Rådet for
Den Europæiske Union

Bruxelles, den 7. december 2018
(OR. en)

15336/18

Interinstitutionel sag:
2018/0331(COD)

CT 198
ENFOPOL 605
JAI 1264
COTER 175
CYBER 313
TELECOM 461
FREMP 222
AUDIO 121
DROIPEN 199
CODEC 2270

RESULTAT AF DRØFTELSERNE

fra:	Generalsekretariatet for Rådet
dato:	6. december 2018
til:	delegationerne
Tidl. dok. nr.:	14978/18 + COR 1
Komm. dok. nr.:	12129/18 + ADD 1-3
Vedr.:	Forslag til Europa-Parlamentets og Rådets forordning om forebyggelse af udbredelsen af terrorrelateret onlineindhold – generel indstilling

På samlingen den 6. december 2018 nåede Rådet til enighed om en generel indstilling, jf. bilaget.

Ændringer til Kommissionens forslag er angivet med ***fed skrift og kursiv*** for tilføjelser og med […] for udeladelser.

BILAG

[…]

[…] ***Udkast til***

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om forebyggelse af udbredelsen af terrorrelateret onlineindhold

[…]

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[1],

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.

[1] EUT C […] af […], s. […].

(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 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[2], 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.

[2] Kommissionens henstilling (EU) 2018/334 af 1. marts 2018 om foranstaltninger til effektiv bekæmpelse af ulovligt indhold på nettet (EUT L 63 af 6.3.2018, s. 50).

(5) Anvendelsen af denne forordning bør ikke påvirke anvendelsen af artikel 14 i direktiv 2000/31/EF[3]. 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. ***Denne forordning finder ikke anvendelse på aktiviteter vedrørende national sikkerhed, da denne forbliver den enkelte medlemsstats eneansvar.***

(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.

---

[3] 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).

(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 ***samt pressefriheden og mediepluralisme***, som er […] […] 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 terrorrelateret indhold 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 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 hostingtjenesteydere og indholdsleverandører reelt kan gøre indsigelse mod påbud om fjernelse ved retten i den medlemsstat, hvis myndigheder har udstedt påbuddet, ***og for, at hostingtjenesteydere kan gøre indsigelse mod afgørelser om at pålægge proaktive foranstaltninger eller sanktioner ved retten i den medlemsstat, hvor de er etableret eller har en retlig repræsentant.***

(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 terrorrelateret indhold, der bygger på definitionen af terrorhandlinger som fastsat i Europa-Parlamentets og Rådets direktiv (EU) 2017/541[4]. I betragtning af behovet for at bekæmpe den mest skadelige terrorpropaganda på nettet bør definitionen omfatte materiale […], som tilskynder til, opfordrer til eller slår til lyd for udførelse af eller bidrag til terrorhandlinger […] eller promoverer deltagelsen i en terrorgruppes aktiviteter. […] ***Definitionen omfatter indhold, der giver vejledning om fremstilling og brug af sprængstoffer, skydevåben eller andre våben eller skadelige eller farlige stoffer samt CBRN-stoffer eller om andre metoder eller teknikker, herunder udvælgelse af mål, med henblik på at begå terrorhandlinger.*** Sådant […] ***materiale*** omfatter især tekst, billeder, lydoptagelser og videoer. Når det vurderes, hvorvidt indholdet udgør terrorrelateret indhold 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 […] formål og ***modfortællings***- eller forskningsformål, bør beskyttes tilstrækkeligt***, idet der skal findes en rimelig balance mellem grundlæggende rettigheder, herunder navnlig ytrings- og informationsfriheden, og behovet for offentlig sikkerhed. Hvis det udbredte materiale offentliggøres under indholdsleverandørens redaktionelle ansvar, bør alle afgørelser om fjernelse af sådant indhold tage hensyn til de journalistiske standarder, der er fastlagt ved presse- eller medielovgivning i overensstemmelse med EU-retten, og retten til ytringsfrihed og retten til mediefrihed og mediernes pluralisme som nedfældet i artikel 11 i chartret om grundlæggende rettigheder.*** Fremsættelse af radikale, polemiske eller kontroversielle holdninger i den offentlige debat om følsomme politiske spørgsmål bør desuden ikke betragtes som terrorrelateret indhold.

