til årsagerne til, at det indhold, som de har uploadet, er blevet fjernet eller adgangen hertil deaktiveret. Hostingstjenesteyderne bør med henblik herpå stille meningsfulde oplysninger til rådighed for indholdsleverandøren, så vedkommende kan gøre indsigelse mod denne beslutning. Dette kræver imidlertid ikke nødvendigvis, at indholdsleverandøren underrettes direkte. Afhængig af omstændighederne kan

hostingtjenesteyderne erstatte det indhold, der betragtes som terrorindhold, med en besked om, at det er blevet fjernet eller deaktiveret i overensstemmelse med denne forordning. Yderligere oplysninger om årsagerne og om indholdsleverandørens muligheder for at gøre indsigelse mod afgørelsen bør gives på anmodning. Hvis de kompetente myndigheder beslutter, at det af hensyn til offentlighedens sikkerhed, herunder i forbindelse med en efterforskning, er upassende eller kontraproduktivt at underrette indholdsleverandøren direkte om, at indholdet er blevet fjernet eller deaktiveret, bør de informere hostingtjenesteyderen herom.

(27) For at undgå dobbeltarbejde og forstyrrelser af efterforskninger bør de kompetente myndigheder informere, koordinere og samarbejde med hinanden og, hvis det er passende, med Europol, når de udsteder påbud om fjernelse eller sender indberetninger til hostingtjenesteydere. I gennemførelsen af bestemmelserne i denne forordning vil Europol kunne yde støtte i henhold til sit nuværende mandat og den gældende retlige ramme.

(28) For at sikre effektiv og tilstrækkeligt sammenhængende gennemførelse af proaktive foranstaltninger bør de kompetente myndigheder i medlemsstaterne kommunikere med hinanden vedrørende deres drøftelser med hostingtjenesteyderne med hensyn til indkredsning, gennemførelse og vurdering af specifikke proaktive foranstaltninger. Der er ligedan brug for et sådant samarbejde med hensyn til vedtagelse af regler om sanktioner såvel som gennemførelse og håndhævelse af sanktioner.

(29) Det er afgørende, at den kompetente myndighed, som er ansvarlig i en medlemsstat for at pålægge sanktioner, er fuldt ud informeret om udstedelsen af påbud om fjernelse og indberetninger og om efterfølgende udvekslinger mellem hostingtjenesteyderen og den relevante kompetente myndighed. Med henblik herpå bør medlemsstaterne tilvejebringe passende kommunikationskanaler og -mekanismer, som sikrer rettidig deling af relevante oplysninger.

(30) For at fremme hurtig udveksling mellem kompetente myndigheder såvel som med hostingtjenesteydere og for at undgå dobbeltarbejde kan medlemsstaterne gøre brug af de værktøjer, som Europol har udviklet, som eksempelvis applikationen til administration af internetindberetning eller opfølgningsværktøjer.

(31) I betragtning af noget terrorindholds særligt alvorlige konsekvenser bør hostingtjenesteyderne øjeblikkeligt informere myndighederne i den berørte medlemsstat eller de kompetente myndigheder, der hvor de er etableret eller har en retlig repræsentant, hvis de bliver bekendt med beviser for terrorhandlinger. For at sikre proportionalitet er denne forpligtelse begrænset til terrorhandlinger som defineret i artikel 3, stk. 1, i direktiv (EU) 2017/541. Forpligtelsen til underretning indebærer ikke, at hostingtjenesteyderne er forpligtet til aktivt at søge efter sådanne beviser. Den berørte medlemsstat er den medlemsstat, som har jurisdiktion med hensyn til efterforskning og retsforfølgning i sager med terrorhandlinger, jf. direktiv (EU) 2017/541, på grundlag af gerningsmandens eller det potentielle offers nationalitet, eller hvor målet for terrorhandlingen befinder sig. I tvivlstilfælde kan hostingtjenesteyderne sende oplysningerne til Europol, som i henhold til sit mandat bør følge op, herunder ved at videresende oplysningerne til de relevante nationale myndigheder.

(32) De kompetente myndigheder i medlemsstaterne bør have lov til at anvende sådanne oplysninger til at træffe efterforskningsforanstaltninger i henhold til national ret eller EU-retten, herunder til at udstede en europæisk editionskendelse i henhold til

forordningen om europæiske editions- og sikringskendelser om elektronisk bevismateriale i straffesager[14].

(33) Både hostingtjenesteyderne og medlemsstaterne bør oprette kontaktpunkter for at fremme en hurtig håndtering af påbud om fjernelse og indberetninger. Modsat den retlige repræsentant tjener kontaktpunkterne et operationelt formål. Hostingtjenesteyderens kontaktpunkt bør bestå af særlige midler, der muliggør elektronisk fremsendelse af påbud om fjernelse og indberetninger, og af tekniske og menneskelige ressourcer, der muliggør hurtig behandling heraf. Hostingtjenesteyderens kontaktpunkt skal ikke nødvendigvis befinde sig i Unionen, og hostingtjenesteyderen kan frit vælge et eksisterende kontaktpunkt under forudsætning af, at dette kontaktpunkt er i stand til at udføre de i denne forordning fastsatte funktioner. Med henblik på at sikre, at terrorindhold fjernes eller adgangen hertil deaktiveres inden for en time efter modtagelsen af påbuddet om fjernelse, bør hostingtjenesteyderne sikre, at deres kontaktpunkter er tilgængelige døgnet rundt. Oplysningerne om kontaktpunktet bør omfatte oplysninger om det sprog, som kontaktpunktet kan kontaktes på. For at lette kommunikationen mellem hostingtjenesteyderne og de kompetente myndigheder opfordres hostingtjenesteyderne til at muliggøre kommunikation på et af Unionens officielle sprog, på hvilket deres vilkår og betingelser foreligger.

