FORSVARSMINISTERIET
DANISH MINISTRY OF DEFENCE

Maj 2015

KOMMENTERET HØRINGSOVERSIGT

vedrørende

forslag til lov om net- og informationssikkerhed

(Lovforslag L 201)

Et udkast til lovforslag har i perioden 21. april 2015 til 4. maj 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.

Heraf har Forsvarsministeriet modtaget høringssvar fra:

Advokatrådet, Dansk Energi, Danske Regioner, Datatilsynet, DI ITEK, Domstolsstyrelsen, Hi3G Denmark ApS, IT-Branchen, IT-Politisk Forening, Nianet A/S, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Rigsrevisionen, Rådet for Digital Sikkerhed, Stofa A/S og Teleindustrien (TI).

Forsvarsministeriet har endvidere modtaget en udtalelse fra Justitia.

HOLMENS KANAL 42
1060 KØBENHAVN K
TELEFON: 33 92 33 20
TELEFAX: 33 32 06 55
MAIL: FMN@FMN.DK
WEB: www.FMN.DK
CVR: 25-77-56-35
EAN: 5798000201200

De væsentligste bemærkninger fra de hørte parter til de enkelte emner i lovforslaget gennemgås og kommenteres nedenfor. Forsvarsministeriets bemærkninger til høringssvarene er anført med kursiv.

Derudover indeholder enkelte høringssvar bemærkninger og opfordringer til initiativer, som ikke vedrører nærværende lovforslag. Disse omtales ikke nærmere.

Høringssvarene

Domstolsstyrelsen, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret og *Rigsrevisionen* har ikke fremsat bemærkninger til lovforslaget.

1. Generelle bemærkninger

Dansk Energi, Nianet A/S og Stofa A/S bifalder, at lovforslaget skaber en mere sammenhængende og overskuelig regulering af informationssikkerhed og beredskab på teleområdet.

IT-Politisk Forening bemærker, at informationssikkerheden i telesektoren er vigtig for hele samfundet, og påpeger, at televirksomheder kan have særlig interesse for hackere, fordi et angreb kan give adgang til telekundernes kommunikation, herunder oplysninger om borgeres private forhold og virksomheders forretningshemmeligheder.

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S konstaterer, at en del af de kritikpunkter, som det første lovudkast fra november 2014 gav anledning til, er imødekommet og forbedret i det reviderede lovudkast. Ikke desto mindre er det fortsat Teleindustriens, IT-Branchens, DI ITEKs og Stofa A/S' opfattelse, at lovudkastet medfører en høj grad af uforudsigelighed om, hvilke forpligtelser som udbyderne kan blive pålagt, uklarhed om, hvilke retssikkerhedsmæssige garantier udbyderne har, samt risiko for, at danske udbydere skal afholde væsentlige omkostninger og pålægges store administrative byrder.

Rådet for Digital Sikkerhed finder det som udgangspunkt positivt, at der med lovforslaget tages skridt til at øge informationssikkerhedsniveauet og skabe en robust informations- og kommunikationsteknologisk infrastruktur (ikt-infrastruktur) i Danmark.

2. Lovforslagets struktur

Dansk Energi, Nianet A/S og Stofa A/S påpeger, at lovforslagets karakter af bemyndigelseslovgivning bevirker, at Center for Cybersikkerhed får vidtstrakte beføjelser. Dansk Energi, Nianet A/S og Stofa A/S er endvidere bekymret for, om kravene i lovforslaget vil afspejle det aktuelle trusselsbillede, og så gerne en mekanisme i lovforslaget, som sikrer bortfald af krav, der på grund af udviklingen i trusselsbilledet bliver uaktuelle.

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S bemærker, at Center for Cybersikkerhed flere steder i lovforslaget tillægges vidtgående beføjelser, og at lovforslaget mangler grundlæggende proportionalitetsbetragtninger og kriterier for skønsudøvelse. Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S finder endvidere, at lovforslaget indeholder vidtgående beføjelser, der alene fremgår af bemærkningerne til lovforslaget, hvilket de finder retssikkerhedsmæssigt betænkeligt. Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S fremhæver i den forbindelse bl.a., at det ikke er nærmere angivet, hvilke kriterier der skal opfyldes for, at det kan udløse påbud efter bestemmelsen i § 5, stk. 4.

Hi3G Denmark ApS vurderer, at lovteksten er alt for bred i sine formuleringer, hvilket vil gøre det vanskeligt og byrdefuldt at drive forretning i Danmark. Virksomheden anfører konkret, at det i påbudsbestemmelsen i § 5, stk. 4, bør beskrives nærmere, hvad "angivne sikkerhedsforanstaltninger" kan være.

Som det er tilfældet i gældende ret på området, giver forslaget til lov om net- og informationssikkerhed på en række områder Center for Cybersikkerhed bemyndigelse til at udstede detaljerede regler på området.