---

[4] 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).

(10) For at omfatte de hostingtjenester online, hvor det terrorrelaterede indhold udbredes, bør denne forordning finde anvendelse på informationssamfundstjenester, som lagrer information ***og materiale*** fra en tjenestemodtager på dennes anmodning, og som gør de lagrede informationer ***og lagret materiale*** tilgængelige for tredjepart, uanset om denne aktivitet udelukkende er af teknisk, automatisk eller passiv karakter. […] ***Lagring af indhold består i at opbevare data i hukommelsen på en fysisk eller virtuel server; dette udelukker simple ledningskanaler og andre elektroniske kommunikationstjenester som defineret i [europæisk kodeks for elektronisk kommunikation] eller tjenesteydere af cachingtjenester fra anvendelsesområdet, eller andre tjenester, der leveres i andre lag af internetinfrastrukturen, f.eks. registre eller registratorer, DNS (domænenavnsystem) eller tilgrænsende tjenester såsom betalingstjenester eller DDoS-beskyttelsestjenester (Distributed Denial of Service). Endvidere skal oplysningerne lagres på indholdsleverandørens anmodning; kun de tjenester, som indholdsleverandøren er direkte modtager af, er omfattet. Endelig gøres de lagrede oplysninger tilgængelige for tredjeparter, forstået som enhver tredjepart, der ikke er indholdsleverandøren. Interpersonelle kommunikationstjenester, der muliggør direkte interpersonel og interaktiv informationsudveksling mellem et afgrænset antal personer, hvor de personer, der indleder eller deltager i kommunikationen, bestemmer hvem modtageren eller modtagerne skal være, er ikke omfattet.*** Sådanne udbydere af ***hostingtjenester*** […] omfatter eksempelvis sociale medieplatforme, videostreamingtjenester, video-, billed- og lyddelingtjenester, fildeling og andre cloud- ***og lagrings***tjenester […]. ***Denne forordning finder anvendelse på aktiviteten at levere hostingtjenester frem for på en specifik udbyder eller dennes fremherskende aktivitet, som kan være en kombination af hostingtjenester og andre tjenester, der ikke er omfattet af denne forordnings anvendelsesområde***.

(10a) 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 terrorrelateret indhold 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.

(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[5]. 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[6] ikke i sig selv anses for at udgøre målretning af aktiviteter mod et givet område inden for Unionen.

---

[5] 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).

[6] 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).

(12) Hostingtjenesteyderne skal udvise rettidig omhu for at forebygge udbredelse af terrorrelateret indhold 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 terrorrelateret ***indhold***. 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 terrorrelateret indhold 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 terrorrelateret indhold hastigt udbredes via onlinetjenester, pålægges hostingtjenesteyderne med denne bestemmelse at sikre, at det terrorrelaterede indhold, der er identificeret i påbuddet om fjernelse, fjernes eller deaktiveres inden for en time efter modtagelse af påbuddet. ***Uden at det berører kravet om at opbevare data i henhold til artikel 7 i denne forordning eller i henhold til [udkastet til lovgivning om elektronisk bevismateriale]***, er det op til hostingtjenesteyderne at beslutte, hvorvidt indholdet skal fjernes, eller adgangen til det skal deaktiveres for brugere i Unionen. ***Dette bør bevirke, at adgangen hindres, eller at det i det mindste gøres vanskeligt at opnå adgang, og at det i høj grad afholder de internetbrugere, der anvender deres tjenester, fra at få adgang til det indhold, hvortil adgang blev deaktiveret***.

