Forsvarsministeriet 21. april 2015

U D K A S T

Forslag

til

Lov om net- og informationssikkerhed[1]

Kapitel 1
Formål og definitioner

§ 1. Lovens formål er at fremme net- og informationssikkerheden i samfundet.

§ 2. I denne lov forstås ved:

1) *Net:* Elektroniske kommunikationsnet i form af radiofrekvens- eller kabelbaseret teleinfrastruktur, der anvendes til formidling af tjenester.
2) *Tjeneste:* Elektronisk kommunikationstjeneste, 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.
3) *Offentligt tilgængelige net og tjenester:* Net og tjenester, der stilles til rådighed for en ikke på forhånd afgrænset kreds af slutbrugere eller udbydere.
4) *Udbyder:* Den, der med et kommercielt formål stiller produkter, net eller tjenester til rådighed for andre.
5) *Erhvervsmæssig udbyder:* En udbyder, der med et kommercielt formål udbyder produkter, net eller tjenester som sin hovedydelse eller som en ikke accessorisk del af virksomheden.

Kapitel 2
Informationssikkerhed i net og tjenester

§ 3. Center for Cybersikkerhed fastsætter regler om minimumskrav til informationssikkerhed for udbydere af offentligt tilgængelige net og tjenester. Reglerne kan omfatte krav om passende tekniske, processuelle og organisatoriske foranstaltninger med henblik på risikostyring i forhold til informationssikkerhed i offentligt tilgængelige net og tjenester og opretholdelse af et passende informationssikkerhedsniveau, herunder krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankrede processer.

Stk. 2. Center for Cybersikkerhed kan påbyde udbydere af offentligt tilgængelige net og tjenester at inddrage nærmere angivne områder af deres virksomhed samt nærmere angivne trusler mod informationssikkerheden i deres risikostyringsprocesser efter stk. 1.

Stk. 3. Såfremt det er af væsentlig samfundsmæssig betydning, kan Center for Cybersikkerhed påbyde udbydere af offentligt tilgængelige net og tjenester at træffe konkrete foranstaltninger med henblik på at sikre informationssikkerheden i offentligt tilgængelige net og tjenester. Centeret fastsætter nærmere regler herom.

§ 4. Center for Cybersikkerhed fastsætter regler om oplysnings- og underretningspligter for udbydere. Reglerne kan omfatte krav om:

1) Erhvervsmæssige udbydere af offentligt tilgængelige net og tjenesters afgivelse af oplysninger til Center for Cybersikkerhed om væsentlige dele af udbyderens net eller tjenester eller driften heraf.
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) Udbydere af offentligt tilgængelige net og tjenesters underretning af Center for Cybersikkerhed ved brud på informationssikkerheden, der har væsentlige følger for driften af net eller tjenester.
4) Udbydere af offentligt tilgængelige net og tjenesters underretning af offentligheden ved brud på informationssikkerheden, der har væsentlige følger for driften af net eller tjenester.

Kapitel 3
Elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer

§ 5. Center for Cybersikkerhed fastsætter regler om, at udbydere skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger for i videst muligt omfang at sikre elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer.

Stk. 2. For erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester kan det i regler efter stk. 1 endvidere fastsættes, at udbyderne med henblik på at sikre elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer skal:

1) Udarbejde beredskabsplaner baseret på en dokumenteret og ledelsesforankret risikostyringsproces.
2) Planlægge og deltage i øvelsesaktiviteter.

Stk. 3. Center for Cybersikkerhed koordinerer og prioriterer beredskabsaktørernes behov for samfundsvigtig elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer. Center for Cybersikkerhed kan fastsætte regler om, at erhvervsmæssige udbydere skal sikre, at de foretagne prioriteringer gennemføres i net og tjenester.

Stk. 4. I beredskabssituationer og i andre ekstraordinære situationer kan Center for Cybersikkerhed påbyde erhvervsmæssige udbydere uden unødigt ophold at iværksætte nærmere angivne sikkerhedsforanstaltninger i tilfælde af en hændelse eller trussel, der i betydeligt omfang påvirker eller vurderes at ville kunne påvirke udbuddet af net eller tjenester negativt.

Kapitel 4
Sikkerhedsgodkendelse

§ 6. Efter indstilling fra en udbyder sikkerhedsgodkender sikkerhedsmyndigheden udbyderens medarbejdere og repræsentanter for udbyderen, når de pågældende som led i deres konkrete opgaveløsning for udbyderen skal behandle klassificerede informationer eller andre informationer, der er særligt beskyttelsesværdige i relation til informationssikkerhed eller beredskab.

Stk. 2. Erhvervsmæssige udbydere af offentligt tilgængelige net er forpligtede til at sikre, at medarbejdere eller repræsentanter for udbyderen, der varetager kontakten til Center for Cybersikkerhed i relation til beredskabet i henhold til § 5, stk. 2, i fornødent omfang sikkerhedsgodkendes efter stk. 1.

Stk. 3. Udbydere, hvis medarbejdere eller repræsentanter sikkerhedsgodkendes efter stk. 1, skal sikre overholdelse af sikkerhedsmyndighedens anvisninger om behandling af klassificerede informationer.

Stk. 4. Udbydere, hvis medarbejdere eller repræsentanter sikkerhedsgodkendes efter stk. 1, skal uden ugrundet ophold underrette sikkerhedsmyndigheden, når sikkerhedsgodkendte personer ikke længere varetager de opgaver for udbyderen, som lå til grund for sikkerhedsgodkendelsen.

Stk. 5. Sikkerhedsmyndigheden kan tilbagekalde en sikkerhedsgodkendelse, når betingelserne for sikkerhedsgodkendelse ikke længere er til stede.

Stk. 6. Center for Cybersikkerhed kan fastsætte regler om sikkerhedsgodkendelse af udbyderes medarbejdere eller repræsentanter for udbydere, der har adgang til udstyr eller systemer, som benyttes i forbindelse med indgreb i meddelelseshemmeligheden.

Kapitel 5
Aktindsigt i underretninger m.v.

§ 7. Det kan i regler udstedt i medfør af § 4 fastsættes, at underretninger samt afgivelse af oplysninger efter § 4, nr. 1-3, er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

§ 8. Myndigheder og virksomheder kan underrette Center for Cybersikkerhed om hændelser, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale services.

Stk. 2. Underretninger efter stk. 1 er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Kapitel 6
Tilsyn m.v.

§ 9. Center for Cybersikkerhed påser overholdelsen af denne lov og regler, der er udstedt i medfør af loven.

Stk. 2. Center for Cybersikkerhed kan som led i sit tilsyn kræve, at udbydere fremlægger alle de oplysninger og det materiale om informationssikkerhed, beredskab og sikkerhedsgodkendelse, der er nødvendige for centerets tilsynsvirksomhed, herunder til afgørelse af, om et forhold falder ind under denne lov eller regler, der er udstedt i medfør af loven.

Stk. 3. Center for Cybersikkerhed kan stille krav om, hvordan og i hvilken form oplysninger og materiale efter stk. 2 skal afgives.

Stk. 4. Center for Cybersikkerhed kan afkræve udbydere skriftlige udtalelser og redegørelser om faktiske forhold.

Stk. 5. Center for Cybersikkerhed kan stille krav om, at udbydere skal foranstalte en uafhængig sikkerhedsrevision og stille resultaterne heraf til rådighed for centeret.

Stk. 6. Hvis det er nødvendigt af hensyn til informationssikkerheden, har Center for Cybersikkerhed efter et varsel på mindst syv arbejdsdage uden retskendelse mod behørig legitimation adgang til udbyderes forretningslokaler med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven. Center for Cybersikkerhed kan ikke i forbindelse med adgang til forretningslokaler tilgå kommunikation til, fra eller mellem udbyderens kunder.

Stk. 7. Hvis det er nødvendigt af hensyn til informationssikkerheden, har Center for Cybersikkerhed efter et varsel på mindst syv arbejdsdage uden retskendelse mod behørig legitimation adgang til forretningslokaler hos udbyderes samarbejdspartnere, leverandører eller underleverandører med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven, i relation til outsourcet aktivitet. Center for Cybersikkerhed kan ikke i forbindelse med adgang til forretningslokaler tilgå kommunikation til, fra eller mellem udbyderens kunder.

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

1) Afgørelser truffet i medfør af § 3, stk. 2 og 3, og § 5, stk. 4, samt afgørelser truffet i medfør af regler, der er udstedt i medfør af §§ 3-5 og § 6, stk. 6.
2) Resultater af tilsyn efter § 9.
3) Resuméer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde for overtrædelse af denne lov eller regler, der er udstedt i medfør af denne lov.
4) Resuméer af domme i retssager, hvor Center for Cybersikkerhed er part.

Stk. 2. Offentliggørelse efter stk. 1 må ikke indeholde

1) oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold eller lignende, for så vidt det er af væsentlig økonomisk betydning for den udbyder, som oplysningerne angår,
2) oplysninger, der er af væsentlig betydning for statens sikkerhed eller rigets forsvar,
3) klassificerede informationer,
4) fortrolige oplysninger, der hidrører fra nationale tilsynsmyndigheder i andre EU-medlemsstater, medmindre de myndigheder, der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse til offentliggørelse, eller
5) oplysninger om enkeltpersoners forhold.

Stk. 3. Center for Cybersikkerhed fastsætter nærmere regler om sagsbehandlingen i forbindelse med offentliggørelse efter stk. 1.

§ 11. Center for Cybersikkerhed kan fastsætte regler om, at skriftlig kommunikation til og fra centeret om nærmere bestemte forhold, som er omfattet af denne lov eller af regler udstedt i medfør af denne lov, skal foregå digitalt.

Stk. 2. Center for Cybersikkerhed kan fastsætte regler om digital kommunikation, herunder om anvendelsen af bestemte it-systemer og særlige digitale formater samt digital signatur eller lignende.

Stk. 3. En digital meddelelse anses for at være kommet frem, når den er tilgængelig for adressaten for meddelelsen.

§ 12. Center for Cybersikkerhed kan hos udbydere indsamle oplysninger med henblik på at videregive disse til Europa-Kommissionen, Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) eller nationale tilsynsmyndigheder i andre EU-medlemsstater, således at disse kan opfylde deres opgaver i forhold til traktatmæssige forpligtelser eller forpligtelser i henhold til den gældende fællesskabsret og EU-retten.

Stk. 2. Center for Cybersikkerhed orienterer de udbydere, der er indsamlet oplysninger fra, forud for videregivelse af oplysningerne til Europa-Kommissionen, Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) eller nationale tilsynsmyndigheder i andre EU-medlemsstater.

Stk. 3. Oplysninger, der modtages eller stammer fra nationale tilsynsmyndigheder i andre EU-medlemsstater, behandles som fortrolige, hvis den afgivende nationale tilsynsmyndighed betragter oplysningerne som forretningshemmeligheder i henhold til EU-regler eller nationale regler.

Kapitel 7
EU-retsakter

§ 13. Center for Cybersikkerhed kan fastsætte regler, som er nødvendige for at gennemføre retsakter udstedt af Den Europæiske Union vedrørende informationssikkerhed og beredskab på teleområdet, herunder regler om sanktioner i form af bøder for manglende overholdelse af retsakterne.

Kapitel 8
Straffebestemmelser

§ 14. Med bøde straffes den, der:

1) Undlader at efterkomme Center for Cybersikkerheds påbud efter § 3, stk. 2 og 3, samt § 5, stk. 4.
2) Overtræder § 6, stk. 2-4.
3) Undlader at efterkomme Center for Cybersikkerheds krav efter § 9, stk. 2, 4 og 5.
4) Hindrer Center for Cybersikkerhed i at få adgang efter § 9, stk. 6 og 7.

Stk. 2. I regler, som udfærdiges i medfør §§ 3-5 og § 6, stk. 6, kan der fastsættes straf af bøde for overtrædelse af bestemmelserne i reglerne.

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

Kapitel 9

Ikrafttræden m.v.

§ 15. Loven træder i kraft den 1. december 2015.

§ 16. I lov om elektroniske kommunikationsnet og -tjenester, jf. lovbekendtgørelse nr. 128 af 7. februar 2014, foretages følgende ændringer:

1. *§ 8 a*, *§ 20, stk. 3*, *§ 62*, *§ 63*, *§ 64 a* og *§ 66 a* ophæves.

2. *§ 73, stk. 3*, ophæves.
Stk. 4 og 5 bliver herefter stk. 3 og 4.

3. I *§ 73, stk. 5*, der bliver stk. 4, udgår », Forsvarsministeriet«.

4. *§ 75 a, stk. 5*, og *§ 75 b, stk. 2*, ophæves.

5. I *§ 75 c, stk. 1*, ændres »jf. § 75 a, stk. 1, 4 og 5,« til: »jf. § 75 a, stk. 1 og 4,«.

6. I *§ 75 c, stk. 2*, udgår »og forsvarsministeren« og »for deres respektive områder«.

7. *§ 76, stk. 2*, ophæves.
Stk. 3 bliver herefter stk. 2.

8. I *§ 79, stk. 1*, udgår », Forsvarsministeriet«.

9. I *§ 81, stk. 1, nr. 1*, ændres »§ 31, stk. 4-7, § 35 eller § 63, stk. 2, 3 og 5« til: »§ 31, stk. 4-7, eller § 35«.

10. I *§ 81, stk. 2*, ændres »§ 8, stk. 1, § 8 a, stk. 1, og §§ 9, 13 b, 13 c, 61 og 62« til: »§ 8, stk.1, og §§ 9, 13 b, 13 c og 61«.

§ 17. Loven gælder ikke for Færøerne og Grønland.

[1] *Loven indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet), EU-Tidende 2002, nr. L 108, side 33, som ændret ved Europa-Parlamentets og Rådets forordning (EF) nr. 717/2007 af 27. juni 2007 om roaming på offentlige mobiltelefonnet i Fællesskabet og om ændring af direktiv 2002/21/EF, EU-tidende 2007, L 171, side 32; Europa-Parlamentets og Rådets forordning (EF) nr. 544/2009 af 18. juni 2009 om ændring af forordning (EF) nr. 717/2007 om roaming på offentlige mobiltelefonnet i Fællesskabet og af direktiv 2002/21/EF om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester, EU-tidende 2009, L 167, side 12; samt Europa-Parlamentets og Rådets direktiv 2009/140/EF af 25. november 2009 om ændring af direktiv 2002/21/EF om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester, direktiv 2002/19/EF om adgang til og samtrafik mellem elektroniske kommunikationsnet og tilhørende faciliteter og direktiv 2002/20/EF om tilladelser til elektroniske kommunikationsnet og -tjenester, EU-tidende 2009, L 337, side 37; og Europa-Parlamentets og Rådets direktiv 2002/22/EF af 7. marts 2002 om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester (forsyningspligtdirektivet), EU-Tidende 2002, nr. L 108, side 51, som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 om ændring af direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester, direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor og forordning (EF) nr. 2006/2004 om samarbejde mellem nationale myndigheder med ansvar for håndhævelse af lovgivning om forbrugerbeskyttelse, EU-tidende 2009, L 337, side 11.*

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning
2. Baggrunden for og formålet med lovforslaget
3. Lovforslagets hovedindhold
    - 3.1. Informationssikkerhed
    - 3.2. Beredskab
    - 3.3. Aktindsigt i underretninger m.v.
    - 3.4. Tilsyn og offentliggørelse
4. Økonomiske og administrative konsekvenser for det offentlige
5. Økonomiske og administrative konsekvenser for erhvervslivet m.v.
6. Administrative konsekvenser for borgerne
7. Miljømæssige konsekvenser
8. Forholdet til EU-retten
9. Hørte myndigheder og organisationer m.v.
10. Sammenfattende skema

1. Indledning

Et stærkt digitaliseret samfund som det danske er i stigende grad afhængigt af telenettet, der bl.a. anvendes som platform for telefoni og datakommunikation. Det samlede telenet er således en af de mest kritiske dele af samfundets informations- og kommunikationsteknologiske infrastruktur (ikt-infrastruktur).

Dermed er samfundet også særdeles sårbart, hvis dele af telenettet i kortere eller længere perioder er ude af drift, hvad enten det skyldes, at et kabel er blevet gravet over, at en storm har beskadiget mobilmaster, eller at en oversvømmelse har ramt en telefoncentral – eller det skyldes cyberangreb, hærværk eller sabotage. De store datamængder, som sendes via telenettet, indebærer desuden, at telenettet er et oplagt mål for aktører, der vil udøve industrispionage mod virksomheder eller spionage mod myndigheder og personer.