Denne model skal ses i lyset af, at der er tale om et område, hvor den teknologiske udvikling går særdeles stærkt, samtidig med at trusselsbilledet løbende ændrer sig. Det skaber behov for en smidig regulering, der f.eks. kan sikre, at bebyrdende krav til teleudbyderne, som ikke længere er relevante, hurtigt kan ophæves. Endvidere gør områdets tekniske kompleksitet, at det ikke vurderes som hensigtsmæssigt, at de meget detaljerede og tekniske regler fastsættes ved lov.

Med henblik på at sikre, at den fremtidige regulering af området er forudsigelig for teleudbyderne, er de enkelte bemyndigelser beskrevet detaljeret i lovforslagets bemærkninger. I forbindelse med hver enkel bemyndigelse er rammerne for bemyndigelsens udmøntning således beskrevet, herunder rammerne for myndighedernes udøvelse af skøn, ligesom der i bemærkningerne anføres en lang række illustrative eksempler på, hvad de bekendtgørelser, der vil blive udstedt i medfør af loven, vil indeholde. Det bemærkes i den forbindelse, at bekendtgørelserne vil blive udarbejdet i tæt dialog med telebranchen, og at bekendtgørelserne vil blive sendt i offentlig høring.

Den valgte model er i overensstemmelse med den almindelige lovgivningstradition, som indebærer, at der i et lovforslags specielle bemærkninger gives en detaljeret anvisning på de enkelte spørgsmål, som lovforslagets bestemmelser kan rejse. I det omfang det – som i det aktuelle tilfælde – er nødvendigt at anvende relativt brede bemyndigelser, følger det ligeledes af principperne for udarbejdelse af lovforslag, at disse bemyndigelser afgrænses og præciseres i bemærkningerne, således som det er sket i forslaget til lov om net- og informationssikkerhed.

Dansk Energi, Nianet A/S og Stofa A/S vurderer i forhold til lovforslagets § 3, at rammerne for Center for Cybersikkerheds regeludstedelse er upræcise, og at bestemmelsens anvendelsesområde bør afgrænses nærmere i bemærkningerne til bestemmelsen.

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S finder, at flere af hjemmelsbestemmelserne i lovforslaget er for bredt formuleret. Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S fremhæver i den forbindelse, at det ikke er nærmere angivet, hvilke kriterier der skal opfyldes for, at der kan påbydes konkrete foranstaltninger efter lovforslagets § 3, stk. 3.

Særligt for så vidt angår den foreslåede § 3, kan der henvises til, at der i bemærkningerne til denne bestemmelse er en beskrivelse på tre sider, som detaljeret redegør for, hvilke krav og foranstaltninger som vil kunne indgå i udmøntningen af bestemmelsen. I denne beskrivelse indgår endvidere en række eksempler, der illustrerer rammerne for udmøntningen.

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S opfordrer til, at kompetencen til at udstede bekendtgørelser i medfør af lovforslaget lægges hos Forsvarsministeriet, mens tilsynsopgaven lægges hos Center for Cybersikkerhed.

Lovforslaget indebærer, 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. I lyset af bekendtgørelsernes forventede tekniske kompleksitet, der forudsætter en særlig grad af teleteknisk ekspertise, anser Forsvarsministeriet fortsat denne ordning for hensigtsmæssig.

Det bemærkes, at bekendtgørelserne under alle omstændigheder udstedes under forsvarsministerens ansvar.

3. Forholdet til EU-regulering

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S henviser til det af kommissionen fremsatte forslag til et direktiv om foranstaltninger, der skal sikre et højt fælles niveau for net- og informationssikkerhed i EU (det såkaldte NIS-direktiv). Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S henviser til grund- og nærhedsnotatet om direktivet til Folketingets Europaudvalg, hvor det anføres, at det er regeringens holdning, at der på direktivets område er behov for regler på EU-niveau, der sikrer et ensartet og højt niveau af net- og informationssikkerhed på tværs af medlemsstaterne. Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S opfordrer på den baggrund til, at området ikke gøres til genstand for dansk enegang, men afventer en harmoniseret europæisk tilgang.

Det anførte bygger på en misforståelse.

Kommissionens direktivforslag om net- og informationssikkerhed (NIS-direktiv) af 7. februar 2013 vil således ikke omfatte teleudbydere, da disse allerede er omfattet af direktivet om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (direktiv 2002/21/EF – rammedirektivet). Dette fremgår klart af artikel 1(3) i forslaget til NIS-direktiv.

Det skal dog nævnes, at det under forhandlingerne i Rådet har været diskuteret, om "internet exchange points", i det omfang de ikke allerede er omfattet af rammedirektivet, skal være omfattet af de sikkerheds- og rapporteringskrav, som direktivet ventes at indføre. Der arbejdes derfor i EU-regi på at finde en formulering, der sikrer, at de to direktiver ikke kommer til at overlappe hinanden.