(34) Da der ikke findes et generelt krav til hostingtjenesteyderne om at sikre en fysisk tilstedeværelse i Unionen, er der behov for at skabe klarhed om, under hvilken medlemsstats jurisdiktion en hostingtjenesteyder, der udbyder tjenester i Unionen, hører. Generelt hører hostingtjenesteyderen under jurisdiktionen i den medlemsstat, hvor den har sit hovedsæde, eller hvor den har udpeget sin retlige repræsentant. Hvis en anden medlemsstat udsteder et påbud om fjernelse, bør dets myndigheder ikke desto mindre være i stand til at håndhæve deres påbud ved at træffe indgribende foranstaltninger, som ikke er af præventiv karakter, som eksempelvis tvangsbøder. Med hensyn til hostingtjenesteydere, som ikke har noget hovedsæde i Unionen, og som ikke har udpeget en retlig repræsentant, bør enhver medlemsstat have mulighed for at pålægge sanktioner under forudsætning af, at ne bis in idem-princippet overholdes.

(35) De hostingtjenesteydere, som ikke er etableret i Unionen, bør skriftligt udpege en retlig repræsentant for at sikre overholdelse og håndhævelse af forpligtelserne i denne forordning.

(36) Den retlige repræsentant bør have retlig beføjelse til at agere på vegne af hostingtjenesteyderen.

(37) Medlemsstaterne bør med henblik på denne forordning udpege kompetente myndigheder. Kravet om at udpege kompetente myndigheder indebærer ikke nødvendigvis, at der bliver etableret nye myndigheder; eksisterende organer kan tildeles de i denne forordning fastsatte opgaver. Denne forordning kræver, at der udpeges myndigheder, som har kompetence til at udstede påbud om fjernelse, foretage indberetninger, føre tilsyn med proaktive foranstaltninger og pålægge sanktioner. Det er op til medlemsstaterne at afgøre, hvor mange myndigheder de ønsker at udpege til at løse disse opgaver.

[14] COM(2018) 225 final.

(38) Sanktioner er nødvendige for at sikre, at hostingtjenesteyderne på effektiv vis opfylder forpligtelserne i henhold til denne forordning. Medlemsstaterne bør vedtage regler om sanktioner, herunder, hvis det er nødvendigt, bøderetningslinjer. Der skal pålægges særligt alvorlige sanktioner i tilfælde, hvor hostingtjenesteyderen systematisk undlader at fjerne terrorindhold eller deaktivere adgangen dertil inden for en time efter modtagelse af et påbud om fjernelse. Manglende overholdelse i enkeltsager vil kunne sanktioneres under hensyntagen til ne bis in idem-princippet og proportionalitetsprincippet, og idet det sikres, at sådanne sanktioner tager højde for systematisk forsømmelse. For at sikre retssikkerheden bør forordningen fastsætte, i hvilket omfang forsømmelse af de relevante forpligtelser kan medføre sanktioner. Sanktioner for manglende overholdelse af artikel 6 bør kun pålægges i forbindelse med forpligtelser som følge af en anmodning om rapportering, jf. artikel 6, stk. 2, eller en afgørelse om pålæggelse af yderligere proaktive foranstaltninger, jf. artikel 6, stk. 4. Når det afgøres, hvorvidt der skal pålægges økonomiske sanktioner eller ej, bør der tages behørigt hensyn til hostingtjenesteyderens finansielle ressourcer. Medlemsstaterne skal sikre, at sanktionerne ikke tilskynder til fjernelse af indhold, som ikke er terrorrelateret.

(39) Anvendelsen af standardiserede formularer letter samarbejdet og informationsudvekslingen mellem de kompetente myndigheder og tjenesteydere og gør det muligt for dem at kommunikere hurtigere og mere effektivt. Det er særlig vigtigt at sikre, at der skrides hurtigt til handling efter modtagelse af et påbud om fjernelse. Formularer mindsker udgifterne til oversættelse og bidrager til en høj kvalitetsstandard. Svarformularerne bør ligeledes give mulighed for en standardiseret informationsudveksling, hvilket er særlig vigtigt, hvis tjenesteyderne ikke kan efterkomme påbuddet. Autentificerede transmissionskanaler kan garantere påbuddets autenticitet, herunder nøjagtigheden af datoen og tidspunktet for afsendelse og modtagelse af påbuddet.

(40) For at muliggøre hurtige ændringer, hvis det er nødvendigt, af indholdet af de formularer, der skal anvendes med henblik på denne forordning, bør beføjelsen til at vedtage retsakter i overensstemmelse med artikel 290 i traktaten om Den Europæiske Unions funktionsmåde uddelegeres til Kommissionen med henblik på at ændre bilag I, II og III til denne forordning. For at kunne tage højde for den teknologiske udvikling og den dertil knyttede retlige ramme bør Kommissionen ligeledes tillægges beføjelse til at vedtage delegerede retsakter med henblik på at supplere denne forordning med tekniske krav til de elektroniske midler, som de kompetente myndigheder skal anvende til at fremsende påbud om fjernelse. Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning[15]. For at sikre lige deltagelse i forberedelsen af delegerede retsakter modtager Europa-Parlamentet og Rådet navnlig alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter har systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.