Regeringen anser en robust ikt-infrastruktur for at være af afgørende betydning for landets økonomi og sikkerhed. På teleområdet har regeringen derfor også fokus på at sikre, at teleudbyderne opretholder en høj grad af informationssikkerhed. Det indebærer, at teleudbyderne skal sikre tilgængelighed, integritet og fortrolighed i deres telenet. Som led heri skal teleudbyderne også have et beredskab, der understøtter, at samfundets funktioner i videst muligt omfang kan videreføres i tilfælde af, at telenettet påvirkes af ulykker, katastrofer og egentlige angreb.

Dette lovforslag er et led i udmøntningen af regeringsgrundlaget "Et Danmark, der står sammen" og den nationale strategi for cyber- og informationssikkerhed.

Lovforslaget indebærer, at den eksisterende regulering af informationssikkerhed og beredskab på teleområdet samles i en ny lov. Samtidig sker der en skærpelse af kravene til teleudbydernes informationssikkerhed, således at kravene i højere grad tager højde for samfundets afhængighed af telenettet og afspejler det aktuelle trusselsbillede, hvor især cyberangreb og avanceret industrispionage er stærkt stigende.

Med lovforslaget sker der en styrkelse af net- og informationssikkerheden i Danmark med henblik på at skabe en endnu mere robust ikt-infrastruktur.

2. Baggrunden for og formålet med lovforslaget

Det fremgår af regeringsgrundlaget af 3. oktober 2011, "Et Danmark, der står sammen", at "[r]egeringen vil med respekt for retssikkerheden og den personlige frihed styrke beskyttelsen mod cyberangreb. En robust infrastruktur for informations- og kommunikationsteknologi er vigtig for landets økonomi og sikkerhed. For at styrke beskyttelsen mod cyberangreb mv. samles de forskellige myndigheders indsats i et IT sikkerhedscenter (under Forsvarsministeriet), der skal varetage opgaven som den nationale IT-sikkerhedsmyndighed (…)".

Ved kongelig resolution af samme dato blev IT- og Telestyrelsen nedlagt, og ressortansvaret for sager vedrørende beskyttelse af kritisk it-infrastruktur samt statens varslingstjeneste for internettrusler (GovCERT) blev overført til Forsvarsministeriet. Herudover blev ressortansvaret for tele- og internetregulering samt administration af frekvenser overført til Erhvervs- og Vækstministeriet.

Som konsekvens af ressortomlægningen er ansvaret for lov om elektroniske kommunikationsnet og -tjenester (teleloven) i dag delt mellem to ministerier: Erhvervs- og Vækstministeriet administrerer lovens bestemmelser vedrørende teleudbydernes generelle virksomhed, mens Forsvarsministeriet administrerer lovens bestemmelser om informationssikkerhed og beredskab.

Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste varetager myndighedsopgaverne inden for informationssikkerhed og beredskab på teleområdet. Center for Cybersikkerhed træffer som led i centerets almindelige myndighedsudøvelse og tilsynsvirksomhed afgørelser ved manglende overholdelse af teleloven eller regler, der er udstedt i medfør af loven. Center for Cybersikkerheds organisatoriske tilhørsforhold indebærer, at centerets afgørelser kan påklages til Forsvarsministeriet i medfør af den almindelige rekursadgang.

Med lovforslaget overflyttes telelovens bestemmelser om informationssikkerhed og beredskab til en ny net- og informationssikkerhedslov under Forsvarsministeriet, hvilket skaber en mere sammenhængende og overskuelig regulering på området.

Lovforslaget indebærer desuden, at bekendtgørelser, der udstedes i medfør af net- og informationssikkerhedsloven, fremover udstedes af Center for Cybersikkerhed. Dette svarer til den ordning, der var gældende frem til ressortomlægningen i 2011, hvor den daværende IT- og Telestyrelse udstedte bekendtgørelserne på området.

Med lovforslaget vil der endvidere ske en skærpelse af kravene til teleudbydernes informationssikkerhed, således at kravene i højere grad tager højde for samfundets afhængighed af telenettet og afspejler det aktuelle trusselsbillede. Forsvarets Efterretningstjeneste vurderer således, at fremmede efterretningstjenester, statsstøttede grupper og enkeltpersoner i stigende grad bruger internettet til at spionere mod Danmark og forsøger at afdække vigtige it-systemer og stjæle viden. Der har endvidere i de seneste år været adskillige cyberangreb, som i en kortere periode har forstyrret eller hindret anvendelsen af dansk it- og teleinfrastruktur, ligesom der er konstateret cyberangreb mod væsentlige mål i Danmark, hvor informationssikkerheden er blevet kompromitteret.

Denne udvikling skaber behov for, at kravene til teleudbydernes risikostyring på informationssikkerhedsområdet skærpes. Som led heri er der bl.a. behov for, at der kan stilles krav til teleudbyderne om, at de inddrager konkrete trusler, som f.eks. er konstateret af Forsvarets Efterretningstjeneste, i grundlaget for deres risikostyring, ligesom risikostyringsprocessen skal være forankret hos teleudbydernes øverste ledelse.

I Danmark anvender teleudbyderne i stigende grad egentlige driftsleverandører – frem for blot at anvende leverandører af enkeltkomponenter. Dermed varetager leverandørerne i stigende omfang driften af centrale dele af den danske ikt-infrastruktur.

En særlig udfordring på informationssikkerhedsområdet er, at visse af de leverandører, som teleudbyderne anvender, i sig selv kan udgøre en trussel mod informationssikkerheden. Det gælder bl.a. i forhold til nogle leverandører, som har en tæt tilknytning til udenlandske myndigheder, og hvor der er risiko for, at adgangen til teleinfrastrukturen udnyttes til spionage, industrispionage og – i krisesituationer – direkte sabotage. Denne type trusler betegnes også som supply chain threats.

Hidtil har de danske myndigheder valgt at indgå i dialog med de teleudbydere, som har indgået større aftaler med visse leverandører. Dialogen har haft til formål at opnå enighed om en række sikkerhedsmæssige tiltag, som kan reducere risikoen ved at anvende de pågældende leverandører.

Der vil også med de nye regler være fokus på at sikre, at den løbende indsats for at fremme net- og informationssikkerheden i samfundet sker i et konstruktivt samarbejde mellem myndighederne og teleudbyderne. Hensynet til den nationale sikkerhed tilsiger imidlertid, at der i forhold til alle teleudbydere – og ikke blot dem, som er indstillede på at indgå aftaler om sikkerhedsmæssige tiltag med myndighederne – fastsættes nye og skærpede regler om informationssikkerheden, der kan tage højde for de særlige problemstillinger, som er knyttet til teleudbydernes stigende anvendelse af bl.a. driftsleverandører, der kan udgøre en trussel mod informationssikkerheden.

3. Lovforslagets hovedindhold

3.1. Informationssikkerhed

3.1.1. Gældende ret

Informationssikkerhed på teleområdet omfatter som begreb myndighedernes og virksomhedernes samlede indsats for at forebygge nedbrud i informationssystemer samt beskytte data, som behandles i systemerne, mod manipulation, tab eller tyveri.

Informationssikkerhed i teleudbydernes net og tjenester reguleres i dag i § 8 a i lov om elektroniske kommunikationsnet og -tjenester (teleloven), jf. lovbekendtgørelse nr. 128 af 7. februar 2014. Efter denne bestemmelse kan der fastsættes regler om minimumskrav til informationssikkerhed i forbindelse med udbuddet af net og tjenester, herunder krav om passende tekniske og organisatoriske foranstaltninger med henblik på at styre risici for informationssikkerheden i net og tjenester og sikre et sikkerhedsniveau, der står i forhold til risici. Bestemmelsen gennemfører artikel 13 a i Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet), som ændret ved Europa-Parlamentets og Rådets direktiv 2009/140/EF af 25. november 2009.

På informationssikkerhedsområdet er der bl.a. med hjemmel i den dagældende § 8 i teleloven (nu § 8 a) udstedt bekendtgørelse nr. 396 af 21. april 2011 om rammerne for informationssikkerhed og beredskab, som ændret ved bekendtgørelse nr. 1026 af 21. august 2013. Bestemmelserne om informationssikkerhed i bekendtgørelse nr. 445 af 11. maj 2011 om informationssikkerhed og beredskab for elektroniske kommunikationsnet og -tjenester, som ændret ved bekendtgørelse nr. 1025 af 21. august 2013, er udstedt med hjemmel i den dagældende § 8 i teleloven (nu § 8 a) samt § 3, stk. 1-3, i bekendtgørelse nr. 396 af 21. april 2011 om rammerne for informationssikkerhed og beredskab, som ændret ved bekendtgørelse nr. 1026 af 21. august 2013.

3.1.2. Forsvarsministeriets overvejelser

Teleudbydernes net og tjenester er en del af den samfundsvigtige ikt-infrastruktur, som bl.a. anvendes til virksomheders og myndigheders elektroniske kommunikation. Et højt informationssikkerhedsniveau i teleudbydernes net og tjenester er således et vigtigt element i den samlede beskyttelse af den samfundsvigtige ikt-infrastruktur.

Der er allerede i dag mulighed for at stille minimumskrav til teleudbydernes informationssikkerhed. Forsvarsministeriet finder imidlertid, at der er behov for øget fokus på informationssikkerheden, ligesom der generelt er behov for en mere overskuelig og entydig regulering af området.

En særlig problemstilling er knyttet til de seneste års udvikling på det danske telemarked, som har vist, at især de store teleudbydere i stigende grad indgår aftaler med leverandører om levering og drift af udstyr og systemer, der indgår i den samfundsvigtige ikt-infrastruktur, som bl.a. anvendes af statslige myndigheder og virksomheder, der udfører samfundsvigtige opgaver.

Konsekvensen er, at disse leverandører eksempelvis kan få direkte adgang til myndigheders eller virksomheders elektroniske kommunikation eller få adgang til kundeinformationer, der befinder sig i teleudbydernes faktureringssystemer. Dette kan i særlig grad være et problem i forhold til leverandører, der har en tæt tilknytning til udenlandske myndigheder, som dermed kan få adgang til informationer om danskere og danske interesser. I den forbindelse kan der være en risiko for, at adgangen til kommunikationssystemerne udnyttes til industrispionage og spionage mod myndigheder og personer. Desuden kan der være en risiko for, at adgangen til telenettet f.eks. i en krisesituation kan udnyttes til at påvirke tilgængeligheden af den samfundsvigtige ikt-infrastruktur.

Hensynet til den nationale sikkerhed tilsiger på den baggrund, at der fastsættes regler om informationssikkerhed, der kan tage højde for de særlige problemstillinger, som er knyttet til teleudbydernes anvendelse af leverandører, som kan udgøre en trussel mod informationssikkerheden.

Forsvarsministeriet har overvejet, om de nye krav til informationssikkerhed i net og tjenester tillige burde rettes mod leverandører til telebranchen. Forsvarsministeriet finder imidlertid, at teleudbyderne er nærmest til at fremme informationssikkerheden i net og tjenester i Danmark, idet alene teleudbyderne har forudsætningerne for at foretage en samlet vurdering af informationssikkerheden i deres net og tjenester.

Forsvarsministeriet finder endvidere, at der er behov for, at teleudbydere pålægges yderligere oplysnings- og underretningspligter med henblik på, at Center for Cybersikkerhed kan danne sig et overblik over den samlede teleinfrastruktur. Et sådant overblik er således en afgørende forudsætning for, at centeret kan foretage de nødvendige sårbarheds- og trusselsvurderinger på området. På baggrund af udviklingen på det danske telemarked finder Forsvarsministeriet endvidere, at det er nødvendigt, at Center for Cybersikkerhed får kendskab til aftaler, som udbyderne påtænker at indgå med leverandører. Det vil give Center for Cybersikkerhed mulighed for at vurdere sårbarheder i relation til supply chain threats samt i højere grad muliggøre en fokuseret rådgivningsindsats.

3.1.3. Den foreslåede ordning

Det foreslås, at reguleringen af informationssikkerhed på teleområdet samles i en net- og informationssikkerhedslov, således at reguleringen bliver mere overskuelig.

Endvidere foreslås det, at der skabes en entydig hjemmel til, at Center for Cybersikkerhed som myndighed på området kan fastsætte konkrete krav til teleudbyderes informationssikkerhed. Først og fremmest kan der stilles krav til, at teleudbyderne håndterer informationssikkerheden gennem dokumenterede og ledelsesforankrede risikostyringsprocesser. Herudover kan der fastsættes nærme-

re krav til teleudbydernes risikostyring på informationssikkerhedsområdet i forbindelse med indgåelse og gennemførelse af aftaler med leverandører.

Samtidig foreslås det, at Center for Cybersikkerhed fremover skal kunne påbyde teleudbydere at inddrage nærmere angivne områder af deres virksomhed samt nærmere angivne trusler mod informationssikkerheden i deres risikostyringsprocesser. Dermed kan Center for Cybersikkerhed eksempelvis påbyde en teleudbyder at tage højde for en konkret trussel mod informationssikkerheden, som ud fra et samfundsmæssigt perspektiv vurderes som værende alvorlig. Det kan bl.a. ske med udgangspunkt i de trusselsvurderinger, som løbende udarbejdes af Center for Cybersikkerhed og den øvrige del af Forsvarets Efterretningstjeneste.

Herudover foreslås det, at Center for Cybersikkerhed fremover skal kunne påbyde teleudbydere at træffe foranstaltninger med henblik på at sikre informationssikkerheden, hvis sådanne foranstaltninger er af væsentlig samfundsmæssig betydning. Dermed kan Center for Cybersikkerhed f.eks. påbyde en teleudbyder at iagttage særlige foranstaltninger, hvis udbyderen har valgt at benytte software, som konkret vurderes at udgøre en sådan trussel mod informationssikkerheden, at det har betydning for varetagelsen af væsentlige samfundsmæssige hensyn.

Det grundlæggende princip om aftalefrihed vil fortsat være gældende. Den foreslåede ordning indebærer således ikke, at der kan ske regulering af ejerforhold, nedlægges forbud mod at indgå aftale med bestemte leverandører eller nedlægges forbud mod ejerskab af bestemte netværk eller produkter.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 3.

Det foreslås endvidere, at Center for Cybersikkerhed bemyndiges til at fastsætte regler om oplysnings- og underretningspligter for teleudbydere.

Den foreslåede oplysningspligt vil indebære, at teleudbydere efter anmodning skal afgive oplysninger om de dele af deres net eller tjenester – eller driften heraf – der anses som væsentlige. Det kan f.eks. være oplysninger om hvilke leverandører, som teleudbyderen anvender. Dermed sikres det, at Center for Cybersikkerhed kan få det nødvendige overblik over de centrale dele af teleinfrastrukturen.

Oplysningspligten foreslås suppleret af en underretningspligt, som indebærer, at teleudbydere skal underrette Center for Cybersikkerhed i forbindelse med påtænkte indgåelser af visse større aftaler om leverancer af hardware, firmware eller software samt driften heraf. Teleudbyderne skal endvidere indsende det endelige aftaleudkast til Center for Cybersikkerhed umiddelbart forud for indgåelsen af aftalen. I den forbindelse påtænkes der indført en kort standstill-periode, således at Center for Cybersikkerhed kan foretage en vurdering af aftaleudkastet. Standstill-periodens korte varighed sikrer, at aftaleindgåelsen ikke forsinkes unødigt.

Formålet med ordningen er at give Center for Cybersikkerhed mulighed for at rådgive teleudbyderen om særlige trusler mod informationssikkerheden samt om mulighederne for at imødegå de trusler, som det pågældende aftaleudkast vurderes at indebære. Dette vil bidrage til, at teleudbyderne får bedre forudsætninger for at vurdere mulige risici ved den påtænkte aftale, således at teleudbyderne kan tage højde herfor inden aftaleindgåelsen. Det bemærkes, at Center for Cybersikkerhed ikke i forbindelse med standstill-perioden kan nedlægge forbud mod indgåelse af aftalen eller påbyde teleudbyderen at ændre aftaleudkastet.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 4.

3.2. Beredskab

3.2.1. Gældende ret

Elektronisk kommunikation er i stigende grad en forudsætning for opretholdelse af samfundets funktioner, hvilket stiller krav til en robust teleinfrastruktur. I beredskabssituationer og i andre ekstraordinære situationer, hvor samfundet rammes af naturskabte eller menneskeskabte ulykker eller katastrofer, vil den elektroniske kommunikation og dermed en fungerende teleinfrastruktur være nødvendig for, at samfundsvigtige funktioner kan opretholdes.

Ikke mindst de forskellige aktører, der indgår i samfundets beredskab, kan i beredskabssituationer og i andre ekstraordinære situationer have behov for elektronisk kommunikation for at udføre en række af deres opgaver, ligesom elektronisk kommunikation er en forudsætning for, at de kan koordinere deres indsats.