Dansk Energi, Nianet A/S og Stofa A/S vurderer, at der er behov for at få afklaret, om – og i givet fald hvordan – kravene og foranstaltningerne i det foreslåede NIS-direktiv afviger fra lovforslaget. Dette skal sikre en koordineret europæisk net- og informationsindsats på teleområdet.

Hi3G Denmark ApS anfører, at lovforslaget er meget indgribende over for teleselskaber i Danmark, og at lovforslaget ikke er proportionalt for teleselskaberne i Danmark i forhold til de krav, der stilles i andre EU-lande. På den baggrund mener Hi3G Denmark ApS, at Danmark bør afvente det arbejde, der pågår i EU, således at der i Danmark er samme krav som i andre EU-lande.

Der henvises til det ovenfor anførte om NIS-direktivet. Det bemærkes i øvrigt, at det er regeringens holdning, at der – også på teleområdet – er behov for et stærkt europæisk samarbejde inden for informationssikkerhed. Forsvarsministeriet deltager aktivt i det eksisterende europæiske samarbejde på informationssikkerhedsområdet.

4. Definitioner af begreber m.v.

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S anfører, at der mangler definitioner og klarhed om væsentlige elementer i lovforslaget og henviser særligt til definition af begreberne "informationssikkerhed" og "brud på informationssikkerheden", idet Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S dog bemærker, at begrebet "informationssikkerhed" ikke er nyt, men er videreført fra gældende ret.

Rådet for Digital Sikkerhed anfører, at lovforslagets bestemmelser indeholder en række begreber, der ikke er nærmere defineret i lovteksten og bemærkningerne. Rådet for Digital Sikkerhed henviser til begreberne "informationssikkerhed", "risiko", "drift", "driftsopgaver", "beredskabssituationer" og "ekstraordinære situationer". Rådet opfordrer til, at begreberne defineres i lovteksten og forklares yderligere i bemærkningerne.

De centrale begreber i lovforslaget er defineret i forslagets § 2, mens en række andre udtryk, som anvendes i lovforslaget, defineres og beskrives i lovforslagets bemærkninger.

I forhold til begrebet informationssikkerhed er der ikke med lovforslaget tilsigtet en ændring af forståelsen af begrebet i forhold til gældende ret.

Det fremgår af afsnit 3.1.1 i bemærkningerne til lovforslaget, at informationssikkerhed på teleområdet som begreb omfatter myndighedernes og virksomhedernes samlede indsats for at forebygge nedbrud i informationssystemer samt beskytte data, som behandles i systemerne, mod manipulation, tab eller tyveri. Endvidere er begrebets nærmere anvendelsesområde detaljeret beskrevet i bemærkningerne til den foreslåede § 3, der omhandler informationssikkerhed i net og tjenester.

Det fremgår af bemærkningerne til lovforslagets § 4, at brud på informationssikkerheden omfatter tab af både tilgængelighed, integritet og fortrolighed i net og tjenester. I samme afsnit eksemplificeres de forskellige former for brud på informationssikkerheden, som er omfattet af bestemmelsen.

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S anfører, at det er uklart, hvordan informationspligt efter lovforslagets § 4, nr. 3, hænger sammen med den underretningspligt, der er over for Erhvervsstyrelsen ved brud på persondatasikkerheden.

IT-Politisk Forening opfordrer til, at ansvarsfordelingen mellem Erhvervsstyrelsen og Center for Cybersikkerhed beskrives mere præcist i lovforslagets bemærkninger.

Det er Forsvarsministeriets opfattelse, at der med lovforslaget sker en tydeliggørelse af ansvarsdelingen mellem Center for Cybersikkerheds opgaver på net- og informationssikkerhedsområdet og Erhvervsstyrelsens opgaver på persondatasikkerhedsområdet, da førstnævnte fremover reguleres i net- og informationssikkerhedsloven, mens sidstnævnte reguleres i lov om elektroniske kommunikationsnet og -tjenester (teleloven).

5. Forholdet til persondataloven

Datatilsynet forudsætter generelt, at eventuelle behandlinger af personoplysninger, som vil ske som følge af lovforslagets bestemmelser, vil ske inden for rammerne af persondataloven. Tilsynet henleder endvidere opmærksomheden på persondatalovens § 57, hvorefter der skal indhentes udtalelse fra tilsynet ved udarbejdelse af bekendtgørelser, cirkulærer eller lignende generelle retsforskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af oplysninger.

Det fremgår af § 8 i lov om Center for Cybersikkerhed, at Center for Cybersikkerheds virksomhed er undtaget fra persondataloven. En række af de centrale principper i persondataloven finder dog også anvendelse på Center for Cybersikkerheds virksomhed, jf. kapitel 6 i lov om Center for Cybersikkerhed. Behandling af personoplysninger efter net- og informationssikkerhedsloven vil derfor ske i overensstemmelse med de centrale principper i persondataloven.

