FORSVARSMINISTERIET

KOMMENTERET HØRINGSOVERSIGT
vedrørende
forslag til lov om ændring af lov om net- og informationssikkerhed
(Implementering af direktivet om oprettelse af en europæisk kodeks for elektronisk kommunikation for så vidt angår sikkerhed i net og tjenester)

Dato: 30. september 2020

Enhed: JSN
Sagsnr.: 2020/004886
Dok.nr.: 138990
Bilag: Ingen

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Et udkast til forslag til lov om ændring af lov om net- og informationssikkerhed (Implementering af direktivet om oprettelse af en europæisk kodeks for elektronisk kommunikation for så vidt angår sikkerhed i net og tjenester) har i perioden fra den 30. juli 2020 til den 27. august 2020 været sendt i høring hos følgende myndigheder og organisationer m.v.:

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

Forsvarsministeriet har modtaget høringssvar fra:

Advokatrådet, Borch Teknik A/S, Datatilsynet, DI Digital, Huawei, Institut for Menneskerettigheder, Præsidenten for Københavns Byret, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Region Nordjylland, Region Sjælland, Region Syddanmark, Rigsrevisionen og Teleindustrien(TI) og IT-Branchen (i fællesskab).

Nedenfor er gengivet de væsentligste punkter i de modtagne høringssvar. Forsvarsministeriets kommentarer til høringssvarene er angivet i kursiv.

Det bemærkes, at visse af høringsparterne i forlængelse af bemærkningerne til nærværende lovforslag også har afgivet bemærkninger til Forsvarsministeriets samtidige høring over udkast til lovforslag om ændring af lov om elektroniske kommunikationsnet og -tjenester vedrørende etablering af et mobilbaseret varslingssystem. Bemærkninger til dette lovforslag fremgår af den separate høringsoversigt herom.

1. Generelt

Advokatrådet har oplyst, at man har besluttet ikke at afgive høringssvar.

Borch Teknik A/S og Institut for Menneskerettigheder har ikke bemærkninger til lovforslaget.

Præsidenterne for henholdsvis Vestre Landsret og Østre Landsret har ikke ønsket at udtale sig om lovforslaget. Præsidenten for Københavns Byret har på byretspræsidenternes vegne oplyst, at byretterne ikke ønsker at udtale sig om lovforslaget.

Rigsrevisionen konstaterer, at lovforslaget ikke omhandler revisions- eller regnskabsforhold i staten eller andre offentlige virksomheder, der revideres af Rigsrevisionen, og Rigsrevisionen har derfor ikke behandlet henvendelsen yderligere.

TI og IT-Branchen kvitterer positivt for, at udbydere af nummeruafhængige interpersonelle kommunikationstjenester til forskel fra tidligere nu bliver genstand for en række forpligtelser i relation til sikkerheden i sådanne tjenester. TI og IT-Branchen finder det væsentligt at sikre en "level playing field" blandt elektroniske kommunikationstjenester, der i stigende grad konkurrerer mod hinanden.

2. EU-implementering

DI Digital støtter en direktivnær implementering og noterer sig, at princippet er indskrevet i de almindelige bemærkninger. DI er dog i tvivl om, hvorvidt dette også praktiseres i de enkelte formuleringer.

Huawei opfordrer til, at implementeringen af EU's teledirektiv gennemføres så tekstnært som muligt.

Teleindustrien og IT-Branchen kvitterer positivt for det, der betegnes som en relativt tekstnær direktivimplementering.

Forsvarsministeriet har ved udarbejdelsen af lovforslaget lagt vægt på, at implementeringen af EU's telekodeks på Forsvarsministeriets område sker i overensstemmelse med regeringens principper for implementering af erhvervsrettet EU-regulering, hvorefter den nationale regulering som udgangspunkt ikke bør gå videre end minimumskravene i EU-reguleringen. Forsvarsministeriet har derfor tilstræbt i videst muligt omfang at implementere direktivets krav tekstnært. Det bemærkes dog også, at direktivets krav er rammebestemmelser, som er forudsat nærmere udmøntet af medlemsstaterne.

3. Definitioner og terminologi

TI og IT-Branchen kvitterer for, at der med ændringen søges en ensretning af definitionerne med de tilsvarende definitioner i teleloven. TI og IT-Branchen anfører dog, at der i enkelte af definitionerne lægges op til visse nuanceforskelle i ordvalget og opfordrer til, at definitionerne affattes fuldstændig ordret i forhold til de tilsvarende definitioner i teleloven, så fortolkningstvivl undgås.