Det er derfor nødvendigt med et beredskab på teleområdet, som sikrer, at den elektroniske kommunikation i videst muligt omfang opretholdes i beredskabssituationer og i andre ekstraordinære situationer, og som tilgodeser beredskabsaktørernes behov for elektronisk kommunikation.

Beredskabet på teleområdet omfatter planlæggende og forberedende tiltag med henblik på at sikre, at net- og tjenesteudbuddet i videst muligt omfang kan opretholdes i beredskabssituationer. Endvidere omfatter beredskabet iværksættelsen af konkrete tiltag i selve beredskabssituationen.

Kravene til beredskabet – i form af krav til sikring af samfundsvigtig elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer – er reguleret i telelovens § 62, der gennemfører artikel 23 i Europa-Parlamentets og Rådets direktiv 2002/22/EF af 7. marts 2002 om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester (forsyningspligtdirektivet), som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009.

Efter telelovens § 62, stk. 1, bemyndiges forsvarsministeren til at fastsætte nærmere regler om, at erhvervsmæssige teleudbydere skal foretage nødvendig planlægning og træffe nødvendige foran-

staltninger for at sikre samfundsvigtig elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer. Herudover bemyndiges forsvarsministeren til at fastsætte nærmere regler om, at ejere af net, der anvendes til erhvervsmæssigt udbud af offentligt tilgængelige tjenester, skal udarbejde beredskabsplaner baseret på en dokumenteret risikostyringsproces, sikre passende beskyttelse af kritisk teleinfrastruktur samt planlægge og deltage i øvelsesaktivitet. Endvidere bemyndiges forsvarsministeren efter telelovens § 62, stk. 3, til at fastsætte tilsvarende regler om beredskab for offentlige myndigheder og for offentlige og private virksomheder og institutioner. Det fremgår desuden af telelovens § 62, stk. 4, at Forsvarsministeriet koordinerer og prioriterer beredskabsmyndighedernes behov for samfundsvigtig elektronisk kommunikation, ligesom forsvarsministeren kan fastsætte nærmere regler herom.

I forhold til beredskabet er der bl.a. med hjemmel i telelovens § 62 udstedt bekendtgørelse nr. 396 af 21. april 2011 om rammerne for informationssikkerhed og beredskab, som ændret ved bekendtgørelse nr. 1026 af 21. august 2013. Bestemmelserne om beredskab i bekendtgørelse nr. 445 af 11. maj 2011 om informationssikkerhed og beredskab for elektroniske kommunikationsnet og -tjenester, som ændret ved bekendtgørelse nr. 1025 af 21. august 2013, er udstedt med hjemmel i telelovens § 62, stk. 1, 2 og 4, samt § 5, stk. 1 og 2, og § 7, stk. 2, i bekendtgørelse nr. 396 af 21. april 2011 om rammerne for informationssikkerhed og beredskab, som ændret ved bekendtgørelse nr. 1026 af 21. august 2013. Herudover er bekendtgørelse nr. 597 af 18. juni 2009 om faste kredsløb til beredskabsmæssige formål samt bekendtgørelse nr. 598 af 18. juni 2009 om sikring af offentlige telenet og teletjenester udstedt med hjemmel i bl.a. bekendtgørelse nr. 575 af 18. juni 2009 om beredskab for elektroniske kommunikationsnet og -tjenester (nu bekendtgørelse nr. 396 af 21. april 2011 om rammerne for informationssikkerhed og beredskab).

3.2.2. Forsvarsministeriets overvejelser

På baggrund af de hidtidige erfaringer med beredskabet på teleområdet finder Forsvarsministeriet, at der er behov for en tilpasning af reguleringen, således at den på visse områder tydeliggøres og får et bredere anvendelsesområde.

Forsvarsministeriet finder således, at der i overensstemmelse med ordlyden af artikel 23 i forsyningspligtdirektivet bør stilles overordnede krav til samtlige teleudbyderes beredskabsplanlægning med henblik på i videst muligt omfang at sikre elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer. En sådan ordning vil indebære, at teleudbyderne i videst muligt omfang skal sikre elektronisk kommunikation og ikke kun samfundsvigtig elektronisk kommunikation.

Herudover finder Forsvarsministeriet, at de skærpede krav til beredskabsplanlægning og øvelsesaktivitet bør stilles til en større gruppe end hidtil, nemlig de erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester. Skærpelsen i form af krav om udvidet beredskabsplanlægning vil dermed blive målrettet de teleudbydere, der er ansvarlige for det samlede erhvervsmæssige udbud af

offentligt tilgængelige net og tjenester – og som dermed har en særligt vigtig rolle i forbindelse med beredskabssituationer og i andre ekstraordinære situationer.

Samtidig finder Forsvarsministeriet, at Center for Cybersikkerheds koordinerende og prioriterende rolle i forhold til telesektoren bør tydeliggøres. I en beredskabssituation eller i en anden ekstraordinær situation er centeret bindeled mellem myndigheder og teleudbydere, og centeret koordinerer og prioriterer i disse situationer beredskabsaktørernes behov for elektronisk kommunikation, således at det ved begrænset kapacitet til elektronisk kommunikation sikres, at den tilgængelige kapacitet stilles til rådighed for de vigtigste beredskabsaktører. Forsvarsministeriet finder derudover, at der bør skabes en klar hjemmel til, at centeret i en beredskabssituation eller i en anden ekstraordinær situation kan udstede påbud til teleudbyderne om at iværksætte akutte sikkerhedsforanstaltninger.

3.2.3. Den foreslåede ordning

Det foreslås, at Center for Cybersikkerhed bemyndiges til at fastsætte regler om, at teleudbydere skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger for i videst muligt omfang at sikre elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer.

Det foreslås endvidere, at Center for Cybersikkerhed bemyndiges til at stille krav til beredskabsplanlægning og deltagelse i øvelsesaktivitet til en større gruppe i form af de erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester. Med denne ordning vil de erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester være omfattet af de overordnede krav til beredskabsplanlægning, men disse udbydere kan herudover forpligtes til at udarbejde beredskabsplaner baseret på en dokumenteret og ledelsesforankret risikostyringsproces samt planlægge og deltage i øvelsesaktivitet med henblik på forberedelse af beredskabssituationer og andre ekstraordinære situationer.

Det foreslås desuden, at det tydeliggøres, at det er Center for Cybersikkerhed, som koordinerer og prioriterer beredskabsaktørernes behov for samfundsvigtig elektronisk kommunikation. Samtidigt foreslås det præciseret, at Center for Cybersikkerhed kan fastsætte regler om, at visse teleudbydere skal sikre, at de foretagne prioriteringer i net og tjenester gennemføres.

Det foreslås herudover, at Center for Cybersikkerhed i beredskabssituationer og i andre ekstraordinære situationer kan påbyde erhvervsmæssige teleudbydere uden unødigt ophold at iværksætte nærmere angivne sikkerhedsforanstaltninger i tilfælde af en hændelse eller trussel, der i betydeligt omfang påvirker – eller vurderes at ville kunne påvirke – udbuddet af net eller tjenester negativt.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 5.

3.3. Aktindsigt i underretninger m.v.

3.3.1. Gældende ret

Efter telelovens § 8 a kan Forsvarsministeren fastsætte regler om minimumskrav til informationssikkerhed i forbindelse med udbuddet af elektroniske komunikationsnet og -tjenester, herunder krav om at teleudbydere skal underrette Forsvarsministeriet ved brud på informationssikkerheden med væsentlige følger for drift af net eller tjenester. Denne underretningspligt er udmøntet ved § 14 i bekendtgørelse nr. 445 af 11. maj 2011 om informationssikkerhed og beredskab for elektroniske kommunikationsnet og -tjenester, som ændret ved bekendtgørelse nr. 1025 af 21. august 2013. Bekendtgørelsen er bl.a. udstedt med hjemmel i den dagældende § 8 i teleloven (nu § 8 a) samt § 3, stk. 1-3, i bekendtgørelse nr. 396 af 21. april 2011 om rammerne for informationssikkerhed og beredskab, som ændret ved bekendtgørelse nr. 1026 af 21. august 2013.

Underretningen sker til Center for Cybersikkerhed, og de modtagne underretninger skal behandles efter lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed, der fastsætter generelle rammer for centerets sagsbehandling, herunder behandling af personoplysninger.

Det følger af § 8 i lov om Center for Cybersikkerhed, at centerets virksomhed er undtaget fra lov om offentlighed i forvaltningen (offentlighedsloven) bortset fra lovens § 13 om notatpligt. Centerets virksomhed er endvidere undtaget fra forvaltningslovens kapitel 4-6. Det fremgår imidlertid af afsnit 3.3.3 i de almindelige bemærkninger til forslaget til lov om Center for Cybersikkerhed (L 192, F.T. 2013-14), 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 om partens aktindsigt.

En anmodning om aktindsigt i underretninger, der er modtaget fra teleudbydere, skal dermed efter gældende ret behandles efter principperne i offentlighedsloven.

3.3.2. Forsvarsministeriets overvejelser

Underretningspligten efter teleloven foreslås videreført i net- og informationssikkerhedsloven, ligesom der foreslås indført en ny underretningspligt, som indebærer, at teleudbydere skal underrette Center for Cybersikkerhed i forbindelse med påtænkte indgåelser af visse større aftaler om leverancer af hardware, firmware eller software samt driften heraf. Endvidere foreslås der indført en oplysningspligt, hvorefter teleudbydere skal afgive oplysninger om de dele af deres net eller tjenester – eller driften heraf – der anses som væsentlige, jf. afsnit 3.1.3 og bemærkningerne til den foreslåede § 4.

De foreslåede oplysnings- og underretningspligter indebærer, at teleudbyderne skal stille en række nye oplysninger til rådighed for Center for Cybersikkerhed. Det kan f.eks. være oplysninger om opbygning og design af teleudbydernes teleinfrastruktur, ligesom teleudbydernes aftaler med leverandører og andre samarbejdspartnere fremover i en række tilfælde skal fremsendes til centeret.

Forsvarsministeriet finder, at en velfungerende ordning på dette område forudsætter, at der ikke er risiko for, at de ofte særligt kommercielt følsomme oplysninger, som vil blive modtaget fra teleudbyderne, kan tilgå teleudbydernes konkurrenter eller potentielle angribere.

Efter gældende ret skal anmodninger om aktindsigt i de modtagne oplysninger behandles efter principperne i offentlighedsloven. Selv om visse af oplysningerne kan undtages fra aktindsigt efter undtagelsesbestemmelserne i offentlighedsloven, kan meddelelse af aktindsigt i de øvrige oplysninger skade teleudbyderne. Således vil selve oplysningen om, at der påtænkes indgået en aftale af en sådan karakter, at der er sket underretning af Center for Cybersikkerhed, potentielt være skadelig for en teleudbyder, hvis oplysningen via aktindsigt bliver tilgængelige for en konkurrent. På samme vis kan selv meget overordnede oplysninger om teleudbydernes infrastruktur, f.eks. deres valg af leverandører, misbruges af hackere og industrispioner, der gennem disse oplysninger får et øget kendskab til den infrastruktur, som er mål for deres angreb. De oplysninger, som Center for Cybersikkerhed som led i underretningsordningen modtager fra udbydere ved brud på informationssikkerheden, vil endvidere ofte indeholde oplysninger om fejl eller sårbarheder i net eller tjenester, som kan misbruges af potentielle angribere, hvis de kommer til uvedkommendes kendskab. Derfor bør disse oplysninger udtrykkeligt være undtaget fra aktindsigt.

Tilsvarende hensyn gør sig gældende i forhold til den mere generelle underretningsordning, som findes på cybersikkerhedsområdet. For statslige myndigheder er der pr. 1. september 2014 som følge af en regeringsbeslutning etableret en egentlig forpligtelse til at underrette Center for Cybersikkerhed ved større it-sikkerhedsmæssige hændelser, f.eks. hacker- og overbelastningsangreb. For øvrige myndigheder og virksomheder er der etableret en helt igennem frivillig ordning, hvor de pågældende organisationer opfordres til at underrette Center for Cybersikkerhed ved større sikkerhedshændelser. Ordningen er etableret efter dialog med en række branche- og interesseorganisationer samt virksomheder.

Underretning af Center for Cybersikkerhed ved større sikkerhedshændelser skaber de bedst mulige forudsætninger for, at centeret kan udnytte erfaringer med cybertrusler og sikkerhedsrisici på tværs af samfundet – og dermed skabe et samlet overblik over den aktuelle sikkerhedstilstand på den danske del af internettet. Underretningerne sætter således Center for Cybersikkerhed i stand til at varsle hurtigere om trusler og styrke grundlaget for centerets rådgivning om risici og passende sikkerhedstiltag.

Oplysninger om, at der f.eks. er gennemført et vellykket hackerangreb, hvor en virksomhed har mistet data, kan imidlertid i høj grad skade virksomhedens omdømme, og risikoen for, at oplysningerne via aktindsigt bliver offentligt tilgængelige, kan i praksis afholde mange virksomheder fra at underrette Center for Cybersikkerhed om et sådant hackerangreb. Derfor bør også disse særlige underretninger være undtaget fra aktindsigt.

Et tilsvarende hensyn gør sig imidlertid ikke gældende i forhold til teleudbyderes og øvrige virksomheders mulighed for at gøre sig bekendt med oplysninger, der vedrører deres egne forhold. For-

svarsministeriet finder derfor, at undtagelsen fra aktindsigt ikke bør omfatte teleudbyderes og øvrige virksomheders adgang til indsigt i egne forhold.

3.3.3. Den foreslåede ordning

Det foreslås, at gældende ret i forhold til aktindsigt som udgangspunkt videreføres. Det indebærer, at der er ret til aktindsigt i Center for Cybersikkerheds sagsbehandling i medfør af denne lov efter principperne i offentlighedsloven samt ret til partsaktindsigt efter principperne i forvaltningsloven.

På to helt særlige områder foreslås det imidlertid, at der fremover ikke skal være ret til aktindsigt, herunder partsaktindsigt. Det gælder 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, samt i forhold til underretninger, der på cybersikkerhedsområdet modtages fra myndigheder og virksomheder om f.eks. hackerangreb.

Det foreslås, at undtagelsen fra aktindsigt ikke omfatter teleudbyderes og øvrige virksomheders adgang til at gøre sig bekendt med oplysninger, der vedrører deres egne forhold.

Der henvises i øvrigt til bemærkningerne til de foreslåede §§ 7 og 8.

Det bemærkes, at Center for Cybersikkerheds behandling af personoplysninger er underlagt tilsyn fra et uafhængigt tilsyn, Tilsynet med Efterretningstjenesterne, jf. kapitel 9 i lov om Center for Cybersikkerhed.

3.4. Tilsyn og offentliggørelse

3.4.1. Gældende ret

Center for Cybersikkerhed fører på vegne af Forsvarsministeriet tilsyn med teleudbydernes overholdelse af bestemmelserne om informationssikkerhed og beredskab i først og fremmest telelovens §§ 8 a og 62. Tilsynsbestemmelserne fremgår af telelovens § 8 a, stk. 3, § 20, stk. 3, og § 64 a, stk. 1.

Der kan i medfør af telelovens § 8 a, stk. 3, og § 64 a, stk. 1, fastsættes nærmere regler om tilsynet med overholdelsen af bestemmelserne om informationssikkerhed og beredskab. Bemyndigelserne er udmøntet i bekendtgørelse nr. 445 af 11. maj 2011 om informationssikkerhed og beredskab for elektroniske kommunikationsnet og -tjenester, som ændret ved bekendtgørelse nr. 1025 af 21. august 2013. Bekendtgørelsen om informationssikkerhed og beredskab er bl.a. udstedt med hjemmel i de dagældende § 8, stk. 4 (nu § 8 a, stk. 3), og § 64, stk. 1 og 2 (nu § 64 a, stk. 1 og 2), i teleloven, samt § 3, stk. 3, i bekendtgørelse nr. 396 af 21. april 2011 om rammerne for informationssikkerhed og beredskab, som ændret ved bekendtgørelse nr. 1026 af 21. august 2013.

Det fremgår af § 20, stk. 2, i bekendtgørelse nr. 445 af 11. maj 2011 om informationssikkerhed og beredskab for elektroniske kommunikationsnet og -tjenester, som gennemfører artikel 13 b (2b) i rammedirektivet, at teleudbydere efter anmodning skal foranstalte en uafhængig sikkerhedsrevision og stille resultaterne heraf til rådighed for Center for Cybersikkerhed. Det fremgår endvidere af bekendtgørelsens § 21, stk. 1, at Center for Cybersikkerhed kan påbyde teleudbyderne at udlevere en årlig redegørelse for deres samlede beredskabsplanlægning.