Det bemærkes i øvrigt, at de bekendtgørelser, der vil blive udstedt i medfør af net- og informationssikkerhedsloven, vil blive sendt i høring hos Datatilsynet.

Rådet for Digital Sikkerhed anbefaler, at det i lovforslaget fastslås, at krav, der stilles til udbydere i medfør af lovforslaget, opfylder persondatalovens krav til beskyttelse af personoplysninger og sikkerhedsbekendtgørelsens krav til sikkerhed, således at udbyderne ikke udsættes for modstridende lovkrav.

Det bemærkes, at spørgsmålet om persondatabeskyttelse i forhold til teleområdet er reguleret i lov om elektroniske kommunikationsnet og -tjenester (teleloven) og henhører under Erhvervsstyrelsen.

Center for Cybersikkerheds interne behandling af personoplysninger, f.eks. i forbindelse med korrespondance med teleudbydere, i medfør af lovforslaget vil skulle ske i overensstemmelse med kapitel 6 i lov om Center for Cybersikkerhed. Teleudbydernes behandling af personoplysninger er fuldt ud underlagt persondataloven.

6. Forholdet til forvaltningsloven, klageadgang m.v.

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S opfordrer til, at de forvaltningsretlige aspekter af Center for Cybersikkerheds beslutninger samt klageadgangen i forhold til centerets afgørelser og påbud mv. eksplicit fremhæves i lovforslaget, således at centeret – eventuelt med undtagelse af handlinger i akutte nødstilfælde – omfattes af forvaltningsloven i sin helhed.

Hi3G Denmark ApS påpeger, at lovforslaget ikke indeholder en ankemulighed for teleudbyderne svarende til den nuværende regulering, hvor der kan klages til Forsvarsministeren.

Som det fremgår af afsnit 2 i lovforslagets almindelige bemærkninger, indebærer Center for Cybersikkerheds organisatoriske tilhørsforhold, at centerets afgørelser kan påklages til Forsvarsministeriet i medfør af den almindelige, ulovbestemte rekursadgang. Dette vil også gælde centerets afgørelser i forbindelse med udstedelse af påbud.

Det bemærkes i den forbindelse, at Center for Cybersikkerheds virksomhed er undtaget fra forvaltningslovens kapitel 4-6, jf. § 8 i lov om Center for Cybersikkerhed. Det fremgår imidlertid af bemærkninger til forslaget til lov om Center for Cybersikkerhed, at det forudsættes, at Center for Cybersikkerhed i videst muligt omfang efterlever principperne i forvaltningslovens kapitel 4-6. I praksis indebærer det, at Center for Cybersikkerhed i virket som myndighed på informationssikkerhedsområdet agerer som om, at forvaltningsloven var fuldt ud gældende for centeret.

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S anfører, at de ikke finder det tilstrækkeligt, at Forsvarsministeriet udgør klageinstans for afgørelser mv. truffet af Center for Cybersikkerhed i medfør af lovforslaget. Teleindustrien, IT-Branchen, DI ITEK og

Stofa A/S foreslår, at der oprettes et klagenævn med henblik på at sikre den fornødne uvildighed og ekspertise.

Det er Forsvarsministeriets opfattelse, at den ovenfor beskrevne klageadgang – samt muligheden for at indbringe afgørelser for domstolene – sikrer en tilstrækkelig (og uvildig) behandling af klager på området.

7. Indførelse af en standstill-periode

Dansk Energi, Nianet A/S og Stofa A/S anfører, at lovforslagets § 4, nr. 2, om underretningspligt ved indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf, er særdeles indgribende i kommerciel aftaleforhandling og -indgåelse på dette område. Dansk Energi, Nianet A/S og Stofa A/S vurderer, at de standstill-perioder, som der efter bestemmelsen kan fastsættes regler om, burde kunne afkortes eller helt undgås, hvis indsatsen fokuserer på en dialog om sikkerhed, inden aftaleforhandling indledes.

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S bemærker, at den foreslåede ordning er vidtgående og meget bebyrdende i praksis for udbyderne. Ordningen beskrives som særligt uproportional, når der henses til de reaktionsmuligheder, som Center for Cybersikkerhed har. Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S mener i stedet, at en løbende drøftelse med Center for Cybersikkerhed om et givent aftaleudkast gennem aftaleprocessen vil være mest hensigtsmæssig. Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S anfører, at hvis Center for Cybersikkerhed herefter ikke mener, at aftalen medfører et tilstrækkeligt sikkerhedsniveau, kan centeret bruge de øvrige muligheder, som lovforslaget vil give, til at gribe ind og få rettet op på dette.

Hi3G Denmark ApS betegner bestemmelsen som alt for vidtgående og anfører, at selskabet er meget bekymret for effekten af bestemmelsen, særligt om den kan få en negativ betydning for det kommercielle forhold mellem teleselskab og leverandører.