(41) Medlemsstaterne bør indhente oplysninger om gennemførelse af lovgivningen. Der bør fastlægges et detaljeret program for overvågning af forordningens output,

[15] EUT L 123 af 12.5.2016, s. 1.

resultater og virkninger af denne forordning, der kan ligge til grund for en evaluering af lovgivningen.

(42) På grundlag af resultaterne og konklusionerne i gennemførelsesrapporten og udfaldet af overvågningen bør Kommissionen tidligst tre år efter forordningens ikrafttræden foretage en evaluering. Evalueringen bør være baseret på de fem kriterier: effektivitet, virkningsfuldhed, relevans, sammenhæng og merværdi for EU. Det vil blive vurderet, hvorvidt de forskellige operationelle og tekniske foranstaltninger i henhold til forordningen fungerer, herunder foranstaltningernes effektivitet med hensyn til at forbedre sporing, identifikation og fjernelse af terrorindhold, sikkerhedsforanstaltningernes effektivitet og virkningerne på tredjeparts potentielt berørte rettigheder og interesser, herunder en revision af kravet om underretning af indholdsleverandører.

(43) Målet for denne forordning, nemlig at sikre et velfungerende digitalt indre marked ved at forebygge udbredelse af terrorrelateret onlineindhold, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne og kan derfor på grund af begrænsningens omfang og virkninger bedre nås på EU-plan; Unionen kan derfor træffe foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke videre, end hvad der er nødvendigt for at nå dette mål —

VEDTAGET DENNE FORORDNING:

AFDELING I
ALMINDELIGE BESTEMMELSER

Artikel 1
Genstand og anvendelsesområde

1. I denne forordning fastlægges der ensartede bestemmelser, der skal forhindre misbrug af hostingtjenester til udbredelse af terrorrelateret onlineindhold. Der fastsættes navnlig:

   (a) regler for den rettidige omhu, som hostingtjenesteydere skal udvise for at forebygge udbredelse af terrorrelateret onlineindhold via deres tjenester og, hvis det er nødvendigt, sikre hurtig fjernelse

   (b) en række foranstaltninger, som medlemsstaterne skal gennemføre for at identificere terrorrelateret indhold, muliggøre hostingtjenesteydernes hurtige fjernelse heraf og fremme samarbejdet med de kompetente myndigheder i andre medlemsstaterne, med hostingtjenesteydere og, hvis det er relevant, med EU-organer.

2. Denne forordning finder anvendelse på hostingtjenesteydere, der udbyder tjenester i Unionen, uanset hvor der deres hovedsæde befinder sig.

Artikel 2
Definitioner

I denne forordning forstås ved:

(1) "hostingtjenesteyder": en udbyder af informationssamfundstjenester, der består i oplagring af information fra en tjenestemodtager på dennes anmodning og tilrådighedsstillelse af de lagrede informationer til tredjeparter

(2) "indholdsleverandør": en bruger, der har leveret oplysninger, som er eller har været lagret af en hostingtjenesteyder på brugerens anmodning

(3) "udbyde tjenester i Unionen": at gøre det muligt for juridiske eller fysiske personer i en eller flere medlemsstater at gøre brug af tjenester fra hostingudbyderen, som har en betydelig forbindelse til denne eller disse medlemsstater såsom:

(a) hostingtjenesteyderens etablering i Unionen

(b) et betydeligt antal brugere i en eller flere medlemsstater

(c) målrettede aktiviteter mod en eller flere medlemsstater.

(4) "terrorhandlinger": handlinger som defineret i artikel 3, stk. 1, i direktiv (EU)

(5) "terrorrelateret indhold": 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

(6) "udbredelse af terrorrelateret indhold": tilrådighedsstillelse af terrorrelateret indhold til tredjepart via hostingtjenesteydernes tjenester

(7) "vilkår og betingelser": alle vilkår, betingelser og klausuler, uanset navn eller form, som kontraktforholdet mellem hostingtjenesteyderen og dens brugere er underlagt

(8) "indberetning": en meddelelse fra en kompetent myndighed eller eventuelt et relevant EU-organ til en hostingtjenesteyder om oplysninger, der kan betragtes som terrorindhold, med henblik på leverandørens frivillige overvejelse af, hvorvidt indholdet er i overensstemmelse med dens egne vilkår og betingelser

(9) "hovedsæde": det hovedkontor eller hjemsted, hvor de primære finansielle funktioner og den operationelle kontrol udøves.

AFDELING II
Foranstaltninger til forebyggelse af udbredelse af terrorrelateret onlineindhold

Artikel 3
Rettidig omhu

1. Hostingtjenesteydere træffer i overensstemmelse med denne forordning passende, rimelige og forholdsmæssige foranstaltninger mod udbredelse af terrorrelateret indhold og til beskyttelse af brugerne mod terrorrelateret indhold. De handler i den forbindelse på en omhyggelig, forholdsmæssig og ikke-diskriminerende måde og under behørigt hensyn til brugernes grundlæggende rettigheder og den grundlæggende betydning af ytrings- og informationsfriheden i et åbent og demokratisk samfund.

2. Hostingtjenesteyderne fastsætter i deres vilkår og betingelser bestemmelser, der skal forebygge udbredelse af terrorrelateret indhold, og anvender disse.

Artikel 4
Påbud om fjernelse

1. Den kompetente myndighed har beføjelser til at træffe afgørelse om, at hostingtjenesteyderen skal fjerne terrorrelateret indhold eller deaktivere adgangen hertil.

2. Hostingtjenesteyderen skal fjerne det terrorrelaterede indhold eller deaktivere adgangen hertil inden for en time efter at have modtaget påbuddet om fjernelse.