Herudover følger det af telelovens § 73, stk. 3, jf. stk. 1, at Center for Cybersikkerhed kan kræve alle oplysninger og alt materiale hos teleudbyderne, som centeret skønner relevant i forbindelse med sit tilsyn m.v.

3.4.2. Forsvarsministeriets overvejelser

Et velfungerende tilsyn på informationssikkerheds- og beredskabsområdet er en væsentlig forudsætning for at sikre en robust teleinfrastruktur og opretholdelse af net- og tjenesteudbuddet.

Med henblik på at skabe et mere effektivt tilsyn finder Forsvarsministeriet, at Center for Cybersikkerhed bør kunne anmode teleudbyderne om at forholde sig skriftligt til problemstillinger, som centeret bliver opmærksom på i forbindelse med sin tilsynsvirksomhed. Derfor bør centeret have mulighed for at kræve, at teleudbyderne udarbejder skriftlige udtalelser og redegørelser om faktiske forhold.

For at kunne konstatere, om teleudbyderne i praksis har gennemført de nødvendige foranstaltninger til at sikre teleinfrastrukturen, er det endvidere nødvendigt, at Center for Cybersikkerhed som led i et rutinemæssigt tilsyn har adgang uden retskendelse til forretningslokaler hos teleudbydere og deres eventuelle samarbejdspartnere, leverandører og underleverandører.

Forsvarsministeriet finder, at Center for Cybersikkerhed bør have en sådan adgang efter samme model, som anvendes på en lang række andre retsområder. Tilsynsbesøgene vil blive foretaget som led i et rutinemæssigt tilsyn, og der vil derfor ikke forud for besøget være indikationer på manglende overholdelse af lovgivningen. Dermed vil der i sagens natur ikke foreligge et mistankegrundlag, som vil kunne danne grundlag for en retskendelse. Spørgsmålet om centerets adgang til bl.a. teleudbydernes forretningslokaler i forbindelse med rutinemæssige tilsynsbesøg vurderes derfor ikke at være egnet til domstolsprøvelse.

Forsvarsministeriet finder endvidere, at der er behov for, at Center for Cybersikkerhed i ikke-anonymiseret form kan offentliggøre afgørelser, tilsynsresultater samt resuméer af domme og bødevedtagelser på informationssikkerheds- og beredskabsområdet.

En sådan offentliggørelsesordning vurderes at udgøre et effektivt redskab til sikring af et højt informationssikkerhedsniveau i net og tjenester. Offentliggørelsesordningen indebærer, at både eksi-

sterende og potentielle kunder vil få mulighed for at lade oplysninger om en teleudbyders informationssikkerhedsniveau indgå i overvejelserne i forbindelse med valg af teleudbyder. Dette vurderes at ville øge teleudbydernes incitament til at sikre et passende informationssikkerhedsniveau i net og tjenester, ligesom en sådan ordning vil give en konkurrencemæssig fordel til de teleudbydere, som efterlever kravene til informationssikkerhed og beredskab.

Offentliggørelsesordningen vil ikke omfatte oplysninger om enkeltpersoner. Desuden vil oplysninger om eksempelvis drifts- eller forretningsforhold blive slettet i det materiale, der offentliggøres, for så vidt det er af væsentlig økonomisk betydning for teleudbyderen.

Forsvarsministeriet finder på den baggrund, at hensynet til den enkelte teleudbyder, som de offentliggjorte oplysninger omhandler, bør vige for hensynet til at sikre et højt informationssikkerhedsniveau, som et højt digitaliseret samfund som det danske er afhængig af.

3.4.3. Den foreslåede ordning

Det foreslås, at Center for Cybersikkerhed som noget nyt skal kunne afkræve teleudbyderne skriftlige udtalelser og redegørelser om faktiske forhold.

Desuden foreslås det, at Center for Cybersikkerhed skal have adgang til teleudbyderes forretningslokaler uden retskendelse mod behørig legitimation og efter et varsel på mindst syv arbejdsdage med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven, hvis det er nødvendigt af hensyn til informationssikkerheden. Denne mulighed – der kun forudsættes anvendt, såfremt et tilsvarende resultat ikke kan opnås ved anvendelse af andre og mindre indgribende tilsynsmuligheder – vil således kun kunne anvendes i forbindelse med Center for Cybersikkerheds tilsynsvirksomhed i forhold til informationssikkerhed og beredskab på teleområdet.

Det foreslås endvidere, at Center for Cybersikkerhed under de samme betingelser uden retskendelse kan få adgang til forretningslokaler hos en udbyders samarbejdspartner, leverandør eller underleverandør med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven i relation til den outsourcede aktivitet.

Center for Cybersikkerhed vil ikke i forbindelse med tilsynsvirksomheden kunne tilgå kommunikation til, fra og mellem teleudbydernes kunder. Der vil således ikke som led i ordningen kunne ske indgreb i meddelelseshemmeligheden. Det bemærkes endvidere, at Center for Cybersikkerhed alene vil kunne foretage tilsynsbesøg, i det omfang forretningslokalerne er placeret i Danmark.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 9.

Herudover foreslås det, at Center for Cybersikkerhed som noget nyt i ikke-anonymiseret form kan offentliggøre afgørelser om overholdelse af krav til informationssikkerhed og beredskab, tilsynsresultater, resuméer af domme og bødevedtagelser, hvor der idømmes eller vedtages en bøde for over-

trædelse af loven eller regler, der er udstedt i medfør heraf samt resuméer af domme i retssager, hvor Center for Cybersikkerhed er part.

Det foreslås samtidig, at der ikke må ske offentliggørelse af visse nærmere opregnede oplysninger, herunder eksempelvis oplysninger om enkeltpersoners forhold og oplysninger vedrørende tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold eller lignende, for så vidt det er af væsentlig økonomisk betydning for den teleudbyder, som oplysningerne angår.

Det foreslås endvidere, at Center for Cybersikkerhed bemyndiges til at fastsætte nærmere regler for sagsbehandlingen i forbindelse med offentliggørelserne.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 10.

4. Økonomiske og administrative konsekvenser for det offentlige

Lovforslaget medfører, at Center for Cybersikkerhed i et vist omfang skal varetage nye opgaver. Disse opgaver forudsættes imidlertid afholdt inden for den eksisterende økonomiske ramme. Lovforslaget vurderes på den baggrund ikke at have økonomiske eller administrative konsekvenser for det offentlige.

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

Lovforslaget medfører økonomiske konsekvenser for teleudbyderne.

Det vil kunne medføre økonomiske merudgifter for udbyderne, såfremt Center for Cybersikkerhed efter § 3, stk. 3, påbyder udbydere at træffe konkrete foranstaltninger med henblik på at sikre informationssikkerheden. Udvidelsen af udbydernes oplysnings- og underretningspligt efter § 4 vil endvidere kunne medføre økonomiske merudgifter. Desuden vil kravet i § 5 om, at udbydere skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger for i videst muligt omfang at sikre elektronisk kommunikation i beredskabssituationer, kunne medføre merudgifter for udbydere, der ikke tidligere har været omfattet af kravet.

Endvidere medfører lovforslaget administrative byrder for teleudbyderne.

De administrative byrder består i, at Center for Cybersikkerhed efter § 4 kan fastsætte regler om oplysnings- og underretningspligter for udbydere, herunder krav om at centeret skal underrettes ved indgåelse af aftaler. Endvidere vil § 5 medføre administrative byrder, herunder omstillingsbyrder for udbydere, der ikke tidligere har været omfattet af kravet, idet de skal foretage planlægning og foranstaltninger for at sikre elektronisk kommunikation i beredskabssituationer. Desuden skal udbydere efter § 6 have medarbejdere og repræsentanter sikkerhedsgodkendt, hvilket også vil medføre administrative byrder. Det vil herudover også kunne medføre administrative byrder for udbyderne, at de i medfør af § 9 efter anmodning skal afgive skriftlige udtalelser og redegørelser om faktiske forhold af betydning for Center for Cybersikkerheds tilsynsvirksomhed.

De økonomiske og administrative konsekvenser vil afhænge af udbydernes eksisterende sikker-

hedsniveau og udviklingen i trusselsbilledet i samfundet, hvilket gør, at det ikke på nuværende tidspunkt er muligt yderligere at kvantificere de økonomiske og administrative konsekvenser for udbyderne.

6. Administrative konsekvenser for borgerne

Lovforslaget har ingen administrative konsekvenser for borgerne.

7. Miljømæssige konsekvenser

Lovforslaget har ingen miljømæssige konsekvenser.

8. Forholdet til EU-retten

Reguleringen af informationssikkerhed og beredskab på teleområdet gennemfører dele af Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet), som bl.a. ændret ved Europa-Parlamentets og Rådets direktiv 2009/140/EF af 25. november 2009, samt Europa-Parlamentets og Rådets direktiv 2002/22/EF af 7. marts 2002 om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester (forsyningspligtdirektivet), som bl.a. ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009.

9. Hørte myndigheder og organisationer m.v.

Et udkast til lovforslaget har i perioden fra xx. xxxx 2015 til xx. xxxx 2015 været sendt i høring hos:

Advokatrådet, Amnesty International, Dansk Beredskabskommunikation A/S, Dansk Energi, Dansk Erhverv, Dansk Industri (DI), DANSK IT, Danske Advokater, Danske Regioner, Datatilsynet, Den Danske Dommerforening, DI ITEK, Domstolsstyrelsen, Forenede Danske Antenneanlæg, Global Connect A/S, Hi3G Denmark ApS, HORESTA, Institut for Menneskerettigheder, IT-Branchen, IT-Politisk Forening, Kommunernes Landsforening (KL), Nianet A/S, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Retspolitisk Forening, Retssikkerhedsfonden, Rigsrevisionen, Rådet for Digital Sikkerhed, Stofa A/S, TDC A/S, Teleindustrien (TI), Telenor A/S, TeliaSonera Danmark A/S, Teracom A/S, TT-Netværket P/S og Waoo! A/S.

Udkastet har endvidere været fremlagt på Forsvarsministeriets og Center for Cybersikkerheds hjemmesider.

10. Sammenfattende skema

	Positive konse-kvenser/	Negative konsekvenser/ merudgifter

	mindreudgifter	
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Administrative konsekvenser for stat, kommuner og regioner	Ingen	Ingen
Økonomiske konsekvenser for erhvervslivet m.v.	Ingen	Lovforslaget medfører økonomiske konsekvenser for teleudbyderne. Det vil kunne medføre økonomiske merudgifter for udbyderne, såfremt Center for Cybersikkerhed efter § 3, stk. 3, påbyder udbydere at træffe konkrete foranstaltninger med henblik på at sikre informationssikkerheden. Udvidelsen af udbydernes oplysnings- og underretningspligt efter § 4 vil endvidere kunne medføre økonomiske merudgifter. Desuden vil kravet i § 5 om, at udbydere skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger for i videst muligt omfang at sikre elektronisk kommunikation i beredskabssituationer, kunne medføre merudgifter for udbydere, der ikke tidligere har været omfattet af kravet. De økonomiske konsekvenser vil afhænge af udbydernes eksisterende sikkerhedsniveau og udviklingen i trusselsbilledet i samfundet, hvilket gør, at det ikke på nuværende tidspunkt er muligt yderligere at kvantificere de økonomiske konsekvenser for udbyderne.
Administrative konsekvenser for erhvervslivet m.v.	Ingen	Lovforslaget medfører administrative byrder for teleudbyderne. De administrative byrder består i, at Center for Cybersikkerhed efter § 4 kan fastsætte regler om oplysnings- og underretningspligter for udbydere, herunder krav om at centeret skal underrettes ved indgåelse af aftaler. Endvidere vil § 5 medføre administrative byrder, herunder omstillingsbyrder for udbydere, der ikke tidligere har været omfattet af kravet, idet de skal foretage planlægning og foranstaltninger for at sikre elektronisk kommunikation i beredskabssituationer. Desuden skal udbydere efter § 6 have medarbejdere og repræsentanter sikkerhedsgodkendt, hvilket også vil medføre administrative byrder. Det vil herudover også kunne medføre administrative byrder for

		udbyderne, at de i medfør af § 9 efter anmodning skal afgive skriftlige udtalelser og redegørelser om faktiske forhold af betydning for Center for Cybersikkerheds tilsynsvirksomhed. De administrative byrder vil afhænge af udbydernes eksisterende sikkerhedsniveau og udviklingen i trusselsbilledet i samfundet, hvilket gør, at det ikke på nuværende tidspunkt er muligt yderligere at kvantificere de administrative byrder for udbyderne.
Administrative konsekvenser for borgerne	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Forholdet til EU-retten	Reguleringen af informationssikkerhed og beredskab på teleområdet gennemfører dele af Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet), som bl.a. ændret ved Europa-Parlamentets og Rådets direktiv 2009/140/EF af 25. november 2009, samt Europa-Parlamentets og Rådets direktiv 2002/22/EF af 7. marts 2002 om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester (forsyningspligtdirektivet), som bl.a. ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009.	

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Den foreslåede bestemmelse i *§ 1* beskriver lovens formål, som er at fremme net- og informationssikkerheden i samfundet.

Det danske samfund har i de seneste år oplevet en rivende teknologisk udvikling i form af digitalisering. Digitaliseringen har i betydelig grad påvirket, hvordan borgere, virksomheder og det offentlige kommunikerer, og hvordan virksomheder og myndigheder organiseres og varetager deres opgaver. Digitaliseringen bliver stedse mere kompleks og har i de senere år været karakteriseret ved, at systemer og produkter i høj grad er online og indbyrdes forbundne.

Digitaliseringen forudsætter derfor en robust informations- og kommunikationsteknologisk infrastruktur (ikt-infrastruktur), som teleområdet er en væsentlig del af. En robust ikt-infrastruktur har dermed fået en helt central rolle i samfundets funktion, sammenhæng og værdiskabelse. Det er derfor af afgørende betydning for samfundet, at ikt-infrastrukturen er sikret, således at elektronisk kommunikation kan opretholdes, og at informationer kan udveksles fortroligt og uforvansket.

Formålet med loven er på den baggrund at medvirke til at sikre en robust ikt-infrastruktur ved at fremme informationssikkerheden i net og tjenester samt sikre, at elektronisk kommunikation kan finde sted i beredskabssituationer og i andre ekstraordinære situationer.

Til § 2

Den foreslåede *§ 2* definerer fem centrale begreber i loven. Definitionerne bygger på de tilsvarende definitioner i teleloven.

Efter *nr. 1* defineres "net" som elektroniske kommunikationsnet i form af radiofrekvens- eller kabelbaseret teleinfrastruktur, der anvendes til formidling af tjenester. Definitionen af net er indholdsmæssigt identisk med definitionen af elektroniske kommunikationsnet i telelovens § 2, nr. 4, og bestemmelsen skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis, da begrebet net er defineret som værende synonymt med begrebet elektroniske kommunikationsnet.

Efter *nr. 2* defineres "tjeneste" som en elektronisk kommunikationstjeneste, 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. Definitionen af en tjeneste er indholdsmæssigt identisk med definitionen af en elektronisk kommunikationstjeneste i telelovens § 2, nr. 7, og bestemmelsen skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis, da begrebet tjeneste er defineret som værende syno-

nymt med begrebet elektronisk kommunikationstjeneste. Begrebet nettermineringspunkt skal forstås i overensstemmelse med definitionen heraf i telelovens § 2, nr. 6.

Efter *nr. 3* defineres "offentligt tilgængelige net og tjenester" som net og tjenester, der stilles til rådighed for en ikke på forhånd afgrænset kreds af slutbrugere eller udbydere. Det svarer til definitionen af såvel offentlige elektroniske kommunikationsnet i telelovens § 2, nr. 5, som offentlig elektronisk kommunikationstjeneste i telelovens § 2, nr. 8, og det foreslåede nr. 3 skal fortolkes i overensstemmelse med disse bestemmelsers forarbejder og relevante praksis. Begrebet slutbruger skal forstås i overensstemmelse med definitionen heraf i telelovens § 2, nr. 3.

En "udbyder" defineres i *nr. 4* som den, der med et kommercielt formål stiller produkter, net eller tjenester til rådighed for andre. Definitionen er indholdsmæssigt identisk med den tilsvarende definition i telelovens § 2, nr. 1, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

En "erhvervsmæssig udbyder" defineres i *nr. 5* som en udbyder, der med et kommercielt formål udbyder produkter, net eller tjenester som sin hovedydelse eller som en ikke accessorisk del af virksomheden. Definitionen er indholdsmæssigt identisk med den tilsvarende definition i telelovens § 2, nr. 2, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

I definitionerne af udbydere og erhvervsmæssige udbydere benyttes – i overensstemmelse med de tilsvarende definitioner i teleloven – begrebet "produkter", som dækker over fysiske genstande, der ikke falder ind under definitionen af et net eller en tjeneste. Sådanne produkter kan eksempelvis være mobiltelefoner. Det bemærkes i den forbindelse, at lovforslaget alene vedrører krav til informationssikkerhed og beredskab i net og tjenester, hvorimod produkter ikke i øvrigt reguleres i lovforslaget.