Formålet med underretningspligten er at sikre, at Center for Cybersikkerhed så tidligt som muligt kan indgå i en dialog med den enkelte udbyder om det risikobillede, herunder trusler og sårbarheder i forhold til informationssikkerheden, som teleudbyderens påtænkte aftale med en leverandør vurderes at indebære.

Udgangspunktet for standstill-perioden er, at der inden aftaleindgåelsen har været en løbende dialog mellem Center for Cybersikkerhed og teleudbyderen, hvor centeret kan rådgive om imødegåelse af trusler mod informationssikkerheden. Såfremt teleudbyderen indgår i denne dialog og følger de anbefalinger, som Center for Cybersikkerhed fremkommer med som et resultat af den forudgående dialog, vil standstill-perioden – som det er anført i lovforslagets bemærkninger – normalt blive af meget kort varighed. Det skyldes, at Center for Cybersikkerhed så blot har behov for at konstatere, at de informationssikkerhedsmæssigt relevante dele af aftaleudkastet er i overensstemmelse med centerets anbefalinger som et resultat af den forudgående dialog.

Standstill-perioden vil alene omfatte de relativt få aftaler, som vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf. Terminologien "væsentlige dele af udbyderens net eller tjenester" anvendes ligeledes i den foreslåede § 4, nr. 1, hvor terminologien beskrives nærmere.

Periodens varighed på op til 10 arbejdsdage er efter Forsvarsministeriets opfattelse proportional, og perioden er væsentligt kortere end tilsvarende perioder på andre retsområder. Som anført i bemærkninger til lovforslaget vil det endvidere blive tilstræbt, at standstill-perioden kan afsluttes inden for fem arbejdsdage.

8. Specifikke sikkerhedskrav

IT-Politisk Forening anfører, at de er skeptiske over for beføjelserne til Center for Cybersikkerhed i den foreslåede § 3, stk. 3, samt at det ikke fremgår klart af lovforslagets bemærkninger til den foreslåede bestemmelse, om beføjelserne til centeret alene vedrører påbud om at foretage visse undersøgelser ved mistanke om sårbarheder i teleselskabernes infrastruktur, eller om det også kan være forbud mod at anvende bestemte tekniske løsninger (udstyr) i infrastrukturen.

Det fremgår af bemærkningerne til den foreslåede § 3, stk. 3, at der ikke med hjemmel i bestemmelsen kan ske regulering af ejerforhold, fastsættes forbud mod at indgå aftale med bestemte leverandører eller forbud mod ejerskab af bestemte netværk eller produkter.

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S finder, at Center for Cybersikkerheds beføjelse til at stille krav om indstationering af medarbejdere hos underleverandører ved outsourcing er vidtgående. Derudover har Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S vanskeligt ved at se, at kravet om indstationering kan gennemføres i praksis overfor globale leverandører af udstyr og driftsydelser.

Det er Forsvarsministeriets opfattelse, at det ved outsourcing af større driftsopgaver er naturligt, at teleudbyderen fører et drifts- og sikkerhedsmæssigt tilsyn med leverandøren. Et krav om, at der skal ske indstationering af medarbejdere fra teleudbyderen, anses derfor ikke for at være vidtgående, men der vil ved udmøntningen og den efterfølgende administration af bestemmelsen blive taget højde for, at en indstationering i visse særlige situationer ikke vil kunne være mulig.

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S anfører, at informationsforpligtelsen efter den foreslåede § 4, stk. 1, nr. 1, og § 9, stk. 2, er vidtgående, herunder at der kan være tale om, at udbyderne bliver forpligtet til at fremskaffe eksempelvis kildekode eller andre forretningshemmeligheder, hvilket kan vise sig at være umuligt, idet udstyrsleverandøren ikke vil udlevere sådanne oplysninger.

I bemærkningerne til den foreslåede § 4, stk. 1, nr. 1, er bestemmelsens anvendelsesområde detaljeret beskrevet. Der vil ikke med hjemmel i bestemmelsen kunne stilles krav om udlevering af kildekode. Der vil i øvrigt ved udmøntningen og den efterfølgende administration af bestemmelsen i størst muligt omfang blive taget hensyn til teleudbydernes eventuelle juridiske forpligtelser overfor leverandører m.v.

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S finder, at den nuværende ordning med frivillige aftaler i forhold til prioriteringsordninger har vist sig at være konstruktiv og afbalanceret og opfordrer derfor til, at det præciseres i lovbemærkningerne til den foreslåede § 5, stk. 3, at Center for Cybersikkerhed vil være tilbageholdende med at udstede påbud på området, og at indgåelse af frivillige aftaler med branchen fortsat er den foretrukne løsningsmodel.

Hi3G Denmark ApS finder det yderst bekymrende, at myndighederne fremadrettet uden videre kan forlange yderligere investeringer i nye mobilprioriteringsløsninger, efter at Hi3G Denmark ApS igennem en årrække har deltaget aktivt i arbejdet omkring mobilprioritering og løbende har vedligeholdt og implementeret økonomisk meget bydefylde løsninger, uden at have set effekten af investeringer i den nuværende løsning.