(13a) Påbuddet om fjernelse bør omfatte en klassificering af det relevante indhold som terrorrelateret indhold og indeholde tilstrækkelige oplysninger med henblik på at lokalisere indholdet ved at angive en URL og eventuelle andre supplerende oplysninger såsom et screenshot af det pågældende indhold. Den kompetente myndighed bør efter anmodning give en supplerende begrundelse for, hvorfor indholdet anses som terrorrelateret indhold. Begrundelsen bør ikke indeholde følsomme oplysninger, der kan skade efterforskningen. Begrundelsen bør dog sætte hostingtjenesteyderen og i sidste ende indholdsleverandøren i stand til effektivt at udøve deres ret til retslig prøvelse.

(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 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[7].

[7] 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).

(15) […] […] **Indberetnings**mekanismen, hvor hostingtjenesteydere gøres bekendt med oplysninger **og materiale**, der kan betragtes som terrorrelateret indhold, og hvor hostingtjenesteyderne frivilligt vurderer, hvorvidt indholdet er i overensstemmelse **med** deres egne vilkår og betingelser, **er en særligt** […] **effektiv, hurtig og forholdsmæssig måde at gøre hostingtjenesteyderne opmærksomme på særligt indhold på deres tjenester** […]. 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[8], uberørt.

(16) I betragtning af omfanget og den nødvendige hastighed for effektiv identifikation og fjernelse af terrorrelateret indhold 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 terrorrelateret indhold via deres tjenester bør hostingtjenesteyderne vurdere, hvorvidt det er hensigtsmæssigt at træffe proaktive foranstaltninger afhængig af risiciene og graden af eksponering for terrorrelateret indhold samt af konsekvenserne for tredjeparts rettighed og offentlighedens interesse i oplysninger. Hostingtjenesteyderne 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 ***risiko eller*** eksponering for terrorrelateret indhold.

---

8 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).

(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 terrorrelateret indhold. 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, bør vurderes med hensyn til underliggende teknologis pålidelighed og de dermed forbundne konsekvenser for de grundlæggende rettidigheder.

(18) For at sikre, at hostingtjenesteydere, der eksponeres for terrorrelateret indhold, 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 terrorrelateret indhold, 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 terrorrelateret indhold. De kan ligeledes gøre brug af pålidelige tekniske værktøjer til identifikation af nyt terrorrelateret indhold; 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 terrorrelateret indhold (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 terrorrelateret indhold, 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, ***"transaktionsdata" og*** […] "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 materiale 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 terrorrelateret indhold er afgørende for at øge tjenesteydernes ansvarlighed over for brugerne og styrke borgernes tillid til det digitale indre marked. Hostingtjenesteyderne, ***der eksponeres for terrorrelateret indhold***, bør offentliggøre årlige gennemsigtighedsrapporter med meningsfulde oplysninger om de foranstaltninger, der er truffet med hensyn til sporing, identifikation og fjernelse af terrorrelateret indhold, hvis det ikke er i strid med formålet med de foranstaltninger, der er iværksat.

(25) Klageprocedurer udgør en nødvendig sikkerhedsforanstaltning mod fejlagtig fjernelse af indhold beskyttet under ytrings- og informationsfriheden ***i forbindelse med foranstaltninger, der træffes i henhold til hostingtjenesteydernes vilkår og betingelser***. 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. ***Desuden bør indholdsleverandører, hvis indhold er blevet fjernet som følge af et påbud om fjernelse, have adgang til effektive retsmidler i overensstemmelse med artikel 19 i TEU og artikel 47 Den Europæiske Unions charter om grundlæggende rettigheder.***

(26) ***Mere generelt kræver e***[…]ffektiv retsbeskyttelse i henhold til artikel 19 i TEU og artikel 47 i Den Europæiske Unions charter om grundlæggende rettigheder, at de berørte personer kan få kendskab til årsagerne til, at det indhold, som de har uploadet, er blevet fjernet eller adgangen hertil deaktiveret. Hostingtjenesteyderne 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 terrorrelateret indhold, 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 eventuelle forstyrrelser af efterforskninger bør de kompetente myndigheder informere, koordinere og samarbejde med hinanden og, hvis det er relevant, med Europol […], ***inden*** de udsteder påbud om fjernelse, eller ***når de*** sender indberetninger til hostingtjenesteydere. Når der træffes afgørelse om udstedelsen af påbud om fjernelse, bør den kompetente myndighed tage behørigt hensyn til alle indberetninger om forstyrrelser af efterforskningsmæssige interesser ("dekonfliktion"). […] ***Når der træffes afgørelse om udstedelse af påbud om fjernelse, bør den kompetente myndighed tage behørigt hensyn til alle indberetninger om forstyrrelser af efterforskningsmæssige interesser ("dekonfliktion"). Når en kompetent myndighed underrettes af en kompetent myndighed i en anden medlemsstat om et eksisterende påbud om fjernelse, bør påbuddet ikke udstedes i to eksemplarer.*** 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 tilsvarende brug for et sådant samarbejde med hensyn til vedtagelse af regler om sanktioner såvel som gennemførelse og håndhævelse af sanktioner. ***Kommissionen bør fremme denne koordinering og dette samarbejde.***

(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 ***opfordres*** medlemsstaterne […] til at gøre brug af ***de særlige*** værktøjer, som Europol har udviklet, som eksempelvis applikationen til administration af internetindberetning eller opfølgningsværktøjer.

(31) I betragtning af noget terrorrelateret indholds 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[9].

(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, ***interne eller eksterne***, der muliggør elektronisk fremsendelse af påbud om fjernelse og indberetninger, […] ***eller*** 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 terrorrelateret indhold fjernes eller adgangen hertil deaktiveres inden for en time efter modtagelsen af påbuddet om fjernelse, bør de ***hostingtjenesteydere, som eksponeres for terrorrelateret indhold, der dokumenteres ved modtagelse af et påbud om fjernelse,*** 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. ***Af hensyn til en effektiv gennemførelse, en påtrængende nødvendighed og den offentlige orden bør enhver medlemsstat dog have jurisdiktion i forbindelse med påbud om fjernelse og indberetninger.***

---

9 COM(2018)225 final.

(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. ***Hostingtjenesteydere kan gøre brug af en eksisterende retlig repræsentant, forudsat at denne retlige repræsentant er i stand til at udføre de opgaver, der er fastsat 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.

(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, ***der kan være af administrativ eller strafferetlig karakter***, herunder, hvis det er nødvendigt, bøderetningslinjer. Der skal pålægges særligt alvorlige sanktioner i tilfælde, hvor hostingtjenesteyderen systematisk undlader at fjerne terrorrelateret indhold 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. ***Ved vurdering af overtrædelsens art og afgørelse om anvendelse af sanktioner bør der tages fuldt hensyn til grundlæggende rettigheder såsom ytringsfriheden***. 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[10]. 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. ***Medlemsstaterne kan anvende hostingtjenesteydernes gennemsigtighedsrapporter og om nødvendigt supplere med mere detaljerede oplysninger.*** Der bør fastlægges et detaljeret program for overvågning af forordningens output, resultater og virkninger, der kan ligge til grund for en evaluering af lovgivningen.

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

(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 terrorrelateret indhold, 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.

3. **Denne forordning indebærer ikke nogen ændring af pligten til at respektere de grundlæggende rettigheder og grundlæggende retsprincipper, således som de er defineret i artikel 6 i traktaten om Den Europæiske Union.**

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 hostingtjenesteyderen, som har en betydelig forbindelse til denne eller disse medlemsstater, såsom hostingtjenesteyderens etablering i Unionen.

I mangel af en sådan etablering baseres vurderingen af en betydelig forbindelse på specifikke faktuelle kriterier såsom

a) ***et*** betydeligt antal brugere i en eller flere medlemsstater

b) ***eller*** målrettede aktiviteter mod en eller flere medlemsstater.

4) "terrorhandlinger": en af de ***forsætlige handlinger på listen*** […] i artikel 3, stk. 1, i direktiv (EU) 2017/541

5) "terrorrelateret indhold": […] ***materiale***, ***der kan bidrage til, at der begås forsætlige handlinger som opført på listen i artikel 3, stk. 1, litra a)-i), i direktiv 2017/541 ved***:

aa) trusler om at begå en terrorhandling

a) opfordring til eller slåen til lyd for, […] ***f.eks. ved*** […] ***forherligelse af terrorhandlinger***, udførelse af terrorhandlinger, hvorved der forårsages fare for, at sådanne handlinger begås

b) ***hvervning af personer eller en gruppe af personer til at begå*** […] eller bidrage til terrorhandlinger

c) promovering af en terrorgruppes aktiviteter, navnlig ved at ***hverve personer eller en gruppe af personer*** […] til at deltage […] i eller støtte en terrorgruppes ***kriminelle aktiviteter***, […] jf. den i artikel 2, stk. 3, i direktiv (EU) 2017/541 fastsatte betydning

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 terrorrelateret indhold, 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 ***i Unionen***.

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, ***at de ikke vil lagre terrorrelateret indhold*** og anvender bestemmelser, der skal forebygge udbredelse af terrorrelateret indhold.

Artikel 4

Påbud om fjernelse

1. Den kompetente myndighed har beføjelser til at udstede et […] ***påbud om fjernelse*** og kræve, 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; […] ***en vurdering af indholdet***, som minimum med en henvisning til de ***relevante*** kategorier af terrorrelateret indhold, der er opført i artikel 2, stk. 5

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

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

d) dato og tidstempel for udstedelsen

e) oplysninger om hostingtjenesteyderens og den pågældende indholdsleverandørs klagemuligheder

f) hvis det er relevant, afgørelsen om ikke at videregive oplysninger om fjernelsen af det terrorrelaterede indhold 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 ***supplerende*** begrundelse ***med en forklaring af, hvorfor indholdet betragtes som terrorrelateret indhold.***

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. ***Uden unødig forsinkelse*** anerkender Hostingtjenesteyderne […] modtagelsen og underretter ved hjælp af formularen i bilag II […] den kompetente myndighed om, at det terrorrelaterede indhold 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 III. 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 4a

Konsultationsprocedure for påbud om fjernelse

1. Den udstedende myndighed fremsender en kopi af påbuddet om fjernelse til den kompetente myndighed, der er omhandlet i artikel 17, stk. 1, litra a), i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde, samtidig med, at den fremsendes til hostingtjenesteyderen i overensstemmelse med artikel 4, stk. 5.

2. I tilfælde hvor den kompetente myndighed i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde, har rimelig grund til at antage, at påbuddet om fjernelse kan have en indvirkning på den medlemsstats grundlæggende interesser, underretter den den udstedende kompetente myndighed.

3. Den udstedende myndighed tager højde for disse omstændigheder, og tilbagetrækker eller tilpasser påbuddet om fjernelse, hvor det er nødvendigt.

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 tilstrækkelige […] […]oplysninger […] ***om*** årsagerne til, at indholdet betragtes som terrorrelateret, og ***angive en*** URL og eventuelt yderligere oplysninger, som muliggør identifikation af det pågældende terrorrelaterede indhold.
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 ***uden unødig forsinkelse*** […] 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 […] ***afhængigt af risikoen og graden af eksponering for terrorrelateret indhold*** 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

   a) […] ***effektivt at sætte en stopper*** for, […] at indhold, der tidligere er blevet fjernet, ***vises igen***, eller hvortil adgangen allerede er blevet deaktiveret, fordi det anses for at være terrorrelateret indhold

   b) at 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. ***Den kompetente myndighed som omhandlet i artikel 17, stk. 1, litra c), har skønsbeføjelse til at bestemme karakteren og omfanget af de proaktive foranstaltninger, jf. målet med denne forordning.*** 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 terrorrelaterede indhold, 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 det terrorrelaterede indhold, […] som er nødvendigt for:

   a) sager med administrativ eller retslig prøvelse

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

2. Det terrorrelaterede indhold og de dertil knyttede data som omhandlet i stk. 1 opbevares i seks måneder. På anmodning fra den kompetente myndighed eller domstol opbevares det terrorrelaterede indhold 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 terrorrelaterede indhold og de dertil knyttede data.

   Disse tekniske og organisatoriske foranstaltninger skal sikre, at det opbevarede terrorrelaterede indhold 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. Hostingtjenesteyderne 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, […] ***som eksponeres for terrorrelateret indhold***, 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 terrorrelateret indhold
   b) oplysninger om hostingtjenesteyderens foranstaltninger med henblik på […] ***effektivt at sætte en stopper for***, […] at indhold, der tidligere er blevet fjernet, ***vises*** igen, eller hvortil adgangen allerede er blevet deaktiveret, fordi det anses for at være terrorrelateret indhold
   c) oplysninger om mængden af det terrorrelaterede 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 terrorrelateret 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 terrorrelateret indhold.

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 deaktiveret 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 hostingtjenesteydere 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 hostingtjenesteyderen 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 […] ***seks*** uger fra afgørelsen. ***Denne periode kan forlænges én gang med yderligere seks uger, hvis det er berettiget.*** Hostingtjenesteyderen videregiver i så tilfælde ikke nogen oplysninger om, at det terrorrelaterede indhold er blevet fjernet, eller at adgangen hertil er blevet deaktiveret.

AFDELING IV

Samarbejde mellem kompetente myndigheder, EU-organer og hostingtjenesteydere

Artikel 12

Udpegelse af kompetente myndigheder

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 […] ***kompetente*** *EU-organer*

1. De kompetente myndigheder i medlemsstaterne informerer, koordinerer og samarbejder med hinanden og, hvis det er passende, med […] ***kompetente*** 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. ***For at denne forordning kan gennemføres effektivt og for at undgå overlapning,*** kan medlemsstaterne og hostingtjenesteyderne vælge at gøre brug af særlige redskaber, herunder […] de redskaber, som ***kompetente*** 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 eller de berørte medlemsstater […]. ***Hvis det er umuligt at identificere den eller de pågældende medlemsstater, underretter h***[…]ostingtjenesteyderne […] ***kontaktpunktet i den medlemsstat, jf. artikel 14, stk. 3, hvor hostingtjenesteyderne har deres hovedsæde eller retlige repræsentant***, og videregiver ***også*** 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. ***Alle medlemsstater har jurisdiktion med henblik på artikel 4 og 5, uanset hvor hostingtjenesteyderen har hovedsæde eller har udpeget en retlig repræsentant.***

2. Hvis en hostingtjenesteyder ikke udpeger en retlig repræsentant, har alle medlemsstater kompetence. ***Hvis en medlemsstat beslutter at udøve sin kompetence, underretter den alle øvrige medlemsstater.***

[…] […]

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 til

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

   b) at spore og identificere terrorrelateret indhold og gøre hostingtjenesteyderne bekendt hermed, jf. artikel 5

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

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

2. Senest [***tolv*** […] *måneder efter denne forordnings ikrafttræden*] giver medlemsstaterne Kommissionen meddelelse om den eller 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 [*...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 ***eller fysiske*** person, der er ansvarlig for overtrædelsen, tidligere har begået

d) den ansvarlige juridiske ***eller fysiske*** 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 III 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 de 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 terrorrelaterede indhold, 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 terrorrelaterede indhold, 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

Gennemførelsesrapporter

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

Ikrafttrædelse

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

Den anvendes fra [***12***[…] måneder efter ikrafttrædelsen].

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

Udfærdiget i Bruxelles, den […].

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