Til § 3

Den foreslåede *§ 3* vedrører informationssikkerhed som led i udbuddet af net og tjenester. Formålet med bestemmelsen er at bidrage til at sikre en robust teleinfrastruktur, således at der kan ske en kontinuerlig og sikker formidling af data. Bestemmelsen viderefører implementeringen af artikel 13 a (1 og 2) i rammedirektivet.

Efter *stk. 1* bemyndiges Center for Cybersikkerhed til at fastsætte regler for udbydere af offentligt tilgængelige net og tjenester om minimumskrav til informationssikkerhed i forbindelse med udbud af offentligt tilgængelige net og tjenester. Den foreslåede bestemmelse viderefører den hidtidige ordning efter telelovens § 8 a, stk. 2, nr. 1.

Der kan med hjemmel i bestemmelsen fastsættes krav om, at udbydere af offentligt tilgængelige net og tjenester skal håndtere informationssikkerheden i offentligt tilgængelige net og tjenester gennem

dokumenterede og ledelsesforankrede processer, herunder risikostyringsprocesser. Den foreslåede bemyndigelse forudsættes anvendt til administrativt at fastsætte regler med nærmere krav til processerne. Der kan således administrativt stilles krav om, at processerne skal fastlægges og gennemføres med udgangspunkt i en relevant og anerkendt international standard eller tilsvarende.

Herudover kan bemyndigelsen anvendes til at fastsætte krav om, at udbyderes risikostyring på informationssikkerhedsområdet skal tage højde for informationssikkerhedsaspekter ved indgåelse og gennemførelse af aftaler med tredjemand om leverance af hardware, firmware eller software samt aftaler om varetagelse af driftsopgaver, der er væsentlige for udbydernes virke, eller som i øvrigt har betydning for informationssikkerheden i udbydernes net og tjenester. Driftsopgaver skal forstås bredt og omfatter bl.a. vedligehold og driftsovervågning. Der kan endvidere med hjemmel i bestemmelsen stilles nærmere krav til udbydernes håndtering af leverancer m.v. fra tredjemand, herunder om at udbyderne skal have dokumenterede procedurer til verificering af, at konfigurationen af det leverede hardware, firmware eller software ikke udgør en trussel mod informationssikkerheden, samt krav om, at der fastsættes dokumenterede procedurer for udbydernes kontrol med leverandørers drift af det leverede hardware, firmware eller software.

Med hjemmel i bestemmelsen kan der desuden stilles krav om, at udbydere skal sikre, at kun autoriserede (eventuelt sikkerhedsgodkendte) personer får adgang til nærmere bestemte dele af udbydernes infrastruktur, herunder f.eks. centrale dele af udbydernes net. Der kan i den forbindelse stilles krav om, at udbyderne skal fastsætte interne retningslinjer for, hvilke medarbejdere hos udbyderne og deres eventuelle leverandører, som må have adgang til udbydernes infrastruktur, ligesom der kan stilles nærmere krav til udbydernes adgangskontrol.

Regler udstedt i medfør af den foreslåede bestemmelse i stk. 1 vil i almindelighed have karakter af erstatningsfri regulering. Det kan imidlertid ikke udelukkes, at krav fastsat i medfør af den foreslåede bestemmelse vil kunne ramme udbydere af offentligt tilgængelige net og tjenester så økonomisk intensivt og atypisk hårdt, at der vil kunne være tale om et ekspropriativt indgreb mod den pågældende udbyder. Det vil bero på en konkret vurdering, om der i det enkelte tilfælde foreligger ekspropriation efter grundlovens § 73. Spørgsmålet om adgang til erstatning efter grundlovens § 73 henhører under domstolene.

Efter s*tk. 2* kan Center for Cybersikkerhed som noget nyt påbyde udbydere af offentligt tilgængelige net og tjenester at inddrage nærmere angivne områder af deres virksomhed eller nærmere angivne trusler mod informationssikkerheden i deres risikostyringsprocesser. Bestemmelsen skal ses i sammenhæng med bestemmelsen i stk. 1, hvorefter der kan fastsættes krav om, at udbydere af offentligt tilgængelige net og tjenester bl.a. skal benytte risikostyringsprocesser til at håndtere informationssikkerheden i offentligt tilgængelige net og tjenester.

Der kan efter den foreslåede bestemmelse stilles krav om, at udbyderne i risikostyringsprocesserne skal tage højde for bestemte (konkrete eller generelle) trusler mod informationssikkerheden efter påbud fra Center for Cybersikkerhed. Det kan f.eks. ske på baggrund af de trusselsvurderinger, som

løbende udarbejdes af Center for Cybersikkerhed og den øvrige del af Forsvarets Efterretningstjeneste.

Endvidere kan Center for Cybersikkerhed ved påbud bestemme, at visse områder af en udbyders virksomhed, der er nærmere specificeret i påbuddet, skal være omfattet af risikostyringsprocesserne, hvis dette ikke i forvejen er tilfældet.

Det foreslås med *stk. 3*, at Center for Cybersikkerhed skal kunne påbyde udbydere af offentligt tilgængelige net og tjenester at træffe andre (og konkrete) foranstaltninger end de i stk. 1 nævnte med henblik på at sikre informationssikkerheden i offentligt tilgængelige net og tjenester, hvis sådanne foranstaltninger er af væsentlig samfundsmæssig betydning.

Foranstaltninger af væsentlig samfundsmæssig betydning kan i denne sammenhæng eksempelvis være tiltag, der skal reducere risikoen for, at uvedkommende får adgang til myndigheders elektroniske kommunikation. Det kan endvidere være foranstaltninger, der skal hindre uvedkommendes adgang via net og tjenester til infrastruktur, som er nødvendige, for at samfundsvigtige funktioner opretholdes. Dette kan være funktioner, som er særligt vigtige for samfundets og demokratiets opretholdelse og sikkerhed samt borgernes tryghed, herunder funktioner inden for sundhed, energi, transport, forsyning, finans, forskning, medier og kommunikation samt funktioner, som har stor økonomisk betydning for samfundet.

Center for Cybersikkerhed fastsætter nærmere regler om omfanget af de foranstaltninger, som vil kunne påbydes med henblik på at sikre informationssikkerheden i offentligt tilgængelige net og tjenester. Sådanne foranstaltninger kan eksempelvis være krav om, at udbyderen skal sikre, at leverancer af hardware, firmware eller software, der kan udgøre en sårbarhed i udbyderens net, skal undersøges for sårbarheder af sikkerhedsgodkendte personer. Det kan endvidere være krav om, at der ved outsourcing af drift af kritiske dele af net og tjenester skal være sporbarhed i forhold til data og systembehandling med henblik på at sikre en effektiv undersøgelse af sikkerhedsbrud. Det kan også være krav om, at udbyderen ved outsourcing af drift af kritiske dele af net og tjenester til en leverandør fast skal indstationere i Danmark sikkerhedsgodkendte informationssikkerhedsmedarbejdere i leverandørens eller dennes underleverandørers organisationer, og at disse medarbejdere får adgang til alle relevante systemer og informationer i leverandørens eller dennes underleverandørers organisationer med henblik på at udføre sikkerhedskontrol for udbyderen.

Center for Cybersikkerhed vil desuden med hjemmel i bestemmelsen kunne påbyde udbydere af offentligt tilgængelige net og tjenester at sikre, at udstyr og systemer, som skal anvendes i forbindelse med indgreb i meddelelseshemmeligheden, skal opsættes i og drives fra Danmark, idet centeret dog i særlige tilfælde kan dispensere fra et sådant krav. Bestemmelsen skal ses som et supplement til § 10, stk. 2, i teleloven, hvorefter erhvervs- og vækstministeren efter forhandling med justitsministeren kan fastsætte nærmere regler om de tekniske krav til udstyr, systemer og gatewaystationer, som skal anvendes i forbindelse med indgreb i meddelelseshemmeligheden.

Den foreslåede påbudsbestemmelse efter stk. 3 vil i almindelighed have karakter af erstatningsfri regulering. Det kan imidlertid ikke udelukkes, at påbud udstedt i medfør af den foreslåede bestemmelse vil kunne ramme udbydere af offentligt tilgængelige net og tjenester så økonomisk intensivt og atypisk hårdt, at der vil kunne være tale om et ekspropriativt indgreb mod den pågældende udbyder. Det vil bero på en konkret vurdering, om der i det enkelte tilfælde foreligger ekspropriation efter grundlovens § 73. Spørgsmålet om adgang til erstatning efter grundlovens § 73 henhører under domstolene.

De foreslåede bestemmelser indebærer ikke, at der ændres ved det grundlæggende princip om aftalefrihed. Der kan således ikke med hjemmel i bestemmelserne ske regulering af ejerforhold, fastsættes forbud mod at indgå aftale med bestemte leverandører eller forbud mod ejerskab af bestemte netværk eller produkter.

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

Til § 4

Den foreslåede *§ 4* bemyndiger Center for Cybersikkerhed til at fastsætte regler om oplysnings- og underretningspligter for udbydere.

Bemyndigelsen i den foreslåede *nr. 1*, der er ny, kan anvendes til at fastsætte nærmere regler om en oplysningspligt, hvorefter erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester skal afgive oplysninger om væsentlige dele af deres net eller tjenester eller driften heraf. Ved begrebet drift forstås i denne lov bl.a. vedligeholdelse og driftsovervågning. Formålet med bestemmelsen er at give Center for Cybersikkerhed et bedre overblik over den samlede teleinfrastruktur.

Den foreslåede bestemmelse indebærer, at der administrativt kan fastsættes regler om, at de erhvervsmæssige udbydere efter anmodning skal oplyse Center for Cybersikkerhed om udbydernes infrastruktur, herunder om, hvilke leverandører og hvilket hardware, firmware og software, som udbyderne anvender. Oplysningspligten kan omfatte oplysninger om hardware, firmware og softwares fabrikat, typebetegnelse, serienummer m.v., oplysninger om netarkitektur og -design, eventuelle leverandører, herunder driftsleverandører, samt den geografiske placering af udbydernes og relevante leverandørers hardware. Der skal være tale om væsentlige dele af udbydernes net eller tjenester, hvorved eksempelvis forstås det transmissionssystem, der forbinder de forskellige større netværkselementer i netværket, samt Value Added Services (VAS), der understøtter tillægstjenester som f.eks. voice mailbox, SMS, MMS og lokationstjenester. Oplysningspligten kan også omfatte forhold vedrørende driften af væsentlige administrative systemer, f.eks. faktureringssystemer, såfremt sådanne systemer har betydning for udbydernes informationssikkerhed. Oplysningspligten kan endvidere omfatte oplysninger om flytning af driften af net og tjenester til udlandet.

Den foreslåede bestemmelse skal ses i sammenhæng med den foreslåede § 9, stk. 2, hvorefter Center for Cybersikkerhed hos udbydere kan kræve udlevering af alle oplysninger og alt materiale, som

centeret skønner relevant i forbindelse med tilsyn med overholdelsen af lovens regler eller regler, der er udstedt i medfør heraf. Den foreslåede oplysningspligt i nr. 1 vedrører imidlertid en generel oplysningspligt om emner af relevans for informationssikkerhed og beredskab på teleområdet.

Det foreslås endvidere, at der med *nr. 2* som noget nyt etableres hjemmel til at fastsætte regler om en underretningspligt, hvorefter erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester skal underrette Center for Cybersikkerhed om påtænkte aftaleindgåelser om leverancer af hardware, firmware eller software til væsentlige dele af udbydernes net eller tjenester eller driften heraf. Formålet med underretningspligten er at sikre, at Center for Cybersikkerhed så tidligt som muligt kan indgå i en dialog med udbyderen om det risikobillede, herunder trusler og sårbarheder i forhold til informationssikkerheden, som den påtænkte aftale vurderes at indebære. Underretningen skal ske, inden udbyderen indleder konkrete forhandlinger med leverandører om den pågældende aftale, og det forudsættes, at der vil være en løbende dialog mellem Center for Cybersikkerhed og udbyderen under det efterfølgende forhandlingsforløb.

De erhvervsmæssige udbydere forpligtes endvidere efter nr. 2 til at indsende det endelige aftaleudkast umiddelbart forud for aftaleindgåelsen. Der kan i den forbindelse fastsættes regler om, at der efter indsendelsen af udkastet til den endelige aftale indtræder en kortere standstill-periode. Standstill-perioden giver Center for Cybersikkerhed mulighed for at indgå i yderligere dialog med udbyderen om imødegåelse af trusler mod informationssikkerheden, som det pågældende aftaleudkast vurderes at indebære.

Standstill-perioden kan have en varighed på op til 10 arbejdsdage fra Center for Cybersikkerheds modtagelse af det endelige aftaleudkast, og perioden kan ikke forlænges. Har Center for Cybersikkerhed som forudsat været inddraget under forhandlingsforløbet, vil centeret som udgangspunkt kun i begrænset omfang have bemærkninger til det indsendte aftaleudkast på dette tidspunkt, og det vil blive tilstræbt, at standstill-perioden kan afsluttes inden for fem arbejdsdage.

Tilpasses det indsendte aftaleudkast som følge af dialogen mellem Center for Cybersikkerhed og udbyderen under standstill-perioden, skal det endelige og tilpassede aftaleudkast sendes til Center for Cybersikkerhed forud for aftaleindgåelsen, hvorefter der indtræder en ny standstill-periode på op til 10 arbejdsdage.

Den foreslåede ordning giver udbyderne mulighed for at tage højde for eventuelle trusler mod informationssikkerheden i forbindelse med aftaleforhandlingerne. Dermed får udbyderne mulighed for at undgå, at de efterfølgende mødes af uforudsete krav til informationssikkerheden i deres net og tjenester.

Der vil ikke være tale om, at Center for Cybersikkerhed skal godkende aftaler, der er omfattet af nr. 2, ligesom centeret ikke kan nedlægge forbud mod indgåelse af en aftale efter standstill-periodens udløb.

Den foreslåede *nr. 3* viderefører ordningen efter telelovens § 8 a, stk. 2, nr. 2. Der kan med hjemmel i den foreslåede bestemmelse fastsættes regler om, at udbydere af offentligt tilgængelige net og tjenester skal underrette Center for Cybersikkerhed ved brud på informationssikkerheden, der har væsentlige følger for driften af net eller tjenester.

Brud på informationssikkerheden omfatter tab af både tilgængelighed, integritet og fortrolighed i net og tjenester. Betingelsen om, at bruddet skal have væsentlige følger for driften af net eller tjenester, skal forstås som opretholdelse af net- eller tjenesteudbuddet.

Et brud på tilgængeligheden af net eller tjenester, som har væsentlige følger for driften af net eller tjenester, kan eksempelvis være en længerevarende afbrydelse af en udbudt tjeneste, som rammer et større geografisk område på baggrund af en overgravning af en central transmissionsforbindelse. Herudover kan brud på fortroligheden i net eller tjenester, som har væsentlige følger for driften, eksempelvis være tilfælde, hvor passwords og brugernavne og lignende følsomme informationer, som er vigtige for den centrale del af driften, bliver gjort offentligt tilgængelige eller på anden vis kompromitteres, således at udbyderen tvinges til at tage betydelige forholdsregler med henblik på at sikre nettet eller tjenesten mod angreb. Forvanskning af centrale data i forbindelse med en uberettiget adgang til net eller tjenester, således at den elektroniske kommunikation ikke overføres til de rette adressater, kan endvidere udgøre et brud på integriteten, som har væsentlige følger for driften af net eller tjenester.

Den foreslåede bemyndigelse i *nr. 4* viderefører ordningen efter telelovens § 8 a, stk. 2, der gennemfører artikel 13 a (3) i rammedirektivet. Der kan med hjemmel i bestemmelsen fastsættes regler om, at udbydere af offentligt tilgængelige net og tjenester efter påbud skal underrette offentligheden ved brud på informationssikkerheden, som har væsentlige følger for driften af deres net og tjenester, hvis det godtgøres, at det er i offentlighedens interesse, at et brud på informationssikkerheden offentliggøres. Der kan endvidere med hjemmel i den foreslåede bestemmelse fastsættes regler om, at Center for Cybersikkerhed kan offentliggøre et brud på informationssikkerheden, som centeret har fået underretning om i medfør af det foreslåede nr. 3, såfremt det er i offentlighedens interesse, at et brud offentliggøres.