3. Påbud om fjernelse skal i overensstemmelse med formularen i bilag I indeholde følgende:

   (a) identifikation af den kompetente myndighed, der udsteder påbuddet om fjernelse, og den kompetente myndigheds autentificering af påbuddet om fjernelse

   (b) en erklæring med en forklaring af, hvorfor indholdet betragtes som terrorrelateret indhold, med som minimum en henvisning til de kategorier af terrorrelateret indhold, der er opført i artikel 2, stk. 5

   (c) en internetadresse (Uniform Resource Locator, URL) og, hvis det er nødvendigt, yderligere oplysninger, som muliggør identifikation af det pågældende indhold

   (d) en henvisning til denne forordning som retsgrundlag for påbuddet om fjernelse

   (e) dato og tidstempel for udstedelsen

   (f) oplysninger om hostingtjenesteyderens og den pågældende indholdsleverandørs klagemuligheder

   (g) hvis det er relevant, afgørelsen om ikke at videregive oplysninger om fjernelsen af terrorindholdet eller deaktiveringen af adgangen hertil, jf. artikel 11.

4. Uden at det berører den forpligtelse, som hostingtjenesteyderen har til at efterkomme påbuddet om fjernelse inden for den i stk. 2 fastsatte frist, fremlægger den kompetente myndighed på anmodning fra hostingtjenesteyderen eller indholdsleverandøren en detaljeret begrundelse.

5. De kompetente myndigheder stiler påbuddet om fjernelse til hostingtjenesteyderens hovedsæde eller til den retlige repræsentant, som hostingtjenesteyderen har udpeget i henhold til artikel 16, og fremsender den til kontaktpunktet som omhandlet i artikel 14, stk. 1. Sådanne påbud sendes af elektronisk vej, som kan efterlade et skriftligt spor på en måde, der gør det muligt at verificere afsenderen, herunder nøjagtigheden af datoen og tidspunktet for afsendelse og modtagelse af påbuddet.

6. Hostingtjenesteyderne anerkender modtagelsen og underretter ved hjælp af formularen i bilag II uden unødig forsinkelse den kompetente myndighed om, at terrorindholdet er blevet fjernet eller adgangen hertil deaktiveret, idet især tidspunktet angives.

7. Hvis hostingtjenesteyderen ikke kan efterkomme påbuddet om fjernelse grundet force majeure eller faktisk umulighed, som ikke kan tilskrives hostingtjenesteyderen, skal den uden unødig forsinkelse informere den kompetente myndighed og begrunde hvorfor ved hjælp af formularen i bilag II. Den frist, der er fastsat i stk. 2, finder anvendelse, så snart de fremhævede årsager ikke længere er til stede.

8. Hvis hostingtjenesteyderen ikke kan efterkomme påbuddet om fjernelse, fordi det indeholder åbenbare fejl eller ikke indeholder tilstrækkelige oplysninger til, at påbuddet kan efterkommes, underretter hostingtjenesteyderen uden unødig forsinkelse den kompetente myndighed og udbeder sig en nærmere forklaring ved hjælp af formularen i bilag III. Den frist, der er fastsat i stk. 2, finder anvendelse ved modtagelsen af den nærmere forklaring.

9. Den kompetente myndighed, som har udstedt påbuddet om fjernelse, informerer den kompetente myndighed, som fører tilsyn med gennemførelsen af proaktive foranstaltninger, jf. artikel 17, stk. 1, litra c), når påbuddet bliver endeligt. Et påbud om fjernelse bliver endeligt, når der ikke er gjort indsigelse inden for den i henhold til national lovgivning fastsatte frist, eller hvis det er blevet stadfæstet efter en klage.

Artikel 5
Indberetninger

1. Den kompetente myndighed eller det relevante EU-organ kan sende en indberetning til en hostingtjenesteyder.

2. Hostingtjenesteydere iværksætter operationelle og tekniske foranstaltninger, som fremmer en hurtig vurdering af det indhold, der er fremsendt af de kompetente myndigheder, og eventuelt af relevante EU-organer til deres frivillige overvejelse.

3. Indberetningen stiles til hostingtjenesteyderens hovedsæde eller til den retlige repræsentant, som tjenesteyderen har udpeget i henhold til artikel 16, og fremsender den til kontaktpunktet som omhandlet i artikel 14, stk. 1. Sådanne indberetninger sendes elektronisk.

4. Indberetningen skal indeholde tilstrækkeligt detaljerede oplysninger, herunder årsagerne til, at indholdet betragtes som terrorrelateret, en URL og eventuelt yderligere oplysninger, som muliggør identifikation af det pågældende terrorindhold.

5. Hostingtjenesteyderen vurderer hurtigst muligt det identificerede indhold i indberetningen ud fra sine egne vilkår og betingelser og beslutter, hvorvidt indholdet skal fjernes eller adgangen dertil deaktiveres.

6. Hostingtjenesteyderen underretter hurtigt den kompetente myndighed eller det relevante EU-organ om resultatet af vurderingen og tidsplanen for enhver foranstaltning, der træffes som resultat af indberetningen.

7. Hvis hostingtjenesteyderen vurderer, at indberetningen ikke indeholder tilstrækkelige oplysninger til at vurdere det pågældende indhold, underretter den uden ophold de kompetente myndigheder eller det relevante EU-organ herom, idet den forklarer, hvilke oplysninger eller præciseringer der er behov for.

