Den Europæiske Unions

Tidende

C 135

64. årgang

Dansk udgave

Meddelelser og oplysninger

16. april 2021

Indhold

DA

([1]) EØS-relevant tekst.

III

(Forberedende retsakter)

RÅDET

RÅDETS FØRSTEBEHANDLINGSHOLDNING (EU) nr. 6/2021

med henblik på vedtagelse af Europa-Parlamentets og Rådets forordning om håndtering af udbredelsen af terrorrelateret indhold online

Vedtaget af Rådet den 16. marts 2021

(EØS-relevant tekst)

(2021/C 135/01)

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 ([2]), 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 håndtere misbrug af hostingtjenester til terrorformål og bidrage til den offentlige sikkerhed i hele Unionen. Det digitale indre markeds funktion bør forbedres ved at højne hostingtjenesteydernes retssikkerhed, øge brugernes tillid til onlinemiljøet og styrke beskyttelsen af ytringsfriheden, herunder friheden til at modtage og meddele oplysninger og tanker i et åbent og demokratisk samfund og mediefriheden og -pluralismen.

(2) Lovgivningsmæssige foranstaltninger til håndtering af udbredelsen af terrorrelateret indhold online bør suppleres af medlemsstaternes terrorbekæmpelsesstrategier, herunder styrkelsen af mediekendskab og kritisk tænkning, udviklingen af alternative narrativer og modnarrativer, og andre initiativer, der kan mindske konsekvenserne af og sårbarheden over for terrorrelateret indhold online, samt investering i socialt arbejde, afradikaliseringsinitiativer og samarbejde med berørte samfund med henblik på at opnå vedvarende forebyggelse af radikalisering i samfundet.

(3) Håndteringen af terrorrelateret indhold online, hvilket er en del af et mere generelt problem med ulovligt indhold online, kræver en kombination af lovgivningsmæssige, ikkelovgivningsmæssige og frivillige foranstaltninger baseret på samarbejde mellem myndigheder og hostingtjenesteydere på en måde, der fuldt ud respekterer de grundlæggende rettigheder.

([1]) EUT C 110 af 22.3.2019, s. 67.

([2]) Europa-Parlamentets holdning af 17.4.2019 (endnu ikke offentliggjort i EUT) og Rådets førstebehandlingsholdning af 16.3.2021. Europa-Parlamentets holdning af … (endnu ikke offentliggjort i EUT).

(4) 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 hostingtjenesteydernes tjenester i visse tilfælde af tredjeparter med henblik på at udføre ulovlige aktiviteter online. Særligt bekymrende er det, at terrorgrupper og deres tilhængere misbruger disse tjenester til at sprede terrorrelateret indhold online med henblik på at udbrede deres budskab, radikalisere og rekruttere tilhængere samt lette og styre terroraktiviteter.

(5) Selv om det ikke er den eneste faktor, har tilstedeværelsen af terrorrelateret indhold online vist sig at være en katalysator for radikalisering af personer, hvilket kan føre til terrorhandlinger og derfor har alvorlige negative konsekvenser for brugere, borgere og samfundet som helhed såvel som for udbydere af onlinetjenester, der hoster sådant indhold, eftersom det underminerer deres brugeres tillid og skader deres forretningsmodeller. Hostingtjenesteydere har i betragtning af deres centrale rolle og de teknologiske midler og kapaciteter, der er forbundet med de tjenester, som de leverer, et særligt samfundsmæssigt ansvar for at beskytte deres tjenester mod terroristers misbrug og hjælpe med at håndtere terrorrelateret indhold, som udbredes via deres onlinetjenester, samtidig med at den grundlæggende betydning af ytringsfriheden, herunder friheden til at modtage og meddele oplysninger og tanker i et åbent og demokratisk samfund, tages i betragtning.

(6) Bestræbelser på EU-niveau for at bekæmpe terrorrelateret indhold online blev påbegyndt i 2015 via en ramme for frivilligt samarbejde mellem medlemsstater og hostingtjenesteydere. Der er behov for at supplere disse bestræbelser med en klar retlig ramme for yderligere at begrænse adgangen til terrorrelateret indhold online og på passende vis gribe ind over for et hastigt udviklende problem. Den retlige ramme har til hensigt at bygge på frivillige indsatser, som blev styrket med Kommissionens henstilling (EU) 2018/334 ([3]), og er en reaktion på opfordringer fra Europa-Parlamentet til at styrke foranstaltninger til at håndtere ulovligt og skadeligt indhold online i overensstemmelse med den horisontale ramme, der blev etableret ved Europa-Parlamentets og Rådets direktiv 2000/31/EF ([4]), samt fra Rådet, om at forbedre afsløringen og fjernelsen af indhold online, der tilskynder terrorhandlinger.

(7) Denne forordning bør ikke påvirke anvendelsen af direktiv 2000/31/EF. Især bør enhver foranstaltning, herunder eventuelle specifikke foranstaltninger, som en hostingtjenesteyder træffer i overensstemmelse med denne forordning ikke i sig selv føre til, at hostingtjenesteyderen mister den ansvarsfritagelse, som er fastsat i nævnte direktiv. Derudover påvirker denne forordning ikke de nationale myndigheder og domstoles beføjelser til at fastslå hostingtjenesteyders ansvar, hvor betingelserne fastlagt i nævnte direktiv for ansvarsfritagelse ikke er opfyldt.

(8) I tilfælde af uoverensstemmelse mellem denne forordning og Europa-Parlamentets og Rådets direktiv 2010/13/EU ([5]) med hensyn til bestemmelser om audiovisuelle medietjenester som defineret i artikel 1, stk. 1, litra a), i nævnte direktiv, bør direktiv 2010/13/EU have forrang. Dette bør ikke påvirke forpligtelserne i henhold til denne forordning, navnlig vedrørende udbydere af videodelingsplatformstjenester.

(9) Denne forordning bør fastsætte regler til at håndtere misbrug af hostingtjenester til udbredelse af terrorrelateret indhold online med henblik på at garantere et velfungerende indre marked. Disse regler bør fuldt ud respektere de grundlæggende rettigheder, der er beskyttet i Unionen, og navnlig dem, der er sikret i Den Europæiske Unions charter om grundlæggende rettigheder (»chartret«).

([3]) 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).

([4]) 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).

([5]) Europa-Parlamentets og Rådets direktiv 2010/13/EU af 10. marts 2010 om samordning af visse love og administrative bestemmelser i medlemsstaterne om udbud af audiovisuelle medietjenester (direktiv om audiovisuelle medietjenester) (EUT L 95 af 15.4.2010, s. 1).

(10) Denne forordning har til hensigt at bidrage til beskyttelsen af den offentlige sikkerhed, mens den fastsætter passende og solide beskyttelsesforanstaltninger til at sikre beskyttelsen af grundlæggende rettigheder, herunder retten til respekt for privatlivet, beskyttelse af personoplysninger, ytringsfriheden, herunder retten til frit at modtage og meddele oplysninger, friheden til at oprette og drive egen virksomhed og have adgang til effektive retsmidler. Derudover er enhver forskelsbehandling forbudt. 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 og mediefriheden og –pluralismen, som udgør hjørnestenene i et pluralistisk og demokratisk samfund og er de værdier, som Unionen bygger på. Foranstaltninger, som påvirker ytrings- og informationsfriheden, bør være yderst målrettede til håndtering af udbredelsen af terrorrelateret indhold online, mens retten til lovligt at modtage og meddele oplysninger respekteres, under hensyntagen til den centrale rolle, som hostingtjenesteydere spiller for den offentlige debat og for formidling og modtagelse af faktuelle oplysninger, synspunkter og idéer i overensstemmelse med gældende ret. Effektive onlineforanstaltninger til håndtering af terrorrelateret indhold online og beskyttelsen af ytrings og informationsfriheden er ikke modstridende, men komplementære og gensidigt forstærkende mål.

(11) For at skabe klarhed om de tiltag, som både hostingtjenesteydere og kompetente myndigheder skal iværksætte for at håndtere udbredelsen af terrorrelateret indhold online, bør denne forordning af forebyggelseshensyn fastsætte en definition af »terrorrelateret indhold«, der stemmer overens med definitionerne af relevante lovovertrædelser i henhold til i Europa-Parlamentets og Rådets direktiv (EU) 2017/541 ([6]). I betragtning af behovet for at håndtere den mest skadelige terrorpropaganda online bør denne definition omfatte materiale, som tilskynder eller hverver nogen til at begå eller medvirke til at begå terrorhandlinger eller hverver nogen til deltagelse i en terrorgruppes aktiviteter eller forherliger terroraktiviteter herunder gennem udbredelse af materiale, der afbilder et terrorangreb. Definitionen bør også omfatte materiale, der giver instruktion om fremstilling eller brug af sprængstoffer, skydevåben eller andre våben eller skadelige eller farlige stoffer samt kemiske, biologiske, radiologiske og nukleare (CBRN) stoffer eller om andre konkrete metoder eller teknikker, herunder udvælgelse af mål, med henblik på at begå eller medvirke til at begå terrorhandlinger. Sådant materiale omfatter tekst, billeder, lydoptagelser og videoer samt direkte transmissioner af terrorhandlinger, der skaber en fare for, at yderligere sådanne lovovertrædelser begås. Ved vurderingen af, om materiale udgør terrorrelateret indhold som defineret i denne forordning, bør de kompetente myndigheder og hostingtjenesteyderne tage højde for faktorer såsom udsagns art og ordlyd, den kontekst, som udsagnene indgik i, og om de potentielt kan have skadelige konsekvenser for menneskers sikkerhed. Det faktum, at materialet er produceret af, kan tilskrives eller udbredes på vegne af en person, gruppe eller enhed, der er opført på Unionens liste over personer, grupper og enheder, som er involveret i terrorhandlinger og omfattet af restriktive foranstaltninger, bør spille en stor rolle for vurderingen.

(12) Materiale, som udbredes til uddannelsesmæssige, journalistiske, kunstneriske eller forskningsmæssige formål eller til oplysningsformål mod terroraktiviteter, bør ikke betragtes som værende terrorrelateret indhold. Når det afgøres, hvorvidt materialet fra en indholdsleverandør udgør »terrorrelateret indhold« som defineret i denne forordning, bør der navnlig tages hensyn til retten ytrings- og informationsfrihed, herunder mediefriheden og -pluralismen, og friheden for kunst og videnskab. Navnlig i tilfælde, hvor indholdsleverandøren har et redaktionelt ansvar, bør enhver afgørelse om fjernelse af det udbredte materiale tage hensyn til de journalistiske standarder, der er fastlagt ved presse- eller medielovgivning i overensstemmelse med EU-retten, herunder chartret. Endvidere bør fremsættelse af radikale, polemiske eller kontroversielle holdninger i den offentlige debat om følsomme politiske spørgsmål ikke betragtes som værende terrorrelateret indhold.

(13) For effektivt at håndtere udbredelsen af terrorrelateret indhold online og samtidig sikre respekt for den enkeltes privatliv bør denne forordning finde anvendelse på udbydere af informationssamfundstjenester, som lagrer og udbreder oplysninger og materiale til offentligheden fra en bruger af tjenesten på dennes anmodning, uanset om lagringen og udbredelsen til offentligheden af sådanne oplysninger og materiale er af ren teknisk, automatisk og passiv

([6]) 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).

karakter. Ved »lagring« bør forstås opbevaring af data i en fysisk eller virtuel servers hukommelse. Udbydere af tjenester vedrørende »ren videreformidling« eller såkaldt »caching« samt andre tjenester, der leveres i andre lag af internetinfrastrukturen, og som ikke involverer lagring, såsom registre og registratorer, samt udbydere af domænenavnsystemer (DNS), betalingstjenester eller DDoS-beskyttelsestjenester (»distributed denial of service«) bør derfor ikke være omfattet af denne forordnings anvendelsesområde.

(14) »Udbredelse til offentligheden« bør indebære, at oplysninger stilles til rådighed for et potentielt ubegrænset antal personer, dvs. at oplysningerne gøres let tilgængelige for brugere generelt, uden krav om at indholdsleverandører skal foretage sig noget yderligere, og uanset om disse personer reelt tilgår de pågældende oplysninger. Hvor adgang til oplysninger kræver registrering eller adgang til en gruppe af brugere, bør disse oplysninger således kun betragtes som udbredelse til offentligheden, hvor brugere, der ønsker adgang til oplysningerne, automatisk registreres eller gives adgang, uden at et menneske træffer beslutning eller foretager udvælgelse af, hvem der skal tildeles adgang. Interpersonelle kommunikationstjenester som defineret i artikel 2, nr. 5, i Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 ([7]) såsom e-mails eller private beskedtjenester bør ikke være omfattet af denne forordnings anvendelsesområde. Oplysninger bør kun betragtes som værende lagret og udbredt til offentligheden som omhandlet i denne forordning, hvor sådanne aktiviteter er udført efter direkte anmodning fra indholdsleverandøren. Udbydere af tjenester såsom cloudinfrastruktur, der leveres efter anmodning fra andre parter end indholdsleverandørerne og kun indirekte gavner disse, bør således ikke være omfattet af denne forordning. Denne forordning bør omfatte for eksempel udbydere af sociale medier, video-, billed- og lyddelingstjenester samt fildeling- og andre cloudtjenester, for så vidt disse tjenester anvendes til at gøre lagrede oplysninger tilgængelige for offentligheden efter direkte anmodning fra indholdsleverandøren. Hvor en hostingtjenesteyder udbyder flere forskellige tjenester, bør denne forordning kun finde anvendelse på de tjenester, der falder ind under dens anvendelsesområde.

(15) Terrorrelateret indhold udbredes ofte til offentligheden via tjenester, der udbydes af hostingtjenesteydere, som er etableret i tredjelande. Med henblik på at beskytte brugere i Unionen og for at sikre, at alle hostingtjenesteydere på det digitale indre marked er omfattet af de samme krav, bør denne forordning finde anvendelse på alle udbydere af relevante tjenester, der udbydes i Unionen, uanset i hvilket land de har hovedsæde. En hostingtjenesteyder bør anses for at udbyde tjenester i Unionen, hvis den gør det muligt for fysiske eller juridiske personer i en eller flere medlemsstater at gøre brug af dens tjenester og har en væsentlig tilknytning til denne medlemsstat eller disse medlemsstater.

(16) En væsentlig tilknytning til Unionen bør eksistere, hvor en hostingtjenesteyder er etableret i Unionen, dens tjenester anvendes af et betydeligt antal brugere i en eller flere medlemsstater, eller dens aktiviteter er målrettet mod en eller flere medlemsstater. Målretningen af aktiviteter mod en eller flere medlemsstater bør bestemmes på baggrund af alle relevante omstændigheder, herunder faktorer såsom anvendelse af et sprog eller en valuta, der normalt benyttes i den pågældende medlemsstat, eller muligheden for at bestille varer eller tjenesteydelser fra den pågældende medlemsstat. En sådan målretning kunne også udledes af, at en applikation er tilgængelig i den relevante nationale applikationsbutik, at der reklameres lokalt eller på et sprog, der normalt tales i den pågældende medlemsstat, eller fra den måde kunderelationer håndteres, såsom at kundeservicen varetages på et sprog, der normalt tales i denne medlemsstat. Det må også antages, at der findes en væsentlig tilknytning, hvor en hostingtjenesteyder retter sin virksomhed mod en eller flere medlemsstater som fastsat i artikel 17, stk. 1, litra c), i Europa-Parlamentets og Rådets forordning (EU) nr. 1215/2012 ([8]). Den blotte kendsgerning, at en hostingtjenesteyders websted, e-mailadresse eller andre kontaktoplysninger kan tilgås i en eller flere medlemsstater, bør isoleret set ikke være tilstrækkeligt til at udgøre en væsentlig tilknytning. Leveringen af en tjeneste alene med henblik på overholdelse af forbuddet mod forskelsbehandling, der er fastsat i Europa-Parlamentets og Rådets forordning (EU) 2018/302 ([9]), bør herudover ikke i sig selv anses for at udgøre en væsentlig tilknytning til Unionen.

([7]) Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (EUT L 321 af 17.12.2018, s. 36).

([8]) 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).

([9]) 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 60I af 2.3.2018, s. 1).

(17) De procedurer og forpligtelser, som følger af påbud om fjernelse med krav om, at hostingtjenesteydere fjerner eller deaktiverer adgangen til terrorrelateret indhold, efter at de kompetente myndigheder har foretaget en vurdering, bør harmoniseres. Eftersom terrorrelateret indhold hastigt udbredes via onlinetjenester, bør hostingtjenesteyderne pålægges en forpligtelse til at sikre, at det terrorrelaterede indhold, der er identificeret i påbuddet om fjernelse, fjernes, eller at adgangen til det deaktiveres i alle medlemsstaterne inden for en time efter modtagelse af påbuddet om fjernelse. Undtagen i behørigt begrundede nødsituationer bør den kompetente myndighed give hostingtjenesteyderen oplysninger om procedurer og gældende frister mindst tolv timer inden udstedelsen af det første påbud om fjernelse til denne hostingtjenesteyder. Behørigt begrundede nødsituationer opstår, hvor fjernelsen af eller deaktiveringen af adgang til det terrorrelateret indhold mere end én time efter modtagelse af påbuddet om fjernelse vil medføre alvorlig skade, såsom i tilfælde af overhængende fare for en persons liv eller fysiske integritet eller når sådant indhold viser igangværende begivenheder, der medfører skade på en persons liv eller fysiske integritet. Den kompetente myndighed bør fastslå, hvorvidt situationer udgør nødsituationer, og behørigt begrunde sin beslutning i påbuddet om fjernelse. Hvor hostingtjenesteyderen ikke kan efterkomme påbuddet om fjernelse inden for én time efter modtagelsen på grund af force majeure eller faktisk umulighed, herunder på grund af objektivt begrundede tekniske eller operationelle årsager, bør den hurtigst muligt underrette den udstedende kompetente myndighed herom og efterkomme påbuddet om fjernelse, så snart situationen er løst.

(18) Påbuddet om fjernelse bør omfatte en detaljeret begrundelse, der kvalificerer materialet, som skal fjernes eller hvortil adgang skal deaktiveres, som terrorrelateret indhold, og give tilstrækkelige oplysninger om dette indholds placering ved at angive den nøjagtige URL og om nødvendigt eventuelle andre supplerende oplysninger såsom et screenshot af det pågældende indhold. Denne begrundelse bør sætte hostingtjenesteyderen og i sidste ende indholdsleverandøren i stand til effektivt at udøve deres ret til retslig prøvelse. Begrundelsen bør ikke indebære afsløring af følsomme oplysninger, der kunne bringe igangværende efterforskninger i fare.

(19) Den kompetente myndighed bør fremsende påbuddet om fjernelse direkte til kontaktpunktet udpeget eller etableret af hostingtjenesteyderen med henblik på denne forordning ved hjælp af enhver form for elektronisk middel, som er i stand til at efterlade et skriftligt spor, og som gør det muligt for hostingtjenesteyderen at fastslå autenticiteten af påbuddet, herunder nøjagtigheden af datoen og tidspunktet for afsendelse og modtagelse heraf, såsom sikker e-mail eller platforme eller andre sikre kanaler, herunder dem, der stilles til rådighed af hostingtjenesteyderen, i overensstemmelse med EU-retten om beskyttelse af personoplysninger. Dette krav bør kunne opfyldes ved brug af bl.a. kvalificerede elektroniske registrerede leveringstjenester som defineret i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 ([10]). Hvor hostingtjenesteyderens hovedsæde er beliggende, eller dens retlige repræsentant har ophold eller er etableret, i en anden medlemsstat end den udstedende kompetente myndigheds, bør en kopi af påbuddet om fjernelse samtidig fremsendes til den kompetente myndighed i denne medlemsstat.

(20) Det bør være muligt for den kompetente myndighed i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde, eller hvor dens retlige repræsentant har ophold eller er etableret, at kontrollere det påbud om fjernelse, der er udstedt af en anden medlemsstats kompetente myndigheder, for at fastslå, om det udgør en alvorlig eller åbenbar overtrædelse af denne forordning eller de grundlæggende rettigheder nedfældet i chartret. Både indholdsleverandøren og hostingtjenesteyderen bør have ret til at anmode den kompetente myndighed i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde, eller hvor dens retlige repræsentant har ophold eller er etableret, om en sådan kontrol. Hvor er sådan anmodning fremsættes, bør denne kompetente myndighed træffe en afgørelse om, hvorvidt påbuddet om fjernelse omfatter en sådan overtrædelse. Hvor denne afgørelse fastslår sådan en overtrædelse, bør påbuddet om fjernelse ophøre med at have retsvirkninger. Kontrollen bør foretages hurtigt for at sikre, at fejlagtigt fjernet eller deaktiveret indhold genindsættes så hurtigt som muligt.

([10]) 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).

(21) Hostingtjenesteydere, som eksponeres for terrorrelateret indhold, bør, hvis de har vilkår og betingelser, deri medtage bestemmelser til håndtering af misbrug af deres tjenester til udbredelse til offentligheden af terrorrelateret indhold. De bør anvende disse bestemmelser på en omhyggelig, gennemsigtig, forholdsmæssig og ikkediskriminerende måde.

(22) I betragtning af problemets omfang og den hastighed, der kræves for effektivt at identificere og fjerne terrorrelateret indhold, er effektive og forholdsmæssige specifikke foranstaltninger et afgørende element i håndteringen af terrorrelateret indhold online. Med henblik på at begrænse adgangen til terrorrelateret indhold via deres tjenester bør hostingtjenesteydere, som eksponeres for terrorrelateret indhold, indføre specifikke foranstaltninger under hensyntagen til risiciene og graden af eksponering for terrorrelateret indhold samt konsekvenserne for tredjeparts rettigheder og offentlighedens interesse i oplysninger. Hostingtjenesteyderne bør beslutte, hvilke passende, effektive og forholdsmæssige specifikke foranstaltninger, der bør iværksættes for at identificere og fjerne terrorrelaterede indhold. Specifikke foranstaltninger kunne omfatte passende tekniske eller operationelle foranstaltninger eller kapaciteter såsom personale eller tekniske midler til at identificere og hurtigt fjerne eller deaktivere adgangen til terrorrelateret indhold, mekanismer, som brugere kan benytte til at indberette eller markere formodet terrorrelateret indhold, eller enhver anden foranstaltning, som hostingtjenesteyderen finder hensigtsmæssig og effektiv til at håndtere forekomsten af terrorrelateret indhold på sine tjenester.

(23) Hostingtjenesteyderne bør, når de iværksætter specifikke foranstaltninger, sikre, at brugernes ytrings- og informationsfrihed samt mediefriheden og -pluralismen som beskyttet i henhold til chartret er bevaret. Ud over at opfylde de krav, der er fastsat i gældende ret, herunder lovgivning om beskyttelsen af personoplysninger, bør hostingtjenesteyderne handle med behørig omhu og gennemføre sikkerhedsforanstaltninger, hvor det er hensigtsmæssigt, herunder menneskeligt tilsyn og kontrol, med henblik på at undgå utilsigtede eller fejlagtige afgørelser, der fører til fjernelsen af eller deaktiveringen af adgang til indhold, som ikke er terrorrelateret indhold.

(24) Hostingtjenesteyderen bør rapportere til den kompetente myndighed om de specifikke foranstaltninger, der er iværksat, så denne myndighed kan vurdere, hvorvidt foranstaltningerne er effektive og forholdsmæssige og, hvis der bruges automatiserede værktøjer, om 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, der er udstedt til hostingtjenesteyderen, hostingtjenesteyderens størrelse og økonomiske kapacitet og betydningen af dens tjenester for udbredelsen af terrorrelateret indhold, f.eks. på grundlag af antallet af brugere i Unionen samt de beskyttelsesforanstaltninger, der er indført for at håndtere misbrug af dens tjenester til udbredelse af terrorrelateret indhold online.

(25) Hvor den kompetente myndighed vurderer, at de specifikke foranstaltninger, der er iværksat, er utilstrækkelige til at håndtere risiciene, bør den om nødvendigt kunne kræve, at der træffes yderligere passende, effektive og forholdsmæssige specifikke foranstaltninger. Kravet om at træffe sådanne yderligere specifikke foranstaltninger bør ikke føre til en general forpligtelse til at overvåge eller aktivt undersøge forhold, der tyder på ulovlig virksomhed som omhandlet i artikel 15, stk. 1, i direktiv 2000/31/EF eller til en forpligtelse til at anvende automatiserede værktøjer. Det bør dog være muligt for hostingtjenesteydere at anvende automatiserede værktøjer, hvis de anser det for at være hensigtsmæssigt eller nødvendigt for effektivt at håndtere misbrug af deres tjenester til udbredelse af terrorrelateret indhold.

(26) Forpligtelsen for hostingtjenesteydere til at opbevare fjernet indhold og dertil knyttede data bør fastsættes til specifikke formål og være begrænset til den periode, der er nødvendig. Der er et behov for at udvide kravet om opbevaring af data, da sådanne data ellers ville gå tabt som konsekvens af fjernelsen af det pågældende terrorrelaterede indhold. Dertil knyttede data kan omfatte data såsom abonnentdata, især data vedrørende indholdsleverandørens identitet, samt adgangsdata, herunder dato og tidspunkt for indholdsleverandørens brug og log-in og log-off fra tjenesten sammen med den IP-adresse, som internetudbyderen har tildelt indholdsleverandøren.

(27) Forpligtelsen til at opbevare indholdet til brug for administrativ eller retslig prøvelse er nødvendig og berettiget i betragtning af behovet for at sikre, at effektive retsmidler er til stede for indholdsleverandører, hvis indhold er blevet fjernet eller adgangen dertil er blevet deaktiveret, og for at sikre, at indholdet genindsættes alt efter udfaldet af denne prøvelse. Forpligtelsen til at opbevare materialet til efterforsknings- eller retsforfølgningsformål er berettiget og nødvendigt i betragtning af den værdi, materialet kan have med hensyn til at afbryde eller forebygge terroraktiviteter. Det bør derfor også anses for værende berettiget at opbevare fjernet terrorrelateret indhold til brug for forebyggelse, afsløring, efterforskning og retsforfølgning af terrorhandlinger. Det terrorrelaterede indhold og de relaterede data bør kun lagres i den periode, som er nødvendig for, at de retshåndhævende myndigheder kan kontrollere dette

terrorrelaterede indhold og afgøre, om det er nødvendigt til disse formål. Med henblik på forebyggelsen, afsløringen, efterforskningen og retsforfølgningen af terrorhandlinger bør den påkrævede opbevaring af data være begrænset til data, som sandsynligvis er knyttet til terrorhandlinger, og som derfor kunne bidrage til retsforfølgningen af terrorhandlinger eller til at forebygge alvorlige risici for den offentlige sikkerhed. Hvor hostingtjenesteyderne fjerner eller deaktiverer adgangen til materiale, navnlig via deres egne specifikke foranstaltninger, bør de omgående underrette de kompetente myndigheder om indhold, der omfatter oplysninger, som indebærer overhængende livsfare eller en formodet terrorhandling.

(28) For at sikre proportionalitet bør opbevaringsperioden være begrænset til seks måneder, så indholdsleverandører har tilstrækkelig tid til at indlede administrativ eller retslige prøvelse, og så de retshåndhævende myndigheder kan tilgå relevante data til brug for efterforskning og retsforfølgning af terrorhandlinger. På anmodning fra den kompetente myndighed eller ret bør det imidlertid være muligt at forlænge denne periode så længe som nødvendigt, hvor denne prøvelse er indledt, men ikke afsluttet inden udløbet af denne periode på seks måneder. Varigheden af opbevaringsperioden bør give de retshåndhævende myndigheder tilstrækkelig tid til at bevare det nødvendige materiale til brug for efterforskning og retsforfølgning, idet balancen i forhold til de grundlæggende rettigheder sikres.

(29) Denne forordning bør ikke påvirke de proceduremæssige garantier eller de proceduremæssige efterforskningsforanstaltninger vedrørende adgang til indhold og de dertil knyttede data, der opbevares med henblik på efterforskning og retsforfølgning af terrorhandlinger, som reguleret i henhold til EU-retten eller national ret.

(30) Gennemsigtigheden af hostingtjenesteyderes politikker med hensyn til terrorrelateret indhold er afgørende for at øge deres ansvarlighed over for brugerne og styrke borgernes tillid til det digitale indre marked. Hostingtjenesteydere, der har iværksat tiltag eller har været forpligtet til at iværksatte tiltag i henhold til denne forordning i et givet kalenderår, bør offentliggøre årlige gennemsigtighedsrapporter med oplysninger om de tiltag, der er iværksat med hensyn til identifikation og fjernelse af terrorrelateret indhold.

(31) De kompetente myndigheder bør offentliggøre årlige gennemsigtighedsrapporter med oplysninger om antallet af påbud om fjernelse, antallet af tilfælde hvor et påbud ikke blev efterkomme og antallet af afgørelser vedrørende specifikke foranstaltninger, antallet af sager, der har været genstand for administrativ eller retslig prøvelse og antallet af afgørelser om pålæggelse af sanktioner.

(32) Retten til adgang til effektive retsmidler er nedfældet i artikel 19 i traktaten om Den Europæiske Union (TEU) og i artikel 47 i chartret. Enhver fysisk eller juridisk person skal have adgang 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 bør navnlig omfatte muligheden for, at hostingtjenesteydere og indholdsleverandører reelt kan gøre indsigelse mod påbud om fjernelse eller eventuelle afgørelser, der følger af kontrollen af påbud om fjernelse i henhold til denne forordning, ved en ret i den medlemsstat, hvis kompetente myndigheder har udstedt påbuddet om fjernelse eller truffet afgørelsen, samt for, at hostingtjenesteydere reelt kan gøre indsigelse mod en afgørelse om specifikke foranstaltninger eller sanktioner ved en ret i den medlemsstat, hvis kompetente myndighed har truffet den pågældende afgørelse.

(33) Klageprocedurer udgør en nødvendig sikkerhedsforanstaltning mod den fejlagtige fjernelse af eller deaktivering af adgang til indhold online, hvor sådant indhold er beskyttet under ytrings- og informationsfriheden. Hostingtjenesteydere bør derfor etablere brugervenlige klagemekanismer og sikre, at klager håndteres hurtigt og i fuld gennemsigtighed over for indholdsleverandøren. Kravet om, at hostingtjenesteyderen skal genindsætte indhold, der ved en fejl er blevet fjernet, eller hvortil adgangen ved en fejl er blevet deaktiveret, bør ikke påvirke hostingtjenesteyderens mulighed for at håndhæve sine vilkår og betingelser.

(34) Effektiv retsbeskyttelse i overensstemmelse med artikel 19 i TEU og artikel 47 i chartret kræver, at indholdsleverandører kan få kendskab til årsagerne til, at det indhold, som de har leveret, er blevet fjernet eller hvortil adgangen er blevet deaktiveret. Hostingtjenesteyderen bør med henblik herpå stille oplysninger til rådighed for indholdsleverandøren, så vedkommende kan gøre indsigelse mod fjernelsen eller deaktiveringen. Alt efter omstændighederne kunne hostingtjenesteydere erstatte det indhold, der er er blevet fjernet eller hvortil adgangen er blevet deaktiveret med en besked om, at indholdet er blevet fjernet eller deaktiveret i overensstemmelse med denne forordning. Yderligere oplysninger om årsagerne til fjernelsen eller deaktiveringen og om retsmidlerne vedrørende fjernelsen eller deaktiveringen bør gives på anmodning fra indholdsleverandøren. Hvor de kompetente myndigheder beslutter, at det af hensyn til den offentlige sikkerhed, herunder i forbindelse med en efterforskning, er upassende eller kontraproduktivt at underrette indholdsleverandøren direkte om fjernelsen eller deaktiveringen, bør de oplyse hostingtjenesteyderen herom.

(35) Medlemsstaterne bør med henblik på denne forordning udpege kompetente myndigheder. Dette bør ikke nødvendigvis indebære, at der skal oprettes en ny myndighed, og det bør være muligt at tildele et eksisterende organ de i denne forordning fastsatte opgaver. Denne forordning bør kræve, at der udpeges myndigheder, som har kompetence til at udstede påbud om fjernelse, kontrollere påbud om fjernelse, føre tilsyn med specifikke foranstaltninger og pålægge sanktioner, idet det bør være muligt for hver enkelt medlemsstat at afgøre antallet af kompetente myndigheder, der skal udpeges og hvorvidt de er administrative, retshåndhævende eller retslige. Medlemsstaterne bør sikre, at de kompetente myndigheder varetager deres opgaver på en objektiv og ikkediskriminerende måde og ikke søger eller modtager instrukser fra noget andet organ i forbindelse med udøvelsen af de opgaver, som de får tildelt i medfør af denne forordning. Dette bør ikke være til hinder for, at der kan føres tilsyn i overensstemmelse med national forfatningsret. Medlemsstaterne bør give Kommissionen meddelelse om de kompetente myndigheder, der udpeges i henhold til denne forordning, og Kommissionen bør offentliggøre et onlineregister over de kompetente myndigheder. Dette onlineregister bør være lettilgængeligt, så hostingtjenesteyderne nemt og hurtigt kan kontrollere autenticiteten af påbud om fjernelse.

(36) Med henblik på at undgå dobbeltarbejde og eventuelle forstyrrelser af efterforskninger og for at minimere byrden for de berørte hostingtjenesteydere bør de kompetente myndigheder udveksle oplysninger koordinere og samarbejde med hinanden og, hvor det er relevant, med Europol, inden de udsteder påbud om fjernelse. Når der træffes afgørelse om, hvorvidt der skal udstedes et påbud om fjernelse, bør den kompetente myndighed tage behørigt hensyn til alle indberetninger om forstyrrelser af efterforskningsmæssige interesser (dekonfliktion). Hvor en kompetent myndighed underrettes af en kompetent myndighed i en anden medlemsstat om et eksisterende påbud om fjernelse, bør den ikke udstede et påbud om fjernelse, der omhandler samme genstand. I gennemførelsen af bestemmelserne i denne forordning kunne Europol yde støtte i overensstemmelse med sit nuværende mandat og den gældende retlige ramme.

(37) For at sikre effektiv og tilstrækkeligt sammenhængende gennemførelse af specifikke foranstaltninger, som iværksættes af hostingtjenesteydere, bør de kompetente myndigheder koordinere og samarbejde med hinanden vedrørende udvekslinger med hostingtjenesteydere med hensyn til et påbud om fjernelse og identifikation, gennemførelse og vurdering af specifikke foranstaltninger. Koordination og samarbejde er også nødvendige med hensyn til andre foranstaltninger til gennemførelse af denne forordning, herunder vedrørende vedtagelsen af regler om sanktioner og om pålæggelse af sanktioner. Kommissionen bør lette sådan koordinering og samarbejde.

(38) Det er afgørende, at den kompetente myndighed i den medlemsstat, som er ansvarlig for at pålægge sanktioner, er fuldt ud oplyst om udstedelsen af påbud om fjernelse og om de efterfølgende udvekslinger mellem hostingtjenesteyderen og de kompetente myndigheder i andre medlemsstater. Med henblik herpå bør medlemsstaterne tilvejebringe passende og sikre kommunikationskanaler og -mekanismer, som muliggør rettidig deling af relevante oplysninger.

(39) For at fremme hurtig udveksling mellem kompetente myndigheder såvel som med hostingtjenesteydere og for at undgå dobbeltarbejde bør medlemsstaterne opfordres til at gøre brug af de særlige værktøjer, som Europol har udviklet, såsom applikationen til administration af internetindberetning eller senere udgaver heraf.

(40) Indberetninger fra medlemsstater og Europol har vist sig at være et effektivt og hurtigt middel til at øge hostingtjenesteyderes kendskab til specifikt indhold til rådighed gennem deres tjenester og sætte dem i stand til hurtigt at skride ind. Sådanne indberetninger, som er en mekanisme hvor hostingtjenesteydere gøres bekendt med oplysninger, der kunne betragtes som værende terrorrelateret indhold, og derefter frivilligt kan vurdere, hvorvidt indholdet er i overensstemmelse med deres egne vilkår og betingelser, bør forblive tilgængelig som supplement til påbud om fjernelse. Hostingtjenesteyderen træffer den endelige afgørelse om, hvorvidt oplysningerne skal fjernes, fordi de er uforenelige med dens vilkår og betingelser. Denne forordning bør ikke berøre Europols mandat som fastlagt i Europa-Parlamentets og Rådets forordning (EU) 2016/794 ([11]). Intet i nærværende forordning bør således forstås som at udelukke, at medlemsstaterne og Europol anvender indberetninger som et instrument til at håndtere terrorrelateret indhold online.

(41) I betragtning af de særligt alvorlige konsekvenser af noget terrorrelateret indhold online bør hostingtjenesteyderne omgående underrette de relevante myndigheder i den berørte medlemsstat eller de kompetente myndigheder i den medlemsstat, hvor de er etableret eller har en retlig repræsentant, om terrorrelateret indhold, der indebærer overhængende livsfare eller en formodet terrorhandling. For at sikre proportionalitet bør denne forpligtelse være begrænset til terrorhandlinger som defineret i artikel 3, stk. 1, i direktiv (EU) 2017/541. Denne forpligtelse til underretning bør ikke indebære, at hostingtjenesteyderne er forpligtet til aktivt at søge efter beviser vedrørende en sådan overhængende livsfare eller en formodet terrorhandling. Den berørte medlemsstat bør forstås som den medlemsstat, som har jurisdiktion med hensyn til efterforskning og retsforfølgning af disse terrorhandlinger på grundlag af gerningsmandens eller det potentielle offers nationalitet, eller hvor målet for terrorhandlingen befinder sig. I tvivlstilfælde bør hostingtjenesteyderne sende oplysningerne til Europol, som i henhold til sit mandat bør iværksætte de relevante opfølgende tiltag, herunder ved at videresende disse oplysninger til de relevante nationale myndigheder. Medlemsstaternes kompetente myndigheder bør have lov til at anvende sådanne oplysninger til at træffe efterforskningsforanstaltninger i henhold til EU-retten eller national ret.

(42) Hostingtjenesteyderne bør udpege eller etablere kontaktpunkter for at fremme en hurtig behandling af påbud om fjernelse. Kontaktpunktet bør kun tjene operationelle formål. Kontaktpunktet bør bestå af særlige midler, interne eller eksterne, der muliggør elektronisk fremsendelse af påbud om fjernelse, og af tekniske og menneskelige ressourcer, der muliggør hurtig behandling heraf. Det er ikke nødvendigt, at kontaktpunktet befinder sig i Unionen. Hostingtjenesteyderen bør frit kunne bruge et eksisterende kontaktpunkt med henblik på denne forordning, forudsat at kontaktpunktet er i stand til at udføre de i denne forordning fastsatte funktioner. Med henblik på at sikre, at terrorrelateret indhold fjernes eller at adgangen dertil deaktiveres inden for en time efter modtagelsen af påbuddet om fjernelse, bør kontaktpunkter, der hører til hostingtjenesteydere, som eksponeres for terrorrelateret indhold, til enhver tid være tilgængelige. Oplysningerne om kontaktpunktet bør omfatte oplysninger om, hvilket sprog den kan kontaktes på. For at lette kommunikationen mellem hostingtjenesteyderne og de kompetente myndigheder opfordres hostingtjenesteyderne til at muliggøre kommunikation på et af EU-institutionernes officielle sprog, på hvilket deres vilkår og betingelser foreligger.

(43) 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 dens retlige repræsentant har ophold eller er etableret. Dette bør ikke berøre de bestemmelser om kompetence, der er fastsat med henblik på påbud om fjernelse og afgørelser, der følger af kontrollen af påbud om fjernelse i henhold til denne forordning. Med hensyn til hostingtjenesteydere, som ikke er etableret i Unionen, og som ikke har udpeget en retlig repræsentant, bør enhver medlemsstat desuagtet have jurisdiktion og derfor mulighed for at pålægge sanktioner under forudsætning af, at ne bis in idem-princippet overholdes.

([11]) 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).

(44) Hostingtjenesteydere, som ikke er etableret i Unionen, bør skriftligt udpege en retlig repræsentant for at sikre overholdelse og håndhævelse af forpligtelserne i denne forordning. Det bør være muligt for hostingtjenesteydere at udpege, med henblik på denne forordning, en retlig repræsentant, der allerede er udpeget til andre formål, forudsat at denne retlige repræsentant er i stand til at udføre de opgaver, der er fastsat i denne forordning. Den retlige repræsentant bør have beføjelse til at agere på vegne af hostingtjenesteyderen.

(45) Sanktioner er nødvendige for at sikre, at hostingtjenesteyderne på effektiv vis gennemfører denne forordning. Medlemsstaterne bør vedtage regler om sanktioner, der kan være af administrativ eller strafferetlig karakter, samt, hvor det er hensigtsmæssigt, bøderetningslinjer. Manglende overholdelse i enkeltsager kunne være underlagt sanktioner med respekt af ne bis in idem-princippet og proportionalitetsprincippet, og idet det sikres, at sådanne sanktioner tager højde for systematisk forsømmelse. Sanktioner kunne antage forskellige former, herunder formelle advarsler i tilfælde af mindre overtrædelser eller økonomiske sanktioner i forbindelse med mere alvorlige eller systematiske overtrædelser. Der bør pålægges særligt alvorlige sanktioner i tilfælde, hvor hostingtjenesteyderen systematisk eller vedvarende undlader at fjerne eller deaktivere adgangen til terrorrelateret indhold inden for en time efter modtagelse af et påbud om fjernelse. For at sikre retssikkerheden bør denne forordning fastsætte hvilke overtrædelser, der er underlagt sanktioner og hvilke omstændigheder, der er relevante for vurderingen af typen og omfanget af sådanne sanktioner Når det afgøres, hvorvidt der skal pålægges økonomiske sanktioner, bør der tages behørigt hensyn til hostingtjenesteyderens finansielle ressourcer. Desuden bør den kompetente myndighed tage hensyn til, om hostingtjenesteyderen er en nyetableret virksomhed eller en mikrovirksomhed eller en lille eller mellemstor virksomhed som defineret i Kommissionens henstilling 2003/361/EF ([12]). Der bør tages hensyn til andre omstændigheder, såsom hvorvidt hostingtjenesteyderens adfærd objektivt set var uforsigtig eller forkastelig, eller hvorvidt overtrædelsen blev begået uagtsomt eller forsætligt. Medlemsstaterne bør sikre, at sanktionerne pålagt for overtrædelse af denne forordning ikke tilskynder til fjernelse af materiale, som ikke er terrorrelateret indhold.

(46) Anvendelsen af standardiserede formularer letter samarbejdet og informationsudvekslingen mellem de kompetente myndigheder og hostingtjenesteydere 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 højere standard for proceduren. Feedbackformularerne giver mulighed for en standardiseret informationsudveksling og er særlig vigtige, hvor hostingtjenesteyderne ikke er i stand til at efterkomme påbuddet om fjernelse. Autentificerede transmissionskanaler kan garantere påbuddets autenticitet, herunder nøjagtigheden af datoen og tidspunktet for afsendelse og modtagelse af påbuddet.

(47) For at muliggøre hurtige ændringer, hvor det er nødvendigt, af indholdet af de formularer, der skal anvendes med henblik på denne forordning, bør beføjelsen til at vedtage retsakter delegeres til Kommissionen i overensstemmelse med artikel 290 i traktaten om Den Europæiske Unions funktionsmåde for så vidt angår ændring bilagene 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 ([13]). 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.

(48) Medlemsstaterne bør indhente oplysninger om gennemførelse af denne forordning. Det bør være muligt for medlemsstaterne at anvende hostingtjenesteydernes gennemsigtighedsrapporter og, hvor det er nødvendigt, supplere dem med mere detaljerede oplysninger såsom deres egne gennemsigtighedsrapporter i henhold til denne forordning. Der bør fastlægges et detaljeret program for overvågning af forordningens output, resultater og virkninger, der kan lægge til grund for en evaluering af gennemførelsen af denne forordning.

([12]) Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder (EUT L 124 af 20.5.2003, s. 36).

([13]) EUT L 123 af 12.5.2016, s. 1.

(49) På grundlag af resultaterne og konklusionerne i gennemførelsesrapporten og udfaldet af overvågningen bør Kommissionen foretage en evaluering af denne forordning senest tre år efter dagen for dens ikrafttræden. Evalueringen bør være baseret på kriterierne effektivitet, nødvendighed, virkningsfuldhed, proportionalitet, relevans, sammenhæng og merværdi for Unionen. Den bør vurdere, hvordan de forskellige operationelle og tekniske foranstaltninger fastsat i forordningen fungerer, herunder foranstaltningernes effektivitet med hensyn til at forbedre afsløring, identifikation og fjernelse af terrorrelateret indhold online, sikkerhedsforanstaltningernes effektivitet og virkningerne på potentielt berørte grundlæggende rettigheder, såsom ytrings- og informationsfriheden, herunder mediefriheden og -pluralismen, friheden til at oprette og drive egen virksomhed, retten til privatliv og retten til beskyttelsen af personoplysninger. Kommissionen bør også vurdere virkningerne på tredjeparters potentielt berørte interesser.

(50) Målet for denne forordning, nemlig at sikre et velfungerende digitalt indre marked ved at håndtere udbredelsen af terrorrelateret indhold online, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af dens omfang og virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i TEU. 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. Denne forordning fastlægger ensartede regler til håndtering af misbrug af hostingtjenester til udbredelse af terrorrelateret indhold online til offentligheden, navnlig om:

a) den rimelige og forholdsmæssige rettidige omhu, som hostingtjenesteydere skal udvise for at håndtere udbredelsen af terrorrelateret indhold til offentligheden via deres tjenester og, hvor det er nødvendigt, sikre hurtig fjernelse af eller deaktivering af adgang til sådant indhold

b) foranstaltningerne, som medlemsstaterne i overensstemmelse med EU-retten og med forbehold af passende sikkerhedsforanstaltninger til beskyttelse af grundlæggende rettigheder, særlig ytrings- og informationsfriheden i et åbent og demokratisk samfund, skal gennemføre for at

   i) identificere og sikre hostingtjenesteydernes hurtige fjernelse af terrorrelateret indhold og

   ii) lette samarbejdet blandt medlemsstaternes kompetente myndigheder, hostingtjenesteydere og, hvor det er relevant, Europol.

2. Denne forordning finder anvendelse på hostingtjenesteydere, der udbyder tjenester i Unionen, uanset hvor deres hovedsæde er beliggende, i det omfang de udbreder oplysninger til offentligheden.

3. Materiale, som udbredes til offentligheden til uddannelsesmæssige, journalistiske, kunstneriske eller forskningsmæssige formål eller med henblik på at forebygge eller bekæmpe terrorisme, herunder materiale, der er udtryk for polemiske eller kontroversielle holdninger i den offentlige debat, betragtes ikke som værende terrorrelateret indhold. En vurdering skal fastslå det egentlige formål med denne udbredelse og hvorvidt materialet udbredes til offentligheden til de nævnte formål.

4. Denne forordning indebærer ikke nogen ændring af pligten til at respektere de rettigheder, friheder og principper, der er omhandlet i artikel 6 i TEU, og finder anvendelse uden at det berører grundlæggende principper vedrørende ytrings- og informationsfriheden, herunder mediefriheden og -pluralismen.

5. Denne forordning berører ikke direktiv 2000/31/EF og 2010/13/EU. For audiovisuelle medietjenester som defineret i artikel 1, stk. 1, litra a), i direktiv 2010/13/EU har direktiv 2010/13/EU forrang.

Artikel 2

Definitioner

I denne forordning forstås ved:

1) »hostingtjenesteyder«: en udbyder af tjenester som defineret i artikel 1, litra b), i Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 ([14]), der består i lagringen af oplysninger fra en indholdsleverandør på dennes anmodning

2) »indholdsleverandør«: en bruger, der har leveret oplysninger, som er eller har været lagret og udbredt til offentligheden af en hostingtjenesteyder

3) »udbredelse til offentligheden «: at stille oplysninger til rådighed for et potentielt ubegrænset antal personer på anmodning fra en indholdsleverandør

4) »udbyde tjenester i Unionen«: at gøre det muligt for fysiske eller juridiske personer i en eller flere medlemsstater at gøre brug af tjenester fra en hostingtjenesteyder, som har en væsentlig tilknytning til denne medlemsstat eller disse medlemsstater

5) »væsentlig tilknytning«: en hostingtjenesteyders tilknytning til en eller flere medlemsstater som følge enten af, at den er etableret i Unionen, eller af specifikke faktuelle kriterier såsom

   a) at den har et betydeligt antal brugere af dens tjenester i en eller flere medlemsstater eller

   b) at den har målrettet sine aktiviteter mod en eller flere medlemsstater

6) »terrorhandlinger«: lovovertrædelser som defineret i artikel 3 i direktiv (EU) 2017/541

7) »terrorrelateret indhold«: et eller flere af de følgende typer materiale, dvs. materiale der:

   a) tilskynder til at begå en af de lovovertrædelser, der er omhandlet i artikel 3, stk. 1, litra a)-i), i direktiv (EU) 2017/541, hvor sådant materiale, direkte eller indirekte, såsom ved forherligelse af terrorhandlinger, slår til lyd for udførelse af terrorhandlinger, hvorved der skabes fare for, at en eller flere af sådanne handlinger måtte blive begået

   b) hverver en person eller en gruppe af personer til at begå eller medvirke til at begå en af de lovovertrædelser, der er omhandlet i artikel 3, stk. 1, litra a)-i), i direktiv (EU) 2017/541

   c) hverver en person eller en gruppe af personer til at deltage i en terrorgruppes aktiviteter som omhandlet i artikel 4, litra b), i direktiv (EU) 2017/541

   d) oplærer i fremstilling eller brug af sprængstoffer, skydevåben eller andre våben eller skadelige eller farlige stoffer eller i andre konkrete metoder eller teknikker med henblik på at begå eller medvirke til at begå en af de terrorhandlinger, der er omhandlet i artikel 3, stk. 1, litra a)-i), i direktiv (EU) 2017/541

   e) udgør en trussel om at begå en af de lovovertrædelser, der er omhandlet i artikel 3, stk. 1, litra a)-i), i direktiv (EU) 2017/541

([14]) Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 af 9. september 2015 om en informationsprocedure med hensyn til tekniske forskrifter samt forskrifter for informationssamfundets tjenester (EUT L 241 af 17.9.2015, s. 1).

8) »vilkår og betingelser«: alle vilkår, betingelser og klausuler, uanset deres navn eller form, som kontraktforholdet mellem en hostingtjenesteyder og dens brugere er underlagt

9) »hovedsæde«: en hostingtjenesteyders hovedkontor eller hjemsted, hvor de primære finansielle funktioner og den operationelle kontrol udøves.

Afdeling II

Foranstaltninger til at håndtere udbredelse af terrorrelateret indhold online

Artikel 3

Påbud om fjernelse

1. Enhver medlemsstats kompetente myndighed har beføjelser til at udstede et påbud om fjernelse, der kræver, at hostingtjenesteydere fjerner terrorrelateret indhold eller deaktiverer adgangen til terrorrelateret indhold i alle medlemsstater.

2. Hvor en kompetent myndighed ikke tidligere har udstedt et påbud om fjernelse til en hostingtjenesteyder, giver den denne hostingtjenesteyder oplysninger om de gældende procedurer og frister mindst 12 timer, før den udsteder påbuddet om fjernelse.

Første afsnit finder ikke anvendelse i behørigt begrundede nødsituationer.

3. Hostingtjenesteyderen skal fjerne terrorrelateret indhold eller deaktivere adgangen til terrorrelateret indhold i alle medlemsstater hurtigst muligt og under alle omstændigheder inden for en time efter at have modtaget påbuddet om fjernelse.

4. Kompetente myndigheder udsteder påbud om fjernelse ved brug af formularen i bilag I. Påbud om fjernelse skal indeholde følgende elementer:

a) den kompetente myndighed der udsteder påbuddet om fjernelses identifikationsdetaljer og denne kompetente myndigheds autentifikation af påbuddet om fjernelse

b) en tilstrækkeligt detaljeret begrundelse af, hvorfor indholdet betragtes som værende terrorrelateret indhold, og en henvisning til den relevante type af terrorrelateret indhold, der er omhandlet i artikel 2, nr. 7)

c) en nøjagtig internetadresse (Uniform Resource Locator, URL) og om nødvendigt supplerende oplysninger til identifikation af det terrorrelaterede indhold

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

e) dato, tidstempel og elektronisk signatur fra den kompetente myndighed, der udsteder påbuddet om fjernelse

f) letforståelige oplysninger om hostingtjenesteyderens og indholdsleverandørens klagemuligheder, herunder oplysninger om muligheden for at klage til den kompetente myndighed og retslig prøvelse samt klagefristerne

g) hvor det er nødvendigt og forholdsmæssigt, afgørelsen om ikke at videregive oplysninger om fjernelsen af eller deaktiveringen af adgang til det terrorrelaterede indhold i overensstemmelse med artikel 11, stk. 3.

5. Den kompetente myndighed stiler påbuddet om fjernelse til hostingtjenesteyderens hovedsæde eller til dens retlige repræsentant udpeget i overensstemmelse med artikel 17.

Denne kompetente myndighed fremsender påbuddet om fjernelse til kontaktpunktet, der er omhandlet i artikel 15, stk. 1, ved elektroniske midler, som er i stand til at efterlade et skriftligt spor på en måde, der gør det muligt at autentificere afsenderen, herunder nøjagtigheden af datoen og tidspunktet for afsendelse og modtagelse af påbuddet.

6. Hostingtjenesteyderen underretter uden unødigt ophold ved hjælp af formularen i bilag II den kompetente myndighed om, at det terrorrelaterede indhold er blevet fjernet eller at adgangen til det terrorrelaterede indhold er blevet deaktiveret i alle medlemsstater, idet navnlig tidspunktet for denne fjernelse eller deaktivering angives.

7. Hvis hostingtjenesteyderen ikke kan efterkomme påbuddet om fjernelse grundet force majeure eller faktisk umulighed, som ikke kan tilskrives hostingtjenesteyderen, herunder af objektivt begrundede tekniske eller operationelle årsager, oplyser den uden unødigt ophold den kompetente myndighed, der udstedte påbuddet om fjernelse, om årsagerne hertil ved hjælp af formularen i bilag III.

Den frist, der er fastsat i stk. 3, begynder at løbe, så snart årsagerne omhandlet i dette stykkes første afsnit er ophørt.

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 unødigt ophold den kompetente myndighed, der udstedte påbuddet om fjernelse, og anmoder om den nødvendige forklaring ved hjælp af formularen i bilag III.

Den frist, der er fastsat i stk. 3, begynder at løbe, så snart hostingtjenesteyderen modtager den nødvendige forklaring.

9. Et påbud om fjernelse bliver endeligt ved udløbet af klagefristen, såfremt der ikke er iværksat nogen klage i henhold til national ret, eller når det er blevet stadfæstet efter en klage.

Når et påbud om fjernelse bliver endeligt, underretter den kompetente myndighed, som udstedte påbuddet om fjernelse, den i artikel 12, stk. 1, litra c), omhandlede kompetente myndighed i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde, eller hvor dens retlige repræsentant har ophold eller er etableret, herom.

Artikel 4

Procedure for grænseoverskridende påbud om fjernelse

1. Udover hvad der gælder i henhold til artikel 3, hvor hostingtjenesteyderen ikke har sit hovedsæde eller sin retlige repræsentant i den medlemsstat, hvor den kompetente myndighed, der har udstedt påbuddet om fjernelse, er beliggende, fremsender denne myndighed samtidig en kopi af påbuddet om fjernelse til den kompetente myndighed i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde eller hvor dens retlige repræsentant har ophold eller er etableret.

2. Hvor en hostingtjenesteyder modtager et påbud om fjernelse som omhandlet i denne artikel, træffer den de foranstaltninger, der er fastsat i artikel 3, samt de nødvendige foranstaltninger for at kunne genindsætte indholdet eller genaktivere adgangen dertil i overensstemmelse med nærværende artikels stk. 7.

3. Den kompetente myndighed i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde eller hvor dens retlige repræsentant har ophold eller er etableret, kan af egen drift inden for 72 time efter modtagelse af kopien af påbuddet om fjernelse i overensstemmelse med stk. 1 kontrollere påbuddet om fjernelse for at fastslå, om det udgør en alvorlig eller åbenbar overtrædelse af denne forordning eller de grundlæggende rettigheder og friheder, der er sikret ved chartret.

Hvor den konstaterer en overtrædelse, vedtager den inden for samme periode en begrundet afgørelse herom.

4. Hostingtjenesteydere og indholdsleverandører har ret til inden for 48 timer efter modtagelse enten af et påbud om fjernelse eller af oplysninger i henhold til artikel 11, stk. 2, at indgive en begrundet anmodning til den kompetente myndighed i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde, eller hvor dens retlige repræsentant har ophold eller er etableret, om at kontrollere påbuddet om fjernelse som omhandlet i nærværende artikels stk. 3, første afsnit.

Den kompetente myndighed træffer indenfor 72 timer efter modtagelse af anmodningen en begrundet afgørelse efter at have kontrolleret påbuddet om fjernelse med angivelse af dens konklusioner om, hvorvidt der er tale om en overtrædelse.

5. Den kompetente myndighed underretter, før den træffer en afgørelse i henhold til stk. 3, andet afsnit, eller en afgørelse om en overtrædelse i henhold til stk. 4, andet afsnit, den kompetente myndighed, der udstedte påbuddet om fjernelse, om sin hensigt om at træffe afgørelsen og om grundene hertil.

6. Hvor den kompetente myndighed i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde eller dens retlige repræsentant har ophold eller er etableret, træffer en begrundet afgørelse i henhold til denne artikels stk. 3 eller 4, meddeler den straks denne afgørelse til den kompetente myndighed, der udstedte påbuddet om fjernelse, hostingtjenesteyderen, indholdsleverandøren, der anmodede om kontrol i henhold til denne artikels stk. 4, og, i henhold til artikel 14, Europol. Hvor afgørelsen fastslår, at der er tale en overtrædelse i henhold til denne artikels stk. 3 eller 4, ophører påbuddet om fjernelse med at have retsvirkninger.

7. Efter modtagelse af en afgørelse, der fastslår en overtrædelse, meddelt i henhold til stk. 6 genindsætter den pågældende hostingtjenesteyder omgående indholdet eller genaktiverer adgangen dertil, uden at dette berører muligheden for at håndhæve dens vilkår og betingelser i overensstemmelse med EU-retten og national ret.

Artikel 5

Specifikke foranstaltninger

1. En hostingtjenesteyder, der eksponeres for terrorrelateret indhold som omhandlet i stk. 4, medtager, hvor det er relevant, i sine vilkår og betingelser bestemmelser til håndtering af misbrug af dets tjenester til udbredelse af terrorrelateret indhold til offentligheden og anvender disse bestemmelser.

Den skal gøre dette på en omhyggelig, forholdsmæssig og ikkediskriminerende måde under behørigt hensyn under alle omstændigheder til brugernes grundlæggende rettigheder og navnlig den grundlæggende betydning af ytrings- og informationsfriheden i et åbent og demokratisk samfund med henblik på at undgå at fjerne materiale, som ikke er terrorrelateret indhold.

2. En hostingtjenesteyder, der eksponeres for terrorrelateret indhold som omhandlet i stk. 4, træffer specifikke foranstaltninger til beskyttelse af sine tjenester mod udbredelse af terrorrelateret indhold til offentligheden.

Valget af specifikke foranstaltninger forbliver hostingtjenesteyderens beslutning. Sådanne foranstaltninger kan indebære en eller flere af de følgende:

a) passende tekniske og operationelle foranstaltninger eller kapaciteter såsom passende personale eller tekniske midler til at identificere og hurtigt fjerne eller deaktivere adgangen til terrorrelateret indhold

b) lettilgængelige og brugervenlige mekanismer, som brugere kan benytte til at indberette eller markere formodet terrorrelateret indhold til hostingtjenesteyderen

c) alle andre mekanismer, der kan øge kendskabet til terrorrelateret indhold på dens tjenester, såsom mekanismer til brugermoderation

d) enhver anden foranstaltning, som hostingtjenesteyderen finder hensigtsmæssig til at håndtere forekomsten af terrorrelateret indhold på sine tjenester.

3. Specifikke foranstaltninger skal opfylde samtlige følgende krav:

a) de skal være effektive med hensyn til at afbøde graden af eksponering på hostingtjenesteyderens tjenester for terrorrelateret indhold

b) de skal være målrettede og forholdsmæssige, idet der navnlig tages hensyn til, hvor alvorlig graden af eksponering på hostingtjenesteyderens tjenester for terrorrelateret indhold er, samt de tekniske og operationelle kapaciteter, den finansielle styrke, antal brugere af hostingtjenesteyderens tjenester og den mængde indhold, de leverer

c) de skal anvendes under fuld hensyntagen til brugernes rettigheder og legitime interesser, navnlig brugernes grundlæggende rettigheder vedrørende ytrings- og informationsfrihed, respekt for privatlivet og beskyttelse af personoplysninger

d) de skal anvendes på en omhyggelig og ikkediskriminerende måde.

Hvor de specifikke foranstaltninger omfatter brugen af tekniske foranstaltninger, skal der træffes passende og effektive sikkerhedsforanstaltninger, navnlig gennem menneskeligt tilsyn og kontrol, for at sikre nøjagtighed og undgå fjernelse af materiale, der ikke er terrorrelateret indhold.

4. En hostingtjenesteyder er eksponeret for terrorrelateret indhold, hvor den kompetente myndighed i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde eller hvor dens repræsentant har ophold eller er etableret, har

a) truffet en afgørelse baseret på objektive faktorer, såsom at hostingtjenesteyderen inden for de seneste 12 måneder har modtaget to eller flere endelige påbud om fjernelse, der konstaterer, at hostingtjenesteyderen er eksponeret for terrorrelateret indhold og

b) underrettet hostingtjenesteyderen om den i litra a) omhandlede afgørelse.

5. Efter at have modtaget en afgørelse som omhandlet i stk. 4 eller, hvor det relevant, i stk. 6, aflægger hostingtjenesteyderen rapport til den kompetente myndighed om de specifikke foranstaltninger, som den har truffet, og som den agter at træffe for at overholde stk. 2 og 3. Den gør dette senest tre måneder efter modtagelsen af afgørelsen og derefter hvert år. Denne forpligtelse ophører, når den kompetente myndighed efter en anmodning i henhold til stk. 7 har afgjort, at hostingtjenesteyderen ikke længere er eksponeret for terrorrelateret indhold.

6. Hvor den kompetente myndighed på grundlag af de i stk. 5 omhandlede rapporter og, hvor det er relevant, andre objektive faktorer finder, at de specifikke foranstaltninger, som er truffet, ikke overholder stk. 2 og 3, retter denne kompetente myndighed en afgørelse til hostingtjenesteyderen, hvori den pålægges at træffe de nødvendige foranstaltninger, for at sikre, at stk. 2 og 3 overholdes.

Hostingtjenesteyderen kan beslutte, hvilken type specifik foranstaltning vedkommende vil træffe.

7. En hostingtjenesteyder kan til enhver tid anmode den kompetente myndighed om at genoptage en afgørelse, som omhandlet i stk. 4 eller 6 og, hvor det er relevant, ændre eller tilbagekalde den.

Den kompetente myndighed træffer senest tre måneder efter modtagelsen af anmodningen en begrundet afgørelse om anmodningen baseret på objektive faktorer og underretter hostingtjenesteyderen om denne afgørelse.

8. Ethvert krav om at træffe specifikke foranstaltninger berører ikke artikel 15, stk. 1, i direktiv 2000/31/EF og medfører hverken en generel forpligtelse for hostingtjenesteydere til at overvåge de oplysninger, som de fremsender eller lagrer, eller en generel forpligtelse til aktivt at undersøge forhold eller omstændigheder, der tyder på ulovlig virksomhed.

Ethvert krav om at træffe specifikke foranstaltninger omfatter ikke en forpligtelse for hostingtjenesteyderen til at anvende automatiserede værktøjer.

Artikel 6

Opbevaring af indhold og dertil knyttede data

1. Hostingtjenesteydere opbevarer det terrorrelaterede indhold, som er blevet fjernet eller hvortil adgang er blevet deaktiveret som følge af et påbud om fjernelse eller af specifikke foranstaltninger i henhold til artikel 3 eller 5, samt eventuelt dertil knyttede data, som er blevet fjernet som konsekvens af fjernelsen af sådant terrorrelaterede indhold, som er nødvendig for:

a) administrativ eller retslig prøvelse eller behandling af klager i henhold til artikel 10 over en afgørelse om fjernelse eller deaktivering af adgang til terrorrelateret indhold og dertil knyttede data eller

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

2. Det terrorrelaterede indhold og de dertil knyttede data som omhandlet i stk. 1 opbevares i seks måneder fra fjernelsen eller deaktiveringen. På anmodning fra den kompetente myndighed eller domstol opbevares det terrorrelaterede indhold i en yderligere fastsat periode, alene hvis og så længe det er nødvendigt for verserende administrativ eller retslig prøvelse som omhandlet i stk. 1, litra a).

3. Hostingtjenesteyderne sikrer, at det terrorrelaterede indhold og de dertil knyttede data, der opbevares i henhold til stk. 1, er omfattet af passende tekniske og organisatoriske sikkerhedsforanstaltninger.

Disse tekniske og organisatoriske sikkerhedsforanstaltninger skal sikre, at det opbevarede terrorrelaterede indhold og de dertil knyttede data kun tilgås og bruges til de formål, der er omhandlet i stk. 1, og at der er et højt sikkerhedsniveau for opbevaringen af de berørte personoplysninger. Hostingtjenesteydere reviderer og ajourfører disse foranstaltninger, hvor det er nødvendigt.

Afdeling III

Sikkerhedsforanstaltninger og ansvarlighed

Artikel 7

Hostingtjenesteyderes forpligtelser vedrørende gennemsigtighed

1. Hostingtjenesteyderne fastsætter tydeligt i deres vilkår og betingelser deres politik for at håndtere udbredelsen af terrorrelateret indhold, herunder, hvor det er hensigtsmæssigt, en meningsfuld beskrivelse af de specifikke foranstaltningers funktionsmåde, herunder, hvor det er relevant, anvendelsen af automatiserede værktøjer.

2. En hostingtjenesteyder, der har iværksat tiltag for at håndtere udbredelsen af terrorrelateret indhold eller har været forpligtet til at iværksatte tiltag i henhold til denne forordning i et givet kalenderår, offentliggør en gennemsigtighedsrapport om disse tiltag i den pågældende år. Den offentliggør denne rapport inden den 1. marts det følgende år.

3. Gennemsigtighedsrapporter indeholder mindst følgende oplysninger:

a) oplysninger om hostingtjenesteyderens foranstaltninger for så vidt angår identifikation og fjernelse af eller deaktivering af adgang til terrorrelateret indhold

b) oplysninger om hostingtjenesteyderens foranstaltninger for at forhindre, at materiale, der tidligere er blevet fjernet, eller hvortil adgangen er blevet deaktiveret, fordi det blev anset for at være terrorrelateret indhold, navnlig hvor der er anvendt automatiserede værktøjer, atter vises online

c) antallet af indslag med terrorrelaterede indhold, der er fjernet, eller hvortil adgangen er blevet deaktiveret som følge af påbud om fjernelse eller specifikke foranstaltninger, og antallet af påbud om fjernelse, hvor indholdet ikke er blevet fjernet eller adgangen dertil ikke er blevet deaktiveret i henhold til artikel 3, stk. 7, første afsnit, og artikel 3, stk. 8, først afsnit, samt begrundelsen herfor

d) antallet og udfaldet af klager, som hostingtjenesteyderen har behandlet i overensstemmelse med artikel 10

e) antallet og udfaldet af sager om administrativ eller retslig prøvelse, der er indbragt af hostingtjenesteyderen

f) antallet af tilfælde, hvor det blev krævet, at hostingtjenesteyderen genindsatte indhold eller genaktiverede adgang dertil som følge af sager om administrativ eller retslig prøvelse

g) antallet af tilfælde, hvor hostingtjenesteyderen genindsatte indhold eller genaktiverede adgangen dertil efter en klage fra indholdsleverandøren.

Artikel 8

De kompetente myndigheders gennemsigtighedsrapporter

1. De kompetente myndigheder offentliggør årlige gennemsigtighedsrapporter om deres aktiviteter i henhold til denne forordning. Disse rapporter skal mindst indeholde følgende oplysninger om det givne kalenderår:

a) antallet af påbud om fjernelse, der er udstedt i henhold til artikel 3, der angiver antallet af påbud om fjernelse omfattet af artikel 4, stk. 1, antallet af påbud om fjernelse kontrolleret i henhold til artikel 4, og oplysninger om, hvordan de berørte hostingtjenesteydere har gennemført disse påbud om fjernelse, herunder antallet af sager, hvor terrorrelateret indhold blev fjernet eller adgang dertil blev deaktiveret og antallet af sager, hvor terrorrelateret indhold ikke blev fjernet eller adgang dertil ikke blev deaktiveret

b) antallet af afgørelser, der er truffet i medfør af artikel 5, stk. 4, 6 eller 7, og oplysninger om, hvordan hostingtjenesteyderne har gennemført disse afgørelser, herunder en beskrivelse af de specifikke foranstaltninger

c) antallet af sager, hvor påbud om fjernelse og afgørelser truffet i overensstemmelse med artikel 5, stk. 4 og 6, var genstand for administrativ eller retslig prøvelse og oplysninger om udfaldet af de pågældende sager

d) antallet af afgørelser om pålæggelse af sanktioner i medfør af artikel 18 og en beskrivelse af den pålagte sanktionstype.

2. De i stk. 1 omhandlede årlige gennemsigtighedsrapporter må ikke indeholde oplysninger, der kan skade igangværende aktiviteter til forebyggelse, afsløring, efterforskning eller retsforfølgning af terrorhandlinger eller nationale sikkerhedsinteresser.

Artikel 9

Retsmidler

1. Hostingtjenesteydere, der har modtaget et påbud om fjernelse udstedt i henhold til artikel 3, stk. 1, eller en afgørelse i henhold til artikel 4, stk. 4, eller artikel 5, stk. 4, 6 eller 7, skal have adgang til effektive retsmidler. Denne ret omfatter retten til at gøre indsigelse mod et sådant påbud om fjernelse ved domstolene i den medlemsstat, hvor den kompetente myndighed, der har udstedt påbuddet om fjernelse, er beliggende, og retten til at gøre indsigelse mod afgørelsen i henhold til artikel 4, stk. 4, eller artikel 5, stk. 4, 6 eller 7, ved domstolene i den medlemsstat, hvor den kompetente myndighed, der har truffet afgørelsen, er beliggende.

2. Indholdsleverandører, hvis indhold er blevet fjernet, eller hvortil adgangen er blevet deaktiveret som følge af et påbud om fjernelse, har adgang til effektive retsmidler. Denne ret omfatter retten til at gøre indsigelse mod et påbud om fjernelse, der er udstedt i henhold til artikel 3, stk. 1, ved domstolene i den medlemsstat, hvor den kompetente myndighed, der har udstedt påbuddet om fjernelse, er beliggende, og retten til at gøre indsigelse mod en afgørelse i henhold til artikel 4, stk. 4, ved domstolene i den medlemsstat, hvor den kompetente myndighed, der har truffet afgørelsen, er beliggende.

3. Medlemsstaterne skal fastsætte effektive procedurer for udøvelsen af rettighederne i denne artikel.

Artikel 10

Klagemekanismer

1. Hver hostingtjenesteyder indfører en effektiv og tilgængelig mekanisme, som gør det muligt for indholdsleverandører, hvor deres indhold er blevet fjernet eller hvortil adgangen er blevet deaktiveret som følge af specifikke foranstaltninger i henhold til artikel 5, at indgive en klage over denne fjernelse eller deaktivering med anmodning om genindsættelse af det fjernede indholdet eller adgangen dertil.

2. Hver hostingtjenesteyder undersøger hurtigt samtlige klager, som den modtager gennem den i stk. 1 omhandlede mekanisme og genindsætter indholdet eller adgangen dertil uden unødigt ophold, hvor fjernelsen eller deaktiveringen var uberettiget. Den underretter klageren om udfaldet af klagen senest to uger efter modtagelsen heraf.

Hvor klagen afvises, giver hostingtjenesteyderen en begrundelses for sin afgørelse til klageren.

Genindsættelse af indhold eller af adgangen dertil udelukker ikke yderligere administrativ eller retslig prøvelse af hostingtjenesteyderens eller den kompetente myndigheds afgørelse.

Artikel 11

Oplysninger til indholdsleverandører

1. Hvor en hostingtjenesteyder fjerner eller deaktiverer adgangen til terrorrelateret indhold, stiller den oplysninger til rådighed for indholdsleverandøren om en sådan fjernelse eller deaktivering.

2. På indholdsleverandørens anmodning skal hostingtjenesteyderen enten oplyse indholdsleverandøren om årsagerne til fjernelsen eller deaktiveringen og om dennes ret til at gøre indsigelse mod påbuddet om fjernelse, eller give indholdsleverandøren en kopi af påbuddet om fjernelse.

3. Forpligtelsen i henhold til stk. 1 og 2 finder ikke anvendelse, hvor den kompetente myndighed, der udsteder påbuddet om fjernelse, beslutter, at det er nødvendigt og proportionalt, at der ikke sker videregivelse af oplysninger af hensyn til den offentlige sikkerhed, såsom forebyggelse, efterforskning, afsløring og retsforfølgning af terrorhandlinger så længe som nødvendigt, dog ikke længere end seks uger fra denne afgørelse. Hostingtjenesteyderen videregiver i så fald ikke nogen oplysninger om, at det terrorrelaterede indhold er blevet fjernet, eller at adgangen dertil er blevet deaktiveret.

Denne kompetente myndighed kan forlænge denne periode med yderligere seks uger, hvor sådan undladelse af videregivelse stadig er begrundet.

Afdeling IV

Kompetente myndigheder og samarbejde

Artikel 12

Udpegning af kompetente myndigheder

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

a) udstede påbud om fjernelse i henhold til artikel 3

b) kontrollere påbud om fjernelse i henhold til artikel 4

c) føre tilsyn med gennemførelsen af specifikke foranstaltninger i henhold til artikel 5

d) pålægge sanktioner i henhold til artikel 18.

2. Hver medlemsstat sikrer, at et kontaktpunkt udpeges eller etableres inden for den kompetente myndighed, der er omhandlet i stk. 1, litra a), for at håndtere anmodninger om præcisering og feedback for så vidt angår påbud om fjernelse udstedt af denne kompetente myndighed.

Medlemsstaterne sikrer, at oplysningerne om kontaktpunktet gøres offentligt tilgængelige.

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

4. Senest den … [*12 måneder efter denne forordnings ikrafttræden*] opretter Kommissionen et onlineregister over de kompetente myndigheder omhandlet i stk. 1 og det kontaktpunkt, der i medfør af stk. 2 er udpeget eller etableret for hver kompetent myndighed. Kommissionen offentliggør regelmæssigt eventuelle ændringer heraf.

Artikel 13

Kompetente myndigheder

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

2. Medlemsstaterne sikrer, at deres kompetente myndigheder udfører deres opgaver i henhold til denne forordning på en objektiv og ikkediskriminerende måde med fuld respekt for de grundlæggende rettigheder. De kompetente myndigheder må ikke søge eller modtage instrukser fra andre organer i forbindelse med udførelsen af deres opgaver i henhold til artikel 12, stk. 1.

Dette stykkes første afsnit forhindrer ikke, at der kan føres tilsyn i overensstemmelse med national forfatningsret.

Artikel 14

Samarbejde mellem hostingtjenesteydere, kompetente myndigheder og Europol

1. De kompetente myndigheder udveksler oplysninger, koordinerer og samarbejder med hinanden og, hvor det er relevant, med Europol med hensyn til påbud om fjernelse, navnlig for at undgå dobbeltarbejde, øge koordineringen og undgå forstyrrelser af efterforskninger i forskellige medlemsstater.

2. Medlemsstaternes kompetente myndigheder udveksler oplysninger, koordinerer og samarbejder med de kompetente myndigheder, der er omhandlet i artikel 12, stk. 1, litra c) og d), med hensyn til specifikke foranstaltninger, der træffes i henhold til artikel 5, og sanktioner pålagt i henhold til artikel 18. Medlemsstaterne sikrer, at de kompetente myndigheder, der er omhandlet i artikel 12, stk. 1, litra c) og d), er i besiddelse af alle relevante oplysninger.

3. Med henblik på stk. 1 tilvejebringer medlemsstaterne passende og sikre kommunikationskanaler eller -mekanismer for at sikre rettidig udveksling af relevante oplysninger.

4. For at denne forordning kan gennemføres effektivt og for at undgå dobbeltarbejde, kan medlemsstaterne og hostingtjenesteyderne gøre brug af særlige værktøjer, herunder de værktøjer, som Europol har etableret, navnlig for at lette:

a) behandling og feedback vedrørende påbud om fjernelse i henhold til artikel 3 og

b) samarbejde med henblik på at fastlægge og gennemføre specifikke foranstaltninger i henhold til artikel 5.

5. Hvor hostingtjenesteydere bliver bekendt med terrorrelateret indhold, der indebærer en overhængende livsfare, underretter de omgående de myndigheder, der er kompetente til at efterforske og retsforfølge strafbare handlinger i de berørte medlemsstater. Hvor det er umuligt at identificere de berørte medlemsstater, underretter hostingtjenesteyderne kontaktpunktet i medført af artikel 12, stk. 2, i den medlemsstat, hvor de har deres hovedsæde eller hvor deres retlige repræsentant har ophold eller er etableret, og videregiver oplysninger vedrørende dette terrorrelaterede indhold til Europol med henblik på hensigtsmæssig opfølgning.

6. De kompetente myndigheder opfordres til at sende kopier af påbuddene om fjernelse til Europol, så Europol kan udarbejde en årlig rapport, der indeholder en analyse af de typer af terrorrelateret indhold, der er genstand for påbud om at fjerne det eller at deaktivere adgangen dertil i medfør af denne forordning.

Artikel 15

Hostingtjenesteyderes kontaktpunkter

1. Hver hostingtjenesteyder udpeger eller etablerer et kontaktpunkt med henblik på modtagelse af påbud om fjernelse ved elektroniske midler og deres hurtige behandling i medfør af artikel 3 og 4. Hostingtjenesteyderen sikrer, at oplysninger om kontaktpunktet gøres offentligt tilgængelige.

2. De i denne artikels stk. 1 nævnte oplysninger angiver de officielle sprog for Unionens institutioner som omhandlet i forordning nr. 1/58 ([15]), på hvilke(t) der kan rettes henvendelse til kontaktpunktet, og på hvilket yderligere udvekslinger om påbud om fjernelse i henhold til artikel 3 finder sted. Disse sprog skal omfatte mindst ét af de officielle sprog i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde, eller hvor dens retlige repræsentant har ophold eller er etableret.

([15]) Forordning nr. 1 om den ordning, der skal gælde for Det Europæiske Økonomiske Fællesskab på det sproglige område (EFT 17 af 6.10.1958, s. 385).

Afdeling V

Gennemførelse og håndhævelse

Artikel 16

Jurisdiktion

1. Den medlemsstat, hvori hostingtjenesteyderens hovedsæde er beliggende, har jurisdiktion med henblik på artikel 5, 18 og 21. En hostingtjenesteyder, hvis hovedsæde ikke er beliggende i Unionen, anses for at høre under den medlemsstats jurisdiktion, hvor dens retlige repræsentant har ophold eller er etableret.

2. Hvor en hostingtjenesteyder, der ikke har sit hovedsæde i Unionen, ikke udpeger en retlig repræsentant, har alle medlemsstater jurisdiktion.

3. Hvor en medlemsstats kompetente myndighed udøver sin jurisdiktion i medfør af stk. 2, underretter den alle øvrige medlemsstaters kompetente myndigheder.

Artikel 17

Retlig repræsentant

1. En hostingtjenesteyder, der ikke har sit hovedsæde i Unionen, udpeger skriftligt en fysisk eller juridisk person som sin retlige repræsentant i Unionen med henblik på modtagelse, overholdelse og håndhævelse af påbud om fjernelse og afgørelser udstedt af de kompetente myndigheder

2. Hostingtjenesteyderen tildeler sin retlige repræsentant de beføjelser og ressourcer, der er nødvendige for at efterkomme disse påbud om fjernelse og afgørelser og samarbejde med de kompetente myndigheder.

Den retlige repræsentant skal have ophold i eller være etableret i en af de medlemsstater, hvor hostingtjenesteyderen udbyder sine tjenester.

3. Den retlige repræsentant kan drages til ansvar for overtrædelse af denne forordning, uden at det berører hostingtjenesteyderens ansvar eller retlige skridt mod denne.

4. Hostingtjenesteyderen underretter den i artikel 12, stk. 1, litra d), omhandlede kompetente myndighed i den medlemsstat, hvor dens retlige repræsentant har ophold eller er etableret, om udpegelsen.

Hostingtjenesteyderen gør oplysninger om den retlige repræsentant offentligt tilgængelige.

Afdeling VI

Afsluttende bestemmelser

Artikel 18

Sanktioner

1. Medlemsstaterne fastsætter regler om sanktioner, der skal anvendes i tilfælde af hostingtjenesteyderes overtrædelser af denne forordning, og træffer alle nødvendige foranstaltninger for at sikre, at de anvendes. Sådanne sanktioner begrænses til imødegåelse af overtrædelser af artikel 3, stk. 3 og 6, artikel 4, stk. 2 og 7, artikel 5, stk. 1, 2, 3, 5 og 6, artikel 6, 7, 10 og 11, artikel 14, stk. 5, artikel 15, stk. 1 og artikel 17.

De i første afsnit omhandlede sanktioner skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning. Medlemsstaterne giver senest den … [*12 måneder efter denne forordnings ikrafttræden*] Kommissionen meddelelse om disse regler og om disse foranstaltninger og underretter den straks om senere ændringer, der berører dem.

2. Medlemsstaterne sikrer, at de kompetente myndigheder, når de træffer afgørelse om, hvorvidt der skal pålægges en sanktion, og når de fastlægger sanktionernes type og omfang, tager hensyn til alle relevante omstændigheder, herunder:

a) overtrædelsens art, grovhed og varighed

b) hvorvidt overtrædelsen blev begået forsætligt eller uagtsomt

c) hostingtjenesteyderens tidligere overtrædelser

d) hostingtjenesteyderens finansielle styrke

e) hostingtjenesteyderens grad af samarbejde med de kompetente myndigheder

f) hostingtjenesteyderens art og størrelse, navnlig hvorvidt den er en mikrovirksomhed, en lille eller mellemstor virksomhed

g) omfanget af hostingtjenesteyderens skyld, idet der tages hensyn til de tekniske og organisatoriske foranstaltninger, som hostingtjenesteyderen har truffet for at overholde denne forordning.

3. Medlemsstaterne sikrer, at systematisk eller vedvarende manglende overholdelse af forpligtelserne i henhold til artikel 3, stk. 3, medfører økonomiske sanktioner på op til 4 % af hostingtjenesteyderens globale omsætning for det forudgående regnskabsår.

Artikel 19

Tekniske krav og ændringer af bilagene

1. Kommissionen tillægges beføjelse til at vedtage delegerede retsakter i overensstemmelse med artikel 20 med henblik på at supplere denne forordning med de nødvendige 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 delegerede retsakter i overensstemmelse med artikel 20 for at ændre bilagene med henblik på effektivt at imødegå et eventuelt behov for forbedringer af indholdet af formularerne for påbud om fjernelse og oplyse om, hvorfor det ikke er muligt at efterkomme påbud 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 den … [*ét år efter datoen for 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 underrettet 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 tiltag, der er iværksat i det foregående kalenderår 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 indeholde:

a) antallet af udstedte påbud om fjernelse og antallet af indslag med terrorrelaterede indhold, som er blevet fjernet eller hvortil adgangen er blevet deaktiveret, samt hvor hurtigt fjernelsen eller deaktiveringen er sket

b) de specifikke foranstaltninger, der er truffet i henhold til artikel 5, herunder antallet af indslag med terrorrelaterede indhold, som er blevet fjernet eller hvortil adgangen er blevet deaktiveret, samt hvor hurtigt fjernelsen eller deaktiveringen er sket

c) antallet af anmodninger om adgang, som en kompetent myndighed har udstedt vedrørende indhold, der opbevares af hostingtjenesteyderen i henhold til artikel 6

d) antallet af indledte klageprocedurer og de tiltag, som hostingtjenesteyderne har iværksat i henhold til artikel 10

e) antallet af indledte sager om administrativ eller retslig prøvelse og de afgørelser, der er truffet af den kompetente myndighed i overensstemmelse med national ret.

2. Senest den … [*to år efter datoen for denne forordnings ikrafttræden*] 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 iværksætte med hensyn til indsamling og analyse af data og andre beviser for at overvåge fremskridtene og evaluere denne forordning i medfør af artikel 23.

Artikel 22

Gennemførelsesrapporter

Senest den … [*to år efter denne forordnings ikrafttræden*] forelægger Kommissionen en rapport for Europa-Parlamentet og Rådet om anvendelsen af denne forordning. Denne rapport skal indeholde oplysninger om overvågning i henhold til artikel 21, og oplysninger hidrørende fra forpligtelserne vedrørende gennemsigtighed i henhold til artikel 8. Medlemsstaterne giver Kommissionen alle de oplysninger, der er nødvendige for udarbejdelsen af rapporten.

Artikel 23

Evaluering

Senest den … [*tre år efter datoen for denne forordnings ikrafttræden*] foretager Kommissionen en evaluering af denne forordning og forelægger en rapport for Europa-Parlamentet og Rådet om dens anvendelse, herunder om

a) funktionsmåden og effektiviteten af sikkerhedsmekanismerne, navnlig dem fastsat i artikel 4, stk. 4, artikel 6, stk. 3, og artikel 7-11,

b) virkningen af denne forordnings anvendelse på grundlæggende rettigheder, navnlig ytrings- og informationsfriheden, respekten for privatlivet og beskyttelsen af personoplysninger, samt

c) denne forordnings bidrag til beskyttelsen af den offentlige sikkerhed.

Hvor det er hensigtsmæssigt, ledsages rapporten af forslag til retsakter.

Medlemsstaterne giver Kommissionen alle de oplysninger, der er nødvendige for udarbejdelsen af rapporten.

Kommissionen vurderer også nødvendigheden og gennemførligheden af at oprette en europæisk platform om terrorrelateret onlineindhold for at lette kommunikationen og samarbejdet i henhold til denne forordning.

Artikel 24

Ikrafttræden og anvendelse

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

Den anvendes fra den … [*12 måneder efter denne forordnings ikrafttræden*].

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

Udfærdiget i …, den ….

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

BILAG I

PÅBUD OM FJERNELSE

(artikel 3 i Europa-Parlamentets og Rådets forordning (EU) 2021/… ([1]) ([*]))

I medfør af artikel 3 i forordning (EU) 2021/… ([*]) (»forordningen«) skal modtageren af dette påbud om fjernelse fjerne terrorrelateret indhold eller deaktivere adgangen til terrorrelateret indhold i alle medlemsstater hurtigst muligt og under alle omstændigheder inden for en time efter at have modtaget påbuddet om fjernelse.

I medfør af forordningens artikel 6 skal modtageren opbevare indhold og dertil knyttede data, som er blevet fjernet, eller hvor adgangen er blevet deaktiveret, i seks måneder eller længere på anmodning fra de kompetente myndigheder eller domstole.

I medfør af forordningens artikel 15, stk. 2 sendes dette påbud om fjernelse på et af de sprog, som modtageren har valgt.

AFSNIT A:

Den udstedende kompetente myndigheds medlemsstat:

……

NB: Oplysninger om den udstedende kompetente myndighed anføres i afsnit E og F

Modtager og, hvor det er relevant, retlig repræsentant:

……

Kontaktpunkt:

……

Medlemsstaten, hvor hostingtjenesteyderen har sit hovedsæde eller hvor dens retlige repræsentant har ophold eller er etableret:

……

Tidspunkt og dato for udstedelse af påbud om fjernelse:

……

Sagsnummer på påbuddet om fjernelse:

……

([1]) Europa-Parlamentets og Rådets forordning (EU) 2021/… ([*]) af … om håndtering af udbredelsen af terrorrelateret indhold online (EUT L … af …, s. …).

([*]) EUT: Indsæt venligst nummeret på forordningen, der er indeholdt i dokument ST 14308/20 (2018/0331 (COD)).

AFSNIT B: Terrorrelateret indhold, som skal fjernes eller hvortil adgang skal deaktiveres i alle medlemsstater hurtigst muligt og i alle tilfælde inden for en time efter modtagelsen af påbuddet om fjernelse:

URL og eventuelle supplerende oplysninger, som muliggør identifikation og den nøjagtig placering af det terrorrelateret indhold:

……

Begrundelse for, at materialet betragtes som terrorrelateret indhold, jf. forordningens artikel 2, nr. 7).

Materialet (sæt venligst kryds i den eller de relevante bokse):

☐ tilskynder andre til at begå terrorhandlinger, såsom ved forherligelse af terrorhandlinger, ved at slå lyd for udførelsen af sådanne lovovertrædelser (forordningens artikel 2, nr. 7), litra a)

☐ hverver andre til at begå eller medvirke til at begå terrorhandlinger (forordningens artikel 2, nr. 7), litra b)

☐ hverver andre til at deltage i en terrorgruppes aktiviteter (forordningens artikel 2, nr. 7), litra c)

☐ oplærer i fremstilling eller brug af sprængstoffer, skydevåben eller andre våben eller skadelige eller farlige stoffer eller om andre konkrete metoder eller teknikker med henblik på at begå eller medvirke til at begå terrorhandlinger (forordningens artikel 2, nr. 7), litra d)

☐ udgør en trussel om at begå en af terrorhandlingerne (forordningens artikel 2, nr. 7), litra e).

Supplerende oplysninger for at betragte materialet som terrorrelateret indhold:

……

……

……

AFSNIT C: Oplysninger til indholdsleverandøren

Bemærk venligst, at (sæt venligst kryds i en boks, hvis relevant):

☐ modtageren af hensyn til den offentlige sikkerhed **skal afstå fra at underrette indholdsleverandøren** om fjernelsen eller deaktiveringen af adgang til terrorrelateret indhold.

Hvis boksen ikke er relevant, se venligst afsnit G for nærmere oplysninger om muligheden for at gøre indsigelse mod påbuddet om fjernelse i den udstedende kompetente myndigheds medlemsstat i henhold til national ret (en kopi af påbuddet om fjernelse skal sendes til indholdsleverandøren, hvis der anmodes herom).

AFSNIT D: Oplysninger til den kompetente myndighed i medlemsstaten, hvor hostingtjenesteyderen har sit hovedsæde eller hvor dens retlige repræsentant har ophold eller er etableret

(Sæt venligst kryds i den relevante boks):

☐ Den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde eller hvor dens retlige repræsentant har ophold eller er etableret, men ikke den udstedende kompetente myndigheds medlemsstat

☐ En kopi af påbuddet om fjernelse sendes til den kompetente myndighed i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde eller hvor dens retlige repræsentant har ophold eller er etableret

AFSNIT E: Nærmere oplysninger om den udstedende kompetente myndighed

Type (sæt venligst kryds i den relevante boks):

☐ dommer, domstol eller undersøgelsesdommer

☐ retshåndhævende myndighed

☐ anden kompetent myndighed → venligst udfyld også afsnit F

Nærmere oplysninger om den udstedende kompetente myndighed eller dennes repræsentant, der bekræfter, at indholdet i påbuddet om fjernelse er nøjagtigt og korrekt:

Udstedende myndigheds navn:

……

Navn på dens repræsentant og stilling (titel/grad):

……

Sag nr ……

Adresse: ……

Tlf. (landekode) (områdenummer) ……

Fax (landekode) (områdenummer) ……

E-mailadresse: ……

Dato: ……

Officielt stempel (hvis et sådant findes) og underskrift ([2]): ……

([2]) Underskrift er ikke nødvendig, hvis påbuddet om fjernelse sendes via autentificerede transmissionskanaler, der kan garantere påbuddets autenticitet.

AFSNIT F: Kontaktoplysninger til opfølgning

Kontaktoplysninger på den udstedende kompetente myndighed til feedback om tidspunktet for fjernelse eller deaktivering af adgang eller for yderligere præciseringer:

……

Kontaktoplysninger på den kompetente myndighed i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde eller hvor dens retlige repræsentant har ophold eller er etableret:

……

AFSNIT G: Oplysninger om klagemuligheder

Oplysninger om det kompetente organ eller domstol, frister og procedurer for at gøre indsigelse mod påbuddet om fjernelse:

Kompetent organ eller domstol, hvorved der kan gøres indsigelse mod påbuddet om fjernelse:

……

Frist for at gøre indsigelse mod påbuddet om fjernelse:

[dage/måneder fra den]

……

Link til bestemmelser i national lovgivning:

……

BILAG II

FORMULAR TIL FEEDBACK EFTER PÅBUD OM FJERNELSE AF ELLER DEAKTIVERING AF ADGANG TIL TERRORRELATERET INDHOLD

(artikel 3, stk. 6, i Europa-Parlamentets og Rådets forordning (EU) 2021/ … ([1]) ([*]))

AFSNIT A:

Modtager af påbud om fjernelse:

……

Kompetent myndighed, der har udstedt påbuddet om fjernelse:

……

Sagsnummer hos den kompetente myndighed, der udstedte påbuddet om fjernelse:

……

Modtagerens sagsnummer:

……

Tidspunkt og dato for modtagelse af påbud om fjernelse:

……

AFSNIT B: Foranstaltninger truffet i overensstemmelse med påbuddet om fjernelse

(Sæt venligst kryds i den relevante boks):

☐ det terrorrelaterede indhold er fjernet

☐ adgangen til det terrorrelaterede indhold er deaktiveret i alle medlemsstater

Tidspunkt og dato for de foranstaltninger, der er truffet:

……

([1]) Europa-Parlamentets og Rådets forordning (EU) 2021/ … ([*]) af … om håndtering af udbredelsen af terrorrelateret indhold online (EUT L … af …, s. …).

([*]) EUT: Indsæt venligst nummeret på forordningen, der er indeholdt i dokument ST 14308/20 (2018/0331 (COD)).

AFSNIT C: Modtagerens oplysninger

Navn på hostingtjenesteyderen:

……

ELLER

Navn på hostingtjenesteyderens retlige repræsentant:

……

Medlemsstat, hvor hostingtjenesteyderens hovedsæde er beliggende:

……

ELLER

Medlemsstaten, hvor hostingtjenesteyderens retlige repræsentant har ophold eller er etableret:

……

Navn på den autoriserede person:

……

Kontaktpunktets e-mailadresse:

……

Dato:

……

BILAG III

OPLYSNINGER OM, HVORFOR DET IKKE ER MULIGT AT EFTERKOMME PÅBUDDET OM FJERNELSE

(artikel 3, stk. 7 og 8, i Europa-Parlamentets og Rådets forordning (EU) 2021/ … ([1]) ([*]))

AFSNIT A:

Modtager af påbuddet om fjernelse:

……

Kompetent myndighed, der har udstedt påbuddet om fjernelse:

……

Sagsnummer hos den kompetente myndighed, der udstedte påbuddet om fjernelse:

……

Modtagerens sagsnummer:

……

Tidspunkt og dato for modtagelse af påbud om fjernelse:

……

AFSNIT B: Manglende efterkommelse

1) Påbuddet kan ikke efterkommes inden for tidsfristen af de følgende grunde (sæt venligst kryds i den eller de relevante bokse):

   ☐ force majeure eller de facto umulighed, som ikke kan tilskrives hostingtjenesteyderen, herunder af objektivt begrundede tekniske eller operationelle årsager

   ☐ påbuddet om fjernelse indeholder åbenbare fejl

   ☐ påbuddet om fjernelse indeholder ikke tilstrækkelige oplysninger

2) Giv venligst yderligere oplysninger om grundene til manglende efterkommelse:

   ……

3) Hvis påbuddet indeholder åbenbare fejl og/eller ikke indeholder tilstrækkelige oplysninger, redegør venligst for fejlene og de yderligere oplysninger eller præciseringer der er behov for:

   ……

([1]) Europa-Parlamentets og Rådets forordning (EU) 2021/ … ([*]) af … om håndtering af udbredelsen af terrorrelateret indhold online (EUT L … af …, s. …).

([*]) EUT: Indsæt venligst nummeret på forordningen, der er indeholdt i dokument ST 14308/20 (2018/0331 (COD)).

AFSNIT C: Oplysninger om hostingtjenesteyderen eller dennes retlige repræsentant

Navn på hostingtjenesteyderen:

……

ELLER

Navn på hostingtjenesteyderens retlige repræsentant:

……

Navn på den autoriserede person:

……

Kontaktoplysninger (e-mailadresse):

……

Underskrift:

……

Tidspunkt og dato:

……

Rådets begrundelse: Rådets førstebehandlingsholdning (EU) nr. 6/2021 med henblik på vedtagelse af Europa-Parlamentets og Rådets forordning om håndtering af udbredelsen af terrorrelateret indhold online

(2021/C 135/02)

I. INDLEDNING

1. Kommissionen forelagde den 12. september 2018 ovennævnte forslag ([1]) til forordning om forebyggelse af udbredelsen af terrorrelateret onlineindhold for Rådet og Europa-Parlamentet. Retsgrundlaget er artikel 114 [Tilnærmelse af lovgivningerne] i traktaten om Den Europæiske Unions funktionsmåde, og forslaget er underlagt den almindelige lovgivningsprocedure.

2. Det Europæiske Økonomiske og Sociale Udvalg (EØSU) blev hørt af Rådet ved skrivelse af 24. oktober 2018 og afgav udtalelse om forslaget den 12. december 2018 ([2]) på plenarmødet i december.

3. Den 6. december 2018 nåede Rådet til enighed om en generel indstilling ([3]) vedrørende terrorrelateret onlineindhold, som udgjorde mandatet til forhandlinger med Europa-Parlamentet inden for rammerne af den almindelige lovgivningsprocedure.

4. Den 12. februar 2019 sendte Den Europæiske Tilsynsførende for Databeskyttelse »formelle bemærkninger« til forordningsudkastet til Europa-Parlamentet, Kommissionen og Rådet ([4]). Samme dag afgav Den Europæiske Unions Agentur for Grundlæggende Rettigheder efter anmodning fra Europa-Parlamentet af 6. februar 2019 udtalelse om forslaget ([5]).

5. Den 17. april 2019 fastlagde Europa-Parlamentet en førstebehandlingsholdning ([6]) til Kommissionens forslag med 155 ændringsforslag til Kommissionens forslag og med 308 stemmer for, 204 imod og 70 hverken for eller imod.

6. Rådet og Europa-Parlamentet indledte forhandlinger i oktober 2019 med henblik på at nå til tidlig enighed ved andenbehandlingen. Forhandlingerne blev afsluttet med positivt resultat den 10. december 2020, hvor Europa-Parlamentet og Rådet nåede til foreløbig enighed om en kompromistekst.

7. Coreper II analyserede og bekræftede den 16. december 2020 foreløbigt den endelige kompromistekst i betragtning af den enighed, der var opnået med Europa-Parlamentet ([7]).

8. Den 11. januar 2021 blev kompromiset godkendt af Europa-Parlamentets Udvalg om Borgernes Rettigheder og Retlige og Indre Anliggender (LIBE). Den 13. januar sendte formanden for LIBE-udvalget en skrivelse til formanden for Coreper II for at oplyse ham om, at han ville henstille til plenarforsamlingen, at den accepterer Rådets holdning uden ændringer ved Europa-Parlamentets andenbehandling med forbehold af jurist-lingvist-gennemgangen, hvis Rådet formelt fremsender sin holdning i den form, hvori den foreligger i bilaget til nævnte skrivelse, til Europa-Parlamentet ([8]).

([1]) 12129/18 + ADD 1-3.
([2]) EUT C 110 af 22.3.2019, s. 67 (15729/19).
([3]) 15336/18.
([4]) Ref. 2018-0822 D2545 (WK 9232/2019).
([5]) FRA-udtalelse nr. 2/2019 (WK 9235/2019).
([6]) Jf. 8663/19 (orienterende note fra GIP2 (interinstitutionelle forbindelser) til Coreper med resultatet af Europa-Parlamentets førstebehandling); Parlamentets mandat blev bekræftet af plenarforsamlingen den 10.-11. oktober 2019.
([7]) 12906/20.
([8]) 5634/21.

II. FORMÅL

9. Forordningen tilvejebringer en klar retlig ramme, som fastsætter medlemsstaternes og hostingtjenesteydernes ansvar med henblik på at håndtere misbrug af hostingtjenester til udbredelse af terrorrelateret indhold online, idet et velfungerende digitalt indre marked garanteres, samtidig med at der sikres tillid til og sikkerhed i onlinemiljøet. Forordningen søger navnlig at skabe klarhed om hostingtjenesteyderes ansvar for at sørge for, at deres tjenester er sikre, og for hurtigt og effektivt at håndtere, identificere og fjerne eller deaktivere adgangen til terrorrelateret indhold online. Den opretter et nyt og effektivt operationelt instrument til eliminering af terrorrelateret indhold ved at gøre det muligt at udstede påbud om fjernelse, der har grænseoverskridende virkning. Desuden er målet at opretholde beskyttelsesforanstaltninger for at sikre beskyttelsen af grundlæggende rettigheder, herunder ytrings- og informationsfriheden i et åbent og demokratisk samfund og friheden til at oprette og drive egen virksomhed. Forordningen fastsætter, at terrorrelateret indhold skal fjernes inden for højst en time efter modtagelse af påbuddet om fjernelse, og fastsætter, at det er onlineplatformes ansvar at sørge for, at sådant indhold fjernes. Ud over de muligheder for retslig prøvelse, der garanteres ved retten til adgang til effektive retsmidler, indfører forordningen en række beskyttelsesforanstaltninger og klagemekanismer.

10. Den eller de kompetente myndigheder i hver medlemsstat kan udstede et påbud om fjernelse til enhver hostingtjenesteyder, der udbyder tjenester i EU. Den eller de kompetente myndigheder i den medlemsstat, hvor tjenesteyderen har sit hovedsæde, vil have ret — og efter begrundet anmodning fra hostingtjenesteydere eller indholdsleverandører pligt — til at kontrollere påbuddet om fjernelse, hvis påbuddet anses for at udgøre en alvorlig eller åbenbar overtrædelse af selve forordningen eller krænker grundlæggende rettigheder som nedfældet i Den Europæiske Unions charter om grundlæggende rettigheder. Medlemsstaterne bør vedtage regler om sanktioner for overtrædelser af forpligtelserne under hensyntagen til blandt andet arten heraf og den pågældende virksomheds størrelse.

III. ANALYSE AF RÅDETS FØRSTEBEHANDLINGSHOLDNING

GENERELT

11. Europa-Parlamentet og Rådet førte forhandlinger med henblik på at indgå en andenbehandlingsaftale på grundlag af Rådets førstebehandlingsholdning, som Parlamentet som sådan kunne godkende. Teksten til Rådets førstebehandlingsholdning til forordningen om forebyggelse af udbredelsen af terrorrelateret indhold online afspejler fuldt ud det kompromis, der er opnået mellem de to medlovgivere bistået af Europa-Kommissionen.

RESUMÉ AF DE VIGTIGSTE SPØRGSMÅL

12. Efter anmodning fra Europa-Parlamentet blev forordningens titel ændret til »forordning om håndtering [...] af udbredelsen af terrorrelateret indhold online«.

13. Definitionen af »terrorrelateret indhold« er i overensstemmelse med definitionerne af de relevante lovovertrædelser i direktivet om bekæmpelse af terrorisme ([9]). Med hensyn til anvendelsesområde omfatter Rådets førstebehandlingsholdning materiale, som udbredes til offentligheden, dvs. til et potentielt ubegrænset antal personer. Materiale, som udbredes til uddannelsesmæssige, journalistiske, kunstneriske eller forskningsmæssige formål eller til oplysningsformål for at forebygge eller bekæmpe terrorisme, bør ikke betragtes som terrorrelateret indhold. Det omfatter også indhold, der giver udtryk for polemiske eller kontroversielle holdninger i en offentlig debat om følsomme politiske spørgsmål. En vurdering skal fastslå det egentlige formål med udbredelsen. Det er også blevet præciseret, at denne forordning ikke indebærer nogen ændring af pligten til at respektere de rettigheder, friheder og principper, der er omhandlet i artikel 6 i TEU, og finder anvendelse, uden at det berører grundlæggende principper vedrørende ytrings- og informationsfriheden, herunder mediefriheden og -pluralismen.

([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).

14. Hostingtjenesteydere skal træffe passende, rimelige og forholdsmæssige foranstaltninger for effektivt at håndtere misbrug af deres tjeneste til udbredelse af terrorrelateret indhold online. Hvis hostingtjenesteydere eksponeres for terrorrelateret indhold, vil de skulle træffe specifikke foranstaltninger for at beskytte deres tjenester mod udbredelse heraf. Den aftalte tekst slår tre artikler — artikel 3 (Rettidig omhu), artikel 6 (Proaktive foranstaltninger) og artikel 9 (Sikkerhedsforanstaltninger vedrørende proaktive foranstaltninger) — sammen til én artikel om »specifikke foranstaltninger«. Valget af sådanne foranstaltninger er et anliggende for den enkelte hostingtjenesteyder. Rådets førstebehandlingsholdning gør det klart, at en hostingtjenesteyder kan anvende forskellige foranstaltninger for at håndtere udbredelsen af terrorrelateret indhold, herunder automatiserede foranstaltninger, som kan tilpasses hostingtjenesteyderens kapacitet og arten af de udbudte tjenester. Hvor den kompetente myndighed vurderer, at de specifikke foranstaltninger, der er iværksat, er utilstrækkelige til at håndtere risiciene, vil den kunne kræve, at der træffes yderligere passende, effektive og forholdsmæssige specifikke foranstaltninger. Kravet om at træffe sådanne yderligere specifikke foranstaltninger bør dog ikke føre til en generel forpligtelse til at overvåge eller aktivt undersøge forhold, der tyder på ulovlig virksomhed som omhandlet i artikel 15, stk. 1, i direktiv 2000/31/EF ([10]) eller til en forpligtelse til at anvende automatiserede værktøjer. For at sikre gennemsigtighed vil hostingtjenesteydere skulle offentliggøre årlige gennemsigtighedsrapporter om de tiltag, der er iværksat til bekæmpelse af udbredelse af terrorrelateret indhold.

15. Værtsmedlemsstatens rolle i forbindelse med påbud om fjernelse med grænseoverskridende virkninger er blevet styrket ved at indføre en kontrolprocedure: Den kompetente myndighed i den medlemsstat, hvor en hostingtjenesteyder har sit hovedsæde eller sin retlige repræsentant, kan på eget initiativ kontrollere det påbud om fjernelse, der er udstedt af kompetente myndigheder fra en anden medlemsstat, for at fastslå, om det udgør en alvorlig eller åbenbar overtrædelse af forordningen eller de grundlæggende rettigheder som nedfældet i Den Europæiske Unions charter om grundlæggende rettigheder. Efter begrundet anmodning fra en hostingtjenesteyder eller en indholdsleverandør er værtsmedlemsstaten forpligtet til at kontrollere, om der foreligger en sådan overtrædelse.

16. Undtagen i behørigt begrundede nødsituationer bør hostingtjenesteydere, der ikke tidligere har modtaget et påbud om fjernelse fra den pågældende myndighed, 12 timer i forvejen modtage en underretning med oplysninger om de gældende procedurer og frister, navnlig med henblik på at lette byrden for små og mellemstore virksomheder (SMV'er).

17. Artiklen om indberetninger — en mekanisme, hvor hostingtjenesteydere gøres bekendt med terrorrelateret indhold og derefter frivilligt kan vurdere overensstemmelsen med deres egne vilkår og betingelser — er udgået, men en betragtning præciserer, at indberetninger fortsat står til rådighed for medlemsstaterne og Europol.

18. Terrorrelateret indhold, som er blevet fjernet, eller hvortil adgangen er blevet deaktiveret som følge af påbud om fjernelse eller specifikke foranstaltninger, skal opbevares i seks måneder fra fjernelsen eller deaktiveringen, en periode, der kan forlænges, hvis og så længe det er nødvendigt i forbindelse med en prøvelse.

19. Medlemsstaterne skal fastsætte regler om sanktioner for hostingtjenesteyderes overtrædelse af forordningen. Sanktioner kan antage forskellige former, herunder formelle advarsler i tilfælde af mindre overtrædelser eller økonomiske sanktioner i forbindelse med mere alvorlige overtrædelser. Rådets førstebehandlingsholdning fastsætter, hvilke overtrædelser der er underlagt sanktioner, og hvilke omstændigheder der er relevante for vurderingen af typen og omfanget af sådanne sanktioner. Hostingtjenesteydere kan blive pålagt sanktioner på op til 4 % af deres globale omsætning, hvis de systematisk eller vedvarende undlader at overholde entimesreglen om at fjerne eller deaktivere adgangen til terrorrelateret indhold.

IV. **KONKLUSION**

20. Rådets holdning afspejler til fulde det kompromis, der blev opnået enighed om under forhandlingerne mellem Europa-Parlamentet og Rådet med bistand fra Kommissionen. Kompromiset er bekræftet ved skrivelse fra formanden for Europa-Parlamentets LIBE-udvalg til formanden for Coreper II dateret den 13. januar 2021.

([10]) 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).

ISSN 1977-0871 (elektronisk udgave)
ISSN 1725-2393 (papirudgave)

Den Europæiske Unions
Publikationskontor
L-2985 Luxembourg
LUXEMBOURG

DA