Den foreslåede § 5, stk. 3, omhandler 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 nødvendig i beredskabssituationer og i andre ekstraordinære situationer, hvor der kan opstå kapacitetsproblemer eller beskadigelse af teleinfrastrukturen.

Det fremgår af afsnit 2 i bemærkningerne til lovforslaget, at der også med de nye regler vil 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. Det gælder også i forhold til de særlige prioriteringsordninger, som i størst muligt omfang vil blive fastsat efter aftale med teleudbyderne.

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S noterer sig med tilfredshed, at det er præciseret i bemærkningerne til lovforslaget, at der ikke kan kræves sikkerhedsgodkendelse, blot fordi en medarbejder har adgang til udbyderens kritiske infrastruktur, og at kravet om sikkerhedsgodkendelse skal ske ud fra en konkret vurdering. Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S anfører endvidere, at det er uklart, om den foreslåede § 6 indebærer, at teleoperatørerne skal have sikkerhedsgodkendt flere medarbejdere end i dag, da organisationerne efter dialog med Center for Cybersikkerhed har erfaret, at centeret gerne ser, at langt flere er sikkerhedsgodkendte.

Center for Cybersikkerhed kan ikke genkende bemærkningen om, at centeret gerne ser, at langt flere af teleudbydernes medarbejdere er sikkerhedsgodkendte efter den

procedure, der følger af den foreslåede § 6. Det er således hverken Center for Cybersikkerheds eller Forsvarsministeriets forventning, at den foreslåede § 6 vil indebære, at der skal ske sikkerhedsgodkendelse af flere af teleudbydernes medarbejdere, end det er tilfældet efter gældende ret.

Tværtimod fremgår det af bemærkningerne til § 6, at der i modsætning til den hidtil gældende ordning ikke skal 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.

9. Adgang uden retskendelse

Advokatrådet finder, at bestemmelser som lovforslagets § 9, stk. 6 og 7, bør have undtagelsens karakter, da bestemmelserne udgør en undtagelse til grundlovens udgangspunkt om boligens ukrænkelighed. Advokatrådet har noteret, at tilsynsbesøg ikke sker uvarslet og alene vil blive anvendt, såfremt et tilsvarende resultat ikke kan opnås ved anvendelsen af andre og mindre indgribende tilsynsmuligheder. Det er imidlertid Advokatrådets erfaring, at de mest vidtgående tilsynsbeføjelser ofte ender med at blive udgangspunktet i stedet for undtagelsen, hvorfor Advokatrådet finder, at man bør være yderst tilbageholdende med at indføre ordninger som den foreslåede.

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S anfører, at lovforslagets § 9, stk. 6 og 7, hvorefter Center for Cybersikkerhed får adgang uden retskendelse til forretningslokaler hos udbyderne og deres samarbejdspartnere, er en væsentligt indgribende foranstaltning, som bør anvendes med forsigtighed.

Hi3G Denmark ApS anfører, at Center for Cybersikkerhed ikke skal have adgang til udbydernes lokaler uden retskendelse, idet det er et grundlæggende krav i retsplejeloven, som ikke bør tilsidesættes med lovforslaget. Hi3G Denmark ApS bemærker endvidere, at Center for Cybersikkerhed vil få adgang til oplysninger, der ikke må udleveres efter retsplejelovens bestemmelser.

IT-Politisk Forening noterer med tilfredshed, at det af lovforslagets § 9, stk. 6 og 7, nu fremgår, at Center for Cybersikkerhed i forbindelse med adgang til forretningslokalerne ikke kan tilgå kommunikation til, fra og mellem udbydernes kunder. Foreningen antager endvidere, at begrebet kommunikation omfatter såvel indholdet af kommunikationen som såkaldt metadata eller trafikdata og opfordrer til, at begrebet bliver præciseret i lovforslagets bemærkninger.

Justitia anser det for positivt, at det eksplicit fremgår af lovforslaget, at Center for Cybersikkerhed ikke kan indhente oplysninger om udbydernes kunder i forbindelse med centerets adgang til udbyders forretningslokaler. Justitia finder det imidlertid betænke-

ligt, at der ikke stilles krav om retskendelse. Justitia anser dog notifikationskravet i lovforslaget som en forbedring i forhold til andre lignende hjemmelsbestemmelser og anbefaler, at tilsvarende krav stilles på andre områder, hvor myndighederne har adgang til borgeres eller virksomheders bolig eller forretningslokaler uden retskendelse.

Rådet for Digital Sikkerhed vurderer, at nødvendighedskravet i forhold til lovforslagets § 9, stk. 6 og 7, om adgang uden retskendelse bør kvalificeres i lovteksten, således at det klart fremgår, hvilke kriterier der skal være opfyldt, førend kontrolbesøg kan gennemføres.

For at kunne konstatere, om teleudbyderne i praksis har gennemført de nødvendige foranstaltninger til at sikre teleinfrastrukturen, anser Forsvarsministeriet det for 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.

Det følger imidlertid af lovforslaget, at en sådan adgang kun vil ske efter et varsel på mindst syv arbejdsdage. Adgang uden retskendelse vil desuden kun kunne ske, hvis det er nødvendigt af hensyn til informationssikkerheden. Det fremgår endvidere af lovforslagets afsnit 3.4.3, at det forudsættes, at muligheden kun anvendes, såfremt et tilsvarende resultat ikke kan opnås ved anvendelse af andre og mindre indgribende tilsynsmuligheder.

Som det udtrykkeligt fremgår af lovforslagets § 9, stk. 6 og 7, kan Center for Cybersikkerhed ikke i forbindelse med adgang til forretningslokaler tilgå kommunikation til, fra eller mellem udbyderens kunder. Dette omfatter såvel indholdet af kommunikationen som såkaldt metadata eller trafikdata (f.eks. telefonnumre og IP-adresser).

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S anfører, at de danske udbydere ikke kan indestå for, at Center for Cybersikkerhed kan få adgang til forretningslokaler hos udbydernes samarbejdspartnere, leverandører eller underleverandører efter lovforslagets § 9, stk. 7.

Forsvarsministeriet kan bekræfte, at den foreslåede § 9, stk. 7, om adgang til forretningslokaler hos udbyderes samarbejdspartnere, leverandører eller underleverandører er rettet mod de pågældende parter, og således ikke indebærer en forpligtelse for teleudbyderne selv.

10. Offentliggørelse af afgørelser m.v.

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S finder det ikke proportionalt, at der indføres en bestemmelse i § 10, hvorefter Center for Cybersikkerhed kan offentliggøre centerets afgørelser, påbud, resultater af tilsyn mv. Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S fremhæver i den forbindelse, at sikkerhedstruslerne er i konstant forandring, og at sikkerhedsforanstaltninger, der er gældende i dag, ikke altid vil være til-

strækkelige på et senere tidspunkt, hvorfor det altid vil være forbundet med en betydelig grad af usikkerhed, om en given sikkerhedsforanstaltning har været tilstrækkelig.

Offentliggørelse af kontrolresultater efter den foreslåede § 10 vil altid ske efter en konkret vurdering hos Center for Cybersikkerhed. I vurderingen vil bl.a. indgå proportionalitetshensyn og hensyn til, om teleudbyderen uopfordret har oplyst om f.eks. et brud på informationssikkerheden.

Som anført i afsnit 2 i bemærkningerne til lovforslaget er der 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. I overensstemmelse hermed forudsættes det, at ændringer i trusselsbilledet i første omgang fører til en dialog mellem Center for Cybersikkerhed og den enkelte teleudbyder frem for, at der træffes afgørelse om manglende overholdelse af bestemmelserne om informationssikkerhed.

Hi3G Denmark ApS anfører, at der bør indsættes et krav om, at udbyderne skal godkende materiale, der påtænkes offentliggjort, og at forretningshemmeligheder skal kunne undtages fra offentliggørelse.

Det er Forsvarsministeriets opfattelse, at en model, hvor den enkelte teleudbyder skal godkende offentliggørelse af tilsynsresultater m.v., vil medføre, at udbyderne ikke som ellers forudsat får et øget incitament til overholdelse af kravene til informationssikkerhed og beredskab, ligesom bestemmelsen i så fald ikke vil give telekunder mulighed for at vurdere, i hvilket omfang de enkelte udbydere har levet op til lovgivningens krav.

Som det fremgår af den foreslåede § 10, stk. 2, nr. 1, må offentliggørelse ikke indeholde 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.

11. Informationsdeling

IT-Politisk Forening anfører, at der bør være vandtætte skotter mellem Center for Cybersikkerhed og den øvrige del af Forsvarets Efterretningstjeneste for så vidt angår viden om konkrete sårbarheder i teleinfrastrukturen, som centeret erfarer i forbindelse med dets tilsynsopgaver over for danske teleudbydere.

Rådet for Digital Sikkerhed bemærker, at forpligtelsen til at videregive oplysninger til Center for Cybersikkerhed om outsourcet drift, herunder driftens tilrettelæggelse, styring og risikohåndtering, kan få betydning for udbydernes konkurrencemæssige stilling på markedet. Rådet finder, at problematikken understreges af, at centeret er placeret under Forsvarets Efterretningstjeneste. Rådet antager i den forbindelse, at centeret ikke vil kunne orientere udbyderne om, hvad deres oplysninger bliver anvendt til, herunder hvem de videregives til som led i samarbejde med andre efterretningstjenester.

Formålet med lovforslaget er at fremme net- og informationssikkerheden i samfundet. Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste varetager myndighedsopgaverne inden for informationssikkerhed og beredskab på teleområdet.

De oplysninger – herunder oplysninger om sårbarheder i teleinfrastrukturen – som Center for Cybersikkerhed kommer i besiddelse af som led i centerets virke som myndighed for informationssikkerhed og beredskab på teleområdet, vil alene kunne anvendes af centeret som led i dette virke.

Oplysninger, som Center for Cybersikkerhed modtager fra teleudbyderne, vil skulle behandles i overensstemmelse med dels lovforslagets bestemmelser, dels lov om Center for Cybersikkerhed. Centeret er i øvrigt underlagt restriktive sikkerhedsbestemmelser om fysisk sikkerhed, personelsikkerhed og it-sikkerhed. Alle medarbejdere i Center for Cybersikkerhed er sikkerhedsgodkendt til klassifikationsgraden HEMMELIGT eller derover, og alle medarbejdere har tavshedspligt i henhold til straffeloven.

12. Administrative og økonomiske konsekvenser for erhvervslivet m.v.

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S finder, at lovforslagets vurdering af de økonomiske byrder for erhvervslivet mv. ses at være nedtonet til et urealistisk niveau.

Som anført i lovforslagets afsnit 5 vil de økonomiske og administrative konsekvenser 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 og administrative konsekvenser for udbyderne.

Teleindustrien, IT-Branchen, DI ITEK og Stofa A/S anfører, at branchen deler Forsvarsministeriets interesse i at optimere sikkerheden i selskabernes netværk, ligesom det påpeges, at udbyderne ikke har en kommerciel interesse i at gå på kompromis med sikkerheden. På den baggrund må det antages, at en stor del af de krav til informationssikkerhed og beredskab, som følger af lovforslaget, enten allerede er gennemført hos hovedparten af udbyderne eller under alle omstændigheder ville blive gennemført af disse udbydere på eget initiativ.

Det bemærkes i øvrigt, at de bekendtgørelser, der skal udmønte bemyndigelserne i lovforslaget, vil blive udarbejdet under inddragelse af telebranchen og med fokus på at sikre en hensigtsmæssig balance mellem på den ene side de økonomiske og administrative byrder, som reguleringen kan medføre, og på den anden side hensynet til informationssikkerheden.

Dansk Energi, Nianet A/S og Stofa A/S anfører, at der skal tages hensyn til forholdsmæssighed og proportionalitet i forbindelse med Center for Cybersikkerheds udmøntning af bestemmelserne i lovforslaget samt tilrettelæggelsen af centerets tilsynsvirk-

somhed, da det vil blive langt mere byrdefuldt for mindre teleudbydere at efterleve lovforslaget, hvis alle udbydere pålægges samme krav og foranstaltninger.

Ved udmøntningen af de overordnede krav til informationssikkerhed, der foreslås indført med net- og informationssikkerhedsloven, vil der være betydelig fokus på at sikre, at de mere detaljerede regler, der fastsættes i bekendtgørelser, bliver proportionale, samt at der tages hensyn til, at såvel trusselsbillede som risikoen på informationssikkerhedsområdet er forskellige alt efter teleudbydernes størrelse. Ligeledes vil Center for Cybersikkerhed ved den løbende administration af reglerne have fokus på en differentieret tilgang, hvor f.eks. tilsynsvirksomheden er risikobaseret og baseret på en vurdering af den samlede samfundsmæssige effekt af tilsynsaktiviteterne.

Danske Regioner anfører, at den foreliggende konsekvensberegning af lovforslagets økonomiske og administrative konsekvenser for stat, regioner og kommuner er utilstrækkelig, idet der eksempelvis på hospitaler er offentligt tilgængelige net for pårørende og patienter, og at udbyderne af disse net derfor vil være omfattet af lovforslaget.

Forsvarsministeriet kan bekræfte, at i det omfang regioner udbyder net og tjenester, vil de krav, der efter lovforslaget stilles til udbydere, også omfatte regionerne. Det vil kunne medføre økonomiske og administrative konsekvenser for regionerne i samme omfang som for private udbydere.

Dette er afspejlet i lovforslagets afsnit 4 om økonomiske og administrative konsekvenser for stat, kommuner og regioner.

13. Høringsfrist

Advokatrådet bemærker, at høringsmaterialet er fremsendt med en frist på 13 dage, hvorfor det må påregnes, at en række myndigheder og organisationer reelt ikke har haft mulighed for at udfylde den rolle som høringspart, som forudsættes i en almindelig demokratisk proces.

Lovforslaget har været sendt i høring med en frist på 13 dage. Denne frist, der er kortere end det normale udgangspunkt på fire uger, skal imidlertid ses i lyset af, at der i forbindelse med udarbejdelsen af lovforslaget har været en dialog med store dele af telebranchen, som lovforslaget retter sig mod. Under den dialog har telebranchen fremsat en række bemærkninger, som det i stort omfang har været muligt at imødekomme.