Artikel 6
Proaktive foranstaltninger

1. Hostingtjenesteyderne træffer, hvis det er passende, proaktive foranstaltninger til beskyttelse af deres tjenester mod udbredelse af terrorrelateret indhold. Foranstaltningerne skal være effektive og forholdsmæssige, tage højde for risikoen ved og omfanget af eksponering for terrorrelateret indhold, brugernes grundlæggende rettigheder og ytrings- og informationsfrihedens afgørende betydning i et åbent og demokratisk samfund.

2. Hvis den er blevet underrettet i henhold til artikel 4, stk. 9, skal den kompetente myndighed som omhandlet i artikel 17, stk. 1, litra c), anmode hostingtjenesteyderen om inden for tre måneder efter modtagelsen af anmodningen og derefter mindst en gang om året at fremlægge en rapport om de specifikke proaktive foranstaltninger, den har truffet, herunder ved hjælp af automatiserede værktøjer, med henblik på at:

   (a) forebygge genupload af indhold, der tidligere er blevet fjernet, eller hvortil adgangen allerede er blevet deaktiveret, fordi det anses for at være terrorrelateret indhold

   (b) spore, identificere og hurtigt fjerne eller deaktivere adgangen til terrorrelateret indhold.

   En sådan anmodning sendes til hostingtjenesteyderens hovedsæde eller til den retlige repræsentant, som tjenesteyderen har udpeget.

   Rapporterne skal indeholde alle relevante oplysninger, som gør det muligt for den kompetente myndighed som omhandlet i artikel 17, stk. 1, litra c), at vurdere, hvorvidt de proaktive foranstaltninger er effektive og forholdsmæssige, herunder at vurdere, hvordan redskaber til automatisk sporing, menneskeligt tilsyn og kontrolmekanismer anvendes.

3. Hvis den kompetente myndighed som omhandlet i artikel 17, stk. 1, litra c), mener, at de proaktive foranstaltninger, som er truffet og meddelt i henhold til stk. 2, er utilstrækkelige med hensyn til at afbøde og styre risikoen og niveauet for eksponering, kan den anmode hostingtjenesteyderen om at træffe yderligere proaktive foranstaltninger. Hostingtjenesteyderen samarbejder i den forbindelse med den kompetente myndighed som omhandlet i artikel 17, stk. 1, litra c), med henblik på at indkredse de specifikke foranstaltninger, som hostingtjenesteyderen skal iværksætte, fastsætte vigtige målsætninger og benchmarks samt frister for deres gennemførelse.

4. Hvis der ikke kan nås en aftale inden for tre måneder fra anmodningen som omhandlet i stk. 3, kan den kompetente myndighed som omhandlet i artikel 17, stk. 1, litra c), udstede en afgørelse, som pålægger særlige yderligere nødvendige og forholdsmæssige proaktive foranstaltninger. I afgørelsen tages der især højde for hostingtjenesteyderens økonomiske kapacitet og virkningen af sådanne foranstaltninger på brugernes grundlæggende rettigheder og den grundlæggende betydning af ytrings- og informationsfriheden. En sådan afgørelse sendes til hostingtjenesteyderens hovedsæde eller til den retlige repræsentant, som tjenesteyderen har udpeget. Hostingtjenesteyderen rapporterer regelmæssigt om gennemførelsen af sådanne foranstaltninger som specificeret af den kompetente myndighed, jf. artikel 17, stk. 1, litra c).

5. En hostingtjenesteyder kan til enhver tid anmode den kompetente myndighed som omhandlet i artikel 17, stk. 1, litra c), om at tage anmodninger eller afgørelser, jf. henholdsvis stk. 2, 3 og 4, op til revision og, hvis det er passende, tilbagekalde dem. Den kompetente myndighed fremlægger en detaljeret begrundelse inden for et rimeligt tidsrum efter at have modtaget anmodningen fra hostingtjenesteyderen.

Artikel 7
Opbevaring af indhold og dertil knyttede data

1. Hostingtjenesteyderne opbevarer det terrorindhold, som er blevet fjernet eller deaktiveret som følge af et påbud om fjernelse eller en indberetning eller som resultat

af en proaktiv foranstaltning i henhold til artikel 4, 5 og 6, og dertil knyttede data, som er blevet fjernet som konsekvens af fjernelsen af terrorindholdet, og som er nødvendigt for:

(a) sager med administrativ eller retslig prøvelse

(b) forebyggelse, sporing, efterforskning og retsforfølgning af terrorhandlinger.

2. Terrorindholdet og de dertil knyttede data som omhandlet i stk. 1 opbevares i seks måneder. På anmodning fra den kompetente myndighed eller domstol opbevares terrorindholdet i en længere periode, hvis og så længe det er nødvendigt for verserende sager med administrativ eller retslig prøvelse, jf. stk. 1, litra a).

3. Hostingtjenesteyderne sikrer, at der træffes passende tekniske og organisatoriske foranstaltninger til opbevaring af det i stk. 1 og 2 omhandlede terrorindhold og de dertil knyttede data.

Disse tekniske og organisatoriske foranstaltninger skal sikre, at det opbevarede terrorindhold og de dertil knyttede data kun tilgås og bruges til de formål, der er nævnt i stk. 1, og at der er et højt sikkerhedsniveau for opbevaringen af de pågældende personoplysninger. Hostingtjenesteyder reviderer og ajourfører disse foranstaltninger, hvis det er nødvendigt.

AFDELING III
SIKKERHEDSFORANSTALTNINGER OG ANSVARLIGHED

Artikel 8
Forpligtelser til gennemsigtighed

1. Hostingtjenesteyderne fastsætter i deres vilkår og betingelser deres politik for forebyggelse af udbredelse af terrorrelateret indhold, herunder, hvis det er passende, en meningsfuld forklaring af de proaktive foranstaltningers funktion, herunder brugen af redskaber til automatisk sporing.

2. Hostingtjenesteyderne offentliggør årlige gennemsigtighedsrapporter vedrørende de tiltag, der er gjort for at bekæmpe udbredelsen af terrorrelateret indhold.

3. Gennemsigtighedsrapporter skal mindst indeholde følgende oplysninger:

(a) oplysninger om hostingtjenesteyderens foranstaltninger for så vidt angår sporing, identifikation og fjernelse af terrorindhold

(b) oplysninger om hostingtjenesteyderens foranstaltninger for så vidt angår forebyggelse af genupload af indhold, der tidligere er blevet fjernet, eller hvortil adgangen allerede er blevet deaktiveret, fordi det anses for at være terrorrelateret indhold

(c) oplysninger om mængden af det indhold, der er fjernet, eller hvortil adgangen er deaktiveret som følge af henholdsvis påbud om fjernelse, indberetninger og proaktive foranstaltninger

(d) overblik over og udfaldet af klageprocedurer.

Artikel 9
Sikkerhedsforanstaltninger vedrørende brug og gennemførelse af proaktive foranstaltninger

1. Når hostingtjenesteyderne gør brug af automatiserede værktøjer i henhold til denne forordning, bør der være effektive og passende beskyttelsesforanstaltninger, der sikrer, at beslutninger vedrørende dette indhold, navnlig beslutninger om at fjerne

eller deaktivere adgangen til indhold, der anses for ulovligt indhold, er korrekte og velfunderede.

2. Beskyttelsesforanstaltningerne bør navnlig omfatte menneskeligt tilsyn og kontrol, hvor det er relevant og under alle omstændigheder, når en detaljeret vurdering af den relevante sammenhæng er nødvendig for at afgøre, hvorvidt indholdet anses for terrorindhold.

Artikel 10
Klagemekanismer

1. Hostingtjenesteyderne indfører effektive og tilgængelige mekanismer, som gør det muligt for indholdsleverandører, hvis indhold er blevet fjernet, eller hvor adgangen til indholdet er blevet deaktiviteret som følge af en indberetning i henhold til artikel 5 eller som følge af proaktive foranstaltninger i henhold til artikel 6, at indgive en klage mod hostingtjenesteyderens handlinger, idet der anmodes om genindsættelse af indholdet.

2. Hostingtjenesteyderne undersøger straks enhver klage, de modtager, og genindsætter indholdet uden unødig forsinkelse, hvis det uberettiget er blevet fjernet eller deaktiveret. De underretter klageren om udfaldet af undersøgelsen.

Artikel 11
Oplysninger til indholdsleverandører

1. Hvis hostingstjenesteydere fjerner terrorindhold eller deaktiverer adgangen hertil, stiller de oplysninger til rådighed for indholdsleverandøren om, at terrorindholdet er blevet fjernet eller deaktiveret.

2. På indholdsleverandørens anmodning informerer hostingstjenesteyderen denne om årsagerne til, at indholdet er blevet fjernet eller deaktiveret, og om mulighederne for at anfægte denne beslutning.

3. Forpligtelsen i stk. 1 og 2 finder ikke anvendelse, hvis den kompetente myndighed beslutter, at videregivelse af oplysninger ikke må finde sted af hensyn til den offentlige sikkerhed, såsom forebyggelse, efterforskning, sporing og retsforfølgning i terrorsager, så længe som nødvendigt, dog ikke længere end [fire] uger fra afgørelsen. Hostingstjenesteyderen videregiver i så tilfælde ikke nogen oplysninger om, at terrorindholdet er blevet fjernet, eller at adgangen hertil er blevet deaktiveret.

AFDELING IV
Samarbejde mellem kompetente myndigheder, EU-organer og hostingtjenesteydere

Artikel 12
De kompetente myndigheders kapaciteter

Medlemsstaterne sikrer, at deres kompetente myndigheder har de nødvendige kapaciteter og tilstrækkelige ressourcer til at nå målene og opfylde deres forpligtelser i henhold til denne forordning.

Artikel 13

Samarbejde mellem hostingtjenesteydere, kompetente myndigheder og eventuelt relevante EU-organer

1. De kompetente myndigheder i medlemsstaterne informerer, koordinerer og samarbejder med hinanden og, hvis det er passende, 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.

2. De kompetente myndighed i medlemsstaterne informerer, koordinerer og samarbejder med den kompetente myndighed som omhandlet i artikel 17, stk. 1, litra c) og d), med hensyn til de foranstaltninger, der træffes i henhold til artikel 6, og håndhævelsesforanstaltningerne i henhold til artikel 18. Medlemsstaterne sikrer, at den kompetente myndighed som omhandlet i artikel 17, stk. 1, litra c) og d), er i besiddelse af alle relevante oplysninger. Med henblik herpå tilvejebringer medlemsstaterne passende kommunikationskanaler eller -mekanismer, som sikrer rettidig deling af relevante oplysninger.

3. Medlemsstaterne og hostingtjenesteyderne kan vælge at gøre brug af særlige redskaber, herunder, hvis det er passende, de redskaber, som relevante EU-organer som eksempelvis Europol har etableret, for navnlig at fremme:

   (a) behandling og feedback vedrørende påbud om fjernelse i henhold til artikel 4

   (b) behandling og feedback vedrørende indberetninger i henhold til artikel 5

   (c) samarbejde med henblik på indkredsning og gennemførelse af proaktive foranstaltninger i henhold til artikel 6.

4. Hvis hostingtjenesteyderne bliver bekendt med beviser for terrorhandlinger, informerer de omgående de myndigheder, der er kompetente til at efterforske og retsforfølge strafbare handlinger i den berørte medlemsstat, eller kontaktpunktet i den medlemsstat, jf. artikel 14, stk. 2, hvor hostingtjenesteyderne har deres hovedsæde eller retlige repræsentant. Hostingtjenesteyderne kan i tvivlstilfælde videregive oplysningerne til Europol til opfølgning.

Artikel 14

Kontaktpunkter

1. Hostingtjenesteyderne etablerer kontaktpunkter, som gør det muligt at modtage påbud om fjernelse og indberetninger ad elektronisk vej og sikre deres hurtige behandling i henhold til artikel 4 og 5. De sikrer, at disse oplysninger gøres offentligt tilgængelige.

2. De i stk. 1 nævnte oplysninger skal præcisere det eller de officielle EU-sprog, jf. forordning nr. 1/58, på hvilke(t) der kan rettes henvendelse til kontaktpunktet, og på hvilket yderligere udvekslinger om påbud om fjernelse og indberetninger, jf. artikel 4 og 5, skal finde sted. Dette skal omfatte mindst ét af de officielle sprog i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde, eller hvor dens retlige repræsentant, jf. artikel 16, er bosiddende eller etableret.

3. Medlemsstaterne etablerer et kontaktpunkt, som håndterer anmodninger om præcisering og feedback for så vidt angår de påbud om fjernelse og indberetninger, som de har udstedt. Oplysninger om kontaktpunktet gøres offentligt tilgængelige.

AFDELING V
GENNEMFØRELSE OG HÅNDHÆVELSE

Artikel 15
Jurisdiktion

1. Den medlemsstat, hvor hostingtjenesteyderens hovedsæde befinder sig, har jurisdiktion med henblik på artikel 6, 18 og 21. En hostingtjenesteyder, hvis hovedsæde ikke befinder sig i en medlemsstat, anses for at høre under den medlemsstats jurisdiktion, hvor den retlige repræsentant som omhandlet i artikel 16 er bosiddende eller etableret.

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

3. Hvis en myndighed i en anden medlemsstat har udstedt et påbud om fjernelse i henhold til artikel 4, stk. 1, har denne medlemsstat kompetence til at træffe tvangsforanstaltninger i henhold til national ret for at håndhæve påbuddet om fjernelse.

Artikel 16
Retlig repræsentant

1. En hostingtjenesteyder, der ikke er etableret i Unionen, men som udbyder sine tjenester i Unionen, udpeger skriftligt 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 på grundlag af denne forordning. Den retlige repræsentant skal være bosiddende eller etableret i en af de medlemsstater, hvor hostingtjenesteyderen udbyder tjenester.

2. Hostingtjenesteyderen betror den retlige repræsentant at modtage, efterkomme og håndhæve påbud om fjernelse, indberetninger, anmodninger og afgørelser som omhandlet i stk. 1, på hostingtjenesteyderens vegne. Hostingtjenesteyderne giver deres retlige repræsentanter de beføjelser og ressourcer, der er nødvendige for at samarbejde med de kompetente myndigheder og efterkomme disse afgørelser og påbud.

3. Den udpegede retlige repræsentant kan drages til ansvar for manglende overholdelse af nærværende forordnings bestemmelser, uden at det berører hostingtjenesteyderens ansvar og de søgsmål, der vil kunne anlægges over for denne.

4. Hostingtjenesteyderen underretter den kompetente myndighed som omhandlet i artikel 17, stk. 1, litra d), i den medlemsstat, hvor den retlige repræsentant er bosiddende eller etableret, om udpegelsen. Oplysninger om den retlige repræsentant gøres offentligt tilgængelige.

AFDELING VI
AFSLUTTENDE BESTEMMELSER

Artikel 17
Udpegning af kompetente myndigheder

1. Hver medlemsstat udpeger den eller de myndigheder, der er kompetent for at:

(a) udstede påbud om fjernelse, jf. artikel 4

(b) spore og identificere terrorindhold og gøre hostingtjenesteyderne bekendt hermed, jf. artikel 5

(c) føre tilsyn med gennemførelsen af proaktive foranstaltninger, jf. artikel 6

(d) håndhæve forpligtelserne i henhold til denne forordning ved hjælp af sanktioner, jf. artikel 18.

2. Senest [*seks måneder efter denne forordnings ikrafttræden*] giver medlemsstaterne Kommissionen meddelelse om de kompetente myndigheder omhandlet i stk. 1. Kommissionen offentliggør meddelelsen og eventuelle ændringer heraf i *Den Europæiske Unions Tidende*.

Artikel 18
Sanktioner

1. Medlemsstaterne fastsætter de regler vedrørende sanktioner, der anvendes i tilfælde af hostingtjenesteydernes overtrædelser af denne forordning, og træffer alle fornødne foranstaltninger for at sikre sanktionernes gennemførelse. Sådanne sanktioner begrænses til overtrædelser af forpligtelserne i:

(a) artikel 3, stk. 2 (hostingtjenesteydernes vilkår og betingelser)

(b) artikel 4, stk. 2 og 6 (gennemførelse af og feedback om påbud om fjernelse)

(c) artikel 5, stk. 5 og 6 (vurdering af og feedback om indberetninger)

(d) artikel 6, stk. 2 og 4 (rapporter om proaktive foranstaltninger og vedtagelse af foranstaltninger efter en afgørelse, der pålægger specifikke proaktive foranstaltninger)

(e) artikel 7 (opbevaring af data)

(f) artikel 8 (gennemsigtighed)

(g) artikel 9 (sikkerhedsforanstaltninger vedrørende proaktive foranstaltninger)

(h) artikel 10 (klageprocedurer)

(i) artikel 11 (oplysninger til indholdsleverandører)

(j) artikel 13, stk. 4 (oplysninger om beviser på terrorhandlinger)

(k) artikel 14, stk. 1 (kontaktpunkter)

(l) artikel 16 (udpegelse af en retlig repræsentant).

2. Sanktionerne skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning. Medlemsstaterne giver senest den ... [*seks måneder efter denne forordnings ikrafttræden*] Kommissionen meddelelse om disse regler og foranstaltninger og underretter den straks om alle senere ændringer, der berører dem.

3. Medlemsstaterne sikrer, at de kompetente myndigheder ved fastsættelse af sanktionernes art og størrelse tager hensyn til alle relevante omstændigheder, herunder:

(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.

4. Medlemsstaterne sikrer, at systematisk mangel på overholdelse af forpligtelserne i artikel 4, stk. 2, medfører økonomiske sanktioner på op til 4 % af hostingtjenesteyderens samlede omsætning for det seneste regnskabsår.

Artikel 19
Tekniske krav og ændringer af formularen for påbud om fjernelse

1. Kommissionen tillægges beføjelse til at vedtage delegerede retsakter i overensstemmelse med artikel 20 med henblik på at supplere denne forordning med tekniske krav til de elektroniske midler, som de kompetente myndigheder skal anvende til at fremsende påbud om fjernelse.

2. Kommissionen tillægges beføjelse til at vedtage sådanne delegerede retsakter med henblik på at ændre bilag I, II og II for effektivt at imødegå et eventuelt behov for forbedringer af indholdet af formularerne for påbud om fjernelse og de formularer, der skal anvendes til at oplyse om, hvorfor det ikke er muligt at gennemføre påbuddet om fjernelse.

Artikel 20
Udøvelse af delegerede beføjelser

1. Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastlagte betingelser.

2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 19, tillægges Kommissionen for en ubegrænset periode fra [*denne forordnings ikrafttræden*].

3. Den i artikel 19 omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i Den Europæiske Unions Tidende eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.

4. Inden vedtagelsen af en delegeret retsakt hører Kommissionen eksperter, som er udpeget af hver enkelt medlemsstat, i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning.

5. Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidigt Europa-Parlamentet og Rådet meddelelse herom.

6. En delegeret retsakt vedtaget i henhold til artikel 19 træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på to måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har informeret Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med to måneder på Europa-Parlamentets eller Rådets initiativ.

Artikel 21
Overvågning

1. Medlemsstaterne indsamler oplysninger om de foranstaltninger, der er truffet i overensstemmelse med denne forordning, fra deres kompetente myndigheder og hostingtjenesteydere under deres jurisdiktion, og sender dem til Kommissionen senest den [31. marts] hvert år. Disse oplysninger skal omfatte:

   (a) oplysninger om antallet af udstedte påbud om fjernelse og indberetninger, mængden af det terrorindhold, som er blevet fjernet eller deaktiveret, herunder de tilsvarende frister, jf. artikel 4 og 5

   (b) oplysninger om de specifikke proaktive foranstaltninger, der er truffet i henhold til artikel 6, herunder mængden af det terrorindhold, som er blevet fjernet eller deaktiveret og de tilsvarende frister

   (c) oplysninger om antallet af indledte klageprocedurer og de foranstaltninger, som hostingtjenesteyderne har truffet i henhold til artikel 10

   (d) oplysninger om antallet af indledte søgsmålsprocedurer og de afgørelser, der er truffet af den kompetente myndighed i overensstemmelse med national ret.

2. Senest ..... [*et år efter denne forordnings anvendelsesdato*] fastlægger Kommissionen et detaljeret program for overvågning af forordningens output, resultater og virkninger. I overvågningsprogrammet fastlægges metoderne til samt indikatorerne og intervallerne for indsamling af data og anden nødvendig dokumentation. Det specificerer de tiltag, Kommissionen og medlemsstaterne skal gøre med hensyn til indsamling og analyse af data og andre beviser med henblik på at overvåge fremskridtene og evaluere denne forordning, jf. artikel 23.

Artikel 22
Gennemførelsesrapport

Senest ..... [*to år efter denne forordnings ikrafttræden*] forelægger Kommissionen en rapport for Europa-Parlamentet og Rådet om anvendelsen af denne forordning. Der tages i Kommissionens rapport hensyn til oplysninger om overvågning, jf. artikel 21, og oplysninger hidrørende fra forpligtelserne til gennemsigtighed, jf. artikel 8. Medlemsstaterne forlægger Kommissionen alle de oplysninger, der er nødvendige for udarbejdelsen af rapporten.

Artikel 23
Evaluering

Tidligst den ..... [*tre år efter denne forordnings anvendelsesdato*] foretager Kommissionen en evaluering af denne forordning og aflægger rapport til Europa-Parlamentet og Rådet om anvendelsen af denne forordning, herunder om sikkerhedsmekanismernes effektivitet. Om nødvendigt ledsages rapporten af forslag til retsakter. Medlemsstaterne forlægger Kommissionen alle de oplysninger, der er nødvendige for udarbejdelsen af rapporten.

Artikel 24
Ikrafttræden

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

Den anvendes fra den [seks måneder efter ikrafttrædelsen].

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den […].

På Europa-Parlamentets vegne	*På Rådets vegne*
Formand	*Formand*