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

Til § 5

Elektronisk kommunikation er i stigende grad en forudsætning for opretholdelse af samfundets funktioner. Elektronisk kommunikation er i den forbindelse også nødvendig i forhold til de forskellige beredskabsaktørers indsats i beredskabssituationer eller i andre ekstraordinære situationer. Den ordning, der foreslås med *§ 5* bidrager til at sikre en robust teleinfrastruktur, således at samfundets elektroniske kommunikation i videst muligt omfang kan finde sted i beredskabssituationer og i andre ekstraordinære situationer. Endvidere bidrager ordningen til at sikre beredskabsaktørernes behov for samfundsvigtig elektroniske kommunikation.

Ordningen er en del af den samlede beredskabsplanlægning inden for den civile sektor. Det følger således af § 24, stk. 1, i beredskabsloven, jf. lovbekendtgørelse nr. 660 af 10. juni 2009, som ændret ved lov nr. 514 af 26. maj 2014, at hver enkelt minister inden for sit område skal planlægge for opretholdelse og videreførelse af samfundets funktioner i tilfælde af større ulykker og katastrofer, herunder udarbejde beredskabsplaner. Den foreslåede § 5 viderefører desuden implementeringen af artikel 23, 1. pkt., i forsyningspligtdirektivet.

Bestemmelsens anvendelsesområde omfatter beredskabssituationer samt andre ekstraordinære situationer. Dette omfatter såvel situationer med krigshandlinger som situationer, hvor det som følge af en større ulykke, katastrofe eller anden ekstraordinær hændelse eller krise er nødvendigt at indføre særlige foranstaltninger vedrørende net og tjenester med henblik på at opretholde samfundets funktioner. Bestemmelsens anvendelsesområde omfatter således både naturskabte og menneskeskabte ulykker og katastrofer, herunder eksempelvis orkan- og stormflodssituationer og alvorlige cyberangreb.

Det foreslåede *stk. 1* er en delvis videreførelse af telelovens § 62, stk. 1, som gennemfører artikel 23 i forsyningspligtdirektivet. Den foreslåede bestemmelse bemyndiger Center for Cybersikkerhed til at fastsætte regler om, at udbydere skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger for i videst muligt omfang at sikre elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer. Det foreslås, at bestemmelsens anvendelsesområde udvides til at omfatte samtlige udbydere i stedet for alene at omfatte erhvervsmæssige udbydere. Ligeledes foreslås det, at udbyderne i videst muligt omfang skal sikre elektronisk kommunikation og ikke kun samfundsvigtig elektronisk kommunikation.

Der kan med hjemmel i bestemmelsen fastsættes regler om grundlæggende krav til udbydernes beredskab. Det omfatter krav til en robust teleinfrastruktur, således at der tages højde for at beredskabssituationer og andre ekstraordinære situationer kan opstå. Der kan eksempelvis stilles krav om, at udbyderne i deres beredskabsplanlægning skal tage stilling til fremskaffelse af det nødvendige reserveudstyr, adgang til den nødvendige eksterne hjælp, indgåelse af relevante serviceaftaler samt behovet for medarbejdertilkaldeplaner i beredskabssituationer og i andre ekstraordinære situationer. Der kan også stilles krav til sikring af redundans i nettene og om nødstrømsforsyning.

Der kan endvidere med hjemmel i bestemmelsen stilles krav om, at udbyderne etablerer en krisestyringsorganisation, som skal kunne varetage den nødvendige krisestyring i beredskabssituationer eller i andre ekstraordinære situationer.

Den foreslåede bestemmelse i *stk. 2* er en delvis videreførelse af telelovens § 62, stk. 2. Bestemmelsen i telelovens § 62, stk. 2, nr. 2, hvorefter ejere af net, der anvendes til erhvervsmæssigt udbud af offentligt tilgængelige tjenester, skal sikre passende beskyttelse af kritisk teleinfrastruktur, er videreført i den foreslåede bestemmelse i stk. 1.

Det foreslås, at kravene til beredskabsplanlægning og deltagelse i øvelsesaktivitet som noget nyt skal omfatte samtlige erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester, og ikke – som efter gældende ret – alene ejere af net, der anvendes til erhvervsmæssigt udbud af offentligt tilgængelige tjenester. Det bemærkes i den forbindelse, at bestemmelsen først og fremmest forudsættes anvendt over for erhvervsmæssige udbydere af offentlige net.

Udbyderbegrebet, jf. den foreslåede § 2, nr. 4, samt den gældende § 2, nr. 1, i teleloven, omfatter enhver, der med kommercielt formål stiller produkter, net eller tjenester til rådighed for andre. Ejere af net, herunder ejere af net-infrastrukturkomponenter, der anvendes til udbud af offentligt tilgængelige tjenester, er således allerede i dag omfattet af udbyderbegrebet.

Der kan med hjemmel i bestemmelsen fastsættes regler, der – udover hvad der følger af krav fastsat i medfør af det foreslåede stk. 1 – forpligter erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester til at udarbejde beredskabsplaner baseret på en dokumenteret og ledelsesforankret risikostyringsproces samt planlægge og deltage i øvelsesaktivitet med henblik på forberedelse af beredskabssituationer og andre ekstraordinære situationer.

Bemyndigelsen kan anvendes til at fastsætte krav om, at erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester skal gennemføre en sammenhængende, ledelsesforankret risikostyringsproces, som navnlig omfatter løbende trussels- og sårbarhedsanalyser samt risikovurderinger, udarbejdelse af en beredskabspolitik samt konkrete beredskabsplaner. Der kan i den forbindelse stilles krav om, at erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester skal udarbejde planer for deres krisestyringsorganisations virke, hvilket eksempelvis kan omfatte planer for krisekommunikation og samarbejde med Center for Cybersikkerhed i beredskabssituationer og i andre ekstraordinære situationer.

Reglerne kan desuden omfatte krav om, at en udbyder skal underrette Center for Cybersikkerhed i tilfælde, hvor udbyderen aktiverer sit beredskab, eller hvor udbyderen bliver bekendt med en hændelse, som vurderes at kunne føre til en beredskabssituation eller en anden ekstraordinær situation for udbyderen selv eller for en anden udbyder. Samtidig kan der med hjemmel i bestemmelsen fastsættes krav om, at udbydere skal etablere et kontaktpunkt, som i beredskabssituationer kan fungere som forbindelsesled mellem Center for Cybersikkerhed og udbyderen. Der kan desuden stilles krav om, at kontaktpunktet skal kunne udveksle informationer, herunder klassificerede informationer, med Center for Cybersikkerhed og andre myndigheder, ligesom kontaktpunktet skal have bemyndigelse til at aktivere udbyderens beredskab.

Der kan herudover med hjemmel i bestemmelsen fastsættes nærmere krav til planlægning og deltagelse i øvelser, samt til øvelsesrapportering, hvilket kan omfatte både øvelser internt hos udbyder, øvelser på tværs af telesektoren samt tværsektorielle nationale og internationale krisestyringsøvelser.

Den foreslåede bestemmelse i *stk. 3* vedrører koordinering og prioritering af de forskellige beredskabsaktørers behov for elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer. En sådan koordinering og prioritering vil ofte være nødvendigt i beredskabssituationer og i andre ekstraordinære situationer, hvor der kan opstå kapacitetsproblemer eller beskadigelse af teleinfrastrukturen. Bestemmelsen viderefører ordningen efter telelovens § 62, stk. 4, hvorefter Center for Cybersikkerhed på vegne af Forsvarsministeriet koordinerer og prioriterer beredskabsmyndighedernes behov for samfundsvigtig elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer. Det bemærkes i den forbindelse, at bestemmelsen alene vedrører beredskabsaktørernes samfundsvigtige elektroniske kommunikation, der overføres som led i udbuddet af net og tjenester.

Den foreslåede bestemmelse benytter begrebet "beredskabsaktører", i modsætning til det hidtil benyttede begreb "beredskabsmyndigheder". Der er alene tale om en sproglig tilpasning. Ved beredskabsaktører forstås fortsat myndigheder, virksomheder og institutioner samt private virksomheder og institutioner, som skal bidrage til opretholdelse af samfundets funktioner i en beredskabssituation eller i en anden ekstraordinær situation.

Bestemmelsen indebærer, at Center for Cybersikkerhed fortsat varetager den overordnede krisestyring i forhold til telesektoren. Centeret skal i den forbindelse i beredskabssituationer eller i andre ekstraordinære situationer være bindeled mellem beredskabsaktører og udbydere og søge at tilgodese eller prioritere mellem beredskabsaktørernes behov for elektronisk kommunikation. Centeret skal i den forbindelse koordinere teleberedskabet med beredskabsindsatsen i de øvrige samfundssektorer.

Center for Cybersikkerhed bemyndiges til at fastsætte regler om, at erhvervsmæssige udbydere skal foretage visse forberedende tiltag med henblik på at kunne tilgodese beredskabsaktørernes behov for elektronisk kommunikation i beredskabssituationer eller i andre ekstraordinære situationer. Sådanne forberedende tiltag kan eksempelvis være planlægning og forberedelse af prioriteringer i net og tjenester med henblik på, at beredskabsaktørerne kan få forrang til anvendelse af disse, herunder til kald i fastnet og mobilnet i tilfælde af overbelastning eller ved beskadigelse af teleinfrastrukturen. Et forberedende tiltag kan i den forbindelse endvidere være tilvejebringelse og opretholdelse af faste kredsløb til beredskabsmæssige formål. Ved faste kredsløb til beredskabsmæssige formål forstås permanent etablerede fysiske eller logiske forbindelser eller netværk, hvor der stilles nærmere defineret transmissionskapacitet til rådighed for beredskabsaktørerne i forbindelse med varetagelsen af opgaver, som bidrager til opretholdelse af samfundets funktioner i en beredskabssituation.

Der kan desuden med hjemmel i bestemmelsen fastsættes regler om, at erhvervsmæssige udbydere i beredskabssituationer eller andre ekstraordinære situationer efter påbud fra Center for Cybersikkerhed skal foretage visse foranstaltninger med henblik på, at prioriteringerne i net og tjenester kan gennemføres. Der kan i den forbindelse fastsættes nærmere regler om, at Center for Cybersikkerhed kan give påbud om, at erhvervsmæssige udbydere skal prioritere retablering af bestemte dele af en udbyders beskadigede infrastruktur. Behovet for prioritering vil være situationsbestemt og afledt af

centerets samarbejde med andre sektorer. Prioriteringen kan både omfatte bestemte beredskabsaktørers kommunikation, geografiske områder, bestemte forbindelser og net eller tjenester, alt efter hvad den konkrete situation tilsiger.

Herudover kan der efter bestemmelsen fastsættes regler om, at erhvervsmæssige udbydere i beredskabssituationer eller andre ekstraordinære situationer efter påbud fra Center for Cybersikkerhed skal prioritere fremførsel i nettene af bestemte forbindelser eller tjenester i tilfælde af kapacitetsproblemer. En erhvervsmæssig udbyder kan i den forbindelse være nødsaget til at afbryde andre forbindelser eller tjenester helt eller delvis med henblik på at sørge for, at en bestemt forbindelse eller tjeneste opretholdes. Reglerne kan endvidere indeholde krav om, at erhvervsmæssige udbydere i beredskabssituationer eller andre ekstraordinære situationer efter påbud fra Center for Cybersikkerhed skal iværksætte de forberedte prioriteringsordninger ved eksempelvis at indføre generel eller delvis begrænsning af teletrafikken med henblik på at give beredskabsaktører forrang til kald i fastnet og mobilnet.

Det foreslås med *stk. 4* at Center for Cybersikkerhed i beredskabssituationer og i andre ekstraordinære situationer kan påbyde erhvervsmæssige udbydere uden unødigt ophold at iværksætte nærmere angivne sikkerhedsforanstaltninger i tilfælde af en hændelse eller trussel, der i betydeligt omfang påvirker, eller vurderes at ville kunne påvirke, udbuddet af net eller tjenester negativt. En sådan mulighed følger i dag i et vist omfang af § 13 i bekendtgørelse nr. 445 af 11. maj 2011 om informationssikkerhed og beredskab for elektroniske kommunikationsnet og -tjenester.

Center for Cybersikkerhed kan efter bestemmelsen påbyde erhvervsmæssige udbydere at iværksætte akutte sikkerhedsforanstaltninger, forudsat at der er en hændelse eller trussel, der i betydeligt omfang påvirker, eller vurderes at ville kunne påvirke, udbuddet af net og tjenester negativt. En hændelse, der i betydeligt omfang påvirker udbuddet af net og tjenester, kan eksempelvis være et alvorligt cyberangreb eller et terrorangreb, som medfører, at net eller tjenester i en periode ikke er tilgængelige for slutbrugerne. Sådanne hændelser kan endvidere være kraftige vejrfænomener såsom orkaner eller skybrud, der medfører, at større dele af teleinfrastrukturen beskadiges. En trussel, der vurderes i betydeligt omfang at kunne påvirke udbuddet af net eller tjenester, vil eksempelvis være, hvis der foreligger oplysninger om et nært forestående sabotageforsøg eller terrorangreb mod kritiske dele af teleinfrastrukturen.

For at anvende bestemmelsen skal der foreligge en beredskabssituation eller en anden ekstraordinær situation. Det bemærkes i den forbindelse, at en hændelse eller trussel, der i betydeligt omfang påvirker, eller vurderes at ville kunne påvirke, udbuddet af net eller tjenester negativt, i sig selv kan udgøre en beredskabssituation.

Center for Cybersikkerhed kan i sådanne situationer påbyde erhvervsmæssige udbydere at iværksætte akutte sikkerhedsforanstaltninger såsom indførelse af særlige adgangskontroller til udbyderens lokaliteter, begrænsning af adgangsveje til og parkeringsrestriktioner på udbyderens arealer samt eftersyn med udbyderens arealer og bygninger. Center for Cybersikkerhed kan endvidere på-

byde de erhvervsmæssige udbydere foranstaltninger ved håndteringen af postforsendelser, f.eks. gennemlysning af breve og pakker. Desuden kan centeret påbyde de erhvervsmæssige udbydere at udpege særligt kritiske eller aktuelt truede dele af deres teleinfrastruktur og sørge for vagtrundering, kontrol med sikringsforanstaltninger og eventuelt bevogtning af de pågældende dele af teleinfrastrukturen i samarbejde med relevante beredskabsaktører. Centeret kan i øvrigt påbyde de erhvervsmæssige udbydere at foranstalte akutte sikkerhedsforanstaltninger til begrænsning af skadevirkningen af eksempelvis naturskabte hændelser. I beredskabssituationer eller i andre ekstraordinære situationer kan Center for Cybersikkerhed i forhold til cyberangreb eksempelvis påbyde logning eller blokering af IP-adresser, der anvendes som led i et angreb. Centeret kan desuden påbyde de erhvervsmæssige udbydere at gennemgå deres beredskabsplaner med henblik på at kunne iværksatte de forberedte tiltag til sikring af teleinfrastrukturen.

Det bemærkes i øvrigt, at det følger af telelovens § 62, stk. 1 og 2, at udbyderne skal foretage en række foranstaltninger "uden omkostninger for staten". Denne formulering er ikke medtaget i den foreslåede § 5, men der er ikke herved tilsigtet en ændring af ordningen. Det forudsættes således fortsat, at udbyderne skal foretage de pågældende foranstaltninger uden omkostninger for staten, hvilket svarer til, at der heller ikke på andre områder udtrykkeligt er angivet, at de påkrævede foranstaltninger skal foretages uden omkostninger for staten.

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

Til § 6

Den foreslåede *§ 6, stk. 1*, er en delvis videreførelse af telelovens § 63, stk. 1.

Bestemmelsen indebærer, at sikkerhedsmyndigheden efter indstilling fra en udbyder kan sikkerhedsgodkende udbyderens medarbejdere og repræsentanter for udbyderen. Sikkerhedsmyndigheden kan i den forbindelse beslutte at gøre sikkerhedsgodkendelsen tidsbegrænset.

Det følger af lov nr. 602 af 12. juni 2013 om Forsvarets Efterretningstjeneste, som ændret ved lov nr. 1624 af 26. december 2013, lov om Politiets Efterretningstjeneste, jf. lovbekendtgørelse nr. 1600 af 19. december 2014, samt cirkulære nr. 10338 af 17. december 2014 om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt (sikkerhedscirkulæret), at Politiets Efterretningstjeneste er national sikkerhedsmyndighed. Forsvarets Efterretningstjeneste varetager dog funktionen som national sikkerhedsmyndighed inden for Forsvarsministeriets område.

Kravet om, at sikkerhedsgodkendelse skal ske efter indstilling, indebærer, at udbyderen skal foretage den indledende vurdering af, om der er personer, som i forhold til deres konkrete opgaveløsning for virksomheden skal håndtere klassificerede informationer eller andre informationer, der er særligt beskyttelsesværdige, fordi informationerne vedrører kritiske dele af udbyderes teleinfrastruktur eller

vedrører udbyderens beredskabsmæssige opgaver. Sådanne personer kan eksempelvis være personer, der skal håndtere informationer, som er klassificerede i medfør af sikkerhedscirkulæret. Det kan endvidere være personer, som skal have adgang til centrale dele af en udbyders særligt kritiske infrastruktur. Center for Cybersikkerhed anbefaler i den forbindelse, at udbyderne udpeger en personalesikkerhedsansvarlig, der administrerer sikkerhedsgodkendelse af medarbejdere og repræsentanter for udbyderen samt varetager kontakten til sikkerhedsmyndigheden i relation til spørgsmål vedrørende sikkerhedsgodkendelse.

I modsætning til den hidtil gældende ordning vil der ikke efter stk. 1 ske sikkerhedsgodkendelse af personer, alene fordi de har adgang til andre udbyderes kritiske infrastruktur. Der skal således ved afgørelsen af, om der skal ske sikkerhedsgodkendelse, foretages en konkret vurdering, hvor der vil blive lagt vægt på, om hensynet til beskyttelsen af teleinfrastrukturen og varetagelsen af beredskabsmæssige opgaver med en vis vægt taler for, at der er behov for en sikkerhedsgodkendelse.

Såfremt sikkerhedsmyndigheden efter indstilling fra en udbyder vurderer, at en person bør sikkerhedsgodkendes, træffer sikkerhedsmyndigheden afgørelse om, hvorvidt personen kan sikkerhedsgodkendes. Afgørelsen baseres på en sikkerhedsundersøgelse foretaget af Politiets Efterretningstjeneste og træffes ud fra en konkret vurdering af alle foreliggende oplysninger om den pågældende person. I overensstemmelse med ordningen efter sikkerhedscirkulærets § 14 vil der ved afgørelsen om sikkerhedsgodkendelse blive lagt vægt på, om vedkommende har udvist ubestridt loyalitet og har en sådan adfærd og karakter, herunder vaner, forbindelser og diskretion, at der ikke kan være tvivl om den pågældendes pålidelighed i forbindelse med håndtering af klassificerede informationer eller andre beskyttelsesværdige informationer. Der kan ved afgørelsen tilsvarende lægges vægt på oplysninger om en ægtefælles, samlevers, registreret partners eller samboendes adfærd, karakter og forhold i øvrigt.

Efter det foreslåede *stk. 2* skal erhvervsmæssige udbydere af offentligt tilgængelige net på eget initiativ sikre, at medarbejdere eller repræsentanter for udbyderen sikkerhedsgodkendes, såfremt de pågældende medarbejdere eller repræsentanter skal behandle klassificerede informationer eller andre informationer, der er særligt beskyttelsesværdige som led i deres varetagelse af kontakten til Center for Cybersikkerhed i relation til beredskabet på teleområdet.

Bestemmelsen viderefører delvist den hidtidige ordning efter telelovens § 63, stk. 2. Som konsekvens af den foreslåede § 5, stk. 2, udvides kredsen af forpligtede imidlertid til at omfatte alle erhvervsmæssige udbydere af offentligt tilgængelige net i stedet for alene at omfatte ejere af net, der anvendes til erhvervsmæssigt udbud af offentligt tilgængelige tjenester.

Det foreslåede s*tk. 3* er en indholdsmæssigt uændret videreførelse af telelovens § 63, stk. 3. Efter den foreslåede bestemmelse er udbydere, hvis medarbejdere eller repræsentanter sikkerhedsgodkendes, forpligtede til at sikre overholdelsen af sikkerhedsmyndighedens angivelser om behandling af klassificerede informationer. Disse angivelser vil som udgangspunkt svare til de krav, der følger af sikkerhedscirkulæret. Såfremt udbyderens medarbejdere eller repræsentanter for udbyderen skal

modtage og behandle klassificerede informationer, kan det endvidere være aktuelt at sikkerhedsgodkende den pågældende virksomhed.

Den foreslåede s*tk. 4* er en indholdsmæssigt uændret videreførelse af telelovens § 63, stk. 5. Med bestemmelsen pålægges udbyderne at underrette sikkerhedsmyndigheden, når en sikkerhedsgodkendt person – uanset årsagen hertil – ikke længere varetager de opgaver for udbyderen, som lå til grund for sikkerhedsgodkendelsen.

Den foreslåede s*tk. 5* er en indholdsmæssigt uændret videreførelse af telelovens § 63, stk. 4. Med bestemmelsen bemyndiges sikkerhedsmyndigheden til at tilbagekalde en sikkerhedsgodkendelse, hvis grundlaget herfor ikke længere er til stede. Det kan eksempelvis være tilfældet, hvis den pågældende person ikke længere beskæftiger sig med den type opgaver hos udbyderen, der krævede en sikkerhedsgodkendelse, eller hvis den pågældendes personlige forhold ændrer sig, således at der opstår tvivl om vedkommendes pålidelighed i forbindelse med håndtering af klassificerede informationer eller andre informationer, der er særligt beskyttelsesværdige i relation til informationssikkerhed eller beredskab.

Det foreslås med *stk. 6*, at Center for Cybersikkerhed som noget nyt bemyndiges til at fastsætte regler om sikkerhedsgodkendelse af udbyderes medarbejdere eller repræsentanter for udbydere, der har adgang til udstyr eller systemer, som benyttes i forbindelse med indgreb i meddelelseshemmeligheden. Det kan i den forbindelse fastsættes, at udbydere på eget initiativ skal sikre, at medarbejdere eller repræsentanter for udbyderen, der har adgang til det pågældende udstyr eller systemer, sikkerhedsgodkendes til at håndtere klassificerede oplysninger.

Efter § 1 i Justitsministeriets bekendtgørelse nr. 1144 af 20. november 2006 om telenet- og teletjenesteudbyderes praktiske bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden (Sikkerhedsgodkendelse af personale i telebranchen) skal udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere sikre, at medarbejdere eller repræsentanter for udbyderen, der forestår kontakten til politiet i forbindelse med indgreb i meddelelseshemmeligheden, sikkerhedsgodkendes af Rigspolitiet til at håndtere klassificerede oplysninger. I forlængelse heraf kan der efter det foreslåede stk. 6 fastsættes krav om, at udbydere skal sikre, at øvrige medarbejdere eller repræsentanter for udbyderne, der har adgang til de nævnte udstyr og systemer, skal være sikkerhedsgodkendt. Dette kan eksempelvis være teknisk personale med ansvar for driften af udstyret og systemerne.

Til § 7

Efter den foreslåede § 4 bemyndiges Center for Cybersikkerhed bl.a. til at fastsætte regler om, at udbydere af offentligt tilgængelige net og tjenesters skal underrette Center for Cybersikkerhed ved brud på informationssikkerheden, der har væsentlige følger for driften af net eller tjenester. Endvidere kan der med hjemmel i bestemmelsen fastsættes regler om, at Center for Cybersikkerhed skal

underrettes forud for indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens offentligt tilgængelige net eller tjenester eller driften heraf.

Det følger af § 8 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 afsnit 3.3.3 i de almindelige bemærkninger til forslaget til lov om Center for Cybersikkerhed (L 192, F.T. 2013-14), 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.

De oplysninger, som Center for Cybersikkerhed som led i underretningsordningen modtager fra udbydere ved brud på informationssikkerheden, vil ofte indeholde oplysninger om fejl eller sårbarheder i net eller tjenester, som kan misbruges af potentielle angribere, hvis de kommer til uvedkommendes kendskab. Det foreslås derfor med *§ 7*, at der ved udmøntningen af hjemlen i § 4 kan fastsættes regler om, at underretningerne i deres helhed undtages fra aktindsigt, herunder partsaktindsigt efter forvaltningsloven, således at aktindsigtsanmodninger ikke – som det ellers ville være tilfældet – behandles efter principperne i offentlighedsloven. Undtagelsen kan omfatte underretningssagen som helhed.

Tilsvarende kan det i regler udstedt efter § 4 fastsættes, at der ikke er adgang til aktindsigt i de udkast til aftaler, som udbydere indsender til Center for Cybersikkerhed. Aftalerne vil ofte indeholde en lang række oplysninger om udbydernes net og tjenester samt aftaleforhold, som dels er kommercielt fortrolige, dels kan misbruges af potentielle angribere.

Undtagelsen fra aktindsigt vil også gælde i de tilfælde, hvor oplysningerne videregives til Europa Kommissionen, Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) eller nationale tilsynsmyndigheder i andre EU-medlemsstater efter den foreslåede § 12.

Undtagelsen fra aktindsigt omfatter ikke teleudbyderes adgang til at gøre sig bekendt med oplysninger, der vedrører deres egne forhold.

Der henvises i øvrigt til afsnit 3.3 i de almindelige bemærkninger.

Til § 8

Efter den foreslåede *§ 8, stk. 1*, kan myndigheder og virksomheder underrette Center for Cybersikkerhed om hændelser, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale services, hvilket indholdsmæssigt svarer til begrebet "sikkerhedshændelse" efter § 2, nr. 1, i lov om Center for Cybersikkerhed. Det bemærkes i den forbindelse, at begrebet "digitale services" skal forstås i overensstemmelse med begrebet "digitale tjenester" i lov om Center for Cybersikkerhed.

Underretning af Center for Cybersikkerhed ved større sikkerhedshændelser skaber de bedst mulige forudsætninger for, at centeret kan udnytte erfaringer med cybertrusler og sikkerhedsrisici på tværs af samfundet – og dermed skabe et samlet overblik over den aktuelle sikkerhedstilstand på den danske del af internettet. Underretninger sætter således Center for Cybersikkerhed i stand til at varsle hurtigere om trusler og styrke grundlaget for centerets rådgivning om risici og passende sikkerhedstiltag.

For statslige myndigheder er der pr. 1. september 2014 som følge af en regeringsbeslutning etableret en egentlig forpligtelse til at underrette Center for Cybersikkerhed ved større it-sikkerhedsmæssige hændelser, f.eks. hacker- og overbelastningsangreb. For øvrige myndigheder og virksomheder er der etableret en helt igennem frivillig ordning, hvor de pågældende organisationer opfordres til at underrette Center for Cybersikkerhed ved større sikkerhedshændelser. Ordningen er etableret efter dialog med en række branche- og interesseorganisationer samt virksomheder.

Særligt for virksomheder kan oplysninger om, at der f.eks. er gennemført et vellykket hackerangreb, hvor virksomheden har mistet data, i høj grad skade virksomhedens omdømme, og det kan i praksis afholde mange virksomheder fra at underrette Center for Cybersikkerhed om et sådant hackerangreb. Derfor foreslås det med *stk. 2*, at underretningerne i deres helhed undtages fra aktindsigt, herunder partsaktindsigt efter forvaltningsloven, således at aktindsigtsanmodninger ikke – som det ellers ville være tilfældet – behandles efter principperne i offentlighedsloven. Undtagelsen kan omfatte underretningssagen som helhed.

Undtagelsen fra aktindsigt omfatter derimod ikke virksomheders adgang til at gøre sig bekendt med oplysninger, der vedrører deres egne forhold.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 7 og til afsnit 3.3 i de almindelige bemærkninger.

Til § 9

Den foreslåede *§ 9* har til formål at skabe rammerne for et effektivt tilsyn med udbydernes overholdelse af kravene til informationssikkerhed, beredskab og sikkerhedsgodkendelse.

Med bestemmelsen i *stk. 1* foreslås det, at Center for Cybersikkerhed påser overholdelsen af loven og regler udstedt i medfør af loven. Det foreslåede stk. 1 bygger på telelovens § 20, stk. 3, og § 64 a, stk. 1, 1. pkt.

Center for Cybersikkerhed sikres med det foreslåede *stk. 2* adgang til de oplysninger, der er nødvendige til gennemførelse af centerets tilsynsvirksomhed. Bestemmelsen er en indholdsmæssigt uændret videreførelse af ordningen efter telelovens § 73, stk. 3, jf. stk. 1. Bestemmelsen viderefører endvidere implementeringen af artikel 5 (1) i rammedirektivet. Efter stk. 2 kan Center for Cybersik-

kerhed hos udbyderne kræve enhver oplysning og alt materiale af betydning for centerets tilsynsvirksomhed. Sådant materiale kan eksempelvis være udbyderens informationssikkerhedspolitik, risikovurderinger, beredskabsplaner, netarkitektur- og designdokumenter samt testrapporter. Bestemmelsen suppleres af den foreslåede § 4, hvorefter Center for Cybersikkerhed mere generelt med henblik på at sikre informationssikkerheden i net og tjenester kan fastsætte regler om oplysnings- og underretningspligter for udbydere af offentligt tilgængelige net og tjenester.

Det foreslåede *stk. 3* er en indholdsmæssigt uændret videreførelse af telelovens § 73, stk. 5. Det foreslås med bestemmelsen, at Center for Cybersikkerhed fortsat kan stille krav om, hvordan og i hvilken form oplysninger og materiale skal afgives til centeret. Der kan eksempelvis stilles krav om, at oplysninger og materiale skal afgives elektronisk i form af indsendelse af elektroniske dokumenter eller via indtastninger på en hjemmeside.

Efter *stk. 4* kan Center for Cybersikkerhed som noget nyt kræve, at udbydere afgiver skriftlige udtalelser og redegørelser om faktiske forhold af betydning for centerets tilsynsvirksomhed. Centeret kan efter bestemmelsen eksempelvis anmode om en nærmere redegørelse for udbydernes beredskabsplanlægning eller risikostyring i forhold til informationssikkerheden i udbyderens net eller tjenester. Centeret kan endvidere efter bestemmelsen anmode om en udtalelse vedrørende konkrete forhold, som centeret er blevet opmærksom på i forbindelse med sin tilsynsvirksomhed.

Det foreslås med s*tk. 5*, at Center for Cybersikkerhed i forbindelse med tilsynet med udbyderes overholdelse af regler vedrørende informationssikkerhed i net og tjenester kan stille krav om, at udbydere skal foranstalte en uafhængig sikkerhedsrevision og stille resultaterne heraf til rådighed for centeret. Centeret kan stille krav om, at sikkerhedsrevisionen skal udføres af et uafhængigt revisionsfirma. En sådan mulighed følger i dag af § 20, stk. 2, i bekendtgørelse nr. 445 af 11. maj 2011 om informationssikkerhed og beredskab for elektroniske kommunikationsnet og -tjenester. Den foreslåede bestemmelse viderefører implementeringen af artikel 13b (2b) i rammedirektivet. Det bemærkes, at Center for Cybersikkerhed i overensstemmelse med den hidtidige praksis alene vil stille krav om, at en udbyder skal foranstalte en uafhængig sikkerhedsrevision i de tilfælde, hvor der er indikationer på, at en udbyder ikke overholder centrale regler vedrørende informationssikkerhed i net og tjenester.

Det foreslås med *stk. 6*, at Center for Cybersikkerhed uden retskendelse mod behørig legitimation og efter et varsel på mindst syv arbejdsdage har adgang til udbyderes forretningslokaler med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven, hvis det er nødvendigt af hensyn til informationssikkerheden. Begrebet "forretningslokaler" omfatter de lokaler, hvorfra udbyderne driver forretning i bred forstand, herunder lokaler, der rummer tekniske installationer.

Formålet med indførelsen af dette tilsynsværktøj, som også anvendes på en række andre retsområder, er at give Center for Cybersikkerhed mulighed for at konstatere, om udbyderne i praksis har

gennemført de nødvendige foranstaltninger med henblik på at sikre et passende informationssikkerheds- og beredskabsniveau.

Tilsynsbesøgene vil alene blive gennemført, hvis det er nødvendigt af hensyn til informationssikkerheden. Center for Cybersikkerheds adgang til at foretage tilsynsbesøg – der kun forudsættes anvendt, såfremt et tilsvarende resultat ikke kan opnås ved anvendelse af andre og mindre indgribende tilsynsmuligheder – kan derfor kun anvendes i forbindelse med centerets tilsynsvirksomhed.

Center for Cybersikkerhed vil ikke i forbindelse med tilsynsbesøgene kunne få adgang til elektronisk kommunikation til, fra og mellem udbydernes kunder, ligesom centeret alene vil kunne foretage tilsynsbesøg i det omfang, udbyderens forretningslokaler er placeret i Danmark.

Center for Cybersikkerheds tilsynsbesøg vil skulle varsles skriftligt, herunder via e-mail, mindst syv arbejdsdage forud for besøget, og centeret kan således ikke med hjemmel i bestemmelsen foretage uanmeldte tilsynsbesøg.

Det forudsættes endvidere, at Center for Cybersikkerhed i forbindelse med tilsynsbesøgene i videst muligt omfang tager hensyn til udbyderens virksomhed og tilrettelægger besøgene således, at centeret alene skaffer sig kendskab til forhold, der er af betydning for gennemførelsen af centerets tilsynsvirksomhed. Tilsynsbesøgene vil typisk tage udgangspunkt i oplysninger og materiale fra udbyderne, herunder oplysninger om de iværksatte tekniske, processuelle og organisatoriske foranstaltninger.

Såfremt en udbyders net og tjenester drives af eller stilles til rådighed af en samarbejdspartner, leverandør eller underleverandør, foreslås det med *stk. 7*, at Center for Cybersikkerhed uden retskendelse kan få adgang til samarbejdspartnerens, leverandørens eller underleverandørens forretningslokaler, der er placeret i Danmark. Ved tilsynsbesøg hos samarbejdspartnere, leverandører eller underleverandører gælder de samme betingelser som efter stk. 6.

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

Til § 10

Det foreslås med *§ 10* som noget nyt, at Center for Cybersikkerhed i ikke-anonymiseret form kan offentliggøre afgørelser truffet i henhold til § 3, stk. 2 og 3, og § 5, stk. 4, samt afgørelser truffet i henhold til regler, der er udstedt i medfør af §§ 3-5, og § 6, stk. 6, tilsynsresultater, resuméer af domme og bødevedtagelser, hvor der idømmes eller vedtages en bøde for overtrædelse af loven eller regler, der er udstedt i medfør heraf, samt resuméer af domme i retssager, hvor Center for Cybersikkerhed er part.

Den foreslåede bestemmelse har til formål at give udbyderne øget incitament til overholdelse af kravene til informationssikkerhed og beredskab, ligesom bestemmelsen giver telekunder mulighed for at vurdere, i hvilket omfang de enkelte udbydere har levet op til lovgivningens krav.

Offentliggørelse af afgørelser efter *stk. 1, nr. 1,* indebærer, at der kan ske offentliggørelse i sager, hvor en udbyder ikke lever op til kravene til informationssikkerhed eller beredskab, såvel som i sager, hvor Center for Cybersikkerhed giver påbud til en udbyder om eksempelvis at foretage nærmere angivne foranstaltninger til sikring af informationssikkerheden. Der vil også kunne ske offentliggørelse i sager, hvor Center for Cybersikkerhed på baggrund af eksempelvis en klage konstaterer, at en udbyder overholder kravene til informationssikkerhed og beredskab. Center for Cybersikkerheds beslutning om at overgive sager til politimæssig efterforskning vil også kunne offentliggøres efter bestemmelsen.

Efter *stk. 1, nr. 2,* kan centeret endvidere offentliggøre resultater af tilsyn udført efter § 9. Sådanne tilsynsresultater kan omfatte centerets tilsynsrapporter, ligesom det vil kunne omfatte statistik, eksempelvis i form af en kvartalvis eller årlig opgørelse over antallet af påbud til de enkelte teleudbydere.

Det foreslås endvidere med *stk. 1, nr. 3*, at resuméer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde for overtrædelse af denne lov eller regler, der er udstedt i medfør af denne lov, skal kunne offentliggøres.

Herudover skal der efter *stk. 1, nr. 4*, kunne ske offentliggørelse af resuméer af domme i retssager vedrørende informationssikkerhed og beredskab på teleområdet, og hvor Center for Cybersikkerhed er part.

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

Det foreslås imidlertid med *stk. 2, nr. 1*, at offentliggørelsen ikke må indeholde oplysninger vedrørende tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold eller lignende, for så vidt det er af væsentlig økonomisk betydning for den udbyder, oplysningerne angår. Definitionen af oplysninger vedrørende tekniske indretninger m.v. skal forstås i overensstemmelse med § 30, nr. 2, i offentlighedsloven og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

Efter *stk. 2, nr. 2,* vil oplysninger undtages fra offentliggørelse i det omfang, det er af væsentlig betydning for statens sikkerhed eller rigets forsvar. Vurderingen af, hvornår offentliggørelse af oplysninger kan være af væsentlig betydning for statens sikkerhed eller rigets forsvar, skal foretages i overensstemmelse med principperne i § 31 i offentlighedsloven.

Desuden vil klassificerede informationer efter *stk. 2*, *nr. 3,* blive slettet i det materiale, der offentliggøres. Efter *stk. 2, nr. 4*, vil der endvidere ikke ske offentliggørelse af fortrolige oplysninger, der hidrører fra nationale tilsynsmyndigheder i andre EU-medlemsstater, jf. den foreslåede § 12, stk. 3, medmindre de myndigheder, der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse til offentliggørelsen.

Endelig vil enkeltpersoners forhold blive slettet inden offentliggørelsen efter *stk. 2, nr. 5*. Det 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 eller tilsynsresultater, såfremt efterforskningsmæssige hensyn taler derimod.

Efter *stk. 3* bemyndiges Center for Cybersikkerhed til at fastsætte nærmere regler for centerets sagsbehandling i forbindelse med offentliggørelser efter stk. 1.

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

Center for Cybersikkerhed vil herudover kunne fastsætte regler om, at det skal fremgå af offentliggørelsen, såfremt en afgørelse er påklaget til Forsvarsministeriet, eller såfremt der verserer en sag for domstolene.

Endelig vil Center for Cybersikkerhed kunne fastsætte regler om, hvor lang tid den pågældende afgørelse, tilsynsresultat m.v. skal være offentligt tilgængelige på centerets hjemmeside.

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

Til § 11

Den foreslåede *§ 11* er en delvis videreførelse af telelovens § 75 a, stk. 5, jf. stk. 2 og 3.

Efter det foreslåede *stk. 1* kan Center for Cybersikkerhed fastsætte regler om, at skriftlig kommunikation til og fra Center for Cybersikkerhed skal foregå digitalt. Der kan med hjemmel i bestemmelsen fastsættes regler om, hvem der omfattes af pligten til at kommunikere digitalt med Center for Cybersikkerhed, om hvilke forhold, og på hvilken måde.

Det bemærkes i den forbindelse, at pligten til at kommunikere digitalt ikke vil omfatte klassificerede informationer. Baggrunden herfor er, at sikkerhedscirkulæret stiller en række krav til digital for-

sendelse af klassificerede informationer, herunder bl.a. krav om sikkerhedsgodkendelse af informationssystemer samt anvendelse af godkendt kryptoudstyr.

Det foreslåede stk. 1 indebærer, at skriftlige henvendelser til Center for Cybersikkerhed om forhold, som er omfattet af et krav om digital kommunikation, ikke anses for behørigt modtaget af centeret, hvis de indsendes på anden vis end den foreskrevne digitale måde. Hvis en virksomhed retter henvendelse til Center for Cybersikkerhed på anden måde end den foreskrevne digitale måde, eksempelvis ved brev, følger det af den almindelige vejledningspligt, jf. forvaltningslovens § 7, stk. 2, at centeret skal vejlede om reglerne på området, herunder om pligten til at kommunikere digitalt.

Herudover indebærer bestemmelsen, at der kan fastsættes regler om, at en virksomhed, som retter henvendelse til Center for Cybersikkerhed, skal oplyse en e-mailadresse, som virksomheden kan kontaktes på i forbindelse med behandlingen af en konkret sag eller henvendelse til centeret. I den forbindelse kan der også pålægges den pågældende virksomhed en pligt til at underrette centeret om en eventuel ændring af e-mailadressen, inden den konkrete sag afsluttes eller henvendelsen besvares, medmindre e-mails automatisk bliver videresendt til den nye e-mailadresse.

Der kan desuden fastsættes regler om, at Center for Cybersikkerhed kan sende visse meddelelser samt afgørelser, herunder påbud, til virksomhedens digitale postkasse med de retsvirkninger, der følger af lov nr. 528 af 11. juni 2012 om Offentlig Digital Post.

Der kan desuden fastsættes regler om fritagelse for pligten til digital kommunikation. Fritagelsesmuligheden tænkes navnlig anvendt, hvor det er påkrævet at anvende en dansk digital signatur, men der er tale om en virksomhed med hjemsted i udlandet, og som dermed ikke kan få udstedt en dansk digital signatur. Det bemærkes i den forbindelse, at fritagelsesmuligheden er stærkt begrænset, idet der er tale om kommunikation om erhvervsforhold.

Det forhold, at en virksomheds computere ikke fungerer, at virksomheden har mistet koden til sin digitale signatur, eller at der opstår lignende hindringer, som det er op til virksomheden at overvinde, kan ikke føre til fritagelse for pligten til digital kommunikation. I så fald må den pågældende virksomhed eksempelvis anmode en rådgiver om at varetage kommunikationen på virksomhedens vegne.

Efter det foreslåede *stk. 2* kan der fastsættes regler om anvendelse af bestemte it-systemer, digitale formater og digital signatur eller lignende. Den foreslåede bestemmelse indebærer, at det kan gøres obligatorisk for virksomheder at anvende bestemte internetløsninger, herunder selvbetjeningsløsninger.

Det foreslåede *stk. 3* fastsætter, hvornår en digital meddelelse må anses for at være kommet frem til adressaten for meddelelsen. Forslaget indebærer, at meddelelser til eller fra Center for Cybersikkerhed, der sendes på den foreskrevne digitale måde, anses for at være kommet frem til adressaten på det tidspunkt, hvor meddelelsen er tilgængelig digitalt for adressaten. Dermed er der tale om samme

retsvirkning som ved fysisk post, der anses for at være kommet frem, når den pågældende meddelelse m.v. er lagt i adressatens fysiske postkasse. En meddelelse vil normalt anses for at være kommet frem, når meddelelsen er tilgængelig digitalt for adressaten, således at vedkommende har mulighed for at behandle meddelelsen. Dette tidspunkt vil normalt blive registreret automatisk i adressatens it-system.

Til § 12

Formålet med den foreslåede bestemmelse er at sikre udveksling af oplysninger mellem Center for Cybersikkerhed og Europa-Kommissionen, Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) eller nationale tilsynsmyndigheder i andre EU-medlemsstater med henblik på et effektivt og ensartet tilsyn med informationssikkerhed og beredskab i EU-medlemsstaterne.

Det foreslås med *stk. 1*, at Center for Cybersikkerhed kan indsamle oplysninger om informationssikkerhed og beredskab på teleområdet hos udbydere med henblik på at videregive oplysningerne til Europa-Kommissionen, ENISA eller nationale tilsynsmyndigheder i andre EU-medlemsstater. Bestemmelsen er en delvis videreførelse af telelovens § 73, stk. 3, jf. stk. 2, 1. pkt. Den foreslåede bestemmelse viderefører implementeringen af artikel 5 (2) i rammedirektivet. Det foreslås, at bestemmelsen også skal omfatte indsamling af oplysninger om informationssikkerhed med henblik på videregivelse af oplysningerne til ENISA, som har til opgave at sikre en høj grad af net- og informationssikkerhed i EU, og som bl.a. fungerer som et forum for erfaringsudveksling for de nationale tilsynsmyndigheder. Bestemmelsen forventes ikke anvendt i større omfang end efter hidtidig praksis efter teleloven.

Efter det foreslåede s*tk. 2* skal udbydere, hvis oplysninger videregives til Europa-Kommissionen, ENISA eller til nationale tilsynsmyndigheder i andre EU-medlemsstater, orienteres forud for videregivelsen. Center for Cybersikkerhed skal ikke afvente udbyderens eventuelle kommentarer eller accept af videregivelsen. Det vil således være tilstrækkeligt, at der i forbindelse med indsamlingen af oplysningerne orienteres om videregivelsen. Bestemmelsen er en delvis videreførelse af telelovens § 73, stk. 3, jf. stk. 2, 2. pkt. Den foreslåede bestemmelse viderefører desuden implementeringen af artikel 5 (2) i rammedirektivet. Det foreslås, at bestemmelsen konsekvensændres på baggrund af det foreslåede stk. 1, således at Center for Cybersikkerhed også orienterer de udbydere, der er indsamlet oplysninger fra, forud for videregivelse af oplysningerne til ENISA.

Med *stk. 3* foreslås det, at oplysninger, der modtages eller stammer fra nationale tilsynsmyndigheder i andre EU-medlemsstater, og som har karakter af forretningshemmeligheder i henhold til EU-regler eller nationale regler, også behandles som sådanne i Danmark. Bestemmelsen finder anvendelse, uanset om oplysningerne modtages direkte fra den pågældende nationale tilsynsmyndighed eller via andre, herunder Europa-Kommissionen. Bestemmelsen er en indholdsmæssigt uændret videreførelse af telelovens § 74. Den foreslåede bestemmelse viderefører herudover implementeringen af artikel 5 (3) i rammedirektivet.

Til § 13

Den foreslåede *§ 13* er en indholdsmæssigt uændret videreførelse af telelovens § 80.

Det foreslås med bestemmelsen, at Center for Cybersikkerhed får hjemmel til at fastsætte regler, som er nødvendige for at anvende retsakter udstedt af Den Europæiske Union om informationssikkerhed og beredskab på teleområdet. Bemyndigelsen kan benyttes til at gennemføre tekniske gennemførelsesbestemmelser, som Europa-Kommissionen i medfør af artikel 13 a (4) i rammedirektivet vedtager med henblik på at harmonisere foranstaltninger efter artikel 13 (1-3) i rammedirektivet.

Det foreslås endvidere, at Center for Cybersikkerhed kan fastsætte regler om straf af bøde for overtrædelse af bestemmelser indeholdt i retsakter udstedt af Den Europæiske Union vedrørende informationssikkerhed og beredskab på teleområdet. Derved sikres en effektiv gennemførelse af retsakterne.

Til § 14

Det foreslåede *stk. 1* er en delvis videreførelse af telelovens § 81, stk. 1, nr. 1. Efter den foreslåede bestemmelse kan undladelse af at efterkomme Center for Cybersikkerheds påbud efter § 3, stk. 2 og 3, samt § 5, stk. 4, som noget nyt straffes med bøde. Endvidere kan overtrædelse af § 6, stk. 2-4, om sikkerhedsgodkendelse straffes med bøde. Derudover foreslås det som noget nyt, at undladelse af at efterkomme Center for Cybersikkerheds krav i forbindelse med centerets tilsynsvirksomhed efter § 9, stk. 2, 4 og 5, samt hindring af Center for Cybersikkerheds adgang til udbyderes forretningslokaler, samt forretningslokaler hos udbyders samarbejdspartnere, leverandører og underleverandører efter § 9, stk. 6 og 7, kan straffes med bøde.

Center for Cybersikkerhed bemyndiges med det foreslåede *stk. 2* til at fastsætte straf af bøde for overtrædelse af bestemmelser i regler, som udfærdiges i medfør af §§ 3-5 og § 6, stk. 6, herunder for undladelse af at efterkomme centerets påbud. Bestemmelsen er en delvis videreførelse af telelovens § 81, stk. 2. Det foreslås som noget nyt, at Center for Cybersikkerhed bemyndiges til at fastsætte straf af bøde for overtrædelse af regler udstedt i medfør af den foreslåede § 6, stk. 6, om sikkerhedsgodkendelse af udbyderes medarbejdere eller repræsentanter for udbydere, der har adgang til udstyr eller systemer, som benyttes i forbindelse med indgreb i meddelelseshemmeligheden.

Efter det foreslåede *stk. 3* kan der pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel. Bestemmelsen indebærer, at der også i regler, som udfærdiges i medfør af loven, kan fastsættes regler om, at der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel. Bestemmelsen er en indholdsmæssigt uændret videreførelse af telelovens § 81, stk. 4.

Det følger af artikel 21 a i rammedirektivet, at medlemsstaterne skal fastsætte bestemmelser om sanktioner for overtrædelse af bestemmelser fastsat i medfør af rammedirektivet og særdirektiverne.

Til § 15

Bestemmelsen i *§ 15, stk. 1,* fastsætter tidspunktet for lovens ikrafttræden. Det foreslås, at loven træder i kraft den 1. december 2015.

Til § 16

Med *§ 16* foreslås det, at en række bestemmelser i teleloven ophæves, ligesom der som følge af ophævelsen af bestemmelserne foretages konsekvensændringer i en række øvrige bestemmelser i teleloven.

De foreslåede ændringer er en konsekvens af, at telelovens bestemmelser om informationssikkerhed og beredskab med nærværende lovforslag foreslås samlet i en net- og informationssikkerhedslov.

Til § 17

Med *§ 17* fastlægges lovens territoriale gyldighed. Det foreslås, at loven ikke skal gælde for Færøerne og Grønland, hvilket er en videreførelse af ordningen efter telelovens § 83.