Net- og informationssikkerhedsloven bygger på en række begreber og definitioner, der stammer fra teleloven. Lovens terminologi er målrettet lovens særlige formål og sigte, men det fremgår af bemærkningerne til de enkelte definitioner, at disse skal fortolkes i overensstemmelse med de tilsvarende definitioner i teleloven og disses forarbejder og relevante praksis.

Med nærværende lovforslag tilnærmes terminologien – som høringsparterne også anfører – yderligere den, som anvendes i teleloven. Sammenholdt med høringsversionen af lovforslaget vil Forsvarsministeriet dog ændre definitionen af et "elektronisk kommunikationsnet" i overensstemmelse med et lovforslag fra Klima-, Energi- og Forsyningsministeriet, hvor det tilsvarende begreb i teleloven foreslås ændret.

3.1. Lovens titel

TI og IT-Branchen har forståelse for den foreslåede ændring af lovens titel, der er en konsekvens af en tilsvarende begrebsændring i teledirektivet. TI og IT-Branchen finder dog, at begreberne "net og tjenester" ikke bør anvendes i lovens titel og opfordrer i stedet til at anvende telelovens begreber "elektroniske kommunikationsnet og -tjenester". TI og IT-Branchen opfordrer også mere generelt til at anvende "elektroniske kommunikationsnet og -tjenester" konsekvent gennem hele loven i stedet for "net og tjenester", herunder eksempelvis i ændringen af § 2, stk. 1, nr. 8, om "sikkerhed i net og tjenester". TI og IT-Branchen kan i øvrigt ikke se en konkret begrundelse for æn-

dringen til det meget generelle begreb "sikkerhed" og finder, at "informationssikkerhed" er et bredere begreb.

Med lovforslaget foreslås lovens titel ændret fra "lov om net- og informationssikkerhed" til "lov om sikkerhed i net og tjenester". Det skyldes, at EU's telekodeks generelt anvender begrebet "sikkerhed i net og tjenester", som er nærmere defineret i direktivets artikel 2, nr. 21. Det vurderes ikke at være retvisende at anvende begrebet "elektroniske kommunikationsnet og -tjenester" i stedet for "net og tjenester" alle steder i loven, herunder i lovens titel, da det i givet fald ikke vil omfatte de nye NUIK-tjenester, som med lovforslaget bliver omfattet af loven.

3.2. Offentligt tilgængelige elektroniske kommunikationsnet og -tjenester

Region Nordjylland finder definitionen af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester meget bred og vurderer, at den kan omfatte alle borgerrettede løsninger, som regionerne måtte udvikle og/eller stille til rådighed for borgerne.

Der foretages med lovforslaget kun visse sproglige justeringer af definitionen af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester, der således ikke ændres indholdsmæssigt. Definitionen svarer som hidtil til telelovens definitioner af såvel offentlige elektroniske kommunikationsnet som offentlig elektronisk kommunikationstjeneste.

3.3. Udbydere af NUIK-tjenester

Region Syddanmark finder det ikke helt klart, hvilke udbydere eller hvilken type kommunikationsform, der er tænkt på.

Region Nordjylland finder, at lovforslaget skaber forvirring om omfattelsesniveauet, og at det er svært som aktør at vide, hvad man bliver omfattet af, både i umiddelbar, men også i fjernere fremtid. Regionen finder endvidere, at formuleringen "som normalt ydes mod betaling" giver anledning til usikkerhed i forhold til, hvilke borgerrettede løsninger der måtte være omfattet.

TI og IT-Branchen kvitterer positivt for den foreslåede definition, men finder, at definitionen bør være identisk med den definition, som ved et samtidigt lovforslag foreslås indsat som telelovens § 2, nr. 20, hvilket også ifølge lovforslagets bemærkninger er hensigten. TI og IT-Branchen foreslår, at der henvises til definitionen i teleloven og opfordrer i øvrigt til, at begrebet ikke forkortes. TI og IT-Branchen finder endvidere, at udbydere af nummeruafhængige interpersonelle kommu-

nikationstjenester, der opretter forbindelse til offentligt tildelte nummerressourcer, tillige bør være omfattet af definitionen. Sådanne tjenester er allerede omfattet af definitionen af en elektronisk kommunikationstjeneste, jf. teleloven. TI og IT-Branchen finder det desuden uklart, hvorvidt flere af branchens value-added tjenester vil blive omfattet af definitionen, herunder eksempelvis interaktive TV-produkter eller e-mailtjenester tilknyttet slutbrugeres bredbåndsabonnement. TI og IT-Branchen opfordrer desuden til, at det præciseres, hvad der menes med "som normalt ydes mod betaling".

Med lovforslaget bliver udbydere af nummeruafhængige interpersonelle kommunikationstjenester (udbydere af NUIK-tjenester) som noget nyt omfattet af reguleringen vedrørende sikkerