FORSVARSMINISTERIET

December 2020

U d k a s t

Forslag
til
Lov om leverandørsikkerhed i den kritiske teleinfrastruktur

Kapitel 1
Definitioner

§ 1. I denne lov forstås ved:

1) Kritiske netkomponenter, systemer og værktøjer: Operations support systemer, network management systemer og business support systemer, der kan benyttes til at aflæse, ændre indhold af eller dirigere data, som relaterer sig til slutbrugere, samt hardware, firmware og software, der anvendes i eller i forbindelse med core-net i mobilnet, fastnet og internet, eller i centrale routere og servere i backbonenettene eller i kontrolenheder, som anvendes til styring i mobilnettenes radionet.
2) Slutbruger: En bruger af net og tjenester, som ikke på kommercielt grundlag stiller de pågældende net og tjenester til rådighed for andre.
3) Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester:
   a) Udbydere af net, hvor disse net anvendes af mere end 50.000 slutbrugere. Ved opgørelsen medregnes de slutbrugere, der har aftaleforhold med udbyderens kunder. Radio- og tv-stationer, der er udbydere af net, er kun omfattet, såfremt de har landsdækkende public service-forpligtelser.
   b) Udbydere, der gennem aftaler med statslige myndigheder og institutioner betjener mere end 500 slutbrugere. Ved opgørelsen medregnes de statslige myndigheder og institutioners egne slutbrugere.

Kapitel 2
Nedlæggelse af forbud vedrørende visse leverancer til den kritiske teleinfrastruktur

§ 2. Center for Cybersikkerhed kan i særlige tilfælde forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at indgå en aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf, såfremt aftalen vurderes at udgøre en trussel mod statens sikkerhed. Ved vurderingen heraf kan Center for Cybersikkerhed særligt lægge vægt på forhold vedrørende den leverandør, som udbyderen ønsker at anvende. I vurderingen vil blandt andet

kunne indgå, om leverandøren, leverandørens væsentligste underleverandører samt aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren:

1) Er hjemmehørende i eller varetager produktionen eller driften fra et land, som Danmark ikke har indgået en sikkerhedsaftale med, eller som Danmark ikke har et tilsvarende sikkerhedsmæssigt samarbejde med.
2) Er hjemmehørende i eller varetager produktionen eller driften fra et land, hvor det efter lovgivningen er muligt at pålægge leverandører eller deres underleverandører at udføre eller deltage i forhold, som vil udgøre spionage eller sabotage.
3) Direkte eller indirekte kontrolleres af et andet lands statslige organer, herunder militære myndigheder.
4) Er eller tidligere har været involveret i aktiviteter i Danmark eller andre lande, som har medført en negativ påvirkning af statens sikkerhed, informationssikkerheden eller den offentlige orden.

Stk. 2. Center for Cybersikkerhed kan kun nedlægge forbud efter stk. 1, hvis hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger.

§ 3. Center for Cybersikkerhed kan i særlige tilfælde forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at opretholde en indgået aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelsen af driften heraf, såfremt opretholdelse af aftalen vurderes at udgøre en væsentlig trussel mod statens sikkerhed. Ved vurderingen heraf kan Center for Cybersikkerhed særligt lægge vægt på forhold vedrørende leverandøren, leverandørens væsentligste underleverandører samt aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren.

Stk. 2. Center for Cybersikkerhed kan endvidere i særlige tilfælde forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester fortsat at anvende kritiske netkomponenter, systemer og værktøjer, der tidligere er leveret, såfremt fortsat anvendelse vurderes at udgøre en væsentlig trussel mod statens sikkerhed. Ved vurderingen heraf kan Center for Cybersikkerhed særligt lægge vægt på forhold vedrørende leverandøren, leverandørens væsentligste underleverandører samt aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren.

Stk. 3. Center for Cybersikkerhed kan fastsætte en frist for, hvornår en aftale skal være afviklet efter stk. 1, og hvornår anvendelse af kritiske netkomponenter, systemer og værktøjer skal være ophørt efter stk. 2.

Stk. 4. Center for Cybersikkerhed kan kun nedlægge forbud efter stk. 1 og 2, hvis hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger.

Kapitel 3
Ekspropriation

§ 4. Center for Cybersikkerhed kan i det omfang, det er nødvendigt for gennemførelse af forbud efter kapitel 2, iværksætte ekspropriation af privat ejendom.

Stk. 2. Udgør gennemførelse af forbud efter kapitel 2 et ekspropriativt indgreb, ydes der fuldstændig erstatning til den eller de berørte parter.

Kapitel 4
Forholdet til anden lovgivning

§ 5. Lov om offentlighed i forvaltningen, bortset fra lovens § 13, og forvaltningslovens kapitel 4-6 finder ikke anvendelse på sager, der er omfattet af denne lov.

Kapitel 5
Fravigelse af klageadgang

§ 6. Center for Cybersikkerheds afgørelser efter kapitel 2 og 3 kan ikke påklages til anden administrativ myndighed.

Kapitel 6
Domstolsbehandling

§ 7. Afgørelser efter kapitel 2 og 3 kan alene indbringes for Københavns Byret inden seks måneder efter afgørelsens meddelelse. Københavns Byret kan dog undtagelsesvis tillade en indbringelse efter seks måneder. I afgørelsen af sagen ved byretten deltager tre dommere. Forsvarsministeren eller den, ministeren bemyndiger hertil, kan lade personer, der er ansat i Forsvarsministeriet eller myndigheder under Forsvarsministeriet, møde for sig i retten som rettergangsfuldmægtige.

§ 8. Som parter i sagen anses dem, der har en retlig interesse i en afgørelse omfattet af kapitel 2 og 3. Som part i sagen for det offentlige anses forsvarsministeren eller den, ministeren bemyndiger hertil.

Stk. 2. Retten beskikker en særlig advokat til at varetage interesser for parten efter stk. 1, 1. pkt., og på vegne af denne udøve partsbeføjelser med hensyn til oplysninger af betydning for statens sikkerhed. Om salær og godtgørelse for udlæg til den særlige advokat gælder samme regler som i tilfælde, hvor der er meddelt fri proces, jf. retsplejelovens kapitel 31.

Stk. 3. Den særlige advokat efter stk. 2 skal underrettes om alle retsmøder i sagen og er berettiget til at deltage i disse. Den særlige advokat skal gøres bekendt med og have udleveret kopi af det materiale, som indgår i sagen for retten. Forsvarsministeren eller den, ministeren bemyndiger hertil, kan dog bestemme, at der af sikkerhedsmæssige grunde ikke udleveres kopi til den særlige advokat. Spørgsmålet kan af den særlige advokat indbringes for retten.

§ 9. Oplysninger vedrørende statens sikkerhed videregives til den særlige advokat efter § 8, stk. 2. Når sådanne oplysninger er videregivet til den særlige advokat, må vedkommende ikke drøfte sagen med parten eller dennes advokat og må ikke udtale sig i retsmøder, hvor parten eller dennes advokat er til stede. Parten og dennes advokat kan til enhver tid give skriftlige meddelelser til den særlige advokat om sagen.

Stk. 2. Retten kan af egen drift eller efter begæring fra den særlige advokat efter § 8, stk. 2, beslutte, at oplysninger, der er indgået i vurderingen i afgørelser omfattet af kapitel 2 og 3, videregives til parten og dennes advokat, hvis sikkerhedsmæssige forhold ikke kan begrunde, at oplysningerne ikke videregives. Afgørelsen træffes ved kendelse, og efter at den særlige advokat og forsvarsministeren eller den, ministeren bemyndiger hertil, har haft lejlighed til at udtale sig. Kendelsen kan kæres af de personer, der er nævnt i 2. pkt. Kære af en afgørelse om, at oplysninger videregives, har opsættende virkning.

Stk. 3. Har retten truffet afgørelse efter stk. 2, 1. pkt., kan forsvarsministeren eller den, ministeren bemyndiger hertil, bestemme, at de pågældende oplysninger ikke indgår i sagen for retten.

Stk. 4. Ingen må deltage som dommer i sagen, hvis den pågældende har truffet afgørelse efter stk. 2, 1. pkt., eller i øvrigt har haft adgang til oplysninger omfattet af en sådan afgørelse, og forsvarsministeren eller den, ministeren bemyndiger hertil, har truffet beslutning efter stk. 3 om, at de pågældende oplysninger ikke indgår i sagen for retten.

§ 10. Den del af et retsmøde, der angår, eller hvor der fremlægges eller behandles oplysninger af betydning for, statens sikkerhed, som ikke er omfattet af § 9, stk. 2, holdes for lukkede døre. I denne del af et retsmøde deltager den særlige advokat efter § 8, stk. 2, men ikke parten og dennes advokat.

Stk. 2. Retten bestemmer, hvordan retsmøder, der efter stk. 1 helt eller delvis holdes for lukkede døre, gennemføres.

§ 11. Retten træffer afgørelse, efter at parterne og den særlige advokat har haft lejlighed til at udtale sig.

§ 12. Justitsministeren antager et antal advokater, der kan beskikkes efter § 8, stk. 2, 1. pkt. Justitsministeren kan fastsætte nærmere regler om de pågældende advokater, herunder om vagtordninger, om vederlag for at stå til rådighed og om sikkerhedsmæssige spørgsmål.

§ 13. Reglerne i §§ 7-12 om sagens behandling i byretten gælder tilsvarende for sagens behandling i landsretten og Højesteret.

Kapitel 7
Offentliggørelse af afgørelser m.v.

§ 14. Center for Cybersikkerhed kan i ikke-anonymiseret form offentliggøre:

1) Afgørelser truffet i medfør af kapitel 2 og 3.
2) Resuméer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde for overtrædelse af reglerne i kapitel 2.
3) Resuméer af domme i retssager, der vedrører prøvelse af afgørelser efter kapitel 2 og 3.

Stk. 2. Forsvarsministeren kan fastsætte nærmere regler om sagsbehandlingen i forbindelse med offentliggørelse efter stk. 1.

Kapitel 8
Straffebestemmelser

§ 15. Med bøde straffes, medmindre strengere straf er forskyldt efter den øvrige lovgivning, den, der overtræder et forbud efter § 2, stk. 1, og § 3, stk. 1 og 2.

Stk. 2. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Kapitel 9
Ugyldighed

§ 16. Aftaler, der er i strid med et forbud efter § 2, stk. 1, og § 3, stk. 1, er uden gyldighed mellem parterne.

Kapitel 10
Ikrafttrædelse m.v.

§ 17. Loven træder i kraft den […].

Stk. 2. Loven har virkning for aftaler, der er indgået den 7. december 2020 eller senere, jf. dog stk. 3.

Stk. 3. Loven har fra den 1. januar 2026 endvidere virkning for aftaler, der er indgået før den 7. december 2020.

Kapitel 11
Ændring af anden lovgivning

§ 18. I lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed foretages følgende ændring:

1. I *§ 4, nr. 2, 2. pkt.,* ændres »10« til: »25«.

Kapitel 12
Lovens territoriale gyldighed

§ 19. [Loven gælder ikke for Færøerne og Grønland].

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning

Danmark er et af de mest digitaliserede lande i verden. Danske myndigheder, virksomheder og borgere er i vidt omfang afhængige af en fungerende teleinfrastruktur, både til dagligt og i krisesituationer. COVID-19-krisen har i særlig grad tydeliggjort, at det er nødvendigt at forstå kritisk infrastruktur bredere i takt med den teknologiske udvikling. Velfærden og velstanden i det danske samfund afhænger således i høj grad af en velfungerende og sikker teleinfrastruktur.

Digitaliseringen af det danske samfund vil fortsat accelerere i de kommende år. Det vil føre til revolutionerende nye digitale tjenester og løsninger, der løbende vil øge Danmarks afhængighed af teleinfrastrukturen. Der vil ske en stor udbredelse af ny digital teknologi, som f.eks. selvkørende biler og fjernstyring af funktioner i hjemmet, ligesom telenettet vil blive brugt til at transmittere flere og flere følsomme data.

Den teknologiske udvikling skaber stor værdi for samfundet, men medfører samtidig at risikoen for, at teleinfrastrukturen bruges til spionage mod eller pression af den danske stat, løbende vil stige. Danmarks sårbarhed over for disse trusler vil øges markant, og det stiller nye og større krav til vores håndtering af sikkerheden i teleinfrastrukturen.

Virksomheder, der leverer kritisk teleudstyr eller står for driften af teleudbydernes infrastruktur, kan udgøre en selvstændig trussel, fordi deres adgang til teleinfrastrukturen giver dem mulighed for at udføre sabotage eller spionage. Det er derfor helt afgørende, at der kun anvendes pålidelige leverandører til den kritiske teleinfrastruktur.

Mange af Danmarks partnere og allierede er nået til samme erkendelse, og både i EU og NATO er der fokus på, hvordan man effektivt imødegår de sikkerhedsmæssige udfordringer, som senest er blevet aktualiseret af den hastige udrulning af 5G-teknologien i mobilnettet.

For at opnå en tilstrækkelig grad af sikkerhed i teleinfrastrukturen ønsker regeringen at styrke telemyndighedernes muligheder for at sikre den kritiske teleinfrastruktur, bl.a. i forhold til teleudbydernes anvendelse af leverandører af kritisk teleudstyr og -tjenester. Hovedformålet med dette lovforslag er derfor at skabe hjemmel til, at telemyndighederne kan forbyde konkrete leverandøraftaler vedrørende den kritiske teleinfrastruktur, hvis aftalerne vurderes at udgøre en trussel mod statens sikkerhed. Vurderingen vil ske på grundlag af objektive kriterier, og der er således ikke tale om, at lovforslaget er rettet mod bestemte leverandører eller bestemte lande.

Med lovforslaget vil der blive taget et vigtigt skridt for at sikre en robust teleinfrastruktur, og derigennem beskytte Danmark mod bl.a. spionage, sabotage og nedbrud af samfundskritiske funktioner. Desuden vil der ske en væsentlig reduktion af risikoen for, at Danmark kan blive mål for pression fra fremmede stater under konflikter.

Dette tiltag skal ses i sammenhæng med regeringens kommende lovforslag om en dansk screeningsordning og indgrebshjemmel, der kan imødegå de risici, der kan være forbundet med fremmede investeringer og andre særlige økonomiske aktiviteter. Den kommende screeningsordning og indgrebshjemmel vil gøre det muligt at gribe ind over for udenlandske investeringer og andre særlige økonomiske aktiviteter, der kan udgøre en trussel mod den nationale sikkerhed eller den offentlige orden.

2. Lovforslagets baggrund

2.1. Det aktuelle trusselsbillede

Center for Cybersikkerhed vurderer, at der er en høj trussel fra cyberspionage mod telesektoren. Hensigten med cyberspionagen er at få adgang til oplysninger om kunderne og deres kommunikation, forretningshemmeligheder eller viden om teleinfrastrukturen, som kan udnyttes til yderligere cyberspionage.

Telesektoren i Danmark anvender i høj grad eksterne leverandører til levering af it- og teleinfrastruktur samt drift, herunder teknisk support, af teleinfrastruktur. Sektoren er derfor sårbar over for lande, som vil forsøge at udnytte en leverandør fra de pågældende lande til cyberspionage.

Ved outsourcing overlades beskyttelsen af data og it-systemer reelt til leverandøren. Det stiller store krav til teleudbyderens muligheder for at sikre kontrollen med teleinfrastrukturen. Outsourcing til lande, som f.eks. har en anden lovgivning og sikkerhedskultur end Danmark, kan øge teleinfrastrukturens sårbarhed overfor cybertruslen. Eventuel hjemtagelse eller overdragelse til en anden leverandør kan være vanskelig og tidskrævende.

Den teknologiske udvikling medfører endvidere øget afhængighed af teleinfrastrukturen. Store dele af teleinfrastrukturen er baseret på avanceret teknologi, der produceres, leveres og vedligeholdes af leverandører, som er en del af et globaliseret marked. Nye former for telekommunikationsteknologi er desuden i højere grad end tidligere baseret på software i form af flere millioner linjers kode, der løbende vil modtage opdateringer og blive udviklet på afstand. Teleudbydernes leverandørforhold vil derfor fremover spille en endnu mere central rolle end hidtil.

De løbende opdateringer, omfanget af softwaren samt teknologiens kompleksitet medfører, at det er meget svært løbende at verificere, at sikkerheden eller integriteten af Danmarks kritiske teleinfrastruktur ikke undergraves eller kompromitteres.

Ved at presse en leverandør eller underleverandør kan en fremmed stat herudover få viden om, eller adgang til, danske teleudbyderes teleinfrastruktur.

Teleleverandørers centrale rolle for teleinfrastrukturen kan desuden sætte Danmark i et afhængighedsforhold til de lande, som en given leverandør er hjemmehørende i. I en politisk eller militær konflikt kan en fremmed stat via kontrol eller pres på leverandøren potentielt forstyrre eller afbryde teletjenester ved at holde kritiske reservedele eller fejlretninger tilbage eller direkte afbryde driften.

2.2. Udviklingen i andre lande

Der er både i EU-regi og i en række lande stigende fokus på håndtering af risici og sårbarheder i den kritiske teleinfrastruktur, i særdeleshed i forbindelse med udrulningen af 5G-teknologien i mobilnettet. Flere lande har således revideret deres lovgivningsmæssige rammer for håndteringen af disse sikkerhedsmæssige udfordringer.

I det følgende beskrives de overordnede elementer i overvejelserne i EU og ordningerne fra tre sammenlignelige lande.

2.2.1. EU's 5G-toolbox

Foranstaltninger vedrørende sikkerhed i teleinfrastrukturen har været genstand for betydeligt fokus i EU-regi. Der er i den forbindelse udarbejdet en anbefaling, den såkaldte 5G-toolbox, vedrørende cybersikkerhed i 5G-netværket. EU's 5G-toolbox identificerer en række foranstaltninger, der kan afbøde de største cybersikkerhedsrisici ved 5G-netværket.

En af de foranstaltninger, som beskrives i EU's 5G-toolbox, er vurdering af leverandørernes risikoprofil og følgelig anvendelse af relevante begrænsninger for leverandører, der anses for at udgøre en høj risiko. Sådanne begrænsninger vil kunne omfatte nødvendige udelukkelser for at begrænse risici for aktiver, der defineres som kritiske og følsomme.

2.2.2. Sverige

I Sverige kræves der i medfør af loven om elektronisk kommunikation tilladelse fra de svenske myndigheder til anvendelsen af radiosendere. Tilladelse til anvendelse af radiosendere er en forudsætning for bl.a. at kunne anvende de frekvensbånd, der skal bruges til mobilnetværk.

Det er en forudsætning for at få en tilladelse, at det kan antages, at radioanvendelsen ikke kommer til at skade Sveriges sikkerhed. Derudover kan der fastsættes vilkår for tilladelser, hvis dette er af betydning for Sveriges sikkerhed. Sådanne vilkår kan eksempelvis indebære krav til det tekniske udstyr, som er relateret til radioanvendelsen. Vilkårene kan også have til formål at sikre, at komponenter, leverandører eller servicepersonale, der bruges til eller har forbindelse til radioanvendelsen, opretholder et tilstrækkeligt højt sikkerhedsniveau. Desuden er det muligt at tilbagekalde en tilladelse eller ændre tilladelsesvilkår øjeblikkeligt, hvis radioanvendelsen har skadet Sveriges sikkerhed, eller det kan antages, at radioanvendelsen kommer til at skade Sveriges sikkerhed.

Den 20. oktober 2020 udmeldte den svenske Post- og Telestyrelse i forbindelse med en auktion over anvendelse af radiosendere til brug for det kommende 5G-netværk, at det er en forudsætning for at få tilladelse til anvendelsen, at udstyr fra to konkrete leverandører ikke bruges i 5G-netværket. Afgørelsen omfatter 5G-netværkets kerne, periferi, transmissionsnettet samt overvågnings- og kontrolsystemer, der betegnes som centrale funktioner. Afgørelsen specificerer, at allerede eksisterende komponenter i 3G- og 4G-netværket, der også vil blive brugt til at levere 5G-tjenester, skal udskiftes senest 1. januar 2025, såfremt det er leveret af de pågældende leverandører. Derudover stilles der krav om, at såfremt de centrale funktioner i telenettet er afhængige af personel eller funktioner placeret i udlandet, skal en sådan afhængighed afvikles og om nødvendigt udskiftes med personel og funktioner placeret i Sverige senest den 1. januar 2025.

Det fremgår af udmeldingen fra Post- og Telestyrelsen, at afgørelsen hviler på en sikkerhedsmæssig vurdering af, at aftaler med de to leverandører om 5G-udstyr og drift af selve netværket vil udgøre en trussel mod Sveriges nationale sikkerhed. Afgørelsen er påklaget.

2.2.3. Norge

Norges lov om national sikkerhed (sikkerhedsloven) regulerer bl.a. anskaffelser til beskyttelsesværdige informationssystemer, objekter og infrastruktur. Virksomheder skal i medfør af loven sørge for et forsvarligt sikkerhedsniveau for beskyttelsesværdige informationssystemer, objekter og infrastruktur. I forbindelse med udrulningen af 5G-netværket har de norske myndigheder over for teleudbyderne præciseret, at et forsvarligt sikkerhedsniveau i lovens forstand indebærer, at teleudbyderne skal benytte flere leverandører, hvis de anvender basestationer, der leveres af 5G-leverandører fra et land, Norge ikke har en sikkerhedsaftale med, og at mindst 50 pct. af basestationerne skal leveres af leverandører fra lande, som Norge har en sikkerhedsaftale med.

Ved anskaffelser til beskyttelsesværdige informationssystemer, objekter eller infrastruktur har virksomheder en underretningspligt, hvis de vurderer, at anskaffelsen kan indebære en ikke ubetydelig risiko for, at informationssystemet, objektet eller infrastrukturen kan blive ramt af eller brugt til virksomhed, der udgør en trussel mod sikkerheden. I sådanne tilfælde kan der træffes beslutning om, at anskaffelsen ikke kan gennemføres, eller at der skal fastsættes vilkår for denne. Dette gælder også, hvis der allerede er indgået aftale om anskaffelsen. Der vil kunne gribes ind overfor en allerede indgået aftale, hvis virksomheden ikke har overholdt sin underretningspligt. Der vil også kunne gribes ind i tilfælde, hvor trusselsbilledet ændres.

Der er desuden, som en ekstra sikkerhedsmekanisme, en mere generel mulighed for, at der kan træffes nødvendige beslutninger for at hindre virksomhed, der udgør en trussel mod sikkerheden, eller anden planlagt eller pågående aktivitet, som kan indebære en ikke ubetydelig risiko for, at nationale sikkerhedsinteresser bliver truet. Muligheden forudsættes kun benyttet i helt særlige tilfælde.

2.2.4. Nederlandene

Nederlandene har etableret hjemmel til, at det kan besluttes, at teleudbydere ikke må benytte produkter eller tjenester fra leverandører i de kritiske dele af deres netværk. Det er en forudsætning for beslutningen, at det skal være nødvendigt for at kontrollere risici, der påvirker den nationale sikkerhed eller den offentlige orden. Der skal ved beslutningen lægges vægt på, om leverandøren har til hensigt at misbruge eller afbryde et telenet eller en teletjeneste, der udbydes i Nederlandene, eller om leverandøren har tæt tilknytning til eller er under indflydelse fra en part med en sådan intention.

I vurderingen af, hvorvidt det er nødvendigt at træffe beslutning om at udelukke en leverandør, indgår bl.a., hvorvidt leverandøren kommer fra – eller er under kontrol af – en part fra et land, med lovgivning, der forpligter kommercielle eller private parter til at samarbejde med landets regering, herunder særligt samarbejde med statsorganer med ansvar for efterretningsvirksomhed eller militær virksomhed. Det kan også indgå i vurderingen, om leverandøren er en statsejet virksomhed. Endvidere kan det indgå, hvorvidt leverandøren kommer fra et land med en aktiv og offensiv efterretningsstrategi rettet mod Nederlandene eller nederlandske interesser, eller hvorvidt leverandøren kommer fra et land, med hvem Nederlandenes forhold kan være anstrengt i en grad, der kan tænkes at påvirke nederlandske interesser.

2.3. Tilsyn med informationssikkerheden i telesektoren

Center for Cybersikkerhed er myndighed for informationssikkerhed og beredskab i telesektoren. Centeret er en del af Forsvarets Efterretningstjeneste, og centerets virksomhed er nærmere reguleret i lov om Center for Cybersikkerhed, jf. lovbekendtgørelse nr. 836 af 7. august 2019. Centerets opgaver som myndighed for informationssikkerhed og beredskab i telesektoren er reguleret i lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed.

Center for Cybersikkerheds virksomhed er undtaget fra dele af offentlighedsloven og forvaltningsloven. Det er dog forudsat, at Center for Cybersikkerhed i videst muligt omfang efterlever principperne i offentlighedsloven og forvaltningsloven, og at undtagelserne alene anvendes, hvis der er tale om oplysninger, der vedrører Forsvarets Efterretningstjenestes efterretningsmæssige del eller centerets egen netsikkerhedstjeneste. Center for Cybersikkerhed er endvidere undtaget fra EU's databeskyttelsesforordning og databeskyttelsesloven, men der er i stedet i lov om Center for Cybersikkerhed fastsat detaljerede regler om centerets behandling af personoplysninger.

Center for Cybersikkerheds behandling af personoplysninger er under løbende kontrol af Tilsynet med Efterretningstjenesterne, der hvert år udgiver en redegørelse om det tilsyn, der udøves med Center for Cybersikkerhed. Årsredegørelsen er offentligt tilgængelig.

3. Lovforslagets hovedpunkter

3.1. Nedlæggelse af forbud vedrørende visse leverancer til den kritiske teleinfrastruktur

3.1.1. Gældende ret

De gældende regler om informationssikkerhed i den kritiske teleinfrastruktur er fastsat i lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed.

Efter lovens § 4 kan Center for Cybersikkerhed fastsætte regler om oplysnings- og underretningspligter for teleudbydere. Efter § 4, nr. 2, kan reglerne omfatte krav om erhvervsmæssige udbydere af offentligt tilgængelige net og tjenesters underretning af Center for Cybersikkerhed ved påtænkt indgåelse af aftaler om leverancer, der vedrører væsentlige dele af teleudbyderens net eller tjenester eller driften heraf. Der kan endvidere stilles krav om, at teleudbyderne skal indsende et endeligt aftaleudkast til Center for Cybersikkerhed umiddelbart forud for indgåelse af aftalen, og at aftalen først kan indgås op til 10 arbejdsdage efter centerets modtagelse af dette udkast.

Bemyndigelsen i § 4, nr. 2, er udmøntet i bekendtgørelse nr. 1256 af 27. november 2019 om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed.

Efter bekendtgørelsens § 3 skal væsentlige erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester skriftligt underrette Center for Cybersikkerhed forud for, at der indledes forhandlinger om aftaler, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf.

Teleudbyderne skal endvidere skriftligt underrette Center for Cybersikkerhed forud for, at der indledes forhandlinger om tillæg til eksisterende aftaler, som vedrører eller grundet

tillægget vil komme til at vedrøre kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf.

I bekendtgørelsens § 4 er der fastsat en række krav til indholdet af de underretninger, der skal indsendes i medfør af § 3.

Efter bekendtgørelsens § 5, stk. 1, kan Center for Cybersikkerhed udstede påbud om, at det endelige udkast til en aftale, der er omfattet af § 3, skal fremsendes til Center for Cybersikkerhed forud for indgåelse af den endelige aftale. Efter stk. 2 vil den endelige aftale herefter først kunne indgås, når teleudbyderen har modtaget en tilbagemelding fra Center for Cybersikkerhed. Tilbagemeldingen vil blive givet hurtigst muligt og senest 10 arbejdsdage fra Center for Cybersikkerheds modtagelse af aftaleudkastet.

Såfremt indholdet af et aftaleudkast, som en teleudbyder har fremsendt til Center for Cybersikkerhed på baggrund af et påbud efter stk. 1, efterfølgende ændres, skal det ændrede aftaleudkast fremsendes til Center for Cybersikkerhed, hvorefter stk. 2 atter finder anvendelse. Dette gælder dog ikke, hvis ændringerne i aftaleudkastet alene er foretaget på baggrund af Center for Cybersikkerheds tilbagemelding efter stk. 2.

Herudover kan Center for Cybersikkerhed efter § 6 udstede påbud om, at endelige aftaler, der er omfattet af § 3, skal fremsendes til Center for Cybersikkerhed til orientering senest 10 arbejdsdage efter aftaleindgåelsen.

Såfremt teleudbyderne ikke følger Center for Cybersikkerheds rådgivning, har centeret ikke i dag mulighed for at forbyde aftaler eller anvendelse af konkrete komponenter, udstyr og værktøjer.

Efter at en aftale er indgået, vil Center for Cybersikkerhed dog efter § 3, stk. 3, i net- og informationssikkerhedsloven kunne påbyde udbydere af offentligt tilgængelige net og tjenester at træffe konkrete foranstaltninger med henblik på at sikre informationssikkerheden i offentligt tilgængelige net og tjenester. Det er en forudsætning for påbuddet, at det er af væsentlig samfundsmæssig betydning.

3.1.2. Forsvarsministeriets overvejelser

Efter de gældende regler i net- og informationssikkerhedsloven bliver Center for Cybersikkerhed underrettet forud for, at større danske teleudbydere indleder forhandlingerne med leverandører om aftaler, der vedrører leverancer til eller drift af den kritiske teleinfrastruktur. Dermed sikres det, at centeret får mulighed for at rådgive teleudbyderne om de sikkerhedsmæssige aspekter, som teleudbyderne bør være opmærksomme på i det efterfølgende forhandlingsforløb.

I konkrete tilfælde kan Center for Cybersikkerhed endvidere beslutte, at det endelige aftaleudkast skal sendes til Center for Cybersikkerhed, hvorefter aftalen først kan indgås, når Center for Cybersikkerhed har meldt tilbage, hvilket dog maksimalt må tage 10 arbejdsdage.

Forsvarsministeriet finder, at der med denne underretningsordning er skabt et velfungerende system, som sikrer, at Center for Cybersikkerhed til enhver tid har overblik over, hvilke aftaler de danske teleudbydere har indgået eller forventer at indgå, og hvilke aftaler, der potentielt kan udgøre en trussel mod den kritiske teleinfrastruktur. Det er endvidere

Forsvarsministeriets vurdering, at ordningen generelt har understøttet et godt og konstruktivt samarbejde mellem Center for Cybersikkerhed og teleudbyderne, hvor teleudbyderne i langt de fleste tilfælde vælger at følge den rådgivning, som de undervejs i aftaleforløbet får fra Center for Cybersikkerhed.

Forsvarsministeriet finder dog samtidig, at det alvorlige trusselsbillede, jf. afsnit 2.1 ovenfor, gør det nødvendigt at styrke myndighedernes mulighed for at sikre den kritiske teleinfrastruktur. Teleinfrastrukturen er helt afgørende for, at det danske samfund kan fungere. Samfundets velfærd og velstand vil derudover med den teknologiske udvikling i stigende grad være afhængige af en sikker og velfungerende teleinfrastruktur, og der skal derfor sættes effektivt ind for at imødegå trusler mod tilgængelighed og fortrolighed i teleinfrastrukturen. I den forbindelse er teleudbydernes aftaler med leverandører særligt væsentlige. En række aftaler giver således leverandører adgang til de mest kritiske dele af teleinfrastrukturen, enten gennem leverancer af hardware og software eller gennem varetagelse af driftsopgaver. Det skaber en væsentlig sårbarhed, såfremt leverandører vælger – eller presses til – at udnytte denne adgang til at udføre spionage eller sabotage. Det er derfor altafgørende, at der alene anvendes leverandører til den kritiske teleinfrastruktur, som der kan være tillid til.

Det er Forsvarsministeriets vurdering, at der er behov for, at der på objektivt grundlag foretages en telefaglig vurdering af, om de konkrete aftaler, som teleudbyderne ønsker at indgå, kan udgøre en trussel mod statens sikkerhed. Hvis det er tilfældet, finder Forsvarsministeriet, at den nuværende lovgivning, der alene giver myndighederne mulighed for at rådgive teleudbyderne om sikkerhedsmæssige problemer i aftalerne, er utilstrækkelig. Det er således uacceptabelt, at der kan opstå en situation, hvor myndighederne har vurderet, at en aftale vil udgøre en trussel mod statens sikkerhed, men hvor der ikke er nogen mulighed for at forhindre, at aftalen indgås og implementeres.

Indgreb i aftaler mellem private virksomheder bør dog efter Forsvarsministeriets opfattelse kun ske i særlige situationer. En forudsætning for, at indgåelse af en aftale forbydes, bør således være, at der er tale om et særligt tilfælde, hvor der dels er tale om en trussel mod statens sikkerhed, dels ikke er mulighed for at anvende mindre indgribende midler.

Forsvarsministeriet finder endvidere, at der bør være mulighed for at forbyde allerede indgåede aftaler. Det kan f.eks. være tilfældet, hvis en leverandør efterfølgende har fået nye ejere, hvis en leverandør er blevet afsløret i en sabotage- eller spionagehandling i udlandet, eller hvis ændret lovgivning i leverandørens hjemland betyder, at leverandøren kan forpligtes til at udføre eller facilitere sabotage- eller spionagehandlinger. Henset til, at forbud mod en allerede indgået aftale vil være indgribende, bør det dog være en forudsætning, at der vurderes at være tale om en væsentlig trussel mod statens sikkerhed.

Tilsvarende bør der være mulighed for at forbyde den fortsatte anvendelse af kritiske komponenter, systemer m.v., der er leveret som led i en tidligere aftale. Det kan f.eks. være aktuelt, hvis telemyndigheder i udlandet opdager, at en leverandør har indbygget en bagdør i teleudstyr af samme model, som også er leveret til en dansk teleudbyder.

Forsvarsministeriet finder, at en ny og skærpet regulering bør have virkning for aftaler, der indgås fra den dag, hvor dette lovforslag er sendt i høring. Lovforslaget vil dermed få tilbagevirkende kraft fra det tidspunkt, hvor teleudbyderne har haft mulighed for at gøre sig bekendt med den foreslåede regulering og i fornødent omfang tage højde for, at et lovforslag med dette indhold vil blive fremsat for Folketinget. Den tilbagevirkende kraft sikrer, at der

ikke kan ske omgåelse ved, at teleudbyderne fremrykker aftaleindgåelser, således at indgåelserne sker inden lovforslagets ikrafttræden.

Endvidere finder Forsvarsministeriet, at også aftaler, der er indgået før høringstidspunktet, bør omfattes af reguleringen fra den 1. januar 2026. Det er ministeriets vurdering, at meget få aftaler vil have så lang løbetid, men ordningen vil sikre, at der bliver mulighed for at tage stilling til, om sådanne aftaler skal forbydes, dog således, at teleudbyderne har haft næsten fem år til at indrette sig på, at aftalerne bliver omfattet af den skærpede regulering.

3.1.3. Den foreslåede ordning

Det foreslås, at de eksisterende regler i net- og informationssikkerhedsloven suppleres med et ekstra værktøj, så myndighederne kan forhindre, at en teleudbyder indgår eller opretholder en problematisk aftale med en leverandør.

Det foreslås således, at Center for Cybersikkerhed i særlige tilfælde kan forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at indgå en aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf, såfremt aftalen vurderes at udgøre en trussel mod statens sikkerhed. Vurderingen vil typisk ske som sidste trin i forbindelse med den underretningsordning, der i forvejen er etableret i medfør af net- og informationssikkerhedsloven.

Ved vurderingen af, om en aftale udgør en trussel mod statens sikkerhed, vil Center for Cybersikkerhed særligt kunne lægge vægt på forhold vedrørende den leverandør, som teleudbyderen ønsker at anvende. I vurderingen vil kunne indgå forhold vedrørende både leverandøren, leverandørens væsentligste underleverandører samt andre aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren, f.eks. leverandørens ejere eller bestyrelsesmedlemmer.

Der vil være tale om en samlet vurdering, hvori der vil indgå en række objektive kriterier. Eksempelvis vil Center for Cybersikkerhed kunne lægge vægt på, om en leverandør m.v. er hjemmehørende i eller varetager produktionen eller driften fra et land, som Danmark ikke har indgået en sikkerhedsaftale med, eller som Danmark ikke har et tilsvarende sikkerhedsmæssigt samarbejde med. Der vil også kunne lægges vægt på, om leverandøren m.v. er hjemmehørende i eller varetager produktionen eller driften fra et land, hvor det efter lovgivningen er muligt at pålægge leverandører eller deres underleverandører at udføre eller deltage i forhold, som vil udgøre spionage eller sabotage.

Herudover vil Center for Cybersikkerhed kunne lægge vægt på, om leverandøren m.v. direkte eller indirekte kontrolleres af et andet lands statslige organer, herunder militære myndigheder, samt om leverandøren m.v. er eller tidligere har været involveret i aktiviteter i Danmark eller andre lande, som har medført en negativ påvirkning af statens sikkerhed, informationssikkerheden eller den offentlige orden.

Det foreslås desuden, at en forudsætning for, at der nedlægges et forbud mod en aftale, vil være, at Center for Cybersikkerhed konkret har vurderet, at hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger end et forbud. Det vil således være en forudsætning, at Center for Cybersikkerhed har forsøgt at rådgive teleudbyderen om de tilpasninger af aftalen, som vil være nødvendige, for at den ikke længere vurderes at udgøre en trussel mod statens sikkerhed. Center for Cybersikkerhed vil også

skulle have vurderet relevante muligheder i net- og informationssikkerhedsloven, herunder eksempelvis muligheden for at give påbud om, at teleudbyderen skal foretage konkrete sikkerhedsforanstaltninger.

Endvidere foreslås det, at Center for Cybersikkerhed får mulighed for i særlige tilfælde at forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at opretholde en indgået aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelsen af driften heraf, såfremt opretholdelse af aftalen vurderes at udgøre en væsentlig trussel mod statens sikkerhed. Ved vurderingen heraf kan Center for Cybersikkerhed særligt lægge vægt på forhold vedrørende leverandøren, leverandørens væsentligste underleverandører samt aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren.

Dermed sikres det, at Center for Cybersikkerhed kan nedlægge forbud mod en given aftale, f.eks. såfremt der efter aftaleindgåelsen sker ændringer vedrørende leverandøren m.v., som medfører, at en aftale, der ikke oprindeligt blev anset for at udgøre en trussel mod statens sikkerhed, nu vurderes at udgøre en væsentlig trussel mod statens sikkerhed. Der vil være tale om en konkret vurdering, men med kravet om, at der skal vurderes at være tale om en væsentlig trussel, forudsættes det, at muligheden kun vil blive anvendt i sjældne tilfælde.

Da der er tale om en igangværende aftale, kan Center for Cybersikkerhed i den forbindelse fastsætte en frist for, hvornår aftalen skal være afviklet.

Endvidere foreslås det, at Center for Cybersikkerhed i særlige tilfælde kan forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester fortsat at anvende kritiske netkomponenter, systemer og værktøjer, der tidligere er leveret, såfremt fortsat anvendelse vurderes at udgøre en væsentlig trussel mod statens sikkerhed. Ved vurderingen heraf kan Center for Cybersikkerhed særligt lægge vægt på forhold vedrørende leverandøren, leverandørens væsentligste underleverandører samt aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren.

Også her kan Center for Cybersikkerhed fastsætte en frist for, hvornår den fortsatte anvendelse skal ophøre.

Endelig foreslås det, at loven får virkning for aftaler, der er indgået den 7. december 2020, hvor lovforslaget blev sendt i høring, eller senere, samt at loven fra den 1. januar 2026 endvidere får virkning for aftaler, der er indgået før den 7. december 2020.

Der henvises til de foreslåede §§ 2, 3 og 17 samt bemærkningerne hertil.

Center for Cybersikkerhed udgiver en årlig beretning, der beskriver centerets aktiviteter på det forebyggende område og bringer statistiske oplysninger herom. Desuden indeholder beretningen et overblik over de trusselsvurderinger m.v., der er udsendt i årets løb, således at virksomheder og offentligheden kan få et overblik over risikoen for cyberangreb. For at sikre åbenhed om anvendelse af de foreslåede muligheder for at nedlægge forbud, forudsættes det, at statistik om anvendelse af ordningen medtages i Center for Cybersikkerheds årlige beretning.

3.2. Undtagelser fra offentlighedsloven og forvaltningsloven

3.2.1. Gældende ret

Det følger bl.a. af § 8, stk. 1, i lov om Center for Cybersikkerhed, jf. lovbekendtgørelse nr. 836 af 7. august 2019, at Center for Cybersikkerheds virksomhed er undtaget fra lov om offentlighed i forvaltningen bortset fra lovens § 13. Center for Cybersikkerheds virksomhed er endvidere undtaget fra forvaltningslovens kapitel 4-6.

Af bemærkningerne til § 8, stk. 1, i lov om Center for Cybersikkerhed, jf. Folketingstidende 2013-14, A, L 192 som fremsat, side 25, fremgår det, at Center for Cybersikkerhed forudsættes i videst muligt omfang at efterleve principperne i offentlighedsloven og forvaltningslovens kapitel 4-6. Det forudsættes således, at centeret – uanset at dets virksomhed er undtaget fra forvaltningslovens bestemmelser på området – i relevant omfang vurderer, om det i afgørelsessager konkret er muligt at anvende forvaltningslovens principper om partens aktindsigt, partshøring og begrundelse m.v. Tilsvarende forudsættes det, at anmodninger om aktindsigt i videst muligt omfang behandles efter principperne i offentlighedsloven. Ved modtagelse af anmodninger om aktindsigt – herunder egenacces efter offentlighedslovens § 8 – vil Center for Cybersikkerhed i praksis foretage en søgning i centerets elektroniske sags- og dokumenthåndteringssystem. Såfremt der i den forbindelse lokaliseres dokumenter, der er omfattet af aktindsigtsanmodningen, vil disse dokumenter blive behandlet efter principperne i offentlighedsloven. Derimod vil centeret ikke foretage en søgning i de store mængder data, som centerets netsikkerhedstjeneste til enhver tid opbevarer, eller i dokumenter, der vedrører øvrige dele af Forsvarets Efterretningstjeneste.

Det følger endvidere af § 7 i net- og informationssikkerhedsloven, at det i regler udstedt i medfør af lovens § 4 kan fastsættes, at underretninger og afgivelse af oplysninger efter § 4, nr. 1-3, er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven. Efter lovens § 4, nr. 1-3, kan Center for Cybersikkerhed fastsætte regler om oplysnings- og underretningspligter for udbydere. Reglerne kan bl.a. omfatte krav om, at teleudbydere skal underrette Center for Cybersikkerhed ved brud på informationssikkerheden, der har væsentlige følger for driften af net eller tjenester, ligesom teleudbyderne skal underrette centeret ved påtænkt indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf. Endvidere kan reglerne omfatte krav om, at teleudbydere skal afgive oplysninger til Center for Cybersikkerhed om væsentlige dele af udbyderens net eller tjenester eller driften heraf. Bestemmelsen er udmøntet § 13 i bekendtgørelse nr. 1256 af 27. november 2019 om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed.

Det fremgår af bemærkningerne til § 7, jf. Folketingstidende 2015-16, A, L 10 som fremsat, side 10, at det forudsættes, der ikke skal være ret til aktindsigt, herunder partsaktindsigt, i forhold til de oplysninger og underretninger, som modtages fra teleudbydere i forbindelse med aftaleindgåelse, konstaterede brud på informationssikkerheden og generelle oplysninger om teleudbydernes infrastruktur. Undtagelsen fra retten til aktindsigt omfatter derimod ikke teleudbyderes og øvrige virksomheders adgang til at gøre sig bekendt med oplysninger, der vedrører deres egne forhold.

3.2.2. Forsvarsministeriets overvejelser

I dag er det en forudsætning, at Center for Cybersikkerhed i videst muligt omfang efterlever principperne i offentlighedsloven og forvaltningslovens kapitel 4-6, selvom centeret er undtaget fra offentlighedsloven og dele af forvaltningsloven. I praksis betyder det, at der i forbindelse med en begrundelse for en afgørelse og i forbindelse med behandlingen af en aktindsigtssag alene gøres undtagelse fra at anvende principperne i henholdsvis offentlighedsloven samt forvaltningslovens kapitel 4-6 i forhold til oplysninger, der stammer fra den monitoreringsvirksomhed, som Center for Cybersikkerheds netsikkerhedstjeneste foretager, eller som vedrører den efterretningsmæssige del af Forsvarets Efterretningstjeneste.

Den gældende undtagelse fra offentlighedsloven og forvaltningsloven indebærer, at Center for Cybersikkerhed ikke vil være forpligtet til at gengive efterretningsmæssige oplysninger i forbindelse med en begrundelse for en afgørelse truffet i medfør af kapitel 2 og 3. Endvidere vil centeret ikke være forpligtet til at lade de tilsvarende oplysninger indgå i behandlingen af en aktindsigtssag.

De sager, som behandles efter reglerne i dette lovforslag, vil imidlertid også indeholde andre oplysninger, der på tilsvarende vis er følsomme, selvom oplysningerne ikke nødvendigvis stammer fra eller vedrører den efterretningsmæssige del af Forsvarets Efterretningstjeneste. Det vil eksempelvis kunne være oplysninger, der er modtaget fra andre landes telemyndigheder.

Net- og informationssikkerhedsloven undtager derudover specifikt teleudbydernes underretninger fra retten til aktindsigt. Undtagelsen i net- og informationssikkerhedsloven omfatter imidlertid ikke forvaltningslovens krav til begrundelse og partshøring.

Det er på den baggrund Forsvarsministeriets vurdering, at de nuværende undtagelser ikke er tilstrækkelige til at varetage hensynet til beskyttelse af de oplysninger, der vil indgå i sager efter kapitel 2 og 3. Forsvarsministeriet finder endvidere, at de eksisterende undtagelsesmuligheder i forvaltningsloven og offentlighedsloven ikke vil være tilstrækkelige til at varetage beskyttelseshensynet i forhold til disse oplysninger. Der er derfor behov for, at disse oplysninger undtages fra offentlighedsloven og forvaltningslovens kapitel 4-6.

3.2.3. Den foreslåede ordning

Det foreslås, at lov om offentlighed i forvaltningen, bortset fra lovens § 13, og forvaltningslovens kapitel 4-6 ikke finder anvendelse på sager, der er omfattet af denne lov.

Den foreslåede bestemmelse svarer til den eksisterende undtagelse i § 8, stk. 1, i lov om Center for Cybersikkerhed, men med den ændring, at forudsætningen i bemærkningerne til lov om Center for Cybersikkerhed om, at principperne i lov om offentlighed i forvaltningen og forvaltningslovens kapitel 4-6 i videst muligt omfang skal følges, ikke gælder for sager omfattet af loven.

Der henvises til den foreslåede § 5 samt bemærkningerne hertil.

3.3. Særlige rammer for domstolsbehandling

3.3.1. Gældende ret

Det følger af grundlovens § 63, stk. 1, 1. pkt., at domstolene er berettigede til at påkende ethvert spørgsmål om øvrighedsmyndighedens grænser. Det er fast antaget, at domstolenes adgang til efter grundlovens § 63 at prøve forvaltningsafgørelser i et vist omfang nærmere kan bestemmes ved lov. Der kan bl.a. ved lov fastsættes regler om processuelle spørgsmål og spørgsmål om prøvelsens retsgrundlag og retsfølger.

I det omfang en afgørelse om indgreb måtte blive gennemført ved ekspropriation, vil der være adgang til domstolsprøvelse efter de særlige regler herom i grundlovens § 73, stk. 3. Det følger bl.a. heraf, at ethvert spørgsmål om ekspropriationsaktens lovlighed og erstatningens størrelse kan indbringes for domstolene. Det antages, at bestemmelsen indebærer, at domstolene skal foretage en mere intensiv prøvelse af administrative ekspropriationsafgørelser end efter grundlovens § 63.

Der er ikke i net- og informationssikkerhedsloven fastsat nærmere regler om domstolsprøvelsen af Center for Cybersikkerheds afgørelser. Prøvelsen sker således efter retsplejelovens almindelige regler herom.

3.3.2. Forsvarsministeriets overvejelser

Center for Cybersikkerheds afgørelser efter det foreslåede kapitel 2 vil kunne prøves ved domstolene efter grundlovens § 63, stk. 1, 1. pkt. Derudover vil centerets eventuelle afgørelser om ekspropriation efter § 4 også kunne prøves ved domstolene efter grundlovens § 73, stk. 3.

Afgørelserne vil imidlertid oftest være baseret på fortroligt materiale såsom højt klassificerede oplysninger, der, hvis de offentliggøres, vil kunne skade Danmarks sikkerhed. Mod offentliggørelse taler således hensynet til forholdet til fremmede magter, efterretningstjenesternes særlige arbejdsmetoder, beskyttelse af efterretningstjenesternes kilder, samt beskyttelse af efterretningsmæssige samarbejder, der bygger på gensidige tillidsforhold og forsikringer om, at de efterretningsbaserede oplysninger, der deles, ikke videregives til offentligheden uden forudgående tilladelse. De særlige sikkerhedsmæssige fortrolighedshensyn indebærer, at de oplysninger vedrørende statens sikkerhed, som afgørelserne er baseret på, ikke vil kunne fremlægges i en retssag på sædvanlig vis eller udleveres til parterne i retssagen.

Forsvarsministeriet har overvejet, hvordan teleudbyderens eller leverandørens ret til domstolsprøvelse kan forenes med de særlige sikkerhedsmæssige fortrolighedshensyn. Forsvarsministeriet finder, at disse hensyn kan varetages ved, at der etableres særlige procedureregler, hvorefter domstolsprøvelsen opdeles i en åben og en lukket del. Der vil under sagens lukkede del kunne ske fremlæggelse af fortroligt materiale, som af sikkerhedsmæssige grunde ikke kan videregives til parterne i sagen. Til varetagelse af partens interesser under den lukkede del af sagen vil der kunne beskikkes en særlig advokat, som på partens vegne får kendskab til og kan udtale sig om det fortrolige materiale, der fremlægges for retten. Den særlige advokat vil således kunne udøve partsbeføjelser under den lukkede del af sagen, dog således at den særlige advokat ikke må drøfte sagen med parten og partens advokat.

Ved en sådan model kan det bl.a. sikres, at fortroligt materiale alene deles med særligt udpegede, beskikkede advokater, der på betryggende vis kan varetage teleudbyderens eller leverandørens interesser i forbindelse med en retssag om prøvelsen af afgørelser efter kapitel 2 og 3. Det vil være nødvendigt, at de særligt udpegede advokater pålægges tavshedspligt, således at advokaten ikke deler fortroligt materiale.

Det er Forsvarsministeriets vurdering, at fastsættelse af sådanne særlige regler for domstolsbehandlingen vil være hensigtsmæssig i forhold til prøvelse af afgørelser om forbud efter kapitel 2 og 3. Formålet med den særlige domstolsbehandling vil være at skabe en balance mellem på den ene side behovet for at beskytte oplysninger af sikkerhedsmæssige grunde og på den anden side hensynet til, at der er en reel mulighed for effektiv varetagelse af partens interesser under retssagen.

Lignende ordninger er indført i udlændingelovens kapitel 7 b vedrørende domstolsprøvelse af sager om administrativ udvisning af udlændinge, der må anses for en fare for statens sikkerhed, og indfødsretslovens § 8 F vedrørende domstolsprøvelse af afgørelser om administrativ fratagelse af statsborgerskab.

3.3.3. Den foreslåede ordning

Det foreslås, at domstolsprøvelsen vedrørende afgørelser omfattet af kapitel 2 og 3 opdeles i en åben og en lukket del.

Der vil under sagens lukkede del kunne ske fremlæggelse af fortroligt materiale, som af sikkerhedsmæssige grunde ikke kan videregives til parterne i sagen. Til varetagelse af partens interesser under den lukkede del af sagen vil der blive beskikket en særlig advokat, som på partens vegne udøver partsbeføjelser under denne del af sagen, dog således at den særlige advokat ikke må drøfte sagen med parten eller dennes advokat.

Det foreslås, at afgørelser omfattet af kapitel 2 og 3 alene kan indbringes for Københavns Byret inden seks måneder efter afgørelsens meddelelse. Byretten kan dog undtagelsesvis tillade en indbringelse efter udløbet af fristen. I afgørelsen af sagen ved byretten deltager tre dommere. Forsvarsministeren eller den, ministeren bemyndiger hertil, kan lade personer, der er ansat i Forsvarsministeriet eller i myndigheder under Forsvarsministeriet, møde for sig i retten som rettergangsfuldmægtige.

Det foreslås desuden, at det udtrykkeligt i loven fastslås, at parterne i sagen anses for at være dem, som har en retlig interesse i en afgørelse omfattet af kapitel 2 og 3, og at parten i sagen for det offentlige anses for at være forsvarsministeren eller den, ministeren bemyndiger til det.

Der henvises til de foreslåede §§ 7-13 samt bemærkningerne hertil.

3.4. Hjemmel til ekspropriation

3.4.1. Gældende ret

Det følger af grundlovens § 73, stk. 1, at ejendomsretten er ukrænkelig. Ingen kan tilpligtes at afstå sin ejendom, uden hvor almenvellet kræver det. Det kan kun ske ifølge lov og mod fuldstændig erstatning.

To overordnede betingelser skal således være opfyldt for, at der er tale om ekspropriation i grundlovens forstand. For det første skal indgrebet være rettet mod "ejendom", som er beskyttet efter grundlovens § 73. For det andet skal indgrebet være ekspropriativt (der skal være tale om afståelse).

Hvis der er tale om et indgreb, der har karakter af ekspropriation i grundlovens forstand, skal tre betingelser være opfyldt for, at indgrebet er i overensstemmelse med grundloven. Indgrebet skal være krævet af almenvellet, skal ske ifølge lov, og der skal ydes fuldstændig erstatning til den berørte ejer.

Grundloven beskytter ikke blot fysiske personer, men også alle typer af juridiske personer, som er etableret (eller overtaget) af private – selskaber, foreninger, selvejende institutioner m.v. Det er traditionelt antaget, at også staten, kommuner og andre juridiske personer etableret (eller fuldt ud overtaget) af det offentlige er beskyttet. Det fremgår dog af nyere retspraksis, at i hvert fald visse offentlige juridiske personer ikke altid nyder samme beskyttelse som private.

Udtrykket "ejendom" i grundlovens § 73 må forstås i vid betydning. Det er således almindeligt antaget, at bestemmelsen ikke alene beskytter ejendomsret i traditionel forstand. Også begrænsede rådighedsrettigheder, såsom brugsrettigheder, servitutter og panterettigheder, og rettigheder i henhold til private aftaler er beskyttet af grundlovens ejendomsbegreb.

Det er endvidere almindeligt antaget, at bestemmelsen ikke alene beskytter rettigheder af privatretlig karakter, men også særlige rettigheder af erhvervsmæssig karakter stiftet på offentligretligt grundlag, f.eks. næringsrettigheder.

For at der er tale om ekspropriation i grundlovens forstand, skal der være tale om, at der foretages et ekspropriativt indgreb (afståelse).

Det er i den forbindelse almindeligt antaget i den forfatningsretlige litteratur og i praksis, at lovgivningsmagten – uden at der foreligger ekspropriation – kan regulere udøvelsen af de rettigheder, der er beskyttet af grundlovens § 73, idet lovgivningsmagten bl.a. kan opstille almindelige regler om begrænsninger i borgernes handlefrihed og i deres råden over, hvad de ejer. Det er endvidere antaget, at spørgsmålet om, hvorvidt et indgreb har karakter af ekspropriation, må bero på et samlet skøn over indgrebets beskaffenhed. Som momenter, der må tillægges betydning ved udøvelsen af dette skøn, kan der navnlig peges på indgrebets formål, i hvilken grad indgrebet er generelt eller konkret (herunder om det rammer mange eller få personer), indgrebets intensitet, om indgrebet angår en fremtidig eller en aktuel rettighed, om indgrebet går ud på at overføre rettigheden fra den hidtidige ejer til en ny eller på en tilintetgørelse af denne råden, samt indgrebets begrundelse (causa).

Net- og informationssikkerhedsloven indeholder ikke en specifik hjemmel til at foretage ekspropriation.

3.4.2. Forsvarsministeriets overvejelser

Afgørelsen af, om et forbud i medfør af § 2, stk. 1, og § 3, stk. 1 og 2, vil udgøre ekspropriation, vil skulle foretages på grundlag af en samlet vurdering af indgrebets beskaffenhed, herunder indgrebets formål, i hvilken grad indgrebet er generelt eller konkret, indgrebets intensitet samt indgrebets begrundelse (causa).

Navnlig det forhold, at forbud mod indgåelse af en aftale efter § 2, stk. 1, opretholdelse af en indgået aftale efter § 3, stk. 1, eller anvendelse af kritiske komponenter, systemer m.v. efter § 3, stk. 2, er begrundet i hensyn til statens sikkerhed, må antages at tale med en vis vægt imod, at der vil være tale om ekspropriation. Der vil på den anden side være tale om indgreb mod konkrete aftaler, som efter omstændighederne vil kunne være af betydelig intensitet over for den pågældende aftalepart. Det kan på den baggrund ikke udelukkes, at et forbud efter omstændighederne vil kunne anses for ekspropriativt.

I de forventeligt sjældne tilfælde, hvor afgørelserne vil have karakter af ekspropriation, er det væsentligt, at betingelserne i grundlovens § 73 er opfyldt. Indgrebet skal således være krævet af almenvellet, hjemlet i lov og ske mod fuld erstatning.

Det vurderes, at betingelsen om, at et indgreb skal være krævet af almenvellet, vil være opfyldt i relation til forbud efter kapitel 2, idet indgrebene vil ske ud fra et hensyn til statens sikkerhed. Hvis et forbud i medfør af kapitel 2 udgør et ekspropriativt indgreb, skal der i loven være en konkret hjemmel til at foretage ekspropriation. Idet der ikke efter gældende ret er en specifik hjemmel til at foretage ekspropriation i forhold til forbud omfattet af dette lovforslag, finder Forsvarsministeriet, at der vil skulle etableres en hjemmel hertil. Endeligt skal der ydes fuldstændig erstatning til den berørte ejer i de tilfælde, hvor der vil være tale om ekspropriation. Forsvarsministeriet finder, at dette tydeligt bør fremgå af en hjemmel til at foretage ekspropriation.

Spørgsmålet om ekspropriationens lovlighed og erstatningens størrelse kan indbringes for domstolene, jf. grundlovens § 73, stk. 3.

3.4.3. Den foreslåede ordning

Det foreslås, at der indsættes en bestemmelse, hvorefter Center for Cybersikkerhed kan iværksætte ekspropriation, hvis det er nødvendigt for gennemførelse af forbud efter kapitel 2.

Det foreslås endvidere, at det eksplicit fremgår af bestemmelsen, at der ydes fuldstændig erstatning til den eller de berørte parter, såfremt gennemførelse af forbud efter kapitel 2 udgør et ekspropriativt indgreb.

Der henvises til den foreslåede § 4 samt bemærkningerne hertil.

4. Forholdet til Danmarks internationale forpligtelser

4.1. Forholdet til Den Europæiske Menneskerettighedskonvention

Artikel 6 i Den Europæiske Menneskerettighedskonvention (EMRK) stiller krav til indholdet og omfanget af domstolsprøvelsen. Det er som udgangspunkt et krav, at den nationale domstol har "fuld jurisdiktion" med hensyn til tvistens faktiske og retlige omstændigheder.

Det betyder, at den nationale domstol skal have kompetencen til at undersøge parternes anbringender i substansen uden at nægte at undersøge visse af dem og give en klar begrundelse for, hvorfor de ikke tages til følge. I forhold til sagens faktum skal domstolen være i stand til at undersøge det, som er centralt for parternes sag.

En prøvelse af administrative myndigheders afgørelser vil være utilstrækkelig, hvis den ikke omfatter sagens faktiske omstændigheder, eller hvis retten ikke har kompetence til at annullere eller tilsidesætte en myndigheds afgørelser, men må nøjes med at konstatere, at afgørelsen er ugyldig.

Artikel 6 sikrer enhver ret til at indbringe enhver tvist vedrørende en borgerlig rettighed eller forpligtelse for en domstol i konventionens forstand. Retten til domstolsprøvelse er imidlertid ikke absolut, idet retten forudsættes reguleret nærmere af konventionsstaterne. I den forbindelse er staterne overladt en vis skønsmargin. Retten kan derfor underkastes begrænsninger, forudsat at disse ikke begrænser eller udhuler retten på en sådan måde eller i et sådant omfang, at kernen i retten forringes ("the very essence of the right is impaired"). En begrænsning er endvidere kun forenelig med artikel 6, hvis den varetager et anerkendelsesværdigt formål, og der er proportionalitet mellem det forfulgte formål og det valgte middel.

Hvis der efter national ret ikke er adgang til domstolsprøvelse af administrative myndigheders afgørelse, når der er tale om en civil sag i konventionens forstand, vil der allerede af den grund foreligge en krænkelse af artikel 6.

Hvis den nationale domstol er afskåret fra at vurdere en sags faktiske omstændigheder som følge af, at den ikke har adgang til relevante dokumenter, der af administrative myndigheder betegnes som fortrolige, kan dette udgøre en krænkelse. Det kan således f.eks. udgøre en krænkelse, hvis en privat tilbudsgiver er afskåret fra en reel domstolsprøvelse af en myndigheds afgørelse om ikke at tildele en offentlig kontrakt, fordi myndigheden angiver at handle til beskyttelse af nationens sikkerhed eller den offentlige sikkerhed eller orden, og denne vurdering er baseret på fortrolige oplysninger, når domstolen ikke har adgang til samtlige relevante dokumenter og derfor ikke kan foretage en reel prøvelse.

Retten til kontradiktion og princippet om parternes ligestilling, som er nært beslægtede, er fundamentale bestanddele af retten til en retfærdig rettergang i artikel 6, stk. 1. Disse rettigheder er imidlertid ikke absolutte, hvilket også gør sig gældende for adgangen til sagens materiale. Konventionsstaterne har således en skønsmargin ved begrænsningen af disse rettigheder, og modstridende interesser, såsom statens sikkerhed m.v., skal vejes op imod partens rettigheder. Der er i den forbindelse tale om en helhedsvurdering af sagens samlede omstændigheder. Der vil dog alene kunne ske begrænsninger i rettigheder, som ikke berører kernen ("the very essence") af rettighederne i artikel 6, stk. 1.

Med den foreslåede bestemmelse i § 7 kan afgørelser efter kapitel 2 og 3 indbringes for domstolene.

De særlige regler for domstolsbehandlingen, som foreslås i §§ 7-13, svarer med de nødvendige tilpasninger til reglerne om domstolsbehandling i udlændingelovens kapitel 7 b (og indfødsretslovens § 8 F). De foreslåede bestemmelser i §§ 7-13 varetager hensynet til, at fortrolige og sikkerhedsmæssige oplysninger ikke prisgives i forbindelse med en eventuel domstolsbehandling af en afgørelse om nedlæggelse af forbud. Samtidig sikres det, at alle sagens oplysninger som udgangspunkt fremlægges for retten, ligesom den pågældende part beskikkes en særlig advokat til at varetage sine interesser i forhold til det materiale, der af sikkerhedsmæssige grunde vurderes ikke at kunne videregives til den pågældende.

Artikel 6 sikrer også retten til en retfærdig rettergang, når der træffes afgørelse i straffesager, men heller ikke i dette tilfælde er retten til kontradiktion, princippet om parternes ligestilling og adgangen til sagens materiale absolutte. Det er Forsvarsministeriets vurdering, at de samme hensyn til nationale sikkerhedsinteresser som angivet ovenfor tilsiger, at også i sager, hvor der nedlægges påstand om straf efter § 15, prøves Center for Cybersikkerheds afgørelser efter kapitel 2 særskilt efter reglerne i §§ 7-13.

Forsvarsministeriet finder på den baggrund, at lovforslaget ikke rejser spørgsmål i forhold til artikel 6.

4.2. Forholdet til WTO-retten

Verdenshandelsorganisationen (WTO) har ved General Agreement on Trade and Tariffs (GATT) og General Agreement on Trade in Services (GATS) fastsat regler for handel med varer og tjenesteydelser mellem medlemslandene.

De helt grundlæggende bestemmelser i GATT og GATS er bestemmelserne om mestbegunstigelsesprincippet og nationalbehandlingsprincippet. Mestbegunstigelsesprincippet indebærer, at alle medlemslande skal behandles ens. Det betyder, at hvis et WTO-medlemsland opnår en begunstigende behandling i et andet WTO-medlemsland, så har de øvrige medlemslande ret til den samme behandling. Nationalbehandlingsprincippet indebærer, at et medlemsland ikke må favorisere egne produkter og tjenesteydelser frem for andre.

De to aftaler indeholder dog enkelte undtagelser, der giver et medlemsland mulighed for at fravige såvel disse grundregler som alle de øvrige regler i hele WTO-regelsættet.

Det følger bl.a. af GATT artikel XXI og GATS artikel XIV, bis, at intet i aftalerne skal fortolkes, således at medlemslandene forpligtes til eller forhindres i handlinger m.v., hvis det strider mod hensynet til dets væsentlige nationale sikkerhedsinteresser. Disse undtagelser skal imidlertid fortolkes yderst restriktivt.

Udover de specifikke undtagelser indeholder GATT i artikel XX og GATS i artikel XIV en række parallelle generelle undtagelser. De to bestemmelser er udtryk for WTO-medlemsskabets afvejning af legitime offentlige reguleringshensyn over for WTO-aftalernes regler til beskyttelse af handelen, ikke mindst mestbegunstigelsesprincippet og nationalbehandlingsprincippet.

Fælles for alle de generelle undtagelser er, at medlemsstaterne har en vid adgang til at gennemføre offentlig regulering, der er dækket af teksten i undtagelsesbestemmelserne, så længe reguleringen ikke i virkeligheden sigter på at opnå den kommercielle forskelsbehandling, man netop vil undgå med WTO-aftalerne. En sådan udelukkelse kan alene være begrundet i de reguleringshensyn, som er beskrevet i GAT artikel XX eller GATS artikel XIV.

Særligt kan fremhæves GATT artikel XX, (b) og GATS artikel XIV, (b), der omhandler foranstaltninger, som er nødvendige for at beskytte menneskers, dyrs eller planters liv eller sundhed.

I sager vedrørende GATT artikel XX, (b) har Appellant Body, der er anden instans i WTO-tvistbilæggelsessystemet, anlagt en samlet vurdering af medlemsstaternes beskyttelsesforanstaltninger baseret på fire kriterier: 1) Har foranstaltningen et beskyttelsesværdigt formål, 2) er den designet til at opnå dette formål, 3) er den nødvendig for at opnå det, eller kunne det samme formål være opnået med en mindre indgribende foranstaltning, og 4) er foranstaltningen gennemført på en sådan måde, at den ikke resulterer i en urimelig diskrimination af andre medlemslande eller deres virksomheder.

Det er vurderingen, at WTO-aftalerne ikke er til hinder for at indføre den foreslåede forbudsordning, idet sikring af en robust teleinfrastruktur i Danmark er begrundet i hensynet til statens sikkerhed og ultimativt i hensynet til menneskers liv og sundhed. Derudover vurderes ordningen at være nødvendig og egnet til at opfylde formålet. Muligheden for at forbyde konkrete aftaler af hensyn til statens sikkerhed baseres på objektive underkriterier, hvorfor ordningen vurderes at være indrettet på en sådan måde, at der ikke sker urimelig diskrimination af andre medlemslande eller deres virksomheder.

4.3. Forholdet til Danmarks bilaterale investerings- og handelsaftaler

Danmarks bilaterale investerings- og handelsaftaler indeholder almindeligvis bestemmelser om, at investeringer fra de kontraherende parters statsborgere eller selskaber skal gives en retfærdig og rimelig behandling samt ydes beskyttelse og sikkerhed i den anden parts territorium.

Endvidere indeholder disse aftaler almindeligvis også bestemmelser om, at investeringer foretaget af den anden parts statsborgere eller selskaber ikke må underkastes en mindre gunstig behandling end den, der gives investeringer foretaget af statsborgere eller selskaber fra noget tredjeland.

Danmarks bilaterale investerings- og handelsaftaler indebærer således, at der ikke må træffes foranstaltninger, herunder vedtages lovgivning, hvis egentlige motiv er kommerciel forskelsbehandling eller diskrimination.

Danmarks bilaterale investerings- og handelsaftaler vurderes ikke at være til hinder for den foreslåede forbudsordning, som er begrundet i et hensyn til statens sikkerhed.

5. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

Lovforslaget vil medføre, at Center for Cybersikkerhed skal varetage nye opgaver i forbindelse med, at centeret tillægges kompetence til at træffe afgørelser om forbud mod bl.a.

indgåelse eller opretholdelse af aftaler, der vedrører kritiske netkomponenter, systemer og værktøjer, eller varetagelsen af driften heraf. Desuden vil centeret skulle vejlede teleudbydere om kravene i loven, særligt i forbindelse med at teleudbyderne indgår nye aftaler. En stor del af disse opgaver vil dog ligge i naturlig forlængelse af de opgaver, som centeret allerede i dag varetager efter net- og informationssikkerhedsloven.

Udgiften til de nye opgaver forudsættes afholdt inden for Forsvarsministeriets eksisterende økonomiske ramme.

I de forventeligt sjældne tilfælde, hvor afgørelserne måtte have karakter af ekspropriation, vil dette skulle ske mod, at staten yder fuldstændig erstatning for det eventuelle tab, som afgørelsen måtte medføre for den pågældende teleudbyder eller leverandør. Det er forbundet med en stor usikkerhed at vurdere, hvilken økonomisk konsekvens dette i givet fald vil kunne få for det offentlige.

6. Økonomiske og administrative konsekvenser for erhvervslivet m.v.

Lovforslaget kan medføre økonomiske konsekvenser for teleudbyderne og leverandørerne, hvis der træffes afgørelse om forbud mod indgåelse af aftaler, eller om forbud mod opretholdelse af aftaler, som betyder, at en økonomisk fordelagtig aftale, der vedrører kritiske netkomponenter, systemer og værtøjer, eller varetagelsen af driften heraf, ikke kan indgås eller opretholdes. Lovforslaget kan endvidere medføre økonomiske konsekvenser for teleudbyderne, hvis der træffes afgørelse om forbud mod fortsat anvendelse af kritiske netkomponenter, systemer eller værktøjer. I de forventeligt sjældne tilfælde, hvor afgørelserne har karakter af ekspropriation, vil dette dog ske mod fuldstændig erstatning.

Lovforslaget vil endvidere kunne medføre en reduceret konkurrence, fordi teleudbyderne vil kunne vælge mellem færre leverandører, hvilket vil kunne medføre stigende priser og eventuelt have negativ effekt på innovationen på teleområdet.

Den foreslåede ordning baseres på de allerede eksisterende underretningsforpligtelser i net- og informationssikkerhedsloven. Lovforslaget forventes dog at kunne få administrative konsekvenser for teleudbydere og deres leverandører, såfremt et forbud medfører behov for at gennemføre et nyt udbud eller en ny aftaleforhandling.

7. Administrative konsekvenser for borgerne

Lovforslaget har ikke administrative konsekvenser for borgerne.

8. Klima- og miljømæssige konsekvenser

Lovforslaget har ikke klima- og miljømæssige konsekvenser.

9. Forholdet til EU-retten

Efter artikel 4, stk. 2, i Traktaten om Den Europæiske Union (TEU) er området for national sikkerhed den enkelte medlemsstats eneansvar. Ved udøvelsen af dette eneansvar skal medlemsstaterne dog overholde de frie bevægeligheder i Traktaten om Den Europæiske Unions Funktionsmåde (TEUF).

De EU-retlige rammer for den foreslåede forbudsordning sættes bl.a. af TEUF artikel 49 om den frie etableringsret og TEUF artikel 63 om de frie kapitalbevægelser.

De frie bevægeligheder i TEUF kan imidlertid begrænses af hensyn til bl.a. den nationale sikkerhed og den offentlige sikkerhed under iagttagelse af proportionalitetsprincippet. Proportionalitetsprincippet indebærer, at nationale foranstaltninger, der begrænser den frie bevægelighed, skal være egnede til at opfylde formålet med begrænsningen og ikke må gå ud over, hvad der er nødvendigt for at opfylde formålet.

Det er vurderingen, at TEUF ikke er til hinder for at indføre den foreslåede forbudsordning begrundet i hensynet til den nationale sikkerhed og den offentlige sikkerhed. Det er i den forbindelse vurderingen, at den foreslåede ordning er egnet til at opfylde formålet om at sikre, at danske teleudbydere ikke indgår eller opretholder aftaler om kritiske netkomponenter, systemer og værktøjer, eller varetagelsen af driften heraf, der udgør en trussel mod statens sikkerhed, og at ordningen ikke går ud over, hvad der er nødvendigt for at opfylde dette formål.

Europa Parlamentets og Rådets direktiv (EU) 2014/53 af 16. april 2014 om harmonisering af medlemsstaternes love om tilgængeliggørelse af radioudstyr på markedet og om ophævelse af direktiv (EF) 1999/5 (radioudstyrsdirektivet) har til formål at sikre fri bevægelighed for radioudstyr i EU's indre marked, hvis radioudstyret opfylder de krav, som fremgår af direktivet. Den foreslåede ordning er ikke rettet mod konkrete fabrikanter eller leverandører eller konkret radioudstyr. Den foreslåede ordning indebærer, at der efter en konkret vurdering, hvor der indgår en lang række faktorer, kan nedlægges forbud mod enkeltstående aftaler. Et sådant forbud vil ikke indebære et generelt forbud mod salg, tilrådighedsstillelse, ibrugtagning eller anvendelse af bestemte fabrikater eller typer af radioudstyr. Ordningen vil ikke blive administreret på en måde, som vil indebære et de facto forbud mod bestemt radioudstyr omfattet af radioudstyrsdirektivets ordning. Direktivet vurderes på den baggrund ikke at være til hinder for den foreslåede ordning.

Europa-Parlamentets og Rådets direktiv 2018/1972/EU af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (EU's telekodeks) fastsætter endvidere den EU-retlige ramme for regulering af teleområdet. EU's telekodeks fastsætter bl.a. rammen for at sikre frit udbud af elektroniske kommunikationsnet og -tjenester, således at disse kun er underlagt de vilkår, der bl.a. er fastsat i EU's telekodeks, jf. betragtning nr. 5.

Det følger imidlertid af artikel 1, stk. 3, litra c, i EU's telekodeks, at direktivet ikke berører tiltag, der gennemføres af medlemsstaterne ud fra hensynet til den offentlige orden og den offentlige sikkerhed og til forsvaret. I tilknytning hertil fremgår det bl.a. af betragtning nr. 6, at direktivet ikke indskrænker de enkelte medlemsstaters mulighed for at træffe nødvendige foranstaltninger til sikring af deres væsentlige sikkerhedsinteresser, beskyttelse af den offentlige orden og den offentlige sikkerhed.

Det er vurderingen, at EU's telekodeks ikke er til hinder for at indføre den foreslåede forbudsordning, idet ordningen gennemføres ud fra hensynet til statens sikkerhed, og idet direktivet ikke indskrænker muligheden for at træffe nødvendige foranstaltninger til sikring af væsentlige sikkerhedsinteresser og beskyttelse af den offentlige sikkerhed.

10. Hørte myndigheder og organisationer m.v.

Et udkast til lovforslag har i perioden fra den 7. december 2020 til den 4. januar 2021 været sendt i høring hos følgende myndigheder og organisationer m.v.:

Advokatrådet, Amnesty International, Bauer Media, Borch Teknik, Cibicom, Danmarks Radio, Dansk Beredskabskommunikation, Dansk Energi, Dansk Erhverv, Dansk Industri (DI), DANSK IT, Dansk Kabel TV, Danske Advokater, Danske Regioner, Datatilsynet, Den Danske Dommerforening, DI Digital, Domstolsstyrelsen, Fibia, Forenede Danske Antenneanlæg, GLOBALCONNECT, Hi3G Denmark, HORESTA, Institut for Menneskerettigheder, IT-Branchen, IT-Politisk Forening, Justitia, KL, Norlys, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Retspolitisk Forening, Rigsombudsmanden i Grønland, Rigsombudsmanden på Færøerne, Rigsrevisionen, Rådet for Digital Sikkerhed, samtlige byretspræsidenter, TDC, TeleDCIS, Teleindustrien (TI), Telenor, Telia Company Danmark, Tilsynet med Efterretningstjenesterne, TT-Netværket, TV 2 DTT og Waoo.

11. Sammenfattende skema

	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang/Hvis nej, anfør »Ingen«)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang/Hvis nej, anfør »Ingen«)
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen.	Lovforslaget indebærer, at Center for Cybersikkerhed skal varetage nye opgaver, som dog afholdes indenfor Forsvarsministeriets eksisterende ramme. Desuden vil lovforslaget indebære, at der kan træffes afgørelser om ekspropriation, der i det konkrete tilfælde vil skulle ske mod, at staten yder fuldstændig erstatning for det eventuelle tab, som afgørelsen måtte medføre for den pågældende teleudbyder eller leverandør.
Implementeringskonsekvenser for stat, kommuner og regioner	Ingen.	Ingen væsentlige.
Økonomiske konsekvenser for erhvervslivet	Ingen.	Lovforslaget kan medføre økonomiske konsekvenser for teleudbyderne og leverandørerne, hvis der træffes afgørelse om forbud mod indgåelse af aftaler, mod opretholdelse af aftaler eller om forbud mod fortsat anvendelse af kritiske netkomponenter, systemer eller værktøjer. I de forventeligt sjældne tilfælde,

		hvor afgørelserne har karakter af ekspropriation, vil dette dog ske mod fuldstændig erstatning. Lovforslaget vil endvidere kunne medføre en reduceret konkurrence, fordi teleudbyderne vil kunne vælge mellem færre leverandører, hvilket vil kunne medføre stigende priser og eventuelt have negativ effekt på innovationen på teleområdet.
Administrative konsekvenser for erhvervslivet	Ingen.	Lovforslaget forventes at kunne få administrative konsekvenser for teleudbydere og deres leverandører, såfremt et forbud medfører behov for at gennemføre et nyt udbud eller en ny aftaleforhandling.
Administrative konsekvenser for borgerne	Ingen.	Ingen.
Klima- og miljømæssige konsekvenser	Ingen.	Ingen.
Forholdet til EU-retten	Efter Traktaten om Den Europæiske Union er området for national sikkerhed den enkelte medlemsstats eneansvar. Ved udøvelsen af dette eneansvar skal medlemsstaterne dog overholde de frie bevægeligheder i Traktaten om Den Europæiske Unions Funktionsmåde (TEUF). De EU-retlige rammer for den foreslåede forbudsordning sættes bl.a. af TEUF artikel 49 om den frie etableringsret og TEUF artikel 63 om de frie kapitalbevægelser. Det vurderes ikke, at TEUF er til hinder for den foreslåede ordning. Radioudstyrsdirektivet har til formål at sikre fri bevægelighed for radioudstyr i EU's indre marked, hvis radioudstyret opfylder de krav, som fremgår af direktivet. Direktivet vurderes ikke at være til hinder for den foreslåede ordning. EU's telekodeks fastsætter endvidere den EU-retlige ramme for regulering af teleområdet. Det er vurderingen, at EU's telekodeks ikke er til hinder for den foreslåede ordning.	
Er i strid med de fem principper for implementering af	Ja	Nej X

erhvervsrettet EU-regulering / Går videre end mini-mumskrav i EU-regulering (sæt X)		

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Den foreslåede *§ 1* definerer tre centrale begreber i loven. Begreberne svarer til de gældende definitioner i lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed samt bekendtgørelse nr. 1256 af 27. november 2019 om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed og skal fortolkes i overensstemmelse hermed.

Efter *§ 1, nr. 1,* defineres "kritiske netkomponenter, systemer og værktøjer" som operations support systemer, network management systemer og business support systemer, der kan benyttes til at aflæse, ændre indhold af eller dirigere data, som relaterer sig til slutbrugere, samt hardware, firmware og software, der anvendes i eller i forbindelse med core-net i mobilnet, fastnet og internet, eller i centrale routere og servere i backbonenettene eller i kontrolenheder, som anvendes til styring i mobilnettenes radionet.

Definitionen omfatter de tekniske enheder og systemer i teleinfrastrukturen, der vurderes som værende særligt kritiske og dermed særligt beskyttelsesværdige.

Definitionen er identisk med definitonen i § 1, nr. 1, i bekendtgørelsen om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed. Dette skal ses i lyset af, at dette lovforslags ordning vil udgøre en overbygning på den underretningsordning, som er udmøntet i bekendtgørelsen, og som indebærer, at væsentlige erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester skriftligt skal underrette Center for Cybersikkerhed forud for, at der indledes forhandlinger om aftaler, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf. Med lovforslaget vil der blive skabt mulighed for at nedlægge forbud mod samme type aftaler, jf. bemærkningerne til de foreslåede §§ 2 og 3 samt afsnit 3.1 i de almindelige bemærkninger.

Definitionen omfatter bl.a. operations support systemer, der er en samling af softwaresystemer, som bruges til at designe, implementere og drive telenetværkene (både tale og data). Systemerne bruges endvidere i forbindelse med driften til at sikre kundeforbindelserne, så de fungerer efter hensigten. Endvidere omfattes network management systemer, der ofte er tæt integreret til operations support systemerne og anvendes til teknisk at overvåge og styre driften af alle typer af netværk hos teleudbyderne, herunder sikre forbindelserne internt og mellem forskellige teleudbydere. Ligeledes indgår business support systemer, der er tæt integreret til operations support systemerne og har til formål at styre alle kundeforhold, herunder oprettelse og nedlæggelse af abonnementer og forbindelser, samt kundesupport. Business support systemerne anvendes også til afregning af kundens forbrug og til at skabe grundlaget for forretningsudvikling for teleudbyderne ved hjælp af avancerede økonomisystemer (Business Intelligence).

Desuden omfatter definitionen radionet/radio access net (RAN), der er den del af et mobilnet, som består af master med radiobasestationer og dataforbindelser til core-nettet. Det er via radionettet, at en mobiltelefon får trådløs adgang til mobilnettet, som derefter sørger for at skabe forbindelse til eksempelvis en anden telefon eller til internettet. Et radionet i Danmark består typisk af flere tusinde radiobasestationer, der geografisk er spredt ud over hele landet for at sikre den bedst mulige dækning.

Core-net i mobilnet består af et større antal forskellige tekniske enheder (servere, routere og fysiske netværk), som binder mobilnetværket sammen. Operations support systemerne og business support systemerne er normalt integreret direkte ind i core-nettet.

Centrale routere og servere i backbonenettene er de vigtige højkapacitetsdataenheder, der sikrer, at datatrafikken sendes de rigtige steder hen, både i egne netværk og til andre teleudbyderes netværk.

Efter *§ 1, nr. 2,* defineres "slutbruger" som en bruger af net og tjenester, som ikke på kommercielt grundlag stiller de pågældende net og tjenester til rådighed for andre.

Definitionen er identisk med definitonen i § 1, nr. 2, i bekendtgørelsen om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed. Definition svarer med få sproglige forskelle til samme definition i lov om elektroniske kommunikationsnet og -tjenester (teleloven), jf. lovbekendtgørelse nr. 128 af 7. februar 2014 med senere ændringer, og skal fortolkes i overensstemmelse med definitionen af slutbruger i Europa-Parlamentet og Rådets direktiv 2018/1972/EU af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation.

Ved net forstås transmissionssystemer, uanset om det bygger på en permanent infrastruktur eller en centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, elkabelsystemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til radio- og tv-spredning, og kabel-tv-net, uanset hvilken type information der overføres. Net omfatter således alle transmissionssystemer, uanset om de bygger på en permanent infrastruktur eller en centraliseret administrationskapacitet. Ved tjenester forstås elektroniske kommunikationstjenester, der helt eller delvis består i elektronisk overføring af kommunikation i form af lyd, billeder, tekst eller kombinationer heraf ved hjælp af radio- eller telekommunikationsteknik mellem nettermineringspunkter. Et nettermineringspunkt er et fysisk punkt, hvor en slutbruger får adgang til et offentligt elektronisk kommunikationsnet og som for net, hvor der anvendes kobling eller routing, identificeres ved hjælp af en specifik netadresse, som kan være knyttet til slutbrugerens nummer eller navn.

Net skal desuden forstås i overensstemmelse med definitionen af elektronisk kommunikationsnet i telelovens § 2, nr. 4, tjenester skal forstås i overensstemmelse med definitionen af elektronisk kommunikationstjeneste i telelovens § 2, nr. 7, og net-termineringspunkt skal forstås i overensstemmelse med telelovens § 2, nr. 8.

Slutbrugere skal anses som en modsætning til udbydere af elektroniske kommunikationsnet eller -tjenester og kan omfatte såvel erhvervsdrivende som ikke-erhvervsdrivende brugere af elektroniske kommunikationsnet eller -tjenester, herunder storkunder og lignende, som i et vist omfang vælger at etablere deres egen elektroniske kommunikationsinfrastruktur og sammenkoble denne med offentlige elektroniske kommunikationsnet med henblik på udveksling af trafik.

Også udbydere af informations- og indholdstjenester anses for slutbrugere. Det samme gælder f.eks. radio- og tv-virksomheder og andre virksomheder med særlige kommunikationsbehov.

Efter *§ 1, nr. 3,* defineres "væsentlige erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester" som a) udbydere af net, hvor disse net anvendes af mere end 50.000 slutbrugere. Ved opgørelsen medregnes de slutbrugere, der har aftaleforhold med udbyderens kunder. Radio- og tv-stationer, der er udbydere af net, er kun omfattet, såfremt de har landsdækkende public service-forpligtelser samt b) udbydere, der gennem aftaler med statslige myndigheder og institutioner betjener mere end 500 slutbrugere. Ved opgørelsen medregnes de statslige myndigheder og institutioners egne slutbrugere.

Definitionen er identisk med definitonen i § 1, nr. 3, i bekendtgørelsen om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed.

En udbyder er den, der med et kommercielt formål stiller produkter, net eller tjenester omfattet af teleloven til rådighed for andre.

Væsentlige erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester omfatter ikke udbydere af nummeruafhængige interpersonelle kommunikationstjenester (NUIK-tjenester).

Ved net forstås transmissionssystemer, uanset om det bygger på en permanent infrastruktur eller en centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, elkabelsystemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til radio- og tv-spredning, og kabel-tv-net, uanset hvilken type information der overføres. Net omfatter således alle transmissionssystemer, uanset om de bygger på en permanent infrastruktur eller en centraliseret administrationskapacitet. Ved tjenester forstås elektroniske kommunikationstjenester, der helt eller delvis består i elektronisk overføring af kommunikation i form af lyd, billeder, tekst eller kombinationer heraf ved hjælp af radio- eller telekommunikationsteknik mellem nettermineringspunkter. Et nettermineringspunkt er et fysisk punkt, hvor en slutbruger får adgang til et offentligt elektronisk kommunikationsnet og som for net, hvor der anvendes kobling eller routing, identificeres ved hjælp af en specifik netadresse, som kan være knyttet til slutbrugerens nummer eller navn.

Net skal desuden forstås i overensstemmelse med definitionen af elektronisk kommunikationsnet i telelovens § 2, nr. 4, tjenester skal forstås i overensstemmelse med definitionen af elektronisk kommunikationstjeneste i telelovens § 2, nr. 7, og nettermineringspunkt skal forstås i overensstemmelse med telelovens § 2, nr. 8.

Bestemmelsen indebærer desuden, at der ved opgørelsen af, hvor mange slutbrugere, der anvender et givent net, medregnes de slutbrugere, der har aftaleforhold med udbyderens kunder. Derved tages der højde for den situation, hvor en udbyder leverer net til en anden udbyder, der på kommercielt grundlag stiller de pågældende net til rådighed for et stort antal privatpersoner.

I forhold til de udbydere, der betjener statslige myndigheder og institutioner, vil der ved beregningen af, hvor mange slutbrugere, der betjenes, skulle tages højde for de statslige myndigheder og institutioners egne slutbrugere. I det tilfælde, hvor en udbyder f.eks. leverer tjenester til Forsvaret, vil Forsvaret kun udgøre én slutbruger efter den gængse forståelse af begrebet. Efter den foreslåede bestemmelse vil de af Forsvarets medarbejdere, der gør brug af tjenesterne, imidlertid tælle med i opgørelsen af antallet af slutbrugere.

Til § 2

Det foreslås med *§ 2, stk. 1,* at Center for Cybersikkerhed i særlige tilfælde kan forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige net og tjenester at indgå en aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf, såfremt aftalen vurderes at udgøre en trussel mod statens sikkerhed. Ved vurderingen heraf kan Center for Cybersikkerhed særligt lægge vægt på forhold vedrørende den leverandør, som udbyderen ønsker at anvende.

Bestemmelsen vil typisk finde anvendelse, efter at der gennem længere tid har været dialog mellem teleudbyderen og Center for Cybersikkerhed om den pågældende aftale. Bestemmelsens anvendelsesområde svarer således til anvendelsesområdet for den særlige underretningsordning, der er etableret i medfør af lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed. Der er dermed tale om aftaler, hvor teleudbyderne i medfør af §§ 3 og 4 i bekendtgørelse nr. 1256 af 27. november 2019 om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed har underrettet Center for Cybersikkerhed forud for, at forhandlingerne om aftalen er indledt med leverandøren, hvorefter Center for Cybersikkerhed typisk vil have rådgivet teleudbyderen om sikkerhedsmæssige aspekter af den pågældende aftale. Herefter vil Center for Cybersikkerhed typisk have udstedt et påbud om, at det endelige udkast til aftalen skal fremsendes til centeret, eller en sådan fremsendelse vil være sket frivilligt. Ved udstedelse af påbud vil aftalen først kunne indgås, når der er modtaget tilbagemelding fra Center for Cybersikkerhed, hvilket skal være sket senest 25 arbejdsdage efter modtagelsen af aftaleudkastet, jf. den foreslåede ændring af net- og informationssikkerhedsloven i § 18, nr. 1.

I de situationer, hvor bestemmelsen vil finde anvendelse, vil der oftest være tale om, at en teleudbyder ikke har ønsket at følge rådgivningen fra Center for Cybersikkerhed, og at det endelige udkast til aftale derfor på væsentlige punkter ikke tager højde for rådgivningen – og at aftalen på den baggrund vurderes at udgøre en trussel mod statens sikkerhed. Bestemmelsen vil dog også finde anvendelse i situationer, hvor et endeligt aftaleudkast ikke er fremsendt til Center for Cybersikkerhed, men hvor centeret på anden vis er blevet opmærksom på en forestående aftaleindgåelse, f.eks. gennem medieomtale eller gennem oplysninger fra andre myndigheder. Det vil dog påhvile Center for Cybersikkerhed at sikre, at sagen er tilstrækkeligt oplyst til, at der kan træffes afgørelse om et forbud, og dermed vil et forbud normalt ikke alene kunne baseres på f.eks. medieomtale.

Bestemmelsen omfatter både indgåelse af nye aftaler og forlængelse af eksisterende aftaler. Hvis aftalen indeholder en option, der indebærer, at aftalen kan forlænges på helt uændrede vilkår, vil en sådan forlængelse dog ikke være omfattet, men aftalen vil dog være omfattet af den foreslåede § 3. Retsvirkningen af, at der nedlægges forbud mod en aftale, vil være, at såfremt aftalen alligevel indgås, vil dette være strafbart efter den foreslåede § 15, ligesom aftalen vil være ugyldig mellem parterne, jf. den foreslåede § 16.

Center for Cybersikkerhed vil skulle foretage en samlet vurdering af, om aftalen må anses for at udgøre en trussel mod statens sikkerhed. Ved vurderingen heraf vil Center for Cybersikkerhed tage udgangspunkt i en række objektive kriterier i bestemmelsens nr. 1-4, jf. nedenfor. Udtrykket statens sikkerhed anvendes i net- og informationssikkerhedsloven og skal forstås i overensstemmelse med det EU-retlige udtryk den nationale sikkerhed. Der vil dermed som udgangspunkt skulle være tale om trusler mod samfundskritiske funktioner og deres kommunikation, herunder deres medarbejderes kommunikation. Er der alene tale om en trussel om, at der kan ske industrispionage mod private virksomheder, vil det falde udenfor anvendelsesområdet, med mindre industrispionagen har en karakter, hvor den kan udgøre en trussel mod statens sikkerhed, f.eks. hvis der er tale om industrispionage mod virksomheder i forsvarsindustrien eller forskningsindustrien.

Kerneområdet vil være situationer, hvor Center for Cybersikkerhed vurderer, at en aftale vil indebære, at der er risiko for, at en leverandør vil misbruge aftalen til at forberede eller udføre sabotage mod telenettet, som kan medføre, at telenettet helt eller delvist afbrydes. Det vil f.eks. kunne være tilfældet, hvis aftalen omfatter leverancer, hvor Center for Cybersikkerhed vurderer, at der er risiko for, at leverandøren indbygger bagdøre, som gør det muligt for leverandøren at afbryde eller på anden måde foretage uautoriseret påvirkning af dele af telenettet. Det vil også være tilfældet, hvis aftalen omfatter drift af systemer, hvor der er risiko for, at leverandøren gennem adgangen til systemerne vil foretage en hel eller delvis afbrydelse.

Der vil endvidere kunne være tale om situationer, hvor Center for Cybersikkerhed vurderer, at en aftale vil indebære risiko for, at en leverandør vil misbruge aftalen til at foretage spionage mod samfundskritiske funktioner, herunder deres medarbejderes eller samarbejdspartneres kommunikation.

Ved vurderingen vil Center for Cybersikkerhed kunne tage højde for forhold, der både vedrører leverandøren, leverandørens væsentligste underleverandører samt aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren. De væsentligste underleverandører vil være de underleverandører, som leverer en ikke ubetydelig del af den samlede leverance. Aktører, der udøver kontrol over eller betydelig indflydelse på leverandøren, vil være aktører, der direkte eller indirekte er i besiddelse af eller har kontrol over ejerandele eller stemmerettigheder i en virksomhed, eller har tilsvarende kontrol ved andre midler, herunder langfristede lån, som giver betydelig indflydelse på ledelsesmæssige, finansielle eller udviklings- eller driftsmæssige forhold.

Det er således ikke en forudsætning, at leverandøren selv vurderes at udgøre en trussel mod statens sikkerhed. Aftalen vil f.eks. også kunne anses for at udgøre en trussel, hvis leverandøren planlægger at opfylde aftalen ved brug af kritiske komponenter fra en underleverandør, hvor Center for Cybersikkerhed vurderer, at der er risiko for, at der er indbygget bagdøre eller tilsvarende. Centeret vil endvidere kunne foretage en vurdering af, om leverandørens ejerforhold m.v. gør, at aftalen må anses for at udgøre en trussel mod statens sikkerhed. Et element i vurderingen vil således være, om f.eks. et moderselskab, gennem dettes historik eller tilhørsforhold bidrager til en trussel, som medfører, at der bør nedlægges forbud mod aftalen.

Center for Cybersikkerhed vil som nævnt skulle foretage en samlet vurdering. Her vil den potentielle trussel og dennes karakter også skulle vejes op mod aftalens karakter. Jo mere kritiske dele af telenettet, som aftalen omfatter, jo mindre skal der til, for at der kan siges at

være tale om en trussel mod statens sikkerhed. Der kan dermed også efter en konkret vurdering være tale om, at leverandøren og dennes forhold gør, at leverandøren vil kunne udgøre en trussel mod statens sikkerhed, men at de leverancer, som aftalen omfatter, skal anvendes på en måde, som gør det usandsynligt, at der kan ske misbrug.

Centeret vil endvidere kunne lægge vægt på, om et forbud vil kunne have negative konsekvenser for telenettets drift, som overstiger de potentielt negative konsekvenser, hvis den vurderede trussel bliver en realitet. Det kan f.eks. være tilfældet, hvis et forbud mod en aftale gør, at teleudbyderen ikke kan nå at indgå en anden aftale, og hvor konsekvensen dermed kan være, at der sker alvorlige udfald i driften af telenettet. Typisk vil der i sådanne tilfælde have været en forudgående dialog mellem Center for Cybersikkerhed og teleudbyderen, hvor centeret vil have tilkendegivet, hvad den maksimale løbetid på aftalen bør være. Hvis det endelige aftaleudkast indebærer en længere løbetid, må teleudbyderen således påregne, at der kan blive nedlagt forbud mod aftaleindgåelsen.

I vurderingen vil det efter den foreslåede *stk. 1, nr. 1,* bl.a. kunne indgå, om leverandøren, leverandørens væsentligste underleverandører samt aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren, er hjemmehørende i eller varetager produktionen eller driften fra et land, som Danmark ikke har indgået en sikkerhedsaftale med, eller som Danmark ikke har et tilsvarende sikkerhedsmæssigt samarbejde med.

Sikkerhedsaftaler indgås i forskellige former. Typisk vil sikkerhedsaftaler indeholde nærmere bestemmelser om, hvordan landene som led i samarbejdet skal behandle klassificerede eller på anden måde følsomme oplysninger. Sikkerhedsaftaler indgås derfor typisk kun med lande, der anvender samme principper for håndtering af klassificerede oplysninger som Danmark. Sikkerhedsaftaler vil imidlertid også kunne indgås som specifikke aftaler vedrørende informationssikkerhed på teleområdet.

Bestemmelsen omfatter også tilsvarende sikkerhedssamarbejder, hvor der ikke nødvendigvis er indgået en formel sikkerhedsaftale. Mere indirekte sikkerhedssamarbejder, der f.eks. indgås via internationale organisationer, vil ikke være omfattet af begrebet tilsvarende sikkerhedssamarbejder.
En eventuel fastlæggelse, af hvilket land leverandøren, underleverandøren eller aktøren er hjemmehørende i, foretages af Center for Cybersikkerhed efter en konkret vurdering. En leverandør, underleverandør eller aktør kan ikke anses for at være hjemmehørende i flere lande samtidigt.

Ved vurderingen, af hvilket land leverandøren, underleverandøren eller aktøren er hjemmehørende i, vil der for fysiske personer blive lagt vægt på, hvilket land den pågældende er statsborger i, og hvor den pågældende er bosat. For juridiske personer vil der ved vurderingen blive lagt særlig vægt på, hvor virksomheden er registreret. Desuden kan der bl.a. lægges vægt på, hvor virksomhedens eventuelle hovedkontor er placeret, hvorfra ledelsesmæssige beføjelser udøves, og hvor medlemmer af direktionen og bestyrelsen er hjemmehørende.

Ved vurderingen af, hvorfra varetagelsen af driften sker, kan der bl.a. lægges vægt på placeringen af de medarbejdere, der udfører de konkrete drifts- og supportopgaver.

Vurderingen af, hvilket land leverandøren, underleverandøren eller aktøren er hjemmehørende i, vil kunne ændres med tiden, hvis deres forhold ændrer sig.

Efter den foreslåede *stk. 1, nr. 2,* vil det bl.a. også kunne indgå, om leverandøren, leverandørens væsentligste underleverandører samt aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren, er hjemmehørende i eller varetager produktionen eller driften fra et land, hvor det efter lovgivningen er muligt at pålægge leverandører eller deres underleverandører at udføre eller deltage i forhold, som vil udgøre spionage eller sabotage.

Ved anvendelse af bestemmelsen vil der skulle tages højde for, at forskellige lande har forskellige lovgivningstraditioner. Der vil således kunne ses bort fra ældre bestemmelser, der formelt er gældende, men som efter det pågældende lands lovgivningstradition ikke vil kunne anvendes. Omvendt vil der kunne lægges vægt på en fast administrativ praksis, der giver mulighed for give pålæg om at udføre spionage eller sabotage, hvis det pågældende lands lovgivningstradition indebærer, at reguleringen er bindende, selv om der ikke er en udtrykkelig lovhjemmel. En eventuel fastlæggelse, af hvilket land leverandøren, underleverandøren eller aktøren er hjemmehørende i, foretages af Center for Cybersikkerhed efter en konkret vurdering. En leverandør, underleverandør eller aktør kan ikke anses for at være hjemmehørende i flere lande samtidigt.

Ved vurderingen, af hvilket land leverandøren, underleverandøren eller aktøren er hjemmehørende i, vil der for fysiske personer blive lagt vægt på, hvilket land den pågældende er statsborger i, og hvor den pågældende er bosat. For juridiske personer vil der ved vurderingen blive lagt særlig vægt på, hvor virksomheden er registreret. Desuden kan der bl.a. lægges vægt på, hvor virksomhedens eventuelle hovedkontor er placeret, hvorfra ledelsesmæssige beføjelser udøves, og hvor medlemmer af direktionen og bestyrelsen er hjemmehørende.

Ved vurderingen af, hvorfra varetagelsen af driften sker, kan der bl.a. lægges vægt på placeringen af de medarbejdere, der udfører de konkrete drifts- og supportopgaver.

Vurderingen af, hvilket land leverandøren, underleverandøren eller aktøren er hjemmehørende i, vil kunne ændres med tiden, hvis deres forhold ændrer sig.

Efter den foreslåede *stk. 1, nr. 3,* vil det bl.a. også kunne indgå, om leverandøren, leverandørens væsentligste underleverandører samt aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren, direkte eller indirekte kontrolleres af et andet lands statslige organer, herunder militære myndigheder.

Ved vurderingen af, hvilken vægt der skal lægges på, at et andet lands statslige organer direkte eller indirekte kontrollerer en leverandør m.v., vil det skulle indgå, om en sådan kontrol vurderes at indebære en øget trussel mod statens sikkerhed. Det forhold, at en leverandør måtte være statsejet, vil således ikke automatisk medføre, at indgåelse af en aftale med den pågældende leverandør vil udgøre en trussel mod statens sikkerhed.

Efter den foreslåede *stk. 1, nr. 4,* vil det bl.a. også kunne indgå, om leverandøren, leverandørens væsentligste underleverandører samt aktører, der udøver kontrol over eller betydelig indflydelse på leverandøren, er eller tidligere har været involveret i aktiviteter i Danmark eller andre lande, som har medført en negativ påvirkning af statens sikkerhed, informationssikkerheden eller den offentlige orden.

Kerneområdet for bestemmelsen vil være situationen, hvor det i udlandet er blevet konstateret, at en leverandør f.eks. har leveret udstyr med indbyggede bagdøre eller på anden vis har foretaget eller forberedt spionage eller sabotage mod telenettet.

Efter det foreslåede s*tk. 2* kan Center for Cybersikkerhed kun nedlægge forbud efter det foreslåede stk. 1, hvis hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger.

Bestemmelsen udtrykker et proportionalitetsprincip, hvorefter Center for Cybersikkerhed forud for nedlæggelse af et forbud mod en aftale skal have søgt at opnå det ønskede resultat gennem mindre indgribende midler. Det vil således være en forudsætning, at Center for Cybersikkerhed har forsøgt at rådgive teleudbyderen om de tilpasninger af aftalen, som vil være nødvendige, for at den ikke længere vurderes at udgøre en trussel mod statens sikkerhed. Center for Cybersikkerhed vil også skulle have vurderet de relevante muligheder i net- og informationssikkerhedsloven, herunder eksempelvis muligheden for at give påbud om, at teleudbyderen skal foretage konkrete sikkerhedsforanstaltninger.

Der henvises i øvrigt til afsnit 3.1 i de almindelige bemærkninger.

Til § 3

Det foreslås med *§ 3*, *stk. 1,* at Center for Cybersikkerhed i særlige tilfælde kan forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at opretholde en indgået aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelsen af driften heraf, såfremt opretholdelse af aftalen vurderes at udgøre en væsentlig trussel mod statens sikkerhed. Ved vurderingen heraf kan Center for Cybersikkerhed særligt lægge vægt på forhold vedrørende leverandøren, leverandørens væsentligste underleverandører samt aktører, der udøver kontrol over eller betydelig indflydelse på leverandøren.

Mens den foreslåede § 2 finder anvendelse forud for, at en aftale er indgået, så er anvendelsesområdet for den foreslåede § 3, stk. 1, de situationer, hvor der allerede er indgået en aftale. Der vil være tale om aftaler, der er indgået den 7. december 2020 eller senere, idet anvendelsesområdet dog fra 1. januar 2026 udvides til at omfatte alle aftaler, også aftaler indgået før den 7. december 2020, jf. de foreslåede bestemmelser i § 17, stk. 2 og 3.

Bestemmelsen vil først og fremmest finde anvendelse, hvis det ved aftaleindgåelsen er blevet vurderet, at der ikke har været grundlag for at nedlægge forbud mod aftalen efter den foreslåede § 2, men der efterfølgende er sket en ændring, som gør, at der ville været blevet nedlagt forbud, hvis de ændrede forhold havde været en realitet ved aftaleindgåelsen. Disse forhold skal dog udgøre en væsentlig trussel mod statens sikkerhed, hvilket er et skærpet krav i forhold til kravet i den foreslåede § 2. For at der foreligger en væsentlig trussel mod statens sikkerhed, vil det være et krav, at truslen er mere konkretiseret. Ændrede forhold kan f.eks. være, at leverandøren har skiftet ejer, at det efter aftaleindgåelsen er konstateret, at leverandøren negativt har påvirket informationssikkerheden i forbindelse med sammenlignelige aftaler i udlandet, eller at der er sket ændringer i lovgivningen i leverandørens hjemland, således at leverandøren kan pålægges at udføre spionage og sabotage.

Center for Cybersikkerhed vil typisk få oplysninger om ændrede forhold som led i centerets tilsynsvirksomhed efter net- og informationssikkerhedsloven, fra den efterretningsmæssige del af Forsvarets Efterretningstjeneste, fra andre relevante myndigheder i ind- og udland, herunder som led i udvekslingen af oplysninger om screeninger af direkte investeringer i andre EU-lande, samt fra medieomtale.

Bestemmelsen vil imidlertid også finde anvendelse på aftaler, der ikke tidligere er blevet vurderet efter § 2. Det kan både være aftaler, der er indgået i perioden fra lovens virkningstidspunkt til lovens ikrafttræden, og aftaler, der omfattes af lovforslagets ordning, når anvendelsesområdet fra 1. januar 2026 udvides til at omfatte aftaler, der er indgået før den 7. december 2020.

Hvis en aftale tidligere har været vurderet efter den foreslåede § 2, er det en forudsætning for anvendelse af bestemmelsen, at der er sket en ændring af forhold vedrørende leverandøren m.v. Hvis der alene er tale om, at Center for Cybersikkerhed anlægger en anden vurdering af forhold, der allerede var kendt ved en vurdering efter § 2 forud for aftaleindgåelsen, vil der ikke kunne nedlægges forbud efter den foreslåede bestemmelse.

Center for Cybersikkerhed vil skulle foretage en samlet vurdering af, om aftalen må anses for at udgøre en væsentlig trussel mod statens sikkerhed. Udtrykket statens sikkerhed anvendes i net- og informationssikkerhedsloven og skal forstås i overensstemmelse med det EU-retlige udtryk den nationale sikkerhed. Der vil dermed som udgangspunkt skulle være tale om væsentlige trusler mod samfundskritiske funktioner, herunder deres medarbejderes kommunikation. Er der alene tale om en væsentlig trussel om, at der kan ske industrispionage mod private virksomheder, vil det falde udenfor anvendelsesområdet, med mindre industrispionagen har en karakter, hvor den kan udgøre en væsentlig trussel mod statens sikkerhed, f.eks. hvis der er tale om industrispionage mod virksomheder i forsvarsindustrien eller forskningsindustrien.

Kerneområdet vil være situationer, hvor Center for Cybersikkerhed vurderer, at en leverandør nu vil misbruge aftalen til at forberede eller udføre sabotage mod telenettet, som kan medføre, at telenettet helt eller delvist afbrydes. Det vil f.eks. kunne være tilfældet, hvis aftalen omfatter leverancer, hvor Center for Cybersikkerhed vurderer, at der nu er risiko for, at leverandøren indbygger bagdøre, som gør det muligt for leverandøren at afbryde eller på anden måde foretage uautoriseret påvirkning af dele af telenettet. Det vil også være tilfældet, hvis aftalen omfatter drift af systemer, hvor der nu vurderes at være risiko for, at leverandøren gennem adgangen til systemerne vil foretage en hel eller delvis afbrydelse.

Der vil endvidere kunne være tale om situationer, hvor Center for Cybersikkerhed vurderer, at aftalen indebærer risiko for, at en leverandør nu vil misbruge aftalen til at foretage spionage mod samfundskritiske funktioner, herunder deres medarbejderes eller samarbejdspartneres kommunikation.

Ved vurderingen vil Center for Cybersikkerhed kunne tage højde for forhold, der både vedrører leverandøren, leverandørens væsentligste underleverandører samt aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren. De væsentligste underleverandører vil være de underleverandører, som leverer en ikke ubetydelig del af den samlede leverance. Aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren, vil være aktører, der direkte eller indirekte er i besiddelse af eller har kontrol over ejerandele eller stemmerettigheder i en virksomhed eller tilsvarende kontrol ved andre

midler, herunder langfristede lån, som giver betydelig indflydelse på ledelsesmæssige, finansielle eller udviklings- eller driftsmæssige forhold.

Det er således ikke en forudsætning, at leverandøren selv vurderes at udgøre en væsentlig trussel mod statens sikkerhed. Aftalen vil f.eks. også kunne anses for at udgøre en væsentlig trussel, hvis leverandøren planlægger at opfylde aftalen ved brug af kritiske komponenter fra en underleverandør, hvor Center for Cybersikkerhed nu vurderer, at der er risiko for, at der er indbygget bagdøre eller tilsvarende. Centeret vil endvidere kunne foretage en vurdering af, om leverandørens ejerforhold m.v. gør, at aftalen nu må anses for at udgøre en væsentlig trussel mod statens sikkerhed. Et element i vurderingen vil således være, om f.eks. et moderselskab gennem dettes historik eller lignende bidrager til en væsentlig trussel, som gør, at der bør nedlægges forbud mod aftalen.

Center for Cybersikkerhed vil som nævnt skulle foretage en samlet vurdering. Her vil den potentielle trussel og dennes karakter også skulle vejes op mod aftalens karakter. Jo mere kritiske dele af telenettet, som aftalen omfatter, jo mindre skal der til, for at der kan siges at være tale om en væsentlig trussel mod statens sikkerhed. Der kan dermed også efter en konkret vurdering være tale om, at leverandøren og dennes forhold gør, at leverandøren vil kunne udgøre en væsentlig trussel mod statens sikkerhed, men at de leverancer, som aftalen omfatter, skal anvendes på en måde, som gør det usandsynligt, at der kan ske misbrug.

Centeret vil endvidere kunne lægge vægt på, om et forbud vil kunne have negative konsekvenser for telenettets drift, som overstiger de potentielt negative konsekvenser, hvis den vurderede trussel bliver en realitet. Det kan f.eks. være tilfældet, hvis et forbud mod en aftale gør, at teleudbyderen ikke kan nå at indgå en anden aftale, og hvor konsekvensen dermed kan være, at der sker alvorlige udfald i driften af telenettet. I så fald vil der dog kunne tages højde for problemstillingen ved fastsættelse af fristen efter det foreslåede stk. 3.

Retsvirkningen af, at der nedlægges forbud mod en aftale, vil være, at aftalen bliver ugyldig mellem parterne, jf. den foreslåede § 16. Såfremt aftalen videreføres, vil dette være strafbart efter den foreslåede § 15.

Det foreslås med *stk. 2,* at Center for Cybersikkerhed endvidere i særlige tilfælde kan forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester fortsat at anvende kritiske netkomponenter, systemer og værktøjer, der tidligere er leveret, såfremt fortsat anvendelse vurderes at udgøre en væsentlig trussel mod statens sikkerhed. Ved vurderingen heraf kan Center for Cybersikkerhed særligt lægge vægt på forhold vedrørende leverandøren, leverandørens væsentligste underleverandører samt aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren.

Bestemmelsens anvendelsesområde er situationer, hvor en teleudbyder tidligere har fået leveret kritiske komponenter, systemer m.v. som led i en aftale med en leverandør, men hvor aftalen ikke længere er aktiv, f.eks. fordi den alene omfattede den nu gennemførte leverance. Situationen vil i så fald ikke være omfattet af det foreslåede stk. 2. Bestemmelsen giver Center for Cybersikkerhed mulighed for at nedlægge forbud mod, at teleudbyderen fortsat anvender de leverede kritiske komponenter, systemer m.v., hvis den fortsatte anvendelse vurderes at udgøre en væsentlig trussel mod statens sikkerhed.

Bestemmelsen omfatter kritiske komponenter, systemer m.v., der er leveret som led i aftaler, der er indgået den 7. december 2020 eller senere, idet anvendelsesområdet dog fra 1. januar 2026 udvides til at omfatte leverancer, der er sket som led i alle aftaler, også aftaler indgået før den 7. december 2020, jf. den foreslåede § 17, stk. 2 og 3.

Bestemmelsen vil først og fremmest finde anvendelse, hvis det ved aftaleindgåelsen er blevet vurderet, at der ikke har været grundlag for at nedlægge forbud mod aftalen efter den foreslåede § 2, men hvor der efterfølgende er sket en ændring, som gør, at der ville været blevet nedlagt forbud, hvis de ændrede forhold havde været en realitet ved aftaleindgåelsen. Disse forhold skal dog udgøre en væsentlig trussel mod statens sikkerhed, hvilket er et skærpet krav i forhold til kravet i den foreslåede § 2. For at der foreligger en væsentlig trussel mod statens sikkerhed, vil det være et krav, at truslen er mere konkretiseret. Ændrede forhold kan f.eks. være, at det efter aftaleindgåelsen er konstateret, at leverandøren negativt har påvirket informationssikkerheden i sammenlignelige komponenter, systemer m.v.

Bestemmelsen vil imidlertid også finde anvendelse på visse leverancer efter aftaler, der ikke tidligere er blevet vurderet efter § 2. Det kan både være aftaler, der er indgået i perioden fra lovens virkningstidspunkt til lovens ikrafttræden, og aftaler, der omfattes af lovforslagets ordning, når anvendelsesområdet fra 1. januar 2026 udvides til at omfatte aftaler, der er indgået før den 7. december 2020.

Hvis en aftale tidligere har været vurderet efter den foreslåede § 2, er det en forudsætning for anvendelse af bestemmelsen, at der er sket en ændring af forhold vedrørende leverandøren m.v. Hvis der alene er tale om, at Center for Cybersikkerhed anlægger en anden vurdering af forhold, der var kendt ved en vurdering efter § 2 forud for aftaleindgåelsen, vil der ikke kunne nedlægges forbud efter den foreslåede bestemmelse.

Center for Cybersikkerhed vil skulle foretage en samlet vurdering af, om komponenten, systemet m.v. må anses for at udgøre en væsentlig trussel mod statens sikkerhed. Udtrykket statens sikkerhed anvendes i net- og informationssikkerhedsloven og skal forstås i overensstemmelse med det EU-retlige udtryk den nationale sikkerhed. Der vil som udgangspunkt skulle være tale om væsentlige trusler mod samfundskritiske funktioner og deres kommunikation, herunder deres medarbejderes kommunikation. Er der alene tale om en væsentlig trussel om, at der kan ske industrispionage mod private virksomheder, vil det falde udenfor anvendelsesområdet, med mindre industrispionagen har en karakter, hvor det kan udgøre en væsentlig trussel mod statens sikkerhed, f.eks. hvis der er tale om industrispionage mod virksomheder i forsvarsindustrien eller forskningsindustrien.

Kerneområdet vil være situationer, hvor Center for Cybersikkerhed vurderer, at der nu er risiko for, at komponenten, systemet m.v. vil misbruges til at forberede eller udføre sabotage mod telenettet, som kan medføre, at telenettet helt eller delvist afbrydes. Det vil f.eks. kunne være tilfældet, hvis der er tale om kritiske komponenter, systemer m.v., hvor Center for Cybersikkerhed vurderer, at der nu er risiko for, at leverandøren har indbygget bagdøre, som gør det muligt for leverandøren at afbryde eller på anden måde foretage uautoriseret påvirkning af dele af telenettet.

Der vil endvidere kunne være tale om situationer, hvor Center for Cybersikkerhed vurderer, at fortsat brug af kritiske komponenter, systemer m.v. vil indebære risiko for, at en

leverandør nu vil misbruge dem til at foretage spionage mod samfundskritiske funktioner, herunder deres medarbejderes eller samarbejdspartneres kommunikation.

Ved vurderingen vil Center for Cybersikkerhed kunne tage højde for forhold, der både vedrører leverandøren, leverandørens væsentligste underleverandører samt aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren. De væsentligste underleverandører vil være de underleverandører, som leverer en ikke ubetydelig del af den samlede leverance. Aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren, vil være aktører, der direkte eller indirekte er i besiddelse af eller har kontrol over ejerandele eller stemmerettigheder i en virksomhed eller tilsvarende kontrol ved andre midler, herunder langfristede lån, som giver betydelig indflydelse på ledelsesmæssige, finansielle eller udviklings- eller driftsmæssige forhold.

Center for Cybersikkerhed vil som nævnt skulle foretage en samlet vurdering. Her vil den potentielle trussel og dennes karakter også skulle vejes op mod karakteren af komponenten, systemet m.v. Jo mere kritiske dele af telenettet, som komponenten, systemet m.v. anvendes i, jo mindre skal der til, for at der kan siges at være tale om en væsentlig trussel mod statens sikkerhed.

Centeret vil endvidere kunne lægge vægt på, om et forbud vil kunne have negative konsekvenser for telenettets drift, som overstiger de potentielt negative konsevenser, hvis den vurderede trussel bliver en realitet.

Det foreslås med *stk. 3,* at Center for Cybersikkerhed kan fastsætte en frist for, hvornår en aftale skal være afviklet efter stk. 1, og hvornår anvendelse af kritiske netkomponenter, systemer og værktøjer skal være ophørt efter stk. 2.

Det forudsættes, at Center for Cybersikkerhed efter høring af teleudbyderen foretager en vurdering af på den ene side behovet for hurtigst muligt at fjerne en væsentlig trussel mod statens sikkerhed, og på den anden side hensynet til den fortsatte og stabile drift af den kritiske teleinfrastruktur. Nedlæggelse af forbud bør således ikke føre til, at der sker afbrydelser på telenettet, fordi teleudbyderen ikke har haft mulighed for at indgå eller implementere en ny aftale. På den baggrund bør Center for Cybersikkerhed som udgangspunkt fastsætte en nærmere frist, som er baseret på, hvornår en loyalt agerende teleudbyder kan have taget de nødvendige forholdsregler.

I særligt alvorlige tilfælde, hvor der f.eks. konstateres et igangværende misbrug, vil Center for Cybersikkerhed dog kunne fastsætte, at aftalen skal afvikles straks, eller at anvendelsen skal ophøre straks.

Det foreslås med *stk. 4,* at Center for Cybersikkerhed kun kan nedlægge forbud efter stk. 1 og 2, hvis hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger.

Bestemmelsen udtrykker et proportionalitetsprincip, hvorefter Center for Cybersikkerhed forud for nedlæggelse af et forbud have søgt at opnå det ønskede resultat gennem mindre indgribende midler. Det vil således være en forudsætning, at Center for Cybersikkerhed har forsøgt at rådgive teleudbyderen om de tilpasninger af aftalen eller de sikkerhedsmæssige ændringer af kritiske komponenter, systemer m.v., som vil være nødvendige, for at der ikke længere vurderes at være en væsentlig trussel mod statens sikkerhed. Center for

Cybersikkerhed vil også skulle have overvejet de relevante muligheder i net- og informationssikkerhedsloven, herunder eksempelvis muligheden for at give påbud om, at teleudbyderen skal foretage konkrete sikkerhedsforanstaltninger.

Der henvises i øvrigt til afsnit 3.1 i de almindelige bemærkninger.

Til § 4

Den foreslåede *§ 4, stk. 1*, giver Center for Cybersikkerhed hjemmel til at ekspropriere privat ejendom, i det omfang det er nødvendigt for at gennemføre et forbud efter det foreslåede kapitel 2 om nedlæggelse af forbud vedrørende visse leverancer til den kritiske teleinfrastruktur.

Det følger af den foreslåede § 2, stk. 1, at Center for Cybersikkerhed i særlige tilfælde kan forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige net og tjenester at indgå en aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf, såfremt aftalen vurderes at udgøre en trussel mod statens sikkerhed. Ved vurderingen heraf skal Center for Cybersikkerhed særligt lægge vægt på forhold vedrørende den leverandør, som teleudbyderen ønsker at anvende. Efter den foreslåede § 2, stk. 2, kan Center for Cybersikkerhed kun nedlægge forbud efter bestemmelsens stk. 1, hvis hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger.

Center for Cybersikkerhed kan endvidere efter § 3, stk. 1, i særlige tilfælde forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige net og tjenester at opretholde en indgået aftale, der vedrører kritiske netkompenter, systemer og værktøjer, herunder varetagelsen af driften heraf, såfremt opretholdelse af aftalen udgør en væsentlig trussel mod statens sikkerhed. Ved vurderingen heraf kan Center for Cybersikkerhed særligt lægge vægt på forhold vedrørende leverandøren, leverandørens væsentligste underleverandører samt aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren.

Efter den foreslåede § 3, stk. 2, kan Center for Cybersikkerhed i særlige tilfælde forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige net og tjenester at anvende kritiske netkomponenter, systemer og værktøjer, der tidligere er leveret, såfremt fortsat anvendelse vurderes at udgøre en væsentlig trussel mod statens sikkerhed. Ved vurderingen heraf kan Center for Cybersikkerhed særligt lægge vægt på forhold vedrørende leverandøren, leverandørens væsentligste underleverandører samt aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren. Af den foreslåede § 3, stk. 4, fremgår desuden, at Center for Cybersikkerhed kun kan nedlægge forbud efter § 3, stk. 1 og 2, hvis hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger.

Bestemmelsen i § 4, stk. 1, vil sikre, at et forbud mod en aftale omfattet af den foreslåede § 2, stk. 1, eller § 3, stk. 1 og 2, kan gennemføres, selvom det måtte medføre ekspropriation efter grundlovens § 73.

Det følger af grundlovens § 73, stk. 1, at to overordnede betingelser skal være opfyldt, for at der er tale om ekspropriation i grundlovens forstand. For det første skal indgrebet være rettet mod "ejendom", som er beskyttet efter grundlovens § 73. For det andet skal indgrebet være ekspropriativt (der skal være tale om afståelse).

Hvis der er tale om et indgreb, der har karakter af ekspropriation i grundlovens forstand, skal tre betingelser være opfyldt, for at indgrebet er i overensstemmelse med grundloven. Indgrebet skal være krævet af almenvellet, det skal ske ifølge lov, og der skal ydes fuldstændig erstatning til den berørte ejer. Betingelsen om, at et indgreb skal være krævet af almenvellet, vil altid være opfyldt, idet et forbud mod opretholdelse af en indgået aftale skal ske ud fra et hensyn til statens sikkerhed.

Grundloven beskytter ikke blot fysiske personer, men også alle typer af juridiske personer, som er etableret (eller overtaget) af private – selskaber, foreninger, selvejende institutioner m.v. Det er traditionelt antaget, at også staten, kommuner og andre juridiske personer etableret (eller fuldt ud overtaget) af det offentlige er beskyttet. Det fremgår dog af nyere retspraksis, at i hvert fald visse offentlige juridiske personer ikke altid nyder samme beskyttelse som private.

Udtrykket "ejendom" i grundlovens § 73 må forstås i vid betydning. Det er således almindeligt antaget, at bestemmelsen ikke alene beskytter ejendomsret i traditionel forstand. Også begrænsede rådighedsrettigheder, såsom brugsrettigheder, servitutter og panterettigheder, og rettigheder i henhold til private aftaler er beskyttet af grundlovens ejendomsbegreb.

Det er endvidere almindeligt antaget, at bestemmelsen ikke alene beskytter rettigheder af privatretlig karakter, men også særlige rettigheder af erhvervsmæssig karakter stiftet på offentligretligt grundlag, f.eks. næringsrettigheder.

For at der er tale om ekspropriation i grundlovens forstand, skal der være tale om, at der foretages et ekspropriativt indgreb (afståelse).

Det er i den forbindelse almindeligt antaget i den forfatningsretlige litteratur og i praksis, at lovgivningsmagten – uden at der foreligger ekspropriation – kan regulere udøvelsen af de rettigheder, der er beskyttet af grundlovens § 73, idet lovgivningsmagten bl.a. kan opstille almindelige regler om begrænsninger i borgernes handlefrihed og i deres råden over, hvad de ejer. Det er endvidere antaget, at spørgsmålet om, hvorvidt et indgreb har karakter af ekspropriation, må bero på et samlet skøn over indgrebets beskaffenhed. Som momenter, der må tillægges betydning ved udøvelsen af dette skøn, kan der navnlig peges på indgrebets formål, i hvilken grad indgrebet er generelt eller konkret (herunder om det rammer mange eller få personer), indgrebets intensitet, om indgrebet angår en fremtidig eller en aktuel rettighed, om indgrebet går ud på at overføre rettigheden fra den hidtidige ejer til en ny eller på en tilintetgørelse af denne råden, samt indgrebets begrundelse (causa).

Indgreb efter § 2, stk. 1, eller § 3, stk. 1 og 2, vil altid have til formål at beskytte statens sikkerhed. Navnlig det forhold, at forbud mod indgåelse af en aftale efter § 2, stk. 1, opretholdelse af en indgået aftale efter § 3, stk. 1, eller fortsat anvendelse af kritiske komponenter, systemer m.v. efter § 3, stk. 2, er begrundet i hensyn til statens sikkerhed, må antages at tale med en vis vægt imod, at der vil være tale om ekspropriation. Der vil på den anden side være tale om indgreb mod konkrete aftaler, som efter omstændighederne vil kunne være af betydelig intensitet over for den pågældende aftalepart. Det kan på den baggrund ikke udelukkes, at et forbud efter omstændighederne vil kunne anses for ekspropriativt.

Efter *§ 4, stk. 2*, ydes fuldstændig erstatning til en eller de berørte parter, hvis gennemførelsen af foranstaltninger efter denne lov udgør et ekspropriativt indgreb.

Ekspropriation kan alene ske mod fuld erstatning, jf. grundlovens § 73, stk. 1. I det omfang en afgørelse om indgreb måtte blive gennemført ved ekspropriation, vil der være adgang til domstolsprøvelse efter de særlige regler herom i grundlovens § 73, stk. 3.

Der henvises i øvrigt til afsnit 3.4 i de almindelige bemærkninger.

Til § 5

Det foreslås med *§ 5*, at lov om offentlighed i forvaltningen, bortset fra lovens § 13, og forvaltningslovens kapitel 4-6 ikke finder anvendelse på sager, der er omfattet af denne lov.

Det følger af § 8, stk. 1, i lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed, at Center for Cybersikkerheds virksomhed er undtaget fra offentlighedsloven bortset fra lovens § 13 om notatpligt. Centerets virksomhed er endvidere undtaget fra forvaltningslovens kapitel 4-6. Det fremgår imidlertid af de almindelige bemærkninger, jf. Folketingstidende 2013-14, A, L 192 som fremsat, side 25, at det forudsættes, at anmodninger om aktindsigt i videst muligt omfang behandles efter principperne i offentlighedsloven, samt at centeret i alle afgørelsessager konkret vurderer, om det er muligt at anvende forvaltningslovens principper.

Det følger endvidere af § 7 i lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed, at der kan fastsættes regler om, at der i forhold til de oplysninger og underretninger, som modtages fra teleudbydere i forbindelse med aftaleindgåelse, konstaterede brud på informationssikkerheden og generelle oplysninger om teleudbydernes infrastruktur, er undtaget fra aktindsigt efter offentlighedsloven og partsaktindsigt efter forvaltningsloven. Bestemmelsen er udmøntet i § 13 i bekendtgørelse nr. 1256 af 27. november 2019 om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed.

Den foreslåede § 5 har til formål at sikre den nødvendige beskyttelse af oplysninger, der vurderes at være følsomme, ved, at de sager, der behandles efter reglerne i dette lovforslag, undtages i deres helhed.

Den foreslåede bestemmelse indebærer, at retten til aktindsigt efter offentlighedsloven ikke gælder for sager, der er omfattet af denne lov. Offentlighedslovens § 13 om notatpligt vil derimod være gældende for behandling af sager efter loven. Bestemmelsen indebærer endvidere, at forvaltningslovens kapitel 4-6 om partens aktindsigt, partshøring og begrundelse m.v. fraviges, mens forvaltningslovens øvrige bestemmelser vil være gældende for behandling af sager omfattet af denne lov.

Den foreslåede bestemmelse svarer til den eksisterende undtagelse i § 8, stk. 1, i lov om Center for Cybersikkerhed, men uden forudsætningen i bemærkningerne til denne lov om, at principperne i offentlighedsloven og forvaltningslovens kapitel 4-6 i størst muligt omfang skal følges.

Efter den foreslåede bestemmelse vil Center for Cybersikkerhed således ikke være forpligtet til at gengive følsomme oplysninger i forbindelse med en begrundelse for en afgørelse, som centeret træffer i medfør af kapitel 2 eller 3. Endvidere vil Center for Cybersikkerhed ikke være forpligtet til at lade de følsomme oplysninger indgå i behandlingen af en aktindsigtssag.

Der henvises i øvrigt til afsnit 3.2 i de almindelige bemærkninger.

Til § 6

Det foreslås med *§ 6*, at Center for Cybersikkerheds afgørelser efter kapitel 2 og 3 ikke kan påklages til anden administrativ myndighed.

Bestemmelsen indebærer, at den administrative rekurs vil blive afskåret i relation til de afgørelser, som Center for Cybersikkerhed træffer efter kapitel 2 og 3. Afgørelser efter disse kapitler vil således ikke kunne påklages til Forsvarsministeriet som led i den ulovbestemte rekursadgang. Dette skal ses i lyset af, at de pågældende afgørelser forudsætter et særligt fagligt indblik i henholdsvis efterretningsmæssige og teletekniske forhold, som Center for Cybersikkerhed besidder.

Bestemmelsen regulerer ikke klageadgangen til Folketingets Ombudsmand. Der vil således fortsat være adgang til at klage over afgørelser truffet efter kapitel 2 og 3 til Folketingets Ombudsmand i medfør af kapitel 4 i lov om Folketingets Ombudsmand, jf. lovbekendtgørelse nr. 349 af 22. marts 2013.

Til § 7

Med bestemmelsen i *§ 7, 1. pkt.,* foreslås det, at afgørelser efter kapitel 2 og 3 alene kan indbringes for Københavns Byret inden seks måneder efter afgørelsens meddelelse. Bestemmelsen skal tilgodese spørgsmål om bl.a. sikkerhedsgodkendelse af retspersonalet og erfaringsopbygning. Desuden sikrer fastsættelsen af en søgsmålsfrist, at der efter en vis periode ikke kan rejses tvivl om en afgørelse og dennes indhold. Med den foreslåede bestemmelse i *§ 7, 2. pkt.,* kan Københavns Byret dog undtagelsesvist tillade en indbringelse efter seks måneder.

Med den foreslåede bestemmelse i *§ 7, 3. pkt.,* foreslås det, at der i afgørelsen af sagen ved byretten deltager tre dommere.

Efter den foreslåede bestemmelse i *§ 7, sidste punktum,* kan forsvarsministeren eller den, ministeren bemyndiger hertil, helt eller delvist lade personer, der er ansat i Forsvarsministeriet eller myndigheder under Forsvarsministeriet, møde for sig i retten som rettergangsfuldmægtige.

Den foreslåede bestemmelse skal ses i lyset af, at der under sagen eventuelt vil skulle fremlægges fortrolige oplysninger fra efterretningstjenester m.v., som har dannet grundlag for risikovurderingen, og bestemmelsen supplerer i øvrigt retsplejelovens § 260, stk. 1, nr. 4, hvorefter personer, der er ansat hos en part, kan møde som rettergangsfuldmægtig.

Det forudsættes, at det i givet fald vil være en juridisk medarbejder fra Forsvarsministeriet eller myndigheder under Forsvarsministeriet, som møder i retten.

De foreslåede regler for særlig domstolsprøvelse tager udgangspunkt i de lignende bestemmelser i udlændingelovens kapitel 7 b, som indeholder særlige regler for domstolsprøvelse af visse beslutninger om administrativ udvisning af udlændinge, der må anses for en fare for statens sikkerhed, samt indfødsretslovens § 8 F vedrørende domstolsprøvelse af afgørelser om administrativ fratagelse af statsborgerskab.

Til § 8

I *§ 8, stk. 1*, foreslås det, at som parter i sagen anses dem, der har en retlig interesse i en afgørelse omfattet af kapitel 2 og 3, og at som part i sagen for det offentlige anses forsvarsministeren eller den, ministeren bemyndiger hertil. Bestemmelsen hænger sammen med den foreslåede § 7, hvoraf det fremgår, at sager om prøvelse af afgørelser efter lovforslagets kapitel 2 og 3 alene kan indbringes for Københavns Byret.

I *§ 8, stk. 2*, foreslås det, at retten beskikker en særlig advokat til at varetage interesser for parten efter stk. 1, 1. pkt., som har en retlig interesse i en afgørelse omfattet af kapitel 2 og 3, og på vegne af denne udøve partsbeføjelser med hensyn til oplysninger af betydning for statens sikkerhed, der er indgået i vurderingen af, om en aftale vurderes at udgøre en trussel mod statens sikkerhed, hvis disse af sikkerhedsmæssige grunde ikke kan videregives til parten og dennes advokat. Parten efter § 8, stk. 1, 1. pkt., og dennes advokat har ikke adgang til de pågældende oplysninger og har ikke mulighed for at udøve de sædvanlige partsbeføjelser, herunder navnlig at kunne vurdere og udtale sig om de pågældende oplysninger, selv om disse fremlægges for retten og indgår i grundlaget for rettens afgørelse. Dette varetages i stedet af den særlige advokat, der har indsigt i og mulighed for at udtale sig om det materiale, som fremlægges for retten med henblik på at indgå i sagen, herunder de fortrolige oplysninger, som af sikkerhedsmæssige grunde ikke kan videregives til parten og dennes advokat.

Den særlige advokat udøver partsbeføjelser på vegne af parten med hensyn til disse fortrolige oplysninger, men er i øvrigt ikke part eller partsrepræsentant i sagen. I det omfang parten sammen med sin advokat kan udøve sædvanlige civilprocessuelle partsbeføjelser, herunder med hensyn til oplysninger, som er videregivet til parten og fremlagt i retten, optræder den særlige advokat således ikke på vegne af parten. Den særlige advokat har f.eks. indsigt i og kan udtale sig om oplysninger, som er undtaget af sikkerhedsmæssige grunde. Den særlige advokat kan også fremsætte begæring om, at sådanne oplysninger skal videregives til parten og dennes advokat, jf. den foreslåede bestemmelse i § 8, stk. 2, og kan kære rettens afgørelse om, at oplysningerne ikke skal videregives. Den særlige advokat har derimod ikke en almindelig adgang til f.eks. at kære rettens procesledende afgørelser under sagens behandling i den åbne del af domstolsprøvelsen eller at indbringe byrettens endelige afgørelse i sagen for landsretten. Dette tilkommer den, som er part i sagen, jf. forslaget til § 8, stk. 1.

Justitsministeren antager et antal advokater, der kan beskikkes som særlige advokater i sager om domstolsprøvelse af afgørelser efter lovforslagets kapitel 6, jf. den foreslåede bestemmelse i § 12.

Det forudsættes, at retten i almindelighed beskikker den advokat, der »står for tur« til at blive beskikket, men at der beskikkes en anden advokat, hvis parten har begrundede indsigelser mod beskikkelsen af den pågældende.

Med hensyn til salær og godtgørelse for udlæg til den særlige advokat gælder de samme regler, som hvis der var bevilget fri proces, jf. retsplejelovens kapitel 31. Dette indebærer, at salær m.v. betales af det offentlige.

I *§ 8, stk. 3*, forslås det, at den særlige advokat skal underrettes om alle retsmøder i sagen og er berettiget til at deltage i disse med henblik på at sikre den særlige advokats løbende indsigt i sagen ved retten. Henset til advokatens særlige rolle i sagen foreslås det endvidere, at advokatens partsbeføjelser vedrørende de fortrolige oplysninger i sagen, jf. ovenfor, indebærer, at vedkommende skal gøres bekendt med det materiale, som indgår i sagen for retten, dvs. det materiale, som fremlægges af det offentlige med henblik på, at det kan indgå i rettens afgørelse (og eventuelt supplerende materiale, som fremlægges af parten og dennes advokat).

I den foreslåede bestemmelse i § 9, stk. 1, er det endvidere udtrykkeligt bestemt, at de fortrolige oplysninger, som af sikkerhedsmæssige grunde ikke kan videregives til parten og dennes advokat, skal videregives til den særlige advokat.

Den særlige advokat skal endvidere som udgangspunkt have udleveret kopi af materialet. Forsvarsministen eller den, ministeren bemyndiger hertil, kan dog bestemme, at der af sikkerhedsmæssige grunde ikke skal udleveres kopi til den særlige advokat. Dette vil alene kunne være relevant med hensyn til de oplysninger, der af sikkerhedsmæssige grunde ikke kan videregives til parten. I så fald skal den særlige advokat på anden måde have fornøden adgang til materialet, f.eks. ved at gennemse det pågældende materiale i retten.

Spørgsmålet om udlevering af kopi kan indbringes for retten, der også kan tage stilling til en eventuel tvist om, hvordan advokaten i stedet skal have adgang til materialet.

Bestemmelsen svarer med de nødvendige tilpasninger til den lignende bestemmelse i udlændingelovens § 45 e.

Til § 9

Den foreslåede bestemmelse i *§ 9* indeholder regler om videregivelse af de oplysninger, som er undtaget fra videregivelse til parten selv, til den særlige advokat. En beslutning om, at oplysninger, der er indgået i Center for Cybersikkerheds afgørelse efter lovforslagets kapitel 2 og 3, ikke kan videregives til parten, finder også anvendelse i forbindelse med en domstolsprøvelse af afgørelsen. Dette indebærer bl.a., at parten under en retssag ikke har adgang til aktindsigt i de pågældende oplysninger, som fremlægges for retten, efter retsplejelovens § 255 a, som alene gælder »medmindre andet er bestemt«.

De fortrolige oplysninger, der er indgået i vurderingen af, om en aftale udgør en trussel mod statens sikkerhed, vil som det klare udgangspunkt blive fremlagt for retten. Der kan dog i denne vurdering være indgået oplysninger af en sådan særlig karakter, at de af hensyn til statens sikkerhed, herunder efterretningstjenesternes virksomhed, ikke kan videregives til andre og heller ikke som led i domstolsprøvelsen. Hvis sådanne oplysninger ikke fremlægges for retten og den særlige advokat efter den foreslåede bestemmelse i § 8, stk. 2, vil oplysningerne ikke indgå i grundlaget for rettens afgørelse i sagen, da retten på grundlag af det, der er passeret under forhandlingerne og bevisførelsen, må afgøre, hvilke faktiske omstændigheder der skal lægges til grund for sagens pådømmelse, jf. retsplejelovens § 344.

Det foreslås i *§ 9, stk. 1*, at de oplysninger, som ikke kan videregives til parten og dennes advokat, videregives til den særlige advokat, der varetager partens interesser med hensyn til disse oplysninger, jf. også den foreslåede bestemmelse i § 8 og bemærkningerne hertil.

Den særlige advokat kan drøfte sagen med parten og dennes advokat, indtil det tidspunkt, hvor de nævnte fortrolige oplysninger er videregivet til den særlige advokat. Når sådanne oplysninger er videregivet til den særlige advokat, må vedkommende ikke længere drøfte sagen med parten eller dennes advokat. I modsat fald kunne der være en risiko for, at den særlige advokat ved f.eks. at stille supplerende spørgsmål til parten uforvarende kunne komme til at afsløre kendskab til oplysninger, som af sikkerhedsmæssige grunde ikke kan videregives til parten. Den særlige advokat er afskåret fra at drøfte sagen med parten og dennes advokat, men der er ikke noget til hinder for, at den særlige advokat f.eks. skriftligt bekræfter modtagelsen af materiale fra parten eller dennes advokat.

Det forudsættes således, at den særlige advokat indledningsvis drøfter sagen med parten og dennes advokat, herunder deres bemærkninger vedrørende de oplysninger, som er videregivet til de pågældende, således at dette kan indgå i advokatens videre arbejde med sagen i relation til de fortrolige oplysninger, som ikke kan videregives til parten. Parten eller dennes advokat kan herudover når som helst give skriftlige meddelelser til den særlige advokat om sagen og kan således løbende videregive yderligere oplysninger og synspunkter til den særlige advokat, herunder efter at de fortrolige oplysninger er videregivet til den særlige advokat, og denne ikke længere kan drøfte sagen med parten. Den særlige advokat vil endvidere være til stede ved retsmøder i sagen, jf. den foreslåede bestemmelse i § 8, stk. 3, og vil således også ad den vej løbende have kendskab til partens synspunkter.

Ud fra tilsvarende betragtninger som nævnt ovenfor foreslås det endvidere, at den særlige advokat ikke må udtale sig i retsmøder, hvor parten eller dennes advokat er til stede, når de fortrolige oplysninger er videregivet til den særlige advokat. Dette stemmer også med, at parten og dennes advokat i videst muligt omfang varetager sædvanlige civilprocessuelle partsbeføjelser i sagen, herunder udtaler sig i retsmøder om sagen. Det er alene i retsmøder, hvor parten ikke er til stede, fordi der fremlægges de nævnte fortrolige oplysninger, at den særlige advokat varetager partens interesser og kan udtale sig om sagen.

Det foreslås i *§ 9, stk. 2*, at retten af egen drift eller efter begæring fra den særlige advokat kan bestemme, at fortrolige oplysninger, der er indgået i vurderingen i afgørelser omfattet af kapitel 2 og 3, videregives til parten og dennes advokat, hvis sikkerhedsmæssige forhold ikke kan begrunde, at oplysningerne ikke videregives.

Den foreslåede bestemmelse sigter således til tilfælde, hvor retten efter en konkret vurdering finder, at der ikke foreligger sådanne sikkerhedsmæssige forhold, at oplysningerne bør være fortrolige og ikke videregives til parten og dennes advokat, f.eks. hvis retten ikke finder, at der i det konkrete tilfælde er særlige hensyn til efterretningstjenesternes arbejdsmetoder m.v., som medfører, at de pågældende oplysninger bør være fortrolige.

Uanset om spørgsmålet om videregivelse af sådanne fortrolige oplysninger rejses af retten af egen drift eller efter begæring fra den særlige advokat, har både den særlige advokat og forsvarsministeren eller den, som ministeren bemyndiger hertil, adgang til at udtale sig om spørgsmålet om videregivelse, inden retten træffer afgørelse.

Retten træffer afgørelse ved kendelse, som efter de almindelige regler herom skal begrundes, jf. retsplejelovens § 218, stk. 1.

I overensstemmelse med at den særlige advokat med hensyn til disse fortrolige oplysninger varetager partens interesser i sagen, kan afgørelsen kæres af den særlige advokat og af forsvarsministeren eller den, som ministeren bemyndiger hertil.

Kære af rettens afgørelse om, at oplysninger skal videregives, har efter forslaget opsættende virkning, dvs. at oplysningerne ikke videregives til parten og dennes advokat, før der foreligger en endelig retsafgørelse om spørgsmålet. Det er samtidig forudsat, at selve retssagen om prøvelse af afgørelsen efter lovforslagets kapitel 2 og 3 ikke færdigbehandles ved retten, før der er taget endelig stilling til, i hvilket omfang fortrolige oplysninger kan videregives til parten og dennes advokat.

Det foreslås i *§ 9, stk. 3*, at hvis retten har truffet afgørelse om, at fortrolige oplysninger videregives til parten og dennes advokat, skal forsvarsministeren eller den, ministeren bemyndiger hertil, have mulighed for at bestemme, at de pågældende oplysninger ikke indgår i sagen for retten.

Hermed sigtes til tilfælde, hvor forsvarsministeren eller den, ministeren bemyndiger hertil, uanset rettens beslutning finder, at oplysningerne ikke bør videregives, selv om dette medfører, at retten i så fald må træffe afgørelse på det foreliggende grundlag, jf. herved også retsplejelovens § 344 omtalt ovenfor.

Beslutningen kan både omfatte alle oplysninger omfattet af rettens afgørelse om, at oplysninger videregives, og begrænses til at gælde visse oplysninger, så de øvrige oplysninger videregives til parten og dennes advokat.

Hvis det efter forslaget til stk. 3 besluttes, at visse oplysninger ikke længere skal indgå i sagen for retten, foreslås det i *§ 9, stk. 4*, at en dommer, som har deltaget i afgørelsen om, at de pågældende oplysninger videregives til parten og dennes advokat, jf. forslaget til stk. 2, ikke længere kan deltage som dommer i sagen. I modsat fald ville den pågældende dommer have kendskab til disse fortrolige oplysninger, selv om de ikke længere indgår i sagen for retten.

Tilsvarende kan en dommer ikke deltage som dommer i sagen, hvis han eller hun i øvrigt har haft adgang til oplysninger, som er omfattet af en beslutning efter forslaget til stk. 3 om, at oplysningerne ikke længere indgår i sagen for retten. Det vil f.eks. kunne være tilfældet, hvis de pågældende oplysninger har været fremlagt for retten inden en beslutning efter stk. 3 – også i denne situation har den pågældende dommer således fået kendskab til fortrolige oplysninger, som ikke længere indgår i sagen.

Bestemmelsen svarer med de nødvendige tilpasninger til den lignende bestemmelse i udlændingelovens § 45 f.

Til § 10

Efter den foreslåede bestemmelse i *§ 10, stk. 1*, holdes den del af et retsmøde, der angår, eller hvor der fremlægges eller behandles fortrolige oplysninger af betydning for statens sikkerhed, for lukkede døre.

Dette gælder således alle dele af et retsmøde, hvor sådanne oplysninger kommer frem eller omtales, hvad enten det f.eks. sker som led i en bevisførelse eller som led i den særlige advokats eller forsvarsministerens repræsentants procedure for retten.

Dette gælder også retsmøder, hvor retten behandler spørgsmålet om videregivelse af fortrolige oplysninger til parten eller dennes advokat, jf. den foreslåede bestemmelse i § 9, stk. 2.

Hvis retten efter den foreslåede bestemmelse i § 9, stk. 2, har bestemt, at oplysninger af betydning for statens sikkerhed videregives til parten i forbindelse med sagens behandling i retten, finder den foreslåede bestemmelse i stk. 1 om behandling for lukkede døre dog ikke anvendelse.

Det foreslås, at det kommer til at fremgå af lovteksten, at i denne del af et retsmøde deltager den særlige advokat, men ikke den pågældende part og dennes advokat.

Spørgsmålet om, hvorvidt retsmøder i sagen i øvrigt holdes for åbne eller lukkede døre, skal som i dag afgøres efter retsplejelovens almindelige regler herom, jf. navnlig retsplejelovens § 29.

Som det fremgår, vil der ved behandlingen af en sag om en prøvelse af en afgørelse blive tale om, at visse dele af retsmøderne foregår for lukkede døre uden tilstedeværelse af parten og dennes advokat, hvor partens interesser varetages af den særlige advokat, mens retsmøderne i øvrigt foregår med deltagelse af parten og dennes advokat (samt den særlige advokat, jf. den foreslåede bestemmelse i § 8, stk. 3).

På denne baggrund foreslås det i *§ 10, stk. 2*, at retten i den enkelte sag bestemmer, hvordan retsmøder, der efter forslaget til stk. 1 helt eller delvist holdes for lukkede døre, gennemføres mest hensigtsmæssigt.

Det forudsættes, at retsmøderne i videst muligt omfang foregår efter de almindelige regler bl.a. om gennemførelse af hovedforhandlingen, jf. retsplejelovens § 365, men at retten kan træffe beslutning om de fornødne ændringer ved afholdelsen af retsmøderne som følge af, at parten og dennes advokat ikke deltager i alle dele af sagens retsmøder.

Retten vil f.eks. kunne bestemme, at hovedforhandlingen foregår på den måde, at parten og dennes advokat deltager i den første del af retsmødet, hvor der fremlægges alle oplysninger, som ikke er [af betydning for statens sikkerhed], hvorefter parterne gør rede for deres opfattelse af sagen (proceduren). Herefter forlader parten og dennes advokat retsmødet, og der kan i et lukket retsmøde fremlægges de fortrolige oplysninger, der af sikkerhedsmæssige grunde ikke kan videregives til parten. Herefter procederer den særlige advokat og forsvarsministerens repræsentant og gør rede for deres opfattelse af sagen i lyset af de fortrolige oplysninger, som nu er fremlagt for retten. På dette samlede grundlag træffer retten sin afgørelse i sagen, jf. også den foreslåede bestemmelse i § 11.

Bestemmelsen svarer med de nødvendige tilpasninger til den lignende bestemmelse i udlændingelovens § 45 g.

Til § 11

Efter den foreslåede bestemmelse i *§ 11, stk. 1*, træffer retten afgørelse efter, at parterne, jf. § 8, stk. 1, og den særlige advokat beskikket efter den foreslåede bestemmelse i § 8, stk. 2, har haft lejlighed til at udtale sig. Retten bestemmer i den enkelte sag, hvordan dette tilrettelægges mest hensigtsmæssigt, jf. den foreslåede bestemmelse i § 10, stk. 2, og bemærkningerne hertil.

Om den særlige advokats opgaver henvises i øvrigt til de foreslåede bestemmelser i § 8, stk. 2 og 3, og bemærkningerne hertil.

Rettens afgørelse skal begrundes efter de almindelige regler herom, jf. retsplejelovens § 218, stk. 1, og en dom skal bl.a. indeholde en fremstilling af sagen og angive de faktiske og retlige omstændigheder, der er lagt vægt på ved sagens afgørelse, jf. retsplejelovens § 218 a, stk. 2.

En beslutning om, at oplysninger, der er indgået i Center for Cybersikkerheds afgørelse, af sikkerhedsmæssige grunde ikke kan videregives til parten, finder som nævnt i bemærkningerne til den foreslåede bestemmelse også anvendelse i forbindelse med en domstolsbehandling. Rettens afgørelse (dom eller kendelse) må således affattes under hensyntagen hertil, dvs. således at den ikke indeholder fortrolige oplysninger, som ikke kan videregives til parten. Det er således forudsat, at rettens afgørelse affattes og begrundes på grundlag af sagens åbne materiale, som parten har kendskab til og har haft lejlighed til at kommentere, men således at retten i sin afgørelse kan henvise til, at oplysninger i det åbne materiale er godtgjort eller sandsynliggjort i de fortrolige oplysninger, som er fremlagt for retten og den særlige advokat..

Bestemmelsens stk. 1 svarer med de nødvendige tilpasninger til den lignende bestemmelse i udlændingelovens § 45 h, stk. 1.

Til § 12

Det følger af den foreslåede bestemmelse i *§ 12*, at justitsministeren antager et antal advokater, der kan beskikkes efter den foreslåede bestemmelse i § 8, stk. 2, 1. pkt., til at varetage partens interesser i sagen med hensyn til de fortrolige oplysninger, som af sikkerhedsmæssige grunde ikke kan videregives til parten og dennes advokat.

Det foreslås endvidere, at justitsministeren kan fastsætte nærmere regler om de pågældende advokater, herunder om vagtordninger, om vederlag for at stå til rådighed og om sikkerhedsmæssige spørgsmål.

Ligesom udlændingelovens § 45 j, svarer bestemmelsen til retsplejelovens § 784, stk. 2, om advokater, der kan beskikkes i sager om indgreb i meddelelseshemmeligheden, hvor efterforskningen angår overtrædelse af straffelovens kapitel 12 og 13 (om terrorisme m.v.).

De pågældende advokater vil i givet fald blive antaget af justitsministeren efter drøftelse med præsidenterne for Østre Landsret og Københavns Byret samt Advokatrådet.

Hvis lovforslaget vedtages, kan justitsministeren bl.a. fastsætte regler om, at de pågældende advokater kun efter særlig godkendelse af Justitsministeriet må få bistand fra andre ved

udførelsen af deres hverv, om transport og opbevaring af sagens dokumenter og om sikkerhedsgodkendelse af advokaterne. Beslutningen om sikkerhedsgodkendelse af de særlige advokater vil i givet fald blive truffet af Justitsministeriet.

Bestemmelsen svarer med de nødvendige tilpasninger til den lignende bestemmelse i udlændingelovens § 45 j.

Til § 13

Det foreslås, at de foreslåede særlige regler om domstolsprøvelse i lovforslagets kapitel 6 også gælder ved sagens behandling i landsretten og i givet fald i Højesteret, hvis Procesbevillingsnævnet giver tilladelse til, at sagen indbringes for Højesteret.

Bestemmelsen svarer med de nødvendige tilpasninger til den lignende bestemmelse i udlændingelovens § 45 k, stk. 1.

Til § 14

Det foreslås med *§ 14, stk. 1,* at Center for Cybersikkerhed i ikke-anonymiseret form kan offentliggøre afgørelser truffet i medfør af kapitel 2 og 3, resuméer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde for overtrædelse af reglerne i kapitel 2, samt resuméer af domme i retssager, der vedrører prøvelse af afgørelser efter kapitel 2 og 3.

Den foreslåede bestemmelse har til formål at give teleudbyderne øget incitament til overholdelse af lovens kapitel 2, ligesom bestemmelsen giver telekunder mulighed for at få kendskab til, hvorvidt en teleudbyder f.eks. har indgået eller opretholder en aftale, der vurderes at udgøre en trussel mod statens sikkerhed. Forsvarsministeriet finder således, at der ud fra et samlet hensyn til statens sikkerhed er behov for, Center for Cybersikkerhed i ikke-anonymiseret form kan offentliggøre afgørelser, resuméer af domme og bødevedtagelser i relation til overholdelse af lovens kapitel 2. En sådan offentliggørelsesordning vurderes at udgøre et effektivt redskab, der kan medvirke til at sikre et højt sikkerhedsniveau i den kritiske teleinfrastruktur.

Offentliggørelse af afgørelser efter *stk. 1, nr. 1,* indebærer, at der kan ske offentliggørelse i sager, hvor Center for Cybersikkerhed efter den foreslåede § 2 forbyder en teleudbyder at indgå en aftale samt i tilfælde, hvor centeret efter den foreslåede § 3 forbyder en teleudbyder at opretholde en indgået aftale eller forbyder anvendelse af kritiske komponenter, systemer m.v. Der vil også kunne ske offentliggørelse i sager, hvor centeret iværksætter ekspropriation efter det foreslåede kapitel 3. Center for Cybersikkerheds beslutning om at overgive sager til politimæssig efterforskning vil også kunne offentliggøres efter bestemmelsen.

Efter *stk. 1, nr. 2,* kan Center for Cybersikkerhed endvidere offentliggøre resuméer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde for overtrædelse af de foreslåede regler i kapitel 2. Offentliggørelse vil kunne ske i de tilfælde, hvor en teleudbyder straffes for at have handlet i strid med et forbud meddelt i medfør af § 2 eller § 3.

Herudover kan der efter *stk. 1, nr. 3,* ske offentliggørelse af resuméer af domme i retssager, der vedrører prøvelse af afgørelser efter kapitel 2 og 3. Bestemmelsen vedrører de tilfælde, hvor domstolene foretager en prøvelse af Center for Cybersikkerheds afgørelser efter lovens §§ 2 og 3 om forbud mod henholdsvis indgåelse eller opretholdelse af en aftale eller anvendelse af kritiske komponenter, systemer m.v. samt § 4 om ekspropriation. Der sker ikke med bestemmelsen en fravigelse af retsplejelovens regler om aktindsigt i domme.

Offentliggørelse vil ske på Center for Cybersikkerheds hjemmeside i ikke-anonymiseret form. Det vil således fremgå af det offentliggjorte materiale, hvilken teleudbyder afgørelsen, dommen eller bødevedtagelsen er rettet imod.

Offentliggørelse efter stk. 1 må dog ikke indeholde oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold el.lign., for så vidt det er af væsentlig økonomisk betydning for den teleudbyder, som oplysningerne angår. Offentliggørelse må heller ikke indeholde oplysninger, hvis hemmeligholdelse er af væsentlig betydning for statens sikkerhed eller rigets forsvar. Desuden vil klassificerede informationer og oplysninger om enkelt personers forhold blive slettet i det materiale, der offentliggøres. Oplysninger om enkelt personers forhold kan eksempelvis være oplysninger om navne, adresser eller telefonnumre på klagere eller andre berørte parter, som vil skulle undtages fra offentliggørelsen.

Det bemærkes i øvrigt, at Center for Cybersikkerhed forudsættes ikke at offentliggøre afgørelser, såfremt efterforskningsmæssige hensyn taler derimod.

Det foreslås med *§ 14, stk. 2,* at forsvarsministeren kan fastsætte nærmere regler om sagsbehandlingen i forbindelse med offentliggørelse efter stk. 1.

Der vil med hjemmel i bestemmelsen eksempelvis kunne fastsættes regler for, hvornår der kan ske offentliggørelse. Der vil endvidere kunne fastsættes regler om forudgående høring eller orientering af en udbyder vedrørende spørgsmålet om en forestående offentliggørelse af en afgørelse m.v.

Der vil herudover kunne fastsættes regler om, at det skal fremgå af offentliggørelsen, såfremt der verserer en sag for domstolene.

Endelig vil der kunne fastsættes regler om, hvor lang tid den pågældende afgørelse m.v. skal være offentligt tilgængelige på Center for Cybersikkerheds hjemmeside.

Til § 15

Det foreslås med *§ 15, stk. 1,* at den, der overtræder et forbud efter § 2, stk. 1, og § 3, stk. 1 og 2, straffes med bøde, medmindre strengere straf er forskyldt efter den øvrige lovgivning.

Bestemmelsen indebærer, at væsentlige erhvervsmæssige udbydere af offentlige tilgængelige net og tjenester kan straffes, hvis de overtræder Center for Cybersikkerheds forbud efter kapitel 2. De pågældende forbud kan være forbud mod indgåelse af aftaler efter § 2, stk. 1, forbud mod opretholdelse af aftaler efter § 3, stk. 1, eller forbud mod anvendelse af kritiske komponenter, systemer m.v. efter § 3, stk. 2.

For en nærmere beskrivelse af forbuddenes omfang og indhold henvises til bemærkningerne til de foreslåede §§ 2 og 3.

Ved udmåling af bøder som følge af en væsentlig erhvervsmæssig udbyder af offentlige tilgængelige net og tjenesters overtrædelse af et forbud bør der tages særligt hensyn til den økonomiske fordel, teleudbyderen enten har opnået eller har tilsigtet at opnå ved overtrædelsen af forbuddet.

Det foreslås med *stk. 2,* at der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Til § 16

Det foreslås med § 16 at aftaler, der er i strid med et forbud efter § 2, stk. 1, og § 3, stk. 1, er uden gyldighed mellem parterne.

Bestemmelsen indebærer, at væsentlige erhvervsmæssige udbydere af offentlige tilgængelige net og tjenester og disses kontraktsparter ikke vil kunne støtte ret på en aftale, der er i strid med et forbud efter § 2, stk. 1, om indgåelse af aftaler vedrørerende kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf, som vurderes at udgøre en trussel mod statens sikkerhed.

Bestemmelsen indebærer endvidere, at væsentlige erhvervsmæssige udbydere af offentlige tilgængelige net og tjenester og disses kontraktsparter ikke vil kunne støtte ret på en aftale, der er i strid med et forbud efter § 3, stk. 1, om opretholdelse af aftaler vedrørende kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf, som vurderes at udgøre en væsentlig trussel mod statens sikkerhed.

Bestemmelsen viderefører princippet i Danske Lov 5-1-2 om aftaler i strid med lov og ærbarhed, og sikrer dermed, at en sådan aftale ikke skal anerkendes ved domstolene.

Retsvirkningerne af en ugyldig aftale følger af de almindelige regler om ugyldighedsvirkninger, herunder om tilbageførelse af ydelser mellem parterne.

Til § 17

Det forslås med *§ 17, stk. 1,* at loven træder i kraft den […].

Bestemmelsen indebærer, at loven vil kunne håndhæves, og at Center for Cybersikkerhed vil kunne træffe afgørelser efter kapitel 2 og 3, fra den […].

Det foreslås med *stk. 2,* at loven har virkning for aftaler, der er indgået den 7. december 2020 eller senere, jf. dog stk. 3.

Bestemmelsen indebærer, at Center for Cybersikkerhed fra lovens ikrafttræden vil kunne træffe afgørelse om forbud mod opretholdelse af aftaler, jf. § 3, stk. 1, og forbud mod anvendelse af kritiske komponenter, systemer m.v., jf. § 3, stk. 2, når disse aftaler er indgået den 7. december 2020 eller senere. Virkningstidspunktet for loven er fastsat til datoen for iværksættelsen af den offentlige høring over lovforslaget. Loven har således tilbagevirkende kraft for aftaler indgået den 7. december 2020 eller senere.

Med bestemmelsen sikres det, at der ikke opstår et incitament for teleudbyderne til at omgå lovens ordning ved at indgå aftaler, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf, som udgør en væsentlig trussel mod statens sikkerhed, i perioden fra lovforslaget har været sendt i offentlig høring og frem til den […], hvor loven foreslås at træde i kraft.

Det foreslås med *stk. 3,* at loven fra den 1. januar 2026 endvidere har virkning for aftaler, der er indgået før den 7. december 2020.

Bestemmelsen indebærer, at Center for Cybersikkerhed efter den 1. januar 2026 vil kunne træffe afgørelse om forbud mod opretholdelse af aftaler, jf. § 3, stk. 1, eller forbud mod anvendelse af kritiske komponenter, systemer m.v., jf. § 3, stk. 2, samt afgørelse om ekspropriation efter § 4, selv om disse aftaler er indgået før den 7. december 2020, som er datoen for iværksættelsen af den offentlige høring. Loven har således efter 1. januar 2026 tilbagevirkende kraft for alle omfattede aftaler, uanset hvornår de er indgået. Det er dog forventningen, at langt de fleste omfattede aftaler på dette virkningstidspunkt vil være udløbet

Bestemmelsen indebærer, at teleudbyderne fra lovens ikrafttræden vil få en længere periode til at afvikle aftaler, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelsen af driften heraf, der er indgået før den 7. december 2020, hvor forhold hos leverandøren m.v. gør, at fastholdelsen af aftalen udgør en væsentlig trussel mod statens sikkerhed.

Der henvises i øvrigt til afsnit 3.1 i de almindelige bemærkninger.

Til § 18

Det følger af § 4, nr. 2, i lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed, at Center for Cybersikkerhed fastsætter regler om erhvervsmæssige udbydere af offentligt tilgængelige net og tjenesters underretning af Center for Cybersikkerhed ved påtænkt indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf. Der kan endvidere stilles krav om, at udbyderne skal indsende et endeligt aftaleudkast til Center for Cybersikkerhed umiddelbart forud for indgåelse af aftalen, og at aftalen først kan indgås op til 10 arbejdsdage efter centerets modtagelse af dette udkast.

Med den ordning, der foreslås i § 2, vil Center for Cybersikkerhed i særlige tilfælde kunne forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at indgå en aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf, såfremt aftalen vurderes at udgøre en trussel mod statens sikkerhed.

Vurderingen af, om en aftale udgør en trussel mod statens sikkerhed, vil typisk skulle ske, efter at Center for Cybersikkerhed har modtaget det endelige aftaleudkast fra teleudbyderen i medfør af den eksisterende underretningsordning efter net- og informationssikkerhedsloven. Den nuværende frist på 10 arbejdsdage er imidlertid fastsat ud fra et hensyn til, at Center for Cybersikkerhed skal have mulighed for at gennemgå aftalen og rådgive teleudbyderen. Dette vil med den foreslåede ordning fortsat skulle ske, idet Center for Cybersikkerhed i forbindelse med rådgivningen også vil kunne tilkendegive, hvordan centeret

umiddelbart vurderer udsigten til, at der nedlægges forbud, og først hvis rådgivningen ikke følges, vil centeret skulle tage endelig stilling til, om der er grundlag for at nedlægge et forbud. Dette rådgivningsforløb vil ikke være muligt indenfor den samlede frist på 10 arbejdsdage, og det foreslås derfor, at fristen forøges til 25 arbejdsdage.

Til § 19

[Regeringen er i dialog med Færøerne og Grønland om, hvordan en lovgivningsmodel kan udformes for Færøerne og Grønland med respekt for kompetencefordelingen i rigsfællesskabet.]

Bilag 1

Lovforslaget sammenholdt med gældende lov

Gældende formulering	*Lovforslaget*
	§ 18
	I lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed foretages følgende ændring:
§ 4. Center for Cybersikkerhed fastsætter regler om oplysnings- og underretningspligter for udbydere. Reglerne kan omfatte krav om:	
1) ---	**1.** I *§ 4, nr. 2, 2. pkt.,* ændres »10« til: »25«.
2) Erhvervsmæssige udbydere af offentligt tilgængelige net og tjenesters underretning af Center for Cybersikkerhed ved påtænkt indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf. Der kan endvidere stilles krav om, at udbyderne skal indsende et endeligt aftaleudkast til Center for Cybersikkerhed umiddelbart forud for indgåelse af aftalen, og at aftalen først kan indgås op til 10 arbejdsdage efter centerets modtagelse af dette udkast.	
3-4) ---	