Forslag
til
Lov om supplerende bestemmelser til forordning om håndtering af udbredelsen af terrorrelateret indhold online (TCO-loven)[1]

Anvendelsesområde

§ 1. Loven supplerer Europa-Parlamentets og Rådets forordning (EU) 2021/784 af 29. april 2021 om håndtering af terrorrelateret indhold online (TCO-forordningen), jf. bilag 1 til denne lov.

Stk. 2. Loven og TCO-forordningen finder anvendelse på hostingtjenesteydere, der udbyder tjenester i Den Europæiske Union, uanset hvor deres hovedsæde er beliggende, i det omfang de udbreder oplysninger til offentligheden.

Den nationale kompetente myndighed

§ 2. Rigspolitiet udpeges som national kompetent myndighed, jf. TCO-forordningens artikel 12, stk. 1, litra a-c.

Stk. 2. Rigspolitiet må ikke søge eller modtage instrukser fra andre organer i forbindelse med udførelsen af deres opgaver i henhold til TCO-forordningens artikel 12, stk. 1, litra a-c.

Stk. 3. Forvaltningslovens kapitel 5 om partshøring finder ikke anvendelse for Rigspolitiets afgørelser i henhold til TCO-forordningens artikel 3 og 4, stk. 3 og 4, samt underretninger efter denne lovs § 3, stk. 1. Desuden finder forvaltningslovens kapitel 6 om begrundelse m.v. ikke anvendelse for Rigspolitiets underretninger efter denne lovs § 3, stk. 1.

Stk. 4. Rigspolitiets afgørelser i henhold til TCO-forordningen eller underretninger efter denne lovs § 3, stk. 1, kan ikke påklages til anden administrativ myndighed.

Underretning af danske hostingtjenesteydere

§ 3. Modtager Rigspolitiet en underretning i henhold til TCO-forordningens artikel 4, stk. 1, som er rettet til en hostingtjenesteyder med hovedsæde i Danmark eller til hostingtjenesteyders retlige repræsentant i Danmark, underretter Rigspolitiet hostingtjenesteyderen om påbuddets retlige virkning for så vidt angår Danmark.

Stk. 2. Underretning efter stk. 1 skal ske umiddelbart efter, at Rigspolitiet er blevet underrettet om påbuddet.

[1] I loven er der medtaget visse bestemmelser fra forordning (EU) 2021/784 af 29. april 2021 om håndtering af udbredelsen af terrorrelateret indhold online, EU-Tidende 2021, nr. L 172, side 79. Ifølge artikel 288 i EUF-traktaten gælder en forordning umiddelbart i hver medlemsstat. Gengivelsen af disse bestemmelser i loven samt optagelsen af forordningen som bilag til loven er således udelukkende begrundet i praktiske hensyn og berører ikke forordningens umiddelbare gyldighed i Danmark.

Sanktioner

§ 4. Medmindre højere straf er forskyldt efter anden lovgivning, straffes med bøde den, der overtræder TCO-forordningens artikel 3, stk. 3 eller 6, artikel 4, stk. 2 eller 7, artikel 5, stk. 1, 2, 3, 5 eller 6, artikel 6, 7, 10 eller 11, artikel 14, stk. 5, artikel 15, stk. 1, eller artikel 17.

Stk. 2. Ved udmålingen af bøder for overtrædelse af de bestemmelser, der er nævnt i stk. 1, skal der lægges vægt på den årlige omsætning på verdensplan i det regnskabsår, som går forud for tidspunktet for overtrædelsen, samt de øvrige momenter, der følger af TCO-forordningens artikel 18, stk. 2.

Stk. 3. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

§ 5. Justitsministeren kan fastsætte regler, som er nødvendige for at gennemføre de retsakter, der er udstedt af Den Europæiske Union med henblik på at gennemføre TCO-forordningen, eller regler, som er nødvendige for at anvende de retsakter på forordningens område, der er udstedt af Den Europæiske Union. Justitsministeren kan endvidere fastsætte nærmere regler om procedurerne for det administrative samarbejde med kompetente myndigheder i andre EU/EØS-lande, herunder om elektronisk udveksling af oplysninger mellem disse myndigheder.

Ikrafttræden

§ 6. Loven træder i kraft den 7. juni 2022.

Territorialbestemmelse

§ 7. Loven gælder ikke for Færøerne og Grønland.

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2021/784

af 29. april 2021

om håndtering af udbredelsen af terrorrelateret indhold online

(EØS-relevant tekst)

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.

(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«).

(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 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.

(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 12 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.

(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 medfør af 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 medfør af 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 overensstemmelse med 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.

(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 medfør af 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.

(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 fleres 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

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 overensstemmelse med 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 medfør af 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 medfør af stk. 3, andet afsnit, eller en afgørelse om en overtrædelse i medfør af 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 overensstemmelse med 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 medfør af denne artikels stk. 4, og, i overensstemmelse med artikel 14, Europol. Hvor afgørelsen fastslår, at der er tale en overtrædelse i medfør af 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 overensstemmelse med 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 medfør af 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 medfør af 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 nødvendig 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 medfør af 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 medfør af 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 medfør af 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 medfør af artikel 3, stk. 1, eller en afgørelse i medfør af 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 medfør af 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 medfør af 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 medfør af 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 medfør af 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 dets fjernelse eller deaktivering af adgang dertil 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 medfør af 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 medfør af artikel 3

b) kontrollere påbud om fjernelse i medfør af artikel 4

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

d) pålægge sanktioner i medfør af 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 7. juni 2022 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 7. juni 2022 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.

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 medfør af artikel 5, og sanktioner pålagt i medfør af 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 medfør af artikel 3 og

b) samarbejde med henblik på at fastlægge og gennemføre specifikke foranstaltninger i medfør af 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 omhandlet i forordning nr. 1/58 ([15]), på hvilke der kan rettes henvendelse til kontaktpunktet, og på hvilke yderligere udvekslinger om påbud om fjernelse i medfør af artikel 3 skal finde 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.

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 7. juni 2022 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 medfør af 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 7. juni 2022.

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 medfør af 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 medfør af 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 medfør af artikel 6

d) antallet af indledte klageprocedurer og tiltag, som hostingtjenesteyderne har iværksat i medfør af 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 7. juni 2023 fastlægger Kommissionen et detaljeret program for overvågning af forordningens output, resultater og virkninger. I overvågningsprogrammet fastlægges de indikatorer, indikatorer og intervaller, der skal anvendes ved 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 7. juni 2023 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 7. juni 2024 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 finder anvendelse fra den 7. juni 2022.

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

Udfærdiget i Bruxelles, den 29. april 2021.

På Europa-Parlamentets vegne

D.M. SASSOLI

Formand

På Rådets vegne

A.P. ZACARIAS

Formand

([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 (EUT C 135 af 16.4.2021, s. 1). Europa-Parlamentets holdning af 28.4.2021 (endnu ikke offentliggjort i EUT).

([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).

([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).

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

([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).

([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).

([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.

([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).

([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).

BILAG I

PÅBUD OM FJERNELSE

(artikel 3 i Europa-Parlamentets og Rådets forordning (EU) 2021/784)

I medfør af artikel 3 i forordning (EU) 2021/784 (»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:

……

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 eller de relevante bokse:

☐ 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 ([1]):

……

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:

……

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

BILAG II

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

(artikel 3, stk. 6, i Europa-Parlamentets og Rådets forordning (EU) 2021/784)

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

☐ adgang til det terrorrelaterede indhold er deaktiveret i alle medlemsstater

Tidspunkt og dato for de foranstaltninger, der er truffet:

……

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) 2021/784)

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:

……

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:

……

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indhold

1. Indledning

1.1. Lovforslagets baggrund

Nylige terrorangreb i EU har vist, hvordan terrorister misbruger internettet til at træne og rekruttere tilhængere, forberede og fremme terroraktiviteter, forherlige deres ugerninger og tilskynde andre til at følge trop og skabe frygt blandt den almindelige befolkning. Terrorrelateret indhold, der deles online til sådanne formål, udbredes bl.a. via hostingtjenesteydere, som tillader upload af tredjepartsindhold.

Terrorrelateret onlineindhold har således vist sig at spille en stor rolle med hensyn til at radikalisere og inspirere såkaldte "ensomme ulve" til angreb. Indholdet har desuden ikke alene negative virkninger for enkeltpersoner og for samfundet som helhed, men det mindsker også internetbrugerens tillid og påvirker de berørte virksomheders forretningsmodeller og omdømme.

Terrorister misbruger ikke blot store sociale medieplatforme, men de misbruger i stigende grad også mindre udbydere, der udbyder forskellige former for hostingtjenester på globalt plan. Dette misbrug af internettet understreger internetplatformenes særlige samfundsmæssige ansvar for at beskytte deres brugere mod eksponering for terrorrelateret indhold og de alvorlige sikkerhedsrisici, som dette indhold udgør for samfundet som helhed.

På denne baggrund fremsatte Europa-Kommissionen den 12. september 2018 et forslag til Europa-Parlamentets og Rådets forordning om forebyggelse af udbredelsen af terrorrelateret onlineindhold (KOM (2018) 0640).

Forslaget blev fremsat som en del af EU-Kommissionens sikkerhedspakke bestående af tre initiativer, der har til formål at styrke de nationale retshåndhævende myndigheders mulighed for at bekæmpe terrorisme og grænseoverskridende kriminalitet. Forordningen supplerer således de eksisterende frivillige ordninger i regi af EU's internetforum mellem medlemsstater og hostingtjenesteydere, der blev påbegyndt i 2015, og forordningen bygger videre på Kommissionens henstilling (EU) 2018/334 af 1. marts 2018 om foranstaltninger til effektiv bekæmpelse af ulovligt indhold på nettet.

Den 29. april 2021 blev Europa-Parlamentets og Rådets forordning (EU) 2021/784 af 29. april 2021 om håndtering af udbredelsen af terrorrelateret indhold online (herefter TCO-forordningen) vedtaget.

Forordningen trådte i kraft den 17. maj 2021 og finder anvendelse fra den 7. juni 2022.

Med TCO-forordningen skabes en klar og harmoniseret retlig ramme til at håndtere misbrug af hostingtjenester til udbredelse af terrorrelateret indhold på internettet med henblik på at garantere et velfungerende digitalt indre marked. Forordningen er et centralt element i den fælles europæiske kamp mod terrorisme, ekstremisme og radikalisering, og med forordningen etableres et fælles europæisk instrument for alle medlemsstater til dette formål. Forordningen gælder for alle hostingtjenesteydere, der tilbyder tjenester i EU, uanset om de har hovedsæde i medlemsstaterne.

Med TCO-forordningen bliver det muligt for medlemsstaterne at udstede et påbud til hostingtjenesteydere om, at de inden for én time fra modtagelsen af påbuddet skal fjerne eller deaktivere terrorrelateret indhold på deres platforme i alle EU's medlemsstater. Forordningen stiller endvidere krav om, at enhver hostingtjenesteyder, der er udsat for terrorrelateret indhold, skal indføre specifikke foranstaltninger til at beskytte deres tjeneste mod udbredelsen af terrorrelateret indhold, når den nationale kompetente myndighed har truffet afgørelse om, at hostingtjenesteyderen er eksponeret for terrorrelateret indhold, jf. herom pkt. 2.2.2.3.

TCO-forordningen supplerer de eksisterende EU-regler om bekæmpelse af ulovligt indhold på internettet, herunder Europa-Parlamentets og Rådets direktiv (EU) 2010/13 af 10. marts 2010 om samordning af visse love og administrative bestemmelser i medlemsstaterne om udbud af audiovisuelle medietjenester og Europa-Parlamentets og Rådets direktiv (EF) 2000/31 af 8. juni 2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked.

1.2. Lovforslagets indhold

TCO-forordningen gælder umiddelbart i Danmark.

Flere bestemmelser i TCO-forordningen kræver imidlertid, at der foretages visse gennemførelsesforanstaltninger i medlemsstaterne, herunder at der udpeges en national kompetent myndighed, der skal varetage en række opgaver efter forordningen. Der skal derudover fastsættes regler om sanktioner for hostingtjenesteyderes overtrædelse af en række bestemmelser i forordningen. Danmark er således forpligtet til at indrette dansk lovgivning i overensstemmelse med forordningens bestemmelser med virkning fra den 7. juni 2022, hvor forordningen finder anvendelse.

Lovforslaget har *for det første* til formål at bringe dansk ret i overensstemmelse med TCO-forordningen ved at udpege Rigspolitiet som den kompetente myndighed i Danmark efter artikel 12, stk. 1, litra a-c, og fastsætte sanktioner for hostingtjenesteyderes overtrædelse af forordningens 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.

Lovforslaget har *for det andet* til formål at udmønte den ordning, som er beskrevet i den erklæring, som blev afgivet af Danmark i forbindelse med Rådets vedtagelse af førstebehandlingsholdning til Kommissionens forslag til TCO-forordningen den 16. marts 2021. Erklæringen har følgende ordlyd:

> "Med gentagelse af den fulde støtte til Europa-Parlamentets og Rådets forordning om håndtering af udbredelse af terrorrelateret indhold online vil Danmark informere om, at når den kompetente myndighed i Danmark i henhold til forordningens artikel 4, stk. 1, underrettes om et påbud om fjernelse af terrorrelateret indhold, der er udstedt af en kompetent myndighed i en anden medlemsstat, til en dansk hostingtjenesteyder, vil den danske myndighed underrette hostingtjenesteyderen om påbuddets retlige virkning i Danmark."[2]

Om baggrunden for erklæringen kan bl.a. henvises til Justitsministeriets besvarelse af 18. februar 2021 af spørgsmål nr. 7 fra Folketingets Europaudvalg vedrørende KOM (2018) 0640 Forslag til Europa-Parlamentets og Rådets Forordning om forebyggelse af udbredelsen af terrorrelateret onlineindhold og Justitsministeriets notat af 23. december 2020 vedrørende politisk aftale om forslag til forordning om forebyggelse af udbredelsen af terrorrelateret indhold på nettet (KOM (2018) 0640, bilag 5). Det fremgår heraf, at forordningen indebærer, at en national myndighed i en anden medlemsstat skal kunne træffe en retligt bindende afgørelse i form af f.eks. et påbud om fjernelse af terrorrelateret indhold over for en hostingtjenesteyder med hovedsæde i Danmark med virkning i Danmark.

En sådan ordning, hvor en udenlandsk myndighed skal have beføjelse til at udøve myndighed med virkning inden for det danske territorium, rejser som udgangspunkt spørgsmål i forhold til det uskrevne grundlovsforbud, hvorefter danske myndigheder som udgangspunkt anses for enekompetente til at udøve myndighedsbeføjelser inden for det danske territorium. Som en undtagelse hertil følger det af grundlovens § 20, at beføjelser, som efter grundloven tilkommer rigets myndigheder, ved lov i nærmere bestemt omfang kan overlades til mellemfolkelige myndigheder som f.eks. EU. Bestemmelsen giver derimod ikke adgang til at overlade beføjelser til andre stater.

Den ordning, der er beskrevet i erklæringen, indebærer, at når den kompetente myndighed i Danmark i henhold til forordningen underrettes om et påbud om fjernelse af terrorrelateret indhold, der er udstedt af den kompetente myndighed i en anden medlemsstat, og som er adresseret til en dansk hostingtjenesteyder, vil den danske myndighed underrette hostingtjenesteyderen om påbuddets retlige

[2] Erklæringen blev alene afgivet på engelsk, hvorfor den engelske version af erklæringen er den autoritative version. Den engelske version lyder: *"While reiterating the full support for the Regulation of the European Parliament and of the Council on addressing the dissemination of terrorist content online Denmark would like to inform that when the competent authority in Denmark in accordance with Article 4(1) of the Regulation is informed of a removal order issued by the competent authority of another Member State to a Danish hosting service provider, the Danish competent authority will inform the hosting service provider of its legal effect in Denmark."*

virkning for så vidt angår Danmark. Et påbud fra en anden medlemsstats kompetente myndighed til en dansk hostingtjenesteyder får således først retsvirkning i Danmark, når den danske hostingtjenesteyder er underrettet af den danske kompetente myndighed. Denne ordning indebærer, at det i praksis kan sikres, at reglerne om fjernelse af terrorrelateret indhold inden for én time i forordningen overholdes inden for rammerne af dansk ret.

2. Lovforslagets hovedpunkter

2.1. Anvendelsesområde

2.1.1. Gældende ret

Der er i dag ikke regler for, hvilke forpligtelser der gælder for hostingtjenesteydere, hvis platform bliver misbrugt til at udbrede terrorrelateret indhold online til offentligheden.

2.1.2. TCO-forordningen

Det følger af TCO-forordningens artikel 1, stk. 2, at forordningen finder anvendelse på hostingtjenesteydere, der udbyder tjenester i Unionen, uanset hvor deres hovedsæde er beliggende, i det omfang de udbreder oplysninger til offentligheden.

Ved en hostingtjenesteyder forstås en udbyder af tjenester som defineret i artikel 1, litra b, i Europa-Parlamentets og Rådets direktiv (EU) 2015/1535[3], der består i lagringen af oplysninger fra en indholdsleverandør på dennes anmodning, jf. artikel 2, stk. 1. En hostingtjenesteyder er dermed en udbyder 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 karakter, jf. præambelbetragtning 13.

Det afgørende for, at der udbydes tjenester i Unionen, er, at hostingstjenesteyderen gør det muligt for juridiske eller fysiske personer i en eller flere medlemsstater at gøre brug af tjenester fra hostingtjenesteyderen. Den blotte kendsgerning, at en tjenesteyders websted, e-mailadresse eller andre kontaktoplysninger kan tilgås i en eller flere medlemsstater, er dog isoleret set ikke tilstrækkeligt. Der stilles krav om en "væsentlig tilknytning" til den eller de medlemsstater, hvor tjenesterne stilles til rådighed. En sådan væsentlig tilknytning anses for at være til stede, hvis hostingtjenesteyderen er etableret i EU. For hostingtjenesteydere uden for EU vil det være afgørende, om der er et betydeligt antal brugere i en eller flere medlemsstater, eller om tjenesteudbyderen målretter sine tjenester mod en eller flere medlemsstater, f.eks. ved at markedsføre tjenesterne og

[3] Gennemført i dansk ret ved bekendtgørelse nr. 1087 af 8. juli 2016 om EU's informationsprocedure for tekniske forskrifter og forskrifter for informationssamfundets tjenester.

varetage kundeservicen på den pågældende medlemsstats sprog, eller ved at udbyde appliktationer i nationale appbutikker, jf. præambelbetragtning 16.

Begrebet terrorrelateret indhold er i TCO-forordningen artikel 2, stk. 7, defineret som materiale, der indeholder en eller flere af følgende elementer:

1) Tilskyndelse til at begå terrorhandlinger, som de er defineret i artikel 3, stk. 1, litra a)-i), i direktiv (EU) 2017/541 om bekæmpelse af terrorisme, hvor sådant materiale direkte eller indirekte, f.eks. 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.

2) Hvervning af en person eller en gruppe af personer til at begå eller bidrage til terrorhandlinger, jf. ovennævnte direktiv.

3) Hvervning af en person eller en gruppe personer til at deltage i en terrorgruppes aktiviteter som omhandlet i artikel 4, litra b, i direktiv (EU) 20217/541.

4) Oplæring 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 terrorhandling, jf. ovennævnte direktiv.

5) Trusler om at begå terrorhandlinger, jf. ovennævnte direktiv.

Udbredelse til offentligheden af terrorindhold er i TCO-forordningens artikel 2, stk. 3, defineret som på anmodning af indholdsudbyderen at stille oplysninger til rådighed for et potentielt ubegrænset antal personer.

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 terrorrelateret indhold. En vurdering skal fastslå det egentlige formål med denne udbredelse, og hvorvidt materialet udbredes til offentligheden til de nævnte formål, jf. forordningens artikel 1, stk. 3. Det følger endvidere af præambelbetragtning nr. 12, at 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 EU's Charter om Grundlæggende Rettigheder.

TCO-forordningen medfører ikke en ændring af pligten til at respektere de grundlæggende rettigheder i Traktaten om Den Europæiske Union artikel 6, og forordningen finder således anvendelse, uden at

det berører grundlæggende principper vedrørende ytrings- og informationsfriheden, herunder mediefriheden og -pluralismen, jf. forordningens artikel 1, stk. 4.

Endelig følger det af artikel 1, stk. 5, at TCO-forordningen ikke berører Europa-Parlamentets og Rådets direktiv (EF) 2000/31 af 8. juni 2000 ("Direktivet om elektronisk handel")[4] og Europa-Parlamentets og Rådets direktiv (EU) 2010/13 af 10. marts 2010 om samordning af visse love og administrative bestemmelser i medlemsstaterne om udbud af audiovisuelle medietjenester ("direktiv om audiovisuelle medietjenester").[5] Endvidere fremgår det, at for audiovisuelle medietjenester som defineret i artikel 1, stk. 1, litra a, i direktiv om audiovisuelle medietjenester, har direktiv om audiovisuelle medietjenester forrang. Dette bør dog ikke påvirke forpligtelserne i henhold til TCO-forordningen, navnlig vedrørende udbydere af videodelingsplatformstjenester, jf. præambelbetragtning nr. 8.

2.1.3. Justitsministeriets overvejelser og den foreslåede ordning

Med TCO-forordningen er der etableret en fælles europæisk ramme for håndtering af misbrug af hostingtjenester til udbredelse af terrorrelateret indhold på internettet.

Da forordningen gælder umiddelbart i medlemsstaterne, skal forordningens bestemmelser ikke implementeres i Danmark. Forordningen kræver dog, at der fastsættes visse gennemførelsesforanstaltninger i medlemsstaterne, herunder at der udpeges en kompetent national myndighed, der skal varetage en række opgaver efter forordningen, og at der fastsættes sanktionsbestemmelser for overtrædelse af en række bestemmelser i forordningen. Det foreslås på den baggrund, at loven vil supplere forordningen.

Da der med loven foreslås indført regler, der vil supplere reglerne i TCO-forordningen, finder Justitsministeriet det rigtigst, at loven har samme anvendelsesområde som forordningen. Det medfører, at loven vil finde anvendelse på hostingtjenesteydere, der udbyder tjenester i Den Europæiske Union, uanset hvor deres hovedsæde er beliggende, i det omfang de udbreder oplysninger til offentligheden, jf. definitionerne omtalt under pkt. 2.1.2.

Justitsministeriet bemærker, at loven således ikke finder anvendelse, i det omfang TCO-forordningen ikke finder anvendelse, fordi der f.eks. er tale om 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

[4] Gennemført i dansk ret ved lov nr. 227 af 22. april 2002 om tjenester i informationssamfundet, herunder visse aspekter af elektronisk handel.
[5] Senest ændret ved Europa-Parlamentets og Rådets direktiv (EU) 2018/1808 af 14. november 2018 om ændring af direktiv 2010/13/EU om samordning af visse love og administrative bestemmelser i medlemsstaterne om udbud af audiovisuelle medietjenester (direktiv om audiovisuelle medietjenester) i betragtning af de ændrede markedsforhold og gennemført i dansk ret ved bekendtgørelse nr. 1350 af 4. september 2020 af lov om radio og fjernsynsvirksomhed mv.

kontroversielle holdninger i den offentlige debat, som således ikke skal betragtes som terrorrelateret indhold.

2.2. Udpegning af kompetent myndighed

2.2.1 Gældende ret

Der findes i dag ikke regler, der udpeger en dansk kompetent myndighed, der skal varetage opgaver i henhold til TCO-forordningen, herunder udstede påbud til en hostingtjenesteyder i andre lande om fjernelse af terrorrelateret indhold på internettet.

Der findes dog bestemmelser i retsplejeloven, hvorefter politiet har mulighed for at blokere adgangen til en hjemmeside eller beslaglægge hjemmesiden efter forudgående retskendelse, hvis der er grund til at antage, at der fra hjemmesiden begås en overtrædelse af straffelovens terrorbestemmelser.

2.2.1.1. Retsplejelovens regler om blokering af hjemmesider

Det følger af retsplejelovens § 791 d, stk. 1, at der kan ske blokering af en hjemmeside, hvis der er grund til at antage, at der fra hjemmesiden begås en overtrædelse af straffelovens §§ 114-114 i, om terrorisme.

Ved »blokering« forstås en ordning, der er rettet mod danske internetudbydere med henblik på direkte DNS-blokering fra udbyderens side af hjemmesider med ulovligt materiale. DNS-blokering medfører, at forsøg på at opnå adgang til siden automatisk afvises af internetudbyderen. Bestemmelsen forudsætter, at afvisningen vil være ledsaget af en tekst, hvoraf det fremgår, at politiet har opnået rettens kendelse til at blokere den pågældende hjemmeside, og at eventuelle indsigelser kan rettes til politiet, jf. Folketingstidende 2016-17, tillæg A, L 192 som fremsat, s. 32.

Kravet om, at der skal være "grund til at antage", skal forstås i overensstemmelse med det tilsvarende udtryk i retsplejelovens §§ 803 og 804 om beslaglæggelse over for ikke-mistænkte og edition, jf. Folketingstidende 2016-17, tillæg A, L 192 som fremsat, s. 32.

Kravet om, at der fra hjemmesiden begås en overtrædelse af straffelovens §§ 114-114 i, indebærer, at siden skal indeholde tekst, video eller lyd mv., der udgør en sådan overtrædelse, jf. Folketingstidende 2016-17, tillæg A, L 192 som fremsat, s. 32.

Det følger af retsplejelovens § 791, d, stk. 2, at en afgørelse om blokering af en hjemmeside træffes af retten ved kendelse efter politiets begæring. I kendelsen anføres de konkrete omstændigheder i sagen, hvorpå det støttes, at betingelserne for indgrebet er opfyldt. Kendelsen kan til enhver tid omgøres.

Politiet forudsættes at foretage underretning af den, som indgrebet retter sig mod, dvs. lejeren af den hjemmeside (registranten), som retten har givet tilladelse til at blokere. Indeholder hjemmesiden ikke kontaktoplysninger, og kan politiet ikke umiddelbart fremskaffe disse oplysninger på anden vis, kan underretning undlades. Underretning af personer i udlandet vil ske efter de almindelige retshjælpsregler om underretning til personer i andre lande.

Det forudsættes endvidere, at politiet hurtigst muligt skal fjerne blokeringen, hvis politiet bliver bekendt med, at grundlaget for kendelsen ikke længere er til stede, f.eks. fordi det ulovlige indhold er fjernet fra hjemmesiden. Politiet er dog ikke hermed pålagt en pligt til løbende at kontrollere indholdet af de blokerede hjemmesider.

Det følger endvidere af retsplejelovens § 791, d, stk. 3, at blokering ikke må foretages, såfremt indgrebet står i misforhold til sagens betydning og den ulempe, som indgrebet må antages at medføre. Der skal således foretages en proportionalitetsafvejning, inden der træffes afgørelse om blokering.

Det fremgår af retsplejelovens § 791 d, stk. 4, at det påhviler udbydere af elektroniske kommunikationsnet og -tjenester og administratorer af internetdomæner at bistå politiet med at gennemføre blokering af en hjemmeside. Det indebærer bl.a., at udbyderne skal iværksætte en DNS-blokering af den hjemmeside, som rettens kendelse vedrører.

Det påhviler udbydere af elektroniske kommunikationsnet og -tjenester og administratorer af internetdomæner at bistå politiet ved gennemførelsen af kendelser efter stk. 2. Afviser udbyderen eller administratoren uden lovlig grund at bistå politiet, finder bestemmelsen i retsplejelovens § 178 tilsvarende anvendelse, jf. bestemmelsens stk. 4.

Fremsætter den, mod hvem indgrebet retter sig, anmodning herom, skal politiet snarest muligt forelægge sagen for retten. Retten afgør ved kendelse, om indgrebet skal opretholdes, jf. bestemmelsens stk. 5.

2.2.1.2. Retsplejelovens regler om beslaglæggelse

I sager om efterforskningen af lovovertrædelser, som ikke er omfattet af retsplejelovens § 791 d, stk. 1, vil politiet kunne foretage beslaglæggelse af dokumenter på en hjemmeside.

Det følger af retsplejelovens § 803, stk. 1, at genstande, som en person, der ikke er mistænkt, har rådighed over, kan beslaglægges som led i efterforskningen af en lovovertrædelse, der er undergivet offentlig påtale, hvis der er grund til at antage, at genstanden kan tjene som bevis, bør konfiskeres eller ved lovovertrædelsen er fravendt nogen, som kan kræve den tilbage. Efter praksis omfatter genstande også dokumenter på hjemmesider, og der kan derfor ske beslaglæggelse heraf, jf. f.eks. Højesterets kendelse af 13. april 2007 som gengivet i UfR 2007.1831H.

Afgørelse om beslaglæggelse træffes af retten ved kendelse efter politiets begæring, jf. § 806, stk. 1 og 2. Såfremt indgrebets øjemed ville forspildes, hvis retskendelse skulle indhentes, kan politiet træffe beslutning om beslaglæggelse. Fremsætter den, mod hvem indgrebet retter sig, anmodning herom, skal politiet snarest muligt og inden 24 timer forelægge sagen for retten, der ved kendelse afgøre om indgrebet kan godkendes, jf. § 806, stk. 4.

En retskendelse sendes til administratoren af den pågældende hjemmeside (DK Hostmaster), hvorefter administratoren træffer de fornødne tekniske foranstaltninger til at overføre rettighederne til hjemmesiden til politiet. Hvis man herefter forsøger at tilgå hjemmesiden, vil man typisk blive mødt med en besked om, at rettighederne til hjemmesiden er overført til politiet.

Beslaglæggelse af hjemmesider er hovedsageligt blevet anvendt af politiet i sager, hvor hjemmesiden administreres i Danmark. Det vil i praksis være hjemmesider, der ender på ".dk.", som administreres af DK Hostmaster. I det omfang, der er tale om en hjemmeside, som administreres i udlandet, kan det i praksis være vanskeligt at gennemføre en beslaglæggelse, idet det kræver bistand fra det land, hvor hjemmesiden administreres. Det er muligt at anmode udenlandske myndigheder om retshjælp til gennemførelsen af en beslaglæggelse af en udenlandsk hjemmeside, men det er ofte meget tidskrævende, og erfaringsmæssigt er der lande, hvor det ikke er muligt at få en sådan retskendelse.

2.2.1.1.3. Forvaltningslovens regler om partshøring og begrundelse

Forvaltningslovens kapitel 5 indeholder regler om partshøring.

Det følger af lovens § 19, at hvis en part ikke kan antages at være bekendt med, at myndigheden er i besiddelse af bestemte oplysninger om en sags faktiske grundlag eller eksterne faglige vurderinger, må der ikke træffes afgørelse, før myndigheden har gjort parten bekendt med oplysningerne eller vurderingerne og givet denne lejlighed til at fremkomme med en udtalelse. Det gælder dog kun, hvis oplysningerne eller vurderingerne er til ugunst for den pågældende part og er af væsentlig betydning for sagens afgørelse.

Efter § 19, stk. 2, nr. 2 og 3, gælder bestemmelsen i stk. 1 dog ikke, hvis udsættelse vil medføre overskridelse af en lovbestemt frist for sagens afgørelse, eller hvis partens interesse i, at sagens afgørelse udsættes, findes at burde vige for væsentlige hensyn til offentlige eller private interesser, der taler imod en sådan udsættelse.

Forvaltningslovens kapitel 6 indeholder regler om begrundelse mv.

Det følger af lovens § 22, at en afgørelse, når den meddeles skriftligt, skal være ledsaget af en begrundelse, medmindre afgørelsen fuldt ud giver den pågældende part medhold.

Efter lovens § 24, stk. 1, skal en begrundelse for en afgørelse indeholde en henvisning til de retsregler, i henhold til hvilke afgørelsen er truffet. I det omfang, afgørelsen efter disse regler beror på et administrativt skøn, skal begrundelsen tillige angive de hovedhensyn, der har været bestemmende for skønsudøvelsen. Begrundelsen skal endvidere om fornødent indeholde en kort redegørelse for de oplysninger vedrørende sagens faktiske omstændigheder, som er tillagt væsentlig betydning for afgørelsen, jf. stk. 2.

Reglerne om partshøring og begrundelse gælder for behandling af sager, hvori der er eller vil blive truffet afgørelse af en forvaltningsmyndighed, jf. forvaltningslovens § 2, stk. 1.

2.2.2. TCO-forordningen

Det følger af TCO-forordningens artikel 12, stk. 1, at medlemsstaterne skal udpege en eller flere kompetente myndigheder, der har kompetence til at udstede påbud til hostingtjenesteydere om fjernelse af terrorrelateret indhold, jf. artikel 3. Den kompetente myndighed skal herudover kontrollere påbud om fjernelse, jf. artikel 4, føre tilsyn med gennemførelsen af specifikke foranstaltninger, jf. artikel 5, samt pålægge sanktioner, jf. artikel 18.

Udpegningen af en national kompetent myndighed bør ikke nødvendigvis indebære, at der skal oprettes en ny myndighed, og det bør være muligt at udpege et eksisterende organ. Medlemsstaterne kan ved udpegningen af den eller de kompetente myndigheder frit vælge administrative, retshåndhævende eller retslige myndigheder, jf. præambelbetragtning 35.

Medlemsstaterne skal i medfør af TCO-forordningens artikel 12, stk. 2, udpege et kontaktpunkt inden for den eller de kompetente myndigheder til at behandle anmodninger om præcisering og feedback for så vidt angår påbud om fjernelse af terrorrelateret indhold, der er udstedt af dem. Oplysninger om kontaktpunktet skal gøres offentligt tilgængelige.

Det følger af TCO-forordningens artikel 13, stk. 1, at medlemsstaterne skal sikre, at deres kompetente myndigheder har de nødvendige beføjelser og tilstrækkelige ressourcer til at nå målene og til at opfylde deres forpligtelser i henhold til forordningen. Medlemsstaterne skal endvidere sikre, at de kompetente myndigheder kan varetage deres opgaver uafhængigt og på en objektiv og ikke-diskriminerende måde med fuld respekt for grundlæggende rettigheder, og at de kompetente myndigheder ikke søger eller modtager instrukser fra noget andet organ i forbindelse med udøvelsen af de opgaver, som de får tildelt i medfør af forordningen, jf. TCO-forordningens artikel 13, stk. 2.

2.2.2.1 Påbud om fjernelse

Efter TCO-forordningens artikel 3, stk. 1, kan den kompetente nationale myndighed i enhver medlemsstat udstede et påbud til hostingtjenesteydere, der udbyder onlinetjenester i EU, om at fjerne terrorrelateret indhold på deres platforme eller deaktivere adgangen til sådant materiale i samtlige medlemsstater.

Hvis den relevante kompetente myndighed ikke tidligere har udstedt et påbud om fjernelse af terrorrelateret indhold til en hostingtjenesteyder, skal den kompetente myndighed give hostingtjenesteyderen oplysninger om procedurer og gældende frister mindst 12 timer inden, den kompetente myndighed udsteder et påbud om fjernelse af terrorrelateret indhold, medmindre der er tale om en behørigt begrundet nødsituation, jf. artikel 3, stk. 2. Det fremgår af præambelbetragtning 17, at behørigt begrundede nødsituationer er situationer, hvor fjernelsen af eller deaktiveringen af adgang til det terrorrelaterede indhold mere end én time efter modtagelsen af påbuddet om fjernelse vil medføre alvorlig skade. Dette er blandt andet 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. Det er den kompetente myndighed, der afgør, om en situation udgør en nødsituation. Denne beslutning skal fremgå af påbuddet om fjernelse.

Påbuddet om fjernelse skal bl.a. omfatte en tilstrækkeligt detaljeret begrundelse for, hvorfor indholdet, som skal fjernes, eller hvortil adgang skal deaktiveres, betragtes som værende terrorrelateret indhold, jf. artikel 3, stk. 4, litra b. Det følger endvidere af artikel 3, stk. 4, litra c, at påbuddet skal indeholde oplysninger om indholdets placering ved at angive den nøjagtige internetadresse (URL) og om nødvendigt eventuelle andre supplerende oplysninger til identifikation af det terrorrelaterede indhold, såsom et screenshot af det pågældende indhold. Herudover skal påbuddet indeholde letforståelige oplysninger om hostingtjenesteyderens og indholdsleverandørens klagemuligheder, jf. artikel 3, stk. 4, litra f. Begrundelsen bør således sætte hostingtjenesteyderen og i sidste ende indholdsleverandøren i stand til effektivt at udøve deres ret til retlig prøvelse, jf. præambelbetragtning nr. 18.

Hostingtjenesteyderen skal fjerne eller deaktivere adgangen til det terrorrelaterede indhold i alle medlemsstater hurtigst muligt og under alle omstændigheder inden for én time efter modtagelse af et påbud om fjernelse af terrorrelateret indhold, jf. forordningens artikel 3, stk. 3. Hostingtjenesteyderen skal herefter uden unødigt ophold underrette den kompetente myndighed om, at indholdet er blevet fjernet, eller at adgangen til indholdet er blevet deaktiveret samt tidspunktet for dette, jf. TCO-forordningens artikel 3, stk. 6. Underretningen skal ske ved hjælp af en formular, der er indsat som bilag 2 (”Feedback efter påbud om fjernelse af eller deaktivering af adgang til terrorrelateret indhold”) til forordningen.

Hvis en hostingtjenesteyder ikke kan efterkomme et påbud om fjernelse på grund af force majeure eller faktisk umulighed, som ikke kan tilskrives hostingtjenesteyderen, herunder af objektivt begrundede tekniske eller operationelle årsager, skal hostingtjenesteyderen uden unødigt ophold oplyse den kompetente myndighed, der har udstedt påbuddet om fjernelse, herom, jf. TCO-forordningens artikel 3, stk. 7. Det samme gælder, hvis hostingtjenesteyderen ikke kan efterkomme et påbud om fjernelse, fordi det indeholder åbenbare fejl eller ikke indeholder tilstrækkelige oplysninger til, at påbuddet kan efterkommes, jf. artikel 3, stk. 8. Hostingtjenesteyderen skal underrette den kompetente myndighed og anmode om den nødvendige forklaring af påbuddet ved hjælp af en formular, der er indsat som bilag 3 ("Oplysninger om, hvorfor det ikke er muligt at efterkomme påbuddet om fjernelse") til forordningen.

2.2.2.2. Procedure for grænseoverskridende påbud om fjernelse

Hvor hostingtjenesteyderen ikke har hovedsæde eller sin retlige repræsentant i den medlemsstat, som udsteder et påbud om fjernelse af terrorrelateret indhold, skal den kompetente myndighed, samtidig med at påbuddet sendes til hostingtjenesteyderen, sende en kopi af påbuddet om fjernelse til den kompetente myndighed i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde, jf. TCO-forordningens artikel 4, stk. 1. Hostingtjenesteyderen skal i disse situationer i forbindelse med fjernelse eller deaktivering tage de nødvendige foranstaltninger for at være i stand til at kunne genindsætte eller genetablere adgang til indholdet, jf. forordningens artikel 4, stk. 2.

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 timer efter modtagelse af kopien af påbuddet om fjernelse kontrollere, om påbuddet udgør et alvorligt eller åbenbart brud på forordningen eller grundlæggende rettigheder i EU's Charter om grundlæggende rettigheder, jf. forordningens artikel 4, stk. 3. I så fald træffer den kompetente myndighed en begrundet afgørelse herom. Den kompetente myndighed skal forud for, at en sådan afgørelse træffes, underrette den udstedende kompetente myndighed om sin hensigt og om begrundelsen for afgørelsen, jf. artikel 4, stk. 5.

Hvis den kompetente myndighed i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde, eller dens retlige repræsentant har ophold eller er etableret, udsteder en afgørelse om, at påbuddet om fjernelse udgør et alvorligt eller åbenbart brud på forordningen eller grundlæggende rettigheder i EU's Charter om grundlæggende rettigheder, skal dette straks meddeles til den udstedende myndighed, hostingtjenesteyderen og indholdsleverandøren, hvorefter påbuddet om fjernelse ikke længere er juridisk bindende, jf. artikel 4, stk. 6. Hostingtjenesteyderen genindsætter omgående indholdet eller genaktiverer adgangen dertil, efter at have modtaget en afgørelse, der fastslår en overtrædelse, jf. artikel 4, stk. 7. Dette berører dog ikke muligheden for at håndhæve vilkår og betingelser i overensstemmelse med EU-retten og national ret.

En hostingtjenesteyder og en indholdsleverandør har ret til inden for 48 timer efter modtagelse af et påbud om fjernelse af terrorrelateret indhold eller oplysninger herom i medfør af forordningens artikel 11, stk. 2, at indgive en begrundet anmodning til de kompetente myndigheder i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde, eller hvor den retlige repræsentant har ophold eller er etableret, om at undersøge, om påbuddet udgør et alvorligt eller åbenbart brud på forordningen eller grundlæggende rettigheder i EU's Charter om grundlæggende rettigheder, jf. artikel 4, stk. 4. Den kompetente myndighed skal inden for 72 timer efter modtagelse af anmodningen træffe en begrundet afgørelse efter at have kontrolleret påbuddet om fjernelse med angivelse af dens konklusioner om, hvorvidt der er tale om en overtrædelse.

Som anført under pkt. 1.2 har lovforslaget bl.a. til formål at udmønte den ordning, som er beskrevet i den erklæring, som blev afgivet af Danmark i forbindelse Rådets vedtagelse af førstebehandlingsholdning til Kommissionens forslag til TCO-forordningen den 16. marts 2021. Denne ordning indebærer, at det i praksis kan sikres, at reglerne om fjernelse af terrorrelateret indhold inden for en time i forordningen overholdes inden for rammerne af dansk ret.

2.2.2.3. Specifikke foranstaltninger

Ifølge TCO-forordningens artikel 5, stk. 1, skal hostingtjenesteydere, der eksponeres for terrorrelateret indhold, hvor det er relevant, i deres vilkår og betingelser medtage og anvende bestemmelser om håndtering af misbrug af deres tjeneste til formidling til udbredelse af terrorrelateret indhold online. Dette skal ske på en omhyggelig, forholdsmæssig og ikke-diskriminerende måde og under behørig hensyntagen til brugernes grundlæggende rettigheder, herunder ytringsfriheden og informationsfriheden i et åbent og demokratisk samfund.

En hostingtjenesteyder anses efter forordningens artikel 5, stk. 4, for at være eksponeret for terrorrelateret indhold, når den kompetente myndighed i den medlemsstat, hvor hostingtjenesteyderen har hovedsæde, træffer afgørelse herom. Afgørelsen skal baseres på objektive kriterier, som f.eks. at hostingtjenesteyderen har modtaget to eller flere påbud om fjernelse af terrorrelateret indhold inden for 12 måneder.

Hvis en hostingtjenesteyder er at betragte som eksponeret for terrorrelateret indhold, skal hostingtjenesteyderen efter TCO-forordningens artikel 5, stk. 2, træffe specifikke foranstaltninger for at beskytte deres tjenester mod formidling til offentligheden af terrorrelateret indhold. Valget af de konkrete foranstaltninger ligger hos hostingtjenesteydere, men kan bl.a. omfatte passende tekniske og operationelle foranstaltninger eller kapaciteter såsom passende bemanding eller tekniske midler til at identificere og hurtigt fjerne eller deaktivere adgang til terrorrelateret indhold eller let tilgængelige og brugervenlige mekanismer, så brugere kan rapportere muligt terrorrelateret indhold til hostingtjenesteyderen.

Enhver foranstaltning, som en hostingtjenesteyder træffer som følge af eksponering for terrorrelateret indhold, skal leve op til følgende krav, jf. artikel 5, stk. 3:

1) De skal være effektive til at afbøde niveauet for eksponering for terrorrelateret indhold.

2) 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.

3) 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.

4) 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.

En hostingtjenesteyder, der har modtaget en afgørelse om, at de anses for at være eksponeret for terrorindhold, skal senest tre måneder og derefter hvert år efter modtagelse af en sådan afgørelse underrette den kompetente myndighed om de specifikke foranstaltninger den har truffet eller agter at træffe for at imødegå eksponeringen, jf. forordningens artikel 5, stk. 5. Underretningsforpligtelsen ophører, når den kompetente myndighed på baggrund af en anmodning fra hostingtjenesteyderen træffer afgørelse om, at hostingtjenesteyderen ikke længere er at betragte om værende eksponeret for terrorrelateret indhold. Den kompetente myndighed skal træffe afgørelse inden for tre måneder efter modtagelsen af en sådan anmodning fra hostingtjenesteyderen.

Hvis den kompetente myndighed i den medlemsstat, hvor hostingtjenesteyderen har hovedsæde, finder, at de foranstaltninger, som hostingtjenesteyderen har truffet, ikke er tilstrækkelige, træffer den kompetente myndighed afgørelse om, at hostingtjenesteyderen skal træffe de nødvendige foranstaltninger, jf. forordningens artikel 5, stk. 4. Den nærmere afgørelse af, hvilke foranstaltninger der skal iværksættes, forbliver hos hostingtjenesteyderen.

Krav om at træffe foranstaltninger i henhold til forordningen medfører ikke en generel forpligtelse for hostingtjenesteydere til at overvåge det indhold, som de opbevarer, eller en generel forpligtelse til at aktivt at søge efter ulovlig aktivitet. Krav om at træffe foranstaltninger omfatter heller ikke en forpligtelse til at bruge automatiserede værktøjer.

2.2.3. Justitsministeriets overvejelser og den foreslåede ordning

2.2.3.1. Udpegning af kompetent myndighed

Det følger af TCO-forordningens artikel 12, stk. 1, at hver medlemsstat udpeger den eller de kompetente myndigheder, der skal varetage de opgaver, som er nævnt i bestemmelsen.

Lovforslaget har bl.a. til formål at udpege den kompetente myndighed i Danmark. Den kompetente myndighed skal varetage en række opgaver, der efter Justitsministeriets vurdering mest hensigtsmæssigt varetages af en myndighed, der har erfaring med løsningen af forvaltningsretlige opgaver, og som har viden inden for terrorområdet.

Rigspolitiet er politiets øverste myndighed i Danmark, der understøtter politikredsenes arbejde og koordinerer politiets indsats på landsplan. Rigspolitiet har således som forvaltningsmyndighed erfaring med varetagelsen af opgaver, der falder inden for den i henhold til TCO-forordningen kompetente myndigheds kompetence.

Derudover har Rigspolitiet allerede i dag et tæt samarbejde med Politiets Efterretningstjeneste (PET) om identifikation og vurdering af terrorrelateret indhold. Rigspolitiets organisatoriske tilknytning til PET gør derudover, at Rigspolitiet ved varetagelsen af sine forpligtelser kan inddrage PET i relevant omfang og modtage væsentlig bistand i forbindelse med blandt andet identifikation, monitorering, vurdering og indberetning af terrorrelateret indhold. Rigspolitiets samarbejde med PET på dette område vil ligeledes kunne sikre, at der foretages en vurdering af, om nedtagning af terrorrelateret indhold strider imod hensyn til igangværende efterforskning, jf. TCO-forordningens artikel 14. Sådanne hensyn kan alene inddrages i forbindelse med udstedelse af påbud om fjernelse af terrorrelateret indhold, og ikke når Rigspolitiet underretter en dansk hostingtjenesteyder om et påbud om fjernelse af terrorrelateret indhold fra en anden medlemsstat efter dette lovforslags § 3, stk. 1.

Det foreslås på denne baggrund, at Rigspolitiet udpeges som kompetent myndighed i overensstemmelse med TCO-forordningens artikel 12, stk. 1, litra a-c. Dette indebærer, at Rigspolitiet vil få kompetence til at udstede påbud om fjernelse i medfør af artikel 3, kompetence til at kontrollere påbud om fjernelse i medfør af artikel 4 samt kompetence til at føre tilsyn med gennemførelsen af specifikke foranstaltninger i medfør af artikel 5.

Det bemærkes i den forbindelse, at det følger af gældende ret, at det er anklagemyndigheden, der under visse betingelser kan udstede bødeforelæg efter retsplejelovens § 832, og at det er domstolene, der pålægger sanktioner ved afsigelsen af straffedomme. Anklagemyndigheden og domstolene er således efter gældende ret allerede kompetente til at pålægge sanktioner i medfør af artikel 18 i TCO-forordningen, jf. artikel 12, stk. 1, litra d. Mulighederne for udstedelse af bødeforelæg er beskrevet nærmere under pkt. 2.4.3.

I det omfang Rigspolitiet som kompetent myndighed i Danmark får mistanke om en overtrædelse af de bestemmelser i forordningen, der er strafbelagt med dette lovforslag, skal Rigspolitiet indgive en anmeldelse til den stedlige politikreds, der herefter inden for strafferetsplejens rammer kan efterforske sagen og tage stilling til, om der skal ske strafforfølgning. Det vil efter de almindelige regler om ansvarsfordelingen mellem politiet og anklagemyndigheden betyde, at sagerne vil skulle afgøres af den stedlige anklagemyndighed.

Rigspolitiet og anklagemyndigheden er organisatorisk underlagt Justitsministeriet, ligesom det bl.a. følger af retsplejelovens § 98, stk. 3, at justitsministeren kan give de offentlige anklagere pålæg vedrørende behandlingen af konkrete sager. Imidlertid skal den kompetente myndighed leve op til det krav om uafhængighed, der følger af TCO-forordningen, jf. artikel 13, stk. 2, hvoraf det bl.a. fremgår, at den kompetente myndighed ikke må søge eller modtage instrukser fra andre organer i forbindelse med udførelsen af sine opgaver i henhold til TCO-forordningens artikel 12, stk. 1. Rigspolitiet, der udpeges som national kompetent myndighed i medfør af dette lovforslag, samt anklagemyndigheden forudsættes således ved behandlingen af sager i henhold til TCO-forordningen at være uafhængige i overensstemmelse med forordningens krav herom.

2.2.3.2. Den kompetente myndigheds opgaver

Forslaget indebærer for det *første*, at Rigspolitiet vil kunne udstede et påbud til hostingtjenesteudbydere, der udbyder onlinetjenester i EU, om at fjerne terrorrelateret indhold på deres platforme eller deaktivere adgangen til sådant materiale i samtlige medlemsstater inden for én time efter modtagelsen af påbuddet. Påbuddet vil skulle udstedes i overenstemmelse med TCO-forordningens artikel 3, som er beskrevet nærmere under pkt. 2.2.2.1.

Det er Justitsministeriets vurdering, at Rigspolitiets udstedelse af et påbud efter artikel 3 vil være en afgørelse i forvaltningslovens forstand. Det indebærer, at Rigspolitiet som udgangspunkt skal iagttage forvaltningsloven, herunder reglerne om partshøring og begrundelse, samt øvrige forvaltningsretlige regler og grundsætninger ved behandlingen af sådanne sager.

Der lægges med lovforslagets § 2, stk. 3, imidlertid op til at fravige forvaltningslovens kapitel 5 om partshøring i forhold til Rigspolitiets påbud efter artikel 3. Det indebærer, at Rigspolitiet ikke vil skulle foretage partshøring af hostingtjenesteydere mv., inden der træffes afgørelse om udstedelse af et påbud i medfør af forordningens artikel 3. Dette foreslås af hensyn til at sikre, at formålet med påbuddet om fjernelse af terrorrelateret indhold online ikke forspildes.

Justitsministeriet bemærker i den forbindelse, at betingelserne for at undlade at foretage partshøring i sådanne sager efter gældende ret ofte vil være opfyldt, jf. herved forvaltningslovens § 19, stk. 2, nr. 3. Ministeriet finder det imidlertid rigtigst at regulere forholdet udtrykkeligt i loven.

Som det fremgår under pkt. 2.2.2.1, skal et påbud efter TCO-forordningens artikel 3 indeholde en række oplysninger om begrundelsen for påbuddet, jf. artikel 3, stk. 4. Det forudsættes i den forbindelse med lovforslaget, at et påbud, som opfylder kravene i artikel 3, stk. 4, også vil opfylde forvaltningslovens krav til begrundelse for en afgørelse.

Lovforslaget indebærer for det *andet*, at Rigspolitiet vil skulle administrere den ordning for forordningens anvendelse i dansk ret, som er skitseret i erklæringen afgivet i forbindelse med Rådets vedtagelse af førstebehandlingsholdning til Kommissionens forslag til TCO-forordningen den 16. marts 2021, jf. nærmere herom ovenfor pkt. 1.2.

Lovforslagets § 3 er en udmøntning af den ordning, der er skitseret i erklæringen.

Bestemmelsen vil medføre, at når Rigspolitiet i henhold til TCO-forordningens artikel 4, stk. 1, underrettes om et påbud om fjernelse af terrorrelateret indhold, der er udstedt af den kompetente myndighed i en anden medlemsstat, og som er adresseret til en dansk hostingtjenesteyder, skal Rigspolitiet underrette hostingtjenesteyderen eller den retlige repræsentant om påbuddets retlige virkning for så vidt angår Danmark.

Bestemmelsen har den virkning, at et påbud fra en anden medlemsstats kompetente myndighed til en dansk hostingtjenesteyder får retsvirkning for så vidt angår Danmark, når den danske hostingtjenesteyder er underrettet af Rigspolitiet. Dette gælder uanset, at den danske hostingtjenesteyder og Rigspolitiet modtager påbuddet fra den udenlandske kompetente myndighed på samme tid, jf. forordningens artikel 4, stk. 1. Det er dermed en forudsætning for, at en dansk hostingtjenesteyder kan ifalde ansvar for ikke at efterkomme et påbud efter TCO-forordningens artikel 3, stk. 1, om fjernelse eller deaktivering efter artikel 3, stk. 3, at Rigspolitiet har underrettet hostingtjenesteyderen om påbuddets retlige virkning for så vidt angår Danmark. Det bemærkes, at underretningsordningen ikke er til hinder for, at hostingtjenesteyderen ifalder ansvar for ikke at efterkomme et påbud efter TCO-forordningens artikel 3, stk. 1, om fjernelse eller deaktivering efter artikel 3, stk. 3, for så vidt angår de øvrige EU-medlemsstater. Påbuddet har således retlig virkning for så vidt angår de øvrige medlemsstater i overensstemmelse med forordningen, uanset om der er sket underretning i henhold til lovforslagets § 3. Uanset at påbuddet først får retlig virkning for så vidt angår Danmark, når Rigspolitiet har foretaget underretning efter den foreslåede bestemmelse i § 3, begynder den tidsfrist på én time, som er fastsat i forordningen, fra det tidspunkt, hvor den danske hostingtjenesteyder modtager påbuddet fra den udenlandske myndighed.

I den forbindelse bemærkes det, at det er afgørende for overholdelse af TCO-forordningens artikel 3, stk. 3, om, at terrorrelateret indhold skal fjernes inden for én time, at Rigspolitiet som den kompetente danske myndighed videresender påbud fra en anden medlemsstats kompetente myndighed umiddelbart efter modtagelsen heraf, og Rigspolitiet skal således alene foretage en overordnet og indledende vurdering af, om påbuddet opfylder en række formmæssige krav som beskrevet i TCO-

forordningens artikel 3, stk. 4, jf. pkt. 2.2.2.1. Ifølge forordningens artikel 4, stk. 4, kan den kompetente myndighed i det land, hvor hostingtjenesteyderen har hovedsæde, imidlertid inden for 72 timer efter modtagelse af en anmodning udstede en afgørelse om, at påbuddet udgør et alvorligt eller åbenbart brud på forordningen eller grundlæggende rettigheder i EU's Charter om grundlæggende rettigheder, herunder ytringsfriheden, jf. nærmere under pkt. 2.2.2.1.

Det kan efter Justitsministeriets opfattelse give anledning til tvivl, om Rigspolitiets underretning om et påbud udstedt af kompetente myndigheder i andre medlemsstater efter lovforslagets § 3 vil have karakter af en afgørelse i forvaltningslovens forstand. Henset til at sådanne påbud først får retsvirkning for så vidt angår Danmark, når Rigspolitiet har underrettet den hostingtjenesteyder, som påbuddet retter sig mod, finder ministeriet dog, at underretningen i sig selv får karakter af en afgørelse. Rigspolitiets afgørelser efter TCO-forordningens artikel 4, stk. 3 og 4, om, at et påbud udgør et alvorligt eller åbenbart brud på forordningen eller grundlæggende rettigheder i EU's Charter om grundlæggende rettigheder, vil ligeledes udgøre en afgørelse i forvaltningslovens forstand. Dette indebærer, at Rigspolitiet som udgangspunkt skal iagttage forvaltningsloven, herunder reglerne om partshøring og begrundelse, samt øvrige forvaltningsretlige regler og grundsætninger ved behandlingen af de nævnte sagstyper.

Der lægges med lovforslaget dog op til at fravige forvaltningslovens kapitel 5 om partshøring i forhold til Rigspolitiets underretninger efter lovforslagets § 3, stk. 1, og i forhold til Rigspolitiets afgørelser efter TCO-forordningens artikel 4, stk. 3 og 4. Der henvises i den forbindelse til de hensyn, der er anført ovenfor i relation til Rigspolitiets påbud efter TCO-forordningens artikel 3.

Der lægges med lovforslaget desuden op til at fravige forvaltningslovens kapitel 6 om begrundelse mv. i forhold til Rigspolitiets underretninger efter lovforslagets § 3, stk. 1. Det vil indebære, at Rigspolitiet ikke vil være forpligtet til at overholde forvaltningslovens krav til begrundelse i forbindelse med underretningerne. Den foreslåede fravigelse skyldes, at Rigspolitiet skal videresende sådanne påbud umiddelbart efter modtagelsen heraf med henblik på at sikre overholdelse af TCO-forordningens artikel 3, stk. 3.

Lovforslaget indebærer for det *tredje*, at Rigspolitiet vil skulle føre tilsyn med gennemførelsen af specifikke foranstaltninger i overensstemmelse med de i TCO-forordningens artikel 5 fastsatte procedurer.

Som det fremgår af pkt. 2.2.2.3, anses en hostingtjenesteyder efter forordningens artikel 5, stk. 4, for at være eksponeret for terrorrelateret indhold, når den kompetente myndighed i den medlemsstat, hvor hostingtjenesteyderen har hovedsæde, træffer afgørelse herom. Afgørelsen skal baseres på objektive kriterier, som f.eks. at hostingtjenesteyderen har modtaget to eller flere påbud om fjernelse af terrorrelateret inden for 12 måneder.

Rigspolitiet vil således i overensstemmelse med TCO-forordningens artikel 5, stk. 4, kunne træffe afgørelse om, at en hostingtjenesteyder anses for at være eksponeret for terrorrelateret indhold. En sådan afgørelse vil efter Justitsministeriets vurdering have karakter af en afgørelse i forvaltningslovens forstand. Behandlingen af sådanne sager vil derfor skulle ske i overensstemmelse med reglerne i forvaltningsloven, herunder om partshøring og begrundelse, samt øvrige forvaltningsretlige regler og grundsætninger.

2.3. Retsmidler

2.3.1. Gældende ret

Som det fremgår under pkt. 2.2.3.2, vil påbud udstedt efter TCO-forordningens artikel 3 og afgørelser efter artikel 5, stk. 4, være afgørelser i forvaltningslovens forstand. Forvaltningsafgørelser kan som hovedregel påklages til en overordnet forvaltningsmyndighed. Denne klageadgang hviler på en retssædvane. Hovedreglen medfører, at afskæring af en rekursadgang fra en underordnet myndighed til en overordnet myndighed normalt kræver udtrykkelig lovhjemmel.

Der findes i dag ikke regler om adgang til effektive retsmidler for hostingtjenesteydere eller indholdsleverandører, der har modtaget påbud eller afgørelser truffet efter TCO-forordningen.

2.3.2. TCO-forordningen

Det følger af forordningens artikel 9, stk. 1, at hostingtjenesteydere, der har modtaget et påbud om fjernelse udstedt i medfør af artikel 3, stk. 1, eller en afgørelse i medfør af 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 medfør af 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.

På tilsvarende vis skal indholdsleverandører, hvis indhold er blevet fjernet, eller hvortil adgangen er blevet deaktiveret som følge af et påbud om fjernelse, have adgang til effektive retsmidler. Denne ret omfatter retten til at gøre indsigelse mod et påbud om fjernelse, der er udstedt i medfør af 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 medfør af artikel 4, stk. 4, ved domstolene i den medlemsstat, hvor den kompetente myndighed, der har truffet afgørelsen, er beliggende.

2.3.3. Justitsministeriets overvejelser og den foreslåede ordning

Den kompetente myndighed vil efter artikel 13, stk. 2, 2. pkt., i TCO-forordningen ikke være underlagt justitsministerens instruktionsbeføjelse. På denne baggrund er det efter Justitsministeriets vurdering mest hensigtsmæssigt, at adgangen til administrativ rekurs afskæres, således at Rigspolitiets afgørelser i henhold til TCO-forordningen og efter lovens § 3 ikke kan påklages til andre administrative myndigheder, herunder Justitsministeriet, jf. den foreslåede bestemmelse i § 2, stk. 4. Det gælder dog for påbud udstedt af kompetente myndigheder i andre medlemsstater til en hostingtjenesteyder eller en indholdsleverandør med hovedsæde eller retlig repræsentant i Danmark, at disse kan indgive en begrundet anmodning om at undersøge, om påbuddet udgør et alvorligt eller åbenbart brud på forordningen eller grundlæggende rettigheder i EU's Charter om grundlæggende rettigheder, til Rigspolitiet inden for 48 timer efter, at hostingtjenesteyderen eller indholdsleverandøren har modtaget påbuddet i medfør af TCO-forordningens artikel 4, stk. 4, jf. herom pkt. 2.2.2.2.

Rigspolitiets afgørelser vil dog efter TCO-forordningens artikel 9 kunne prøves ved danske domstole eller ved domstolene i det land, hvor påbuddet er udstedt.

Ovenstående indebærer, at en hostingtjenesteyder, der har modtaget et påbud om fjernelse af terrorrelateret indhold efter forordningen, har ret til at anfægte dette ved domstolene i den medlemsstat, hvis kompetente myndighed har udstedt påbuddet, jf. forordningens artikel 9, stk. 1. Indholdsleverandører, hvis indhold er blevet fjernet, eller hvor adgangen hertil er blevet deaktiveret som følge af et påbud om fjernelse af terrorrelateret indhold, har også ret til at anfægte dette ved domstolene i den medlemsstat, hvis kompetente myndighed har udstedt påbuddet, jf. forordningens artikel 9, stk. 2. Dette vil ligeledes være tilfældet for så vidt angår en hostingtjenesteyder eller en indholdsleverandør i Danmark, som vil anfægte påbuddet. Dette gælder uanset den ordning for underretning, der foreslås med lovforslagets § 3. Hvis en hostingtjenesteyder eller en indholdsleverandør ønsker at anfægte et påbud om fjernelse af terrorrelateret indhold efter forordningen, som er udstedt af den kompetente danske myndighed, vil dette skulle ske efter de almindelige civilprocessuelle regler.

Hvis en hostingtjenesteyder eller en indholdsleverandør ønsker at anfægte virkningen i Danmark af et påbud udstedt af en kompetent myndighed i en anden medlemsstat efter den underretningsordning, der foreslås med lovforslagets § 3, vil det være den underretning, som den danske myndighed har foretaget, der anfægtes. Det vil skulle ske ved en dansk domstol efter de almindelige civilprocessuelle regler. Det, som i den forbindelse vil kunne anfægtes, er, om den danske myndighed ved underretningen har handlet inden for rammerne af den med dette lovforslag foreslåede ordning, der skal understøtte og supplere anvendelsen af forordningen i Danmark, og ikke det materielle påbud om fjernelse af indholdet i Danmark. Sidstnævnte kan i overensstemmelse med TCO-forordningen

alene prøves ved domstolene i den medlemsstat, hvis kompetente myndighed har udstedt det påbud, som Rigspolitiet skal underrette den danske hostingtjenesteyder om efter den foreslåede bestemmelse i § 3.

Hvis et påbud, der er udstedt af en kompetent myndighed i et andet medlemsland, underkendes af domstolene i det pågældende land, vil påbuddet automatisk bortfalde her i landet. Den underretning om påbuddet, som Rigspolitiet har foretaget af et sådant påbud, har således ikke i sig selv retsvirkninger, hvis det underliggende påbud falder bort.

2.4. Sanktioner

2.4.1. Gældende ret

Som det fremgår af pkt. 2.1.1, findes der i dag ikke regler, der pålægger en hostingtjenesteyder at fjerne eller deaktivere online terrorrelateret indhold. Der er af samme årsag heller ikke fastsat regler om danske myndigheders håndhævelse heraf, herunder om sanktionsmuligheder.

Det følger af reglerne i straffelovens 5. kapitel, at bestemmelser om strafansvar for selskaber mv., medmindre andet er bestemt, omfatter enhver juridisk person, herunder aktie-, anparts- og andelsselskaber, interessentskaber, foreninger, fonde, boer, kommuner og statslige myndigheder, jf. straffelovens § 26, stk. 1. Endvidere omfatter sådanne bestemmelser enkeltmandsvirksomheder, for så vidt disse navnlig under hensyn til deres størrelse og organisation kan sidestilles med de ovenfor nævnte selskaber, jf. straffelovens § 26, stk. 2. Det følger videre, at strafansvar for en juridisk person forudsætter, at der inden for dens virksomhed er begået en overtrædelse, der kan tilregnes en eller flere til den juridiske person knyttede personer eller den juridiske person som sådan, jf. straffelovens § 27.

Straffelovens 10. kapitel indeholder regler for fastsættelse af straf, herunder § 81 om skærpende omstændigheder for straffastsættelsen. Efter § 81, nr. 1, skal det således i almindelighed indgå som en skærpende omstændighed, at gerningsmanden tidligere er straffet af betydning for sagen.

2.4.2. TCO-forordningen

Det følger af TCO-forordningens artikel 18, at de enkelte medlemsstater skal fastsætte regler om sanktioner for overtrædelser af forordningen og træffe alle nødvendige foranstaltninger for at sikre, at de anvendes. Det er den medlemsstat, hvori en hostingtjenesteyders hovedsæde er beliggende, der har jurisdiktion med henblik på pålæggelse af sanktioner, jf. TCO-forordningens artikel 18, jf. artikel 16.

Sanktioner efter artikel 18 er begrænset til de tilfælde, hvor en hostingtjenesteyder overtræder en eller flere af følgende bestemmelser i forordningen ved ikke:

1) at efterkomme et påbud efter TCO-forordningens artikel 3, stk. 1, om fjernelse eller deaktivering efter artikel 3, stk. 3,
2) uden unødigt ophold at underrette den kompetente myndighed efter TCO-forordningens artikel 3, stk. 6,
3) at træffe de nødvendige foranstaltninger for at kunne genindsætte indholdet eller fjerne adgangen dertil i overensstemmelse med TCO-forordningens artikel 4, stk. 7 efter TCO-forordningen artikel 4, stk. 2,
4) at genindsætte indhold eller genaktivere adgangen dertil efter TCO-forordningens artikel 4, stk. 7,
5) at medtage og anvende bestemmelser om håndtering af misbrug af dets tjenester til udbredelse af terrorrelateret indhold i henhold til TCO-forordningens artikel 5, stk. 1,
6) at træffe specifikke foranstaltninger i henhold til TCO-forordningens artikel 5, stk. 2 og 3,
7) at aflægge rapport til den kompetente myndighed om de trufne specifikke foranstaltninger, jf. TCO-forordningens artikel 5, stk. 5,
8) at efterkomme en afgørelse truffet i henhold til TCO-forordningens artikel 5, stk. 6,
9) at opbevare terrorrelateret indhold, som er blevet fjernet, eller hvortil adgangen er blevet deaktiveret som følge af et påbud eller af specifikke foranstaltninger, samt eventuelt dertil knyttet data i overensstemmelse ned TCO-forordningens artikel 6,
10) at fastsætte tydelige vilkår og betingelser for håndteringen af terrorrelateret indhold i overensstemmelse med TCO-forordningens artikel 7,
11) at indføre og opretholde en effektiv og tilgængelig klagemekanisme i overensstemmelse med TCO-forordningens artikel 10,
12) at holde indholdsleverandøren underrettet om fjernelse eller deaktivering af terrorrelateret indhold i overensstemmelse med TCO-forordningens artikel 11,
13) omgående at underrette den myndighed, der er kompetent til at efterforske og retsforfølge strafbare handlinger i de berørte medlemsstater om terrorrelateret indhold, der indebærer en overhængende livsfare, i overensstemmelse med TCO-forordningens artikel 14, stk. 5,
14) at udpege et kontaktpunkt og gøre oplysninger herom offentligt tilgængelige i overensstemmelse med TCO-forordningens artikel 15, stk. 1, eller
15) at udpege en fysisk eller juridisk person som sin retlige repræsentant, i det omfang hostingtjenesteyderen ikke har sit hovedsæde i Den Europæiske Union, i henhold til TCO-forordningens artikel 17.

Efter forordningens artikel 18, stk. 2, skal de kompetente myndigheder, når de træffer afgørelse om, hvorvidt der skal pålægges en sanktion, og når de fastlægger sanktionernes type og omfang, tage 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 TCO-forordningen.

Det følger af præambelbetragtning nr. 45, at der skal tages hensyn til, om hostingtjenesteyderen er en nyetableret virksomhed eller en mikrovirksomhed eller lille virksomhed som defineret i Kommissionens henstilling 2003/361/EF. Den kompetente myndighed skal også tage hensyn til andre omstændigheder, såsom hvorvidt hostingtjenesteyderens adfærd objektivt set var uforsigtig eller forkastelig, eller hvorvidt overtrædelsen blev begået uagtsomt eller forsætligt. Den kompetente myndighed skal i den forbindelse sikre, at sanktionerne for overtrædelse af forordningen ikke tilskynder til fjernelse af materiale, der ikke er terrorrelateret.

Sanktionerne kan have administrativ eller strafferetlig karakter. Det er et krav, at sanktionerne er effektive, står i rimeligt forhold til overtrædelsen og har en afskrækkende virkning, jf. forordningens artikel 18, stk. 1.

Ved manglende overholdelse af forordningens forpligtelser skal den kompetente myndighed udstede sanktioner med respekt for ne bis in idem-princippet og proportionalitetsprincippet, idet det dog skal sikres, at der tages højde for systematisk forsømmelse.

Det følger desuden af forordningens præambelbetragtning nr. 45, at sanktionerne kan tage forskellige former, herunder formelle advarsler i tilfælde af mindre overtrædelser eller økonomiske sanktioner i forbindelse med mere alvorlige eller systematiske tilfælde. Der skal 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 modtagelsen af et påbud om fjernelse af terrorrelateret indhold.

Endelig følger af det forordningens artikel 18, stk. 3, at systematisk eller vedvarende manglende overholdelse af forpligtelserne i medfør af artikel 3, stk. 3, skal medføre økonomiske sanktioner på op til 4 % af hostingtjenesteyderens globale omsætning for det forudgående regnskabsår.

2.4.3. Justitsministeriets overvejelser og den foreslåede ordning

2.4.3.1. Strafansvar

Det er Justitsministeriets vurdering, at det mest effektive sanktionsmiddel vil være udstedelse af bøder, når betingelserne herfor er opfyldt.

Det foreslås på denne baggrund, at der indføres en bestemmelse i loven om, at overtrædelse af TCO-forordningens artikel 3, stk. 3 eller 6, artikel 4, stk. 2 eller 7, artikel 5, stk. 1, 2, 3, 5 eller 6, artikel 6, 7, 10 eller 11, artikel 14, stk. 5, artikel 15, stk. 1, eller artikel 17, straffes med bøde.

Det foreslås, at der kan pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel. De subjektive krav for at straffe en overtrædelse af bestemmelserne er uagtsomhed, jf. straffelovens § 19, 2. pkt. Efter straffelovens § 19, 2. pkt., er de pågældende straffebud anvendelige på andre lovovertrædelser, også når lovovertrædelsen er begået af uagtsomhed, medmindre det modsatte har særlig hjemmel.

Et moderselskab kan som udgangspunkt ikke holdes ansvarlig for sine datterselskabers overtrædelser af lovgivningen, dvs. tiltale skal som udgangspunkt alene rejses mod det pågældende datterselskab. Moderselskabet kan dog blive ansvarligt efter straffelovens almindelige regel om ansvar for medvirken, jf. lovens § 23. Tiltale vil eksempelvis kunne rejses mod moderselskabet, såfremt moderselskabet har opfordret datterselskabet til den ulovlige handling.

For så vidt angår strafforfølgning af fysiske personer er udgangspunktet, at der rejses tiltale mod hostingtjenesteyderen (dvs. den juridiske person) for overtrædelsen, men at dette kan kombineres med tiltale mod en eller flere fysiske personer med tilknytning til den juridiske person, jf. Rigsadvokatmeddelelsens afsnit om strafansvar for juridiske personer. Strafudmåling for fysiske personer overtrædelser bør tage udgangspunkt i de almindelige regler i straffelovens 10. kapitel om staffens fastsættelse samt TCO-forordningens artikel 18, stk. 1 og 2, i det omfang, momenterne i stk. 2 er relevante.

Rigspolitiet kan som kompetent myndighed af egen drift eller ved klage blive bekendt med, at der er sket en eller flere overtrædelser af de bestemmelser, der foreslås omfattet af strafbestemmelsen i lovforslagets § 4, stk. 1. I det omfang Rigspolitiet som kompetent myndighed i Danmark får mistanke om en overtrædelse af de bestemmelser i forordningen, der er strafbelagt med dette lovforslag, skal Rigspolitiet indgive en anmeldelse til den stedlige politikreds, der herefter inden for strafferetsplejens

rammer kan efterforske sagen og tage stilling til, om der skal ske strafforfølgning. Det vil efter de almindelige regler om roller og ansvarsfordeling mellem politiet og anklagemyndigheden betyde, at sagerne vil skulle afgøres af den stedlige anklagemyndighed.

Der er ikke med lovforslaget tilsigtet ændringer af øvrige myndigheders kompetence til at sanktionere tjenesteudbydere af onlineplatforme og -tjenester for andre lovovertrædelser.

2.4.3.2. Straffastsættelse

Det er Justitsministeriets vurdering, at sanktionsniveauet for overtrædelse af de bestemmelser i TCO-forordningen, der foreslås strafbelagt, skal ligge på et sådant niveau, at bøderne kan have både en følelig og præventiv virkning. Det er ministeriets vurdering, at bødeudmålingen endvidere skal stå i rimeligt forhold til overtrædelsen, og at bøderne skal have en størrelse, så de afskrækker hostingtjenesteyderne fra at overtræde de bestemmelser, der nævnes i den foreslåede § 4, stk. 1.

Fastsættelse af straffen vil for begge nedenstående modeller fortsat bero på domstolenes konkrete vurdering i det enkelte tilfælde af samtlige omstændigheder i sagen, og det angivne strafniveau vil kunne fraviges i op- eller nedadgående retning, hvis der i den konkrete sag foreligger andre skærpende eller formildende omstændigheder, jf. herved de almindelige regler om straffens fastsættelse i straffelovens 10. kapitel samt artikel 18, stk. 2, i TCO-forordningen.

Hvis flere overtrædelser er til samtidig pådømmelse, eksempelvis hvis en virksomhed har overtrådt flere påbud meddelt efter artikel 3, stk. 3, skal der udmåles en fælles bøde for alle overtrædelserne, jf. straffelovens § 88, stk. 1.

Ved udmålingen af bøden vil det i almindelighed skulle indgå som skærpende omstændighed, at gerningsmanden tidligere er straffet af betydning for sagen, jf. straffelovens § 81, nr. 1. Eksempelvis hvis en virksomhed tidligere er idømt en bøde for overtrædelse af et påbud, jf. artikel 3, stk. 3, og samme virksomhed senere meddeles et nyt påbud, som virksomheden overtræder, jf. nærmere pkt. 2.4.3.2.1 nedenfor.

Endelig følger det af retsplejelovens § 832, at hvor den sigtede erklærer sig skyldig i overtrædelsen, kan anklagemyndigheden afslutte sagen med udenretlige bødeforelæg, såfremt den sigtede erklærer sig rede til inden en nærmere angiven frist at betale den i bødeforelægget angivne bøde. Modtageren af bødeforelægget vil kunne indbringe bødeforelægget for domstolene. Det forudsættes, at sager om overtrædelse af de bestemmelser i forordningen, der er strafbelagte, vil blive søgt afsluttet ved udstedelse af et bødeforelæg.

2.4.3.2.1. Straffastsættelse for overtrædelse af artikel 3, stk. 3

Det følger af forordningens artikel 18, stk. 3, at systematisk eller vedvarende manglende overholdelse af forpligtelserne i medfør af artikel 3, stk. 3, medfører sanktioner på op til 4 % af hostingtjenesteyderens årlige omsætning på verdensplan i det regnskabsår, som går forud for overtrædelsen.

Det forudsættes på den baggrund, at udgangspunktet for straffastsættelsen for overtrædelser af artikel 3, stk. 3, afhængig af momenterne i TCO-forordningens artikel 18, stk. 2, vil kunne fastsættes med afsæt i nedenstående model, hvor der tages udgangspunkt i hostingtjenesteyderens årlige omsætning på verdensplan i det regnskabsår, som går forud for overtrædelsen.

I tilfælde, hvor overtrædelsen er sket uagtsomt, og hvor graden af uagtsomhed anses som lav, kan der i 1. gangstilfælde undtagelsesvis meddeles en advarsel for overtrædelse af artikel 3, stk. 3.

Model for straffastsættelse for overtrædelse af artikel 3, stk. 3

1. gangstilfælde	2. gangstilfælde	3. gangstilfælde	4. gangstilfælde
0,5 %	0,75 %	1 %	1,25 %

Ved flere overtrædelser til samtidig pådømmelse enten i førstegangs- eller i gentagelsestilfælde vil der skulle udmåles en fælles bøde for alle overtrædelserne, der er til pådømmelse, jf. straffelovens § 88, stk. 1. Derudover forudsættes det, at der vil blive fastsat højere bøder, når der er tale om yderligere tilfælde end 4. gangstilfælde.

Bestemmelsen i artikel 3, stk. 3, udgør et centralt element i forordningen, hvor den kompetente myndighed selv nemt vil kunne konstatere overtrædelsen, og derfor forudsættes det i overensstemmelse forordningens artikel 18, stk. 3, at systematiske eller vedvarende manglende overholdelse af artikel 3, stk. 3, skal kunne medføre en bøde på op til 4 % af hostingtjenesteyderens årlige omsætning på verdensplan i det regnskabsår, som går forud for overtrædelsen.

2.4.3.2.2. Straffastsættelse for overtrædelse af artikel 3, stk. 6, artikel 4, stk. 2 eller 7, artikel 5, stk. 1, 2, 3, 5 eller 6, artikel 6, 7, 10 eller 11, artikel 14, stk. 5, artikel 15, stk. 1, eller artikel 17

Det er Justitsministeriets vurdering, at der for overtrædelse af de øvrige bestemmelser i TCO-forordningen skal fastsættes en lavere bødestraf, eftersom der bl.a. er tale om forpligtelser, der vedrører hostingtjenesteyderens løbende sagsbehandling, hvor en enkel overtrædelse ikke anses for

ligeså grov som manglende overholdelse af et påbud udstedt efter forordningens artikel 3. Det forudsættes på denne baggrund, at straffen for overtrædelser af artikel 3, stk. 6, artikel 4, stk. 2 eller 7, artikel 5, stk. 1, 2, 3, 5 eller 6, artikel 6, 7, 10 eller 11, artikel 14, stk. 5, artikel 15, stk. 1, eller artikel 17 afhængig af momenterne i TCO-forordningens artikel 18, stk. 2, vil kunne fastsættes med udgangspunkt i nedenstående model, hvor der tages afsæt i hostingtjenesteyderens årlige omsætning på verdensplan i det regnskabsår, som går forud for overtrædelsen.

I tilfælde, hvor overtrædelsen er sket uagtsomt, herunder navnlig hvor graden af uagtsomhed anses som lav, kan der i 1. gangstilfælde undtagelsesvis meddeles en advarsel for overtrædelse af ovennævnte bestemmelser i TCO-forordningen.

Model for straffastsættelse ved overtrædelse af artikel 3, stk. 6, artikel 4, stk. 2 eller 7, artikel 5, stk. 1, 2, 3, 5 eller 6, artikel 6, 7, 10 eller 11, artikel 14, stk. 5, artikel 15, stk. 1, eller artikel 17.

1. gangstilfælde	2. gangstilfælde	3. Gangstilfælde	4. Gangstilfælde
0,25 %	0,5 %	0,75 %	1 %

Ved flere overtrædelser til samtidig pådømmelse enten i førstegangs- eller i gentagelsestilfælde vil der skulle udmåles en fælles bøde for alle overtrædelserne, der er til pådømmelse, jf. straffelovens § 88, stk. 1. Derudover forudsættes det, at der vil blive fastsat højere bøder, når der er tale om yderligere tilfælde end 4. gangstilfælde.

3. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

[Det vurderes, at lovforslaget ikke i sig selv vil medføre økonomiske konsekvenser og implementeringskonsekvenser for det offentlige af betydning.

Lovforslaget medfører, at Rigspolitiet udpeges som national kompetent myndighed. Der henvises til de almindelige bemærkninger pkt. 2.2.3.]

4. Økonomiske og administrative konsekvenser for erhvervslivet mv.

Det vurderes, at lovforslaget ikke i sig selv vil medføre økonomiske eller administrative konsekvenser for erhvervslivet mv.

Det bemærkes, at TCO-forordningen generelt kan have økonomiske og administrative konsekvenser for erhvervslivet. Forordningen pålægger hostingtjenesteydere en række forpligtelser. Hostingtjenesteydere, der eksponeres for terrorrelateret indhold, skal, hvor det er relevant, i deres vilkår og betingelser inkludere og anvende bestemmelser om håndtering af misbrug af deres tjeneste til formidling til offentligheden af terrorrelateret indhold online.

Hvis en hostingtjenesteyder er at betragte som eksponeret for terrorrelateret indhold, skal hostingtjenesteyderen træffe specifikke foranstaltninger for at beskytte deres tjenester mod formidling til offentligheden af terrorrelateret indhold. Valget af de konkrete foranstaltninger ligger hos hostingtjenesteudbydere, men kan bl.a. omfatte passende tekniske og operationelle foranstaltninger eller kapaciteter såsom f.eks. passende bemanding eller tekniske midler til at identificere og hurtigt fjerne eller deaktivere adgang til terrorrelateret indhold eller let tilgængelige og brugervenlige mekanismer, så brugere kan rapportere muligt terrorrelateret indhold til hostingtjenesteyderen.

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

Hostingtjenesteudbydere skal straks undersøge enhver klage, som modtages, og genindsætte indholdet uden unødig forsinkelse, hvis det uberettiget er blevet fjernet eller deaktiveret, og underrette klageren om udfaldet af undersøgelsen inden for to uger efter modtagelsen af klagen med en begrundelse i de tilfælde, hvor hostingtjenesteyderen beslutter ikke at genetablere indholdet.

5. Administrative konsekvenser for borgerne

Lovforslaget vurderes ikke at have administrative konsekvenser for borgerne.

6. Klima- og miljømæssige konsekvenser

Lovforslaget har ikke klima- og miljømæssige konsekvenser.

7. Forholdet til EU-retten

Lovforslaget fastsætter supplerende bestemmelser til Europa-Parlamentets og Rådets forordning (EU) 2021/784 af 29. april 2021 om håndtering af udbredelsen af terrorrelateret indhold online, EU-Tidende 2021, nr. L 172, side 79, som gælder umiddelbart i Danmark fra den 7. juni 2022. Ved lovforslaget skabes grundlaget for at kunne udpege en national kompetent myndighed. Herudover skabes der grundlag for at kunne håndhæve og sanktionere for overtrædelse af forordningen.

8. Hørte myndigheder og organisationer mv.

Et udkast til lovforslag har i perioden fra den 25. februar 2022 til den 25. marts 2022 været sendt i høring hos følgende myndigheder og organisationer mv.:

Østre Landsret, Vestre Landsret, samtlige byretter, Domstolsstyrelsen, Rigsadvokaten, Rigspolitiet, Datatilsynet, Aarhus BSS, Aalborg Universitet, ADIPA – Association of Danish Intellectual Property Attorneys, Advokatrådet, Advokatsamfundet, AE - Arbejderbevægelsen Erhvervsråd, Amnesty, AU - Aarhus Universitet, BL - Danmarks almene boliger, Børns Vilkår, Børnerådet, Copenhagen Business School, Cevea, CEPOS, Den Danske Dommerforening, Danske Advokater, Dommerfuldmægtigforeningen, Danmarks Statistik, Danmarks Nationalbank, Dansk IT, Danske Universiteter, Dansk Standard, Dansk Industri, DAOM - Danske Annoncører og Markedsførere, Dansk Arbejdsgiverforening, Dansk Erhverv, Dansk Journalistforbund, Danske Medier, Danske Regioner, DI Byggeri, Dataetisk Råd, Digitalt Ansvar, Dignity, DKCERT - Danish Computer Security Incident Response Team, Det Kriminalpræventive Råd, Danmarks Tekniske Universitet, Fagbevægelsens Hovedorganisation, Fagligt Fælles Forbund, FDIH - Foreningen for Danske Internethandel, Finans Danmark, Finanstilsynet, Forbrugerombudsmanden, Forbrugerrådet Tænk, Foreningen af Offentlige Anklagere, Foreningen af Statsadvokater, Foreningen Danske Revisorer, Forsikring og Pension, Færøernes Landsstyre, Greenpeace, HK Danmark, Institut for Menneskerettigheder, IT-Branchen, IT-Universitet i København, IT-Politisk Forening, Justitia, KL, KOMBIT, Kreativitet og Kommunikation, Kriminalforsorgsforeningen, Københavns Universitet, Landbrug og Fødevarer, LGBT+ Danmark, Medierådet for Børn og Unge, MINO Danmark, Nets DanID A/S, Naalakkersuisut, Politiforbundet i Danmark, Prosa, Radio- og TV-Nævnet, Red Barnet, Retspolitisk forening, Rettighedsalliancen, Landsstyret via Rigsombudsmanden på Færøerne, Roskilde Universitet, Selvstyret via Rigsombudsmanden i Grønland, Rigsrevisionen, Rådet for digital sikkerhed, Syddansk Universitet, SMV Danmark, Teleindustrien, Telekommunikationsindustrien i Danmark, The Association of Tech start-ups in Denmark.

9. Sammenfattende skema

	Positive konsekvenser/mindre udgifter	Negative konsekvenser/merudgifter
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	[Lovforslaget forventes ikke at have økonomiske konsekvenser for det offentlige af betydning.]
Implementeringskonsekvenser for stat, kommuner og regioner	Ingen	Ingen

Økonomiske konsekvenser for erhvervslivet mv.	Ingen	Ingen
Administrative konsekvenser for erhvervslivet mv.	Ingen	Ingen
Administrative konsekvenser for borgerne	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget fastsætter supplerende bestemmelser til Europa-Parlamentet og Rådets forordning (EU) 2021/784 af 29. april 2021 om håndtering af udbredelsen af terrorrelateret indhold online, EU-Tidende 2021, nr. L 172, side 79. Forordningen gælder umiddelbart i Danmark fra den 7. juni 2022.	
Er lovforslaget i strid med de fem principper for implementering af erhvervsrettet EU-regulering? (sæt X)	JA	Nej
		X

Bemærkninger til lovforslagets enkelte bestemmelser

§ 1

Der findes ingen nationale regler om, at en national myndighed skal kunne udstede og kontrollere påbud om fjernelse af terrorrelateret indhold online eller føre tilsyn med, at hostingtjenesteydere, der er særlig eksponeret for terrorrelateret indhold, gennemfører specifikke foranstaltninger.

Det foreslås i *stk. 1*, at loven supplerer Europa-Parlamentet og Rådets forordning (EU) 2021/784 af 29. april 2021 om håndtering af terrorrelateret indhold online (TCO-forordningen), jf. bilag 1 til denne lov.

Med TCO-forordningen etableres en fælles europæisk ramme til at forebygge misbrug af hostingtjenester til udbredelse af terrorrelateret indhold online. Forordningen gælder umiddelbart i Danmark, men forordningen kræver visse gennemførelsesforanstaltninger. Med den foreslåede bestemmelse fastsættes det derfor, at loven supplerer forordningen, ligesom der henvises til bilag 1 til loven, hvor forordningen er gengivet.

Ved en hostingtjenesteyder forstås i henhold til forordningens artikel 2, stk. 1, en udbyder af tjenester som defineret i artikel 1, litra b, i Europa-Parlamentets og Rådets direktiv (EU) 2015/1535,[6] og hvor tjenesten består i lagring af oplysninger fra en indholdsleverandør på dennes anmodning.

Det foreslås i *stk. 2,* at loven ligesom TCO-forordningen finder anvendelse på hostingtjenesteydere, der udbyder tjenester i Den Europæiske Union, uanset hvor deres hovedsæde er beliggende, i det omfang de udbreder oplysninger til offentligheden.

Det følger af TCO-forordningens artikel 2, stk. 4, at der ved udbydelse af tjenester i Unionen forstås 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.

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

Med den foreslåede bestemmelse vil lovens anvendelsesområde følge anvendelsesområdet for TCO-forordningen, jf. forordningens artikel 1.

Der henvises til pkt. 2.1 i de almindelige bemærkninger.

§ 2

Efter artikel 12, stk. 1, i TCO-forordningen skal hver medlemsstat udpege en eller flere nationale myndigheder, der skal have kompetence til at udstede påbud om fjernelse af terrorrelateret indhold online i medfør af artikel 3, kompetence til at kontrollere påbud om fjernelse i medfør af artikel 4, kompetence til at føre tilsyn med gennemførelsen af specifikke foranstaltninger i medfør af artikel 5, og kompetence til at pålægge sanktioner i medfør af artikel 18.

Da TCO-forordningen endnu ikke finder anvendelse, er der på nuværende tidspunkt ikke udpeget nogen national kompetent myndighed i henhold til forordningens artikel 12, stk. 1.

Efter gældende ret er det anklagemyndigheden, der under visse betingelser kan udstede bødeforelæg efter retsplejelovens § 832, og det er domstolene, der pålægger sanktioner ved afsigelsen af straffedomme. Anklagemyndigheden og domstolene er således efter gældende ret kompetente til at pålægge sanktioner i medfør af artikel 18 i TCO-forordningen, jf. artikel 12, stk. 1, litra d.

[6] Gennemført i dansk ret ved bekendtgørelse nr. 1087 af 8. juli 2016 om EU's informationsprocedure for tekniske forskrifter og forskrifter for informationssamfundets tjenester

Det foreslås i *stk. 1,* at Rigspolitiet udpeges som den kompetente nationale myndighed. Den foreslåede bestemmelse fastsætter dermed, hvilken myndighed der vil skulle varetage rollen som national kompetent myndighed i Danmark i henhold til TCO-forordningens artikel 12, stk. 1, litra a-c.

Dette indebærer, at Rigspolitiet i overensstemmelse med TCO-forordningens artikel 12, stk. 1, litra a-c, vil få kompetence til at udstede påbud om fjernelse i medfør af artikel 3, kompetence til at kontrollere påbud om fjernelse i medfør af artikel 4 samt kompetence til at føre tilsyn med gennemførelsen af specifikke foranstaltninger i medfør af artikel 5.

Det foreslås i *stk. 2*, at Rigspolitiet ikke må søge eller modtage instrukser fra andre organer i forbindelse med udførslen af deres opgaver i henhold til forordningens artikel 12, stk. 1, litra a-c.

Det betyder, at Rigspolitiet, når Rigspolitiet udøver sine opgaver i henhold til TCO-forordningen, ikke er underlagt andre administrative myndigheder, herunder Justitsministeriet, og udøver sine funktioner i fuld uafhængighed. Det bemærkes, at Rigspolitiet ved udøvelse af opgaverne i henhold til forordningen kan inddrage relevante myndigheder efter behov.

Endelig bemærkes det, at anklagemyndigheden forudsættes ved behandlingen af sager i henhold til TCO-forordningen at være uafhængige i overensstemmelse med forordningens krav herom.

Der henvises til pkt. 2.2.3.1 i lovforslagets almindelige bemærkninger.

Bestemmelsen er en udmøntning af TCO-forordningens artikel 13, stk. 2, 2. pkt.

Det foreslås i *stk.* 3, at forvaltningslovens kapitel 5 om partshøring ikke finder anvendelse for Rigspolitiets afgørelser i henhold til TCO-forordningens artikel 3 og 4 eller underretninger efter den foreslåede bestemmelse i § 3, stk. 1. Det foreslås endvidere, at forvaltningslovens kapitel 6 om begrundelse mv. ikke finder anvendelse ved Rigspolitiets underretninger efter den foreslåede bestemmelse i § 3, stk. 1.

Bestemmelsen har til formål at sikre, at Rigspolitiet har mulighed for at behandle de nævnte sagstyper i overensstemmelse med forordningen, herunder navnlig kravet om en hurtig sagsbehandling med henblik på at sikre hurtig og effektiv fjernelse eller deaktivering af adgangen til terrorrelateret indhold.

Den foreslåede bestemmelse vil indebære, at Rigspolitiet ikke vil skulle foretage partshøring af hostingtjenesteydere mv., inden der træffes afgørelse om udstedelse af et påbud i medfør af forordningens artikel 3 og artikel 4, stk. 3 og 4, eller sker underretning i medfør af den foreslåede bestemmelse i § 3, stk. 1.

Den foreslåede bestemmelse vil indebære, at Rigspolitiet ikke vil være forpligtet til at iagttage forvaltningslovens regler om begrundelse mv. i forbindelse med underretninger i medfør af den foreslåede bestemmelse i § 3, stk. 1. Det forudsættes i den forbindelse, at Rigspolitiet i praksis alene vil henvise til begrundelsen i det underliggende påbud.

For nærmere om Justitsministeriets overvejelser om forholdet til forvaltningsloven henvises til pkt. 2.2.3.2 i lovforslagets almindelige bemærkninger.

Det foreslås i *stk. 4*, at Rigspolitiets afgørelser i henhold til TCO-forordningen eller underretninger efter lovforslagets § 3, stk. 1, ikke kan påklages til anden administrativ myndighed. Det betyder bl.a., at klager over sådanne afgørelser ikke vil kunne indbringes for Justitsministeriet.

Der henvises til pkt. 2.2 i de almindelige bemærkninger.

§ 3

Da TCO-forordningen endnu ikke finder anvendelse, er der på nuværende tidspunkt ikke udpeget en national kompetent myndighed i henhold til forordningen, og der er derfor heller ikke fastsat regler om underretning i henhold til artikel 4, stk. 1, i forordningen.

Det foreslås i *stk. 1,* at når Rigspolitiet i henhold til TCO-forordningens artikel 4, stk. 1, modtager en underretning om et påbud om fjernelse af terrorrelateret indhold, der er udstedt af den kompetente myndighed i en anden medlemsstat til en dansk hostingtjenesteyder, vil Rigspolitiet skulle underrette hostingtjenesteyderen om påbuddets retlige virkning for så vidt angår Danmark.

Den foreslåede bestemmelse udmønter den ensidige danske erklæring, der blev afgivet i forbindelse med Rådets vedtagelse af førstebehandlingsholdning til Kommissionens forslag til TCO-forordningen den 16. marts 2021.

Den foreslåede bestemmelse har den virkning, at et påbud fra en anden medlemsstats kompetente myndighed til en dansk hostingtjenesteyder får retsvirkning for så vidt angår Danmark, når den danske hostingtjenesteyder er underrettet af Rigspolitiet. Det er dermed en forudsætning for, at en dansk hostingtjenesteyder kan ifalde ansvar for ikke at efterkomme et påbud efter TCO-forordningens artikel 3, stk. 1, om fjernelse eller deaktivering efter artikel 3, stk. 3, som er udstedt af en kompetent myndighed i en anden medlemsstat, inden for én time, at Rigspolitiet har underrettet den danske hostingtjenesteyder om påbuddets retlige virkning for så vidt angår Danmark.

Det bemærkes, at det følger af det foreslåede § 2, stk. 4, at Rigspolitiets underretninger efter den foreslåede bestemmelse ikke kan påklages til anden administrativ myndighed, ligesom det følger af

det foreslåede § 2, stk. 3, at forvaltningslovens regler om partshøring og begrundelse ikke finder anvendelse for Rigspolitiets underretninger efter den foreslåede bestemmelse.

Det foreslås i *stk. 2,* at underretningen af den danske hostingtjenesteyder om påbuddets retlige virkning for så vidt angår Danmark skal ske umiddelbart efter, at Rigspolitiet i Danmark er blevet underrettet om påbuddet fra den kompetente myndighed i en anden medlemsstat.

Formålet med bestemmelsen i stk. 2 er at udmønte den ordning, som er beskrevet i den erklæring, som blev afgivet af Danmark i forbindelse med Rådets vedtagelse af førstebehandlingsholdning til Kommissionens forslag til TCO-forordningen den 16. marts 2021, hvormed det i praksis kan sikres, at kravet om, at 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, jf. forordningens artikel 3, stk. 3, opfyldes.

Formålet med bestemmelsen er alene at give påbud udstedt af en kompetent myndighed i en anden medlemsstat efter forordningens artikel 3, stk. 3, retlig virkning for så vidt angår Danmark. Bestemmelsen berører ikke den i forordningen fastsatte tidsfrist på én time, der løber fra det tidspunkt, hvor hostingtjenesteyderen modtager påbuddet om fjernelse fra en kompetent myndighed i en anden medlemsstat, jf. herom pkt. 2.2.3.2 i de almindelige bemærkninger.

Der kan i øvrigt henvises til pkt. 2.2 i de almindelige bemærkninger.

§ 4

Det foreslås i *stk. 1,* at den, der overtræder TCO-forordningens artikel 3, stk. 3 eller 6, artikel 4, stk. 2 eller 7, artikel 5, stk. 1, 2, 3, 5 eller 6, artikel 6, 7, 10 eller 11, artikel 14, stk. 5, artikel 15, stk. 1, eller artikel 17 skal kunne straffes med bøde. De anførte bestemmelser i forordningen angår alle hostingtjenesteydere, som er defineret nærmere i forordningens artikel 2, nr. 2. I det omfang f.eks. et moderselskab er medvirkende til overtrædelsen, vil dette også kunne straffes, jf. nærmere herom bemærkningerne til det foreslåede stk. 3 nedenfor.

De bestemmelser i TCO-forordningen som i overensstemmelse med artikel 18, stk. 1, i forordningen foreslås strafbelagt, vil navnlig være tilfælde, hvor en hostingtjenesteyder overtræder en eller flere af følgende bestemmelser ved ikke:

1) at efterkomme et påbud efter TCO-forordningens artikel 3, stk. 1, om fjernelse eller deaktivering efter artikel 3, stk. 3,
2) uden unødigt ophold at underrette den kompetente myndighed efter TCO-forordningens artikel 3, stk. 6,

3) at træffe de nødvendige foranstaltninger for at kunne genindsætte indholdet eller fjerne adgangen dertil i overensstemmelse med TCO-forordningens artikel 4, stk. 7 efter TCO-forordningen artikel 4, stk. 2,
4) at genindsætte indhold eller genaktivere adgangen dertil efter TCO-forordningens artikel 4, stk. 7,
5) at medtage og anvende bestemmelser om håndtering af misbrug af dets tjenester til udbredelse af terrorrelateret indhold i henhold til TCO-forordningens artikel 5, stk. 1,
6) at træffe specifikke foranstaltninger i henhold til TCO-forordningens artikel 5, stk. 2 og 3,
7) at aflægge rapport til den kompetente myndighed om de trufne specifikke foranstaltninger, jf. TCO-forordningens artikel 5, stk. 5,
8) at efterkomme en afgørelse truffet i henhold til TCO-forordningens artikel 5, stk. 6,
9) at opbevare terrorrelateret indhold, som er blevet fjernet, eller hvortil adgangen er blevet deaktiveret som følge af et påbud eller af specifikke foranstaltninger, samt eventuelt dertil knyttet data i overensstemmelse ned TCO-forordningens artikel 6,
10) at fastsætte tydelige vilkår og betingelser for håndteringen af terrorrelateret indhold i overensstemmelse med TCO-forordningens artikel 7,
11) at indføre og opretholde en effektiv og tilgængelig klagemekanisme i overensstemmelse med TCO-forordningens artikel 10,
12) at holde indholdsleverandøren underrettet om fjernelse eller deaktivering af terrorrelateret indhold i overensstemmelse med TCO-forordningens artikel 11,
13) omgående at underrette den myndighed, der er kompetent til at efterforske og retsforfølge strafbare handlinger i de berørte medlemsstater om terrorrelateret indhold, der indebærer en overhængende livsfare, i overensstemmelse med TCO-forordningens artikel 14, stk. 5,
14) at udpege et kontaktpunkt og gøre oplysninger herom offentligt tilgængelige i overensstemmelse med TCO-forordningens artikel 15, stk. 1, eller
15) at udpege en fysisk eller juridisk person som sin retlige repræsentant, i det omfang hostingtjenesteyderen ikke har sit hovedsæde i Den Europæiske Union, i henhold til TCO-forordningens artikel 17.

Det bemærkes særligt, at der – i de sager hvor Rigspolitiet i medfør af lovforslagets § 3, stk. 1, skal underrette en dansk hostingtjenesteyder eller dennes retlige repræsentant – alene vil kunne blive tale om strafansvar for overtrædelse af artikel 3 i forordningen for så vidt angår Danmark, i det omfang Rigspolitiet har underrettet hostingtjenesteyderen om påbuddets retlige virkning. Det anførte ændrer ikke ved hostingtjenesteyderens pligt til i henhold til forordningens artikel 3, stk. 3, uanset underretning i medfør af lovforslagets § 3, stk. 1, at fjerne terrorrelateret indhold eller deaktivere adgangen til terrorrelateret indhold hurtigst muligt og under alle omstændigheder inden for en time efter at have modtaget påbuddet om fjernelse for så vidt angår øvrige medlemsstater.

De subjektive krav for at straffe en overtrædelse af bestemmelserne er uagtsomhed, jf. straffelovens § 19, 2. pkt. Efter straffelovens § 19, 2. pkt., er de pågældende straffebud anvendelige på andre lovovertrædelser, også når lovovertrædelsen er begået af uagtsomhed, medmindre det modsatte har særlig hjemmel.

Det foreslås i *stk. 2,* at der ved udmålingen af bøder for overtrædelse af de bestemmelser, der er nævnt i stk. 1, skal lægges vægt på den årlige omsætning på verdensplan i det regnskabsår, som går forud for tidspunktet for overtrædelsen samt de øvrige momenter, der følger af TCO-forordningens artikel 18, stk. 2.

Det betyder, at der udover den årlige omsætning på verdensplan, jf. nedenfor, skal lægges vægt på overtrædelsens art, grovhed og varighed, hvorvidt overtrædelsen er begået forsætligt eller uagtsomt, hostingtjenesteyderens tidligere overtrædelser, hostingtjenesteyderens finansielle styrke, grad af samarbejde med de kompetente myndigheder, hostingtjenesteyderens art og størrelse, herunder navnlig hvorvidt den er en mikrovirksomhed eller en mellemstor virksomhed, samt omfanget af hostingtjenesteyderens skyld, idet der skal tages hensyn til de tekniske og organisatoriske foranstaltninger, som hostingtjenesteyderen har truffet for at overholde TCO-forordningen.

Fastsættelse af straffen vil for begge modeller nedenfor fortsat bero på domstolenes konkrete vurdering i det enkelte tilfælde af samtlige omstændigheder i sagen, og det angivne strafniveau vil kunne fraviges i op- eller nedadgående retning, hvis der i den konkrete sag foreligger andre skærpende eller formildende omstændigheder, jf. herved de almindelige regler om straffens fastsættelse i straffelovens 10. kapitel.

Hvis flere overtrædelser er til samtidig pådømmelse, eksempelvis hvis en virksomhed har overtrådt flere påbud meddelt efter artikel 3, stk. 3, skal der udmåles en fælles bøde for alle overtrædelserne, jf. straffelovens § 88, stk. 1.

Ved udmålingen af bøden vil det i almindelighed skulle indgå som skærpende omstændighed, at gerningsmanden tidligere er straffet af betydning for sagen, jf. straffelovens § 81, nr. 1. Eksempelvis hvis en virksomhed tidligere er idømt en bøde for overtrædelse af et påbud, jf. artikel 3, stk. 3, og samme virksomhed senere meddeles et nyt påbud, som virksomheden overtræder, jf. nedenfor.

Det følger af forordningens artikel 18, stk. 3, at systematisk eller vedvarende manglende overholdelse af forpligtelserne i medfør af artikel 3, stk. 3, medfører sanktioner på op til 4 % af hostingtjenesteyderens årlige omsætning på verdensplan i det regnskabsår, som går forud for overtrædelsen.

Det forudsættes på den baggrund, at udgangspunktet for straffastsættelsen for overtrædelser af artikel 3, stk. 3, afhængig af momenterne i TCO-forordningens artikel 18, stk. 2, vil kunne fastsættes med

udgangspunkt i nedenstående model, som tager afsæt i hostingtjenesteyderens årlige omsætning på verdensplan i det regnskabsår, som går forud for overtrædelsen.

I tilfælde, hvor overtrædelsen er sket uagtsomt, og hvor graden er uagtsomhed anses som værende lav, kan der i 1. gangstilfælde undtagelsesvist meddeles en advarsel for overtrædelse af artikel 3, stk. 3.

Model for straffastsættelse for overtrædelse af artikel 3, stk. 3

1. gangstilfælde	2. gangstilfælde	3. gangstilfælde	4. Gangstilfælde
0,5 %	0,75 %	1 %	1,25 %

Ved flere overtrædelser til samtidig pådømmelse enten i førstegangs- eller i gentagelsestilfælde vil der skulle udmåles en fælles bøde for alle overtrædelserne, der er til pådømmelse, jf. straffelovens § 88, stk. 1. Derudover forudsættes det, at der vil blive fastsat højere bøder, når der er tale om yderligere tilfælde end 4. gangstilfælde.

Bestemmelsen i artikel 3, stk. 3, udgør et centralt element i forordningen, hvor den kompetente myndighed selv nemt vil kunne konstatere overtrædelsen, og derfor forudsættes det, at systematiske eller vedvarende manglende overholdelse af artikel 3, stk. 3, skal kunne medføre en bøde på 4 % af hostingtjenesteyderens årlige omsætning på verdensplan i det regnskabsår, som går forud for overtrædelsen.

Det er Justitsministeriets vurdering, at der for de øvrige bestemmelser i TCO-forordningen skal fastsættes en lavere bødestraf, eftersom der bl.a. er tale om forpligtelser, der vedrører hostingtjenesteyderens løbende sagsbehandling, hvor en enkelt overtrædelse ikke anses for ligeså grov som manglende overholdelse af et påbud udstedt efter forordningens artikel 3. Det forudsættes på denne baggrund, at der ved fastsættelsen af straffen for overtrædelser af artikel 3, stk. 6, artikel 4, stk. 2 eller 7, artikel 5, stk. 1, 2, 3, 5 eller 6, artikel 6, 7, 10 eller 11, artikel 14, stk. 5, artikel 15, stk. 1, eller artikel 17 afhængig af momenterne i TCO-forordningens artikel 18, stk. 2, vil kunne fastsættes med udgangspunkt i nedenstående model, som tager afsæt i hostingtjenesteyderens årlige omsætning på verdensplan i det regnskabsår, som går forud for overtrædelsen.

I tilfælde, hvor overtrædelsen er sket uagtsomt, og hvor graden af uagtsomhed anses som lav, kan der i 1. gangstilfælde undtagelsesvis meddeles en advarsel for overtrædelse af artikel 3, stk. 3

Model for straffastsættelse ved overtrædelse af artikel 3, stk. 6, artikel 4, stk. 2 eller 7, artikel 5, stk. 1, 2, 3, 5 eller 6, artikel 6, 7, 10 eller 11, artikel 14, stk. 5, artikel 15, stk. 1, eller artikel 17

1. gangstilfælde	2. gangstilfælde	3. gangstilfælde	4. gangstilfælde
0,25 %	0,5 %	0,75 %	1 %

Ved flere overtrædelser til samtidig pådømmelse enten i førstegangs- eller i gentagelsestilfælde vil der skulle udmåles en fælles bøde for alle overtrædelserne, der er til pådømmelse, jf. straffelovens § 88, stk. 1. Derudover forudsættes det, at der vil blive fastsat højere bøder, når der er tale om yderligere tilfælde end 4. gangstilfælde.

I tilfælde, hvor overtrædelsen er sket uagtsomt, herunder navnlig hvor graden af uagtsomhed anses som lav, kan der i 1. gangstilfælde undtagelsesvis meddeles en advarsel for overtrædelse af ovennævnte bestemmelser i TCO-forordningen.

Det foreslås i *stk. 3,* at der kan pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel. Bestemmelsen medfører, at hostingtjenesteyder som juridiske personer kan ifalde strafansvar efter bestemmelserne i TCO-forordningen, jf. lovforslagets § 4, stk. 1.

Det følger af reglerne i straffelovens 5. kapitel, at bestemmelser om strafansvar for selskaber mv. omfatter, medmindre andet er bestemt, enhver juridisk person, herunder aktie-, anparts- og andelsselskaber, interessentskaber, foreninger, fonde, boer, kommuner og statslige myndigheder, jf. straffelovens § 26, stk. 1. Endvidere omfatter sådanne bestemmelser enkeltmandsvirksomheder, for så vidt disse navnlig under hensyn til deres størrelse og organisation kan sidestilles med de ovenfor nævnte selskaber, jf. straffelovens § 26, stk. 2. Det følger videre, at strafansvar for en juridisk person forudsætter, at der inden for dens virksomhed er begået en overtrædelse, der kan tilregnes en eller flere til den juridiske person knyttede personer eller den juridiske person som sådan, jf. straffelovens § 27.

Et moderselskab kan som udgangspunkt ikke holdes ansvarlig for sine datterselskabers overtrædelser af lovgivningen, dvs. tiltale skal som udgangspunkt alene rejses mod det pågældende datterselskab. Moderselskabet kan dog blive ansvarligt efter straffelovens almindelige regel om ansvar for medvirken, jf. lovens § 23. Tiltale vil eksempelvis kunne rejses mod moderselskabet, såfremt moderselskabet har opfordret datterselskabet til den ulovlige handling.

For så vidt angår strafforfølgning af fysiske personer er udgangspunktet, at der rejses tiltale mod hostingtjenesteyderen (dvs. den juridiske person) for overtrædelsen, men at dette kan kombineres med tiltale mod en eller flere fysiske personer med tilknytning til den juridiske person, jf. Rigsadvokatmeddelelsens afsnit om strafansvar for juridiske personer. Strafudmåling for fysiske personer overtrædelser bør tage udgangspunkt i de almindelige regler i straffelovens 10. kapitel om staffens fastsættelse samt TCO-forordningens artikel 18, stk. 1 og 2, i det omfang, at momenterne i stk. 2 er relevante.

Der henvises i øvrigt til de almindelige bemærkninger pkt. 2.4.

§ 5

Der gælder ingen regler om, at justitsministeren kan fastsætte regler med henblik på gennemførelse af TCO-forordningen.

Det foreslås i *§ 5*, at justitsministeren kan fastsætte regler, som er nødvendige for at gennemføre de retsakter, der er udstedt af Den Europæiske Union med henblik på at gennemføre TCO-forordningen, eller regler, som er nødvendige for at anvende de retsakter på forordningens område, der er udstedt af Den Europæiske Union. Det foreslås endvidere, at justitsministeren kan fastsætte nærmere regler om procedurerne for det administrative samarbejde med kompetente myndigheder i andre EU/EØS-lande, herunder om elektronisk udveksling af oplysninger mellem disse myndigheder.

Den foreslåede bestemmelse har den virkning, at justitsministeren bemyndiges til at fastsætte de nødvendige administrative bestemmelser til opfyldelse af de gennemførelsesforanstaltninger, som Kommissionen måtte vedtage efter proceduren i henhold til TCO-forordningens artikel 20, jf. artikel 19. Dette vil kunne være regler om tekniske krav til de elektroniske midler, som de kompetente myndigheder skal anvende til at fremsende påbud om fjernelse eller ændringer af bilagene til TCO-forordningen og procedurerne for det administrative samarbejde med kompetente myndigheder i andre EU/EØS-lande, jf. TCO-forordningens artikel 14.

Endelig har den foreslåede bestemmelse den virkning, at justitsministeren kan fastsætte regler, som er nødvendige for at anvende de retsakter på området for TCO-forordningen, som Unionen har udstedt.

§ 6

Det fremgår af artikel 24 i TCO-forordningen, at forordningen finder anvendelse fra den 7. juni 2022.

Det foreslås i *§ 6,* at loven træder i kraft den 7. juni 2022.

Den foreslåede bestemmelse skal ses i lyset af, at forordningen finder anvendelse – og at dansk lovgivning dermed skal være i overensstemmelse hermed – fra denne dato, og bestemmelsen medfører således, de lovbestemmelser, der skal fastsætte de nødvendige gennemførelsesforanstaltninger, sanktionsbestemmelser m.v. med henblik på at supplere at TCO-forordningen, kan finde anvendelse i Danmark på det tidspunkt, der er angivet i forordningen.

§ 7

Bestemmelsen vedrører lovens territoriale gyldighed.

Det foreslås i *§ 7*, at loven ikke skal gælde for Færøerne og Grønland.

TCO-forordningen finder ikke anvendelse for Færøerne og Grønland, der ikke er medlem af EU. Hvis bestemmelser svarende til TCO-forordningen skal gennemføres for Færøerne og Grønland, vil det skulle ske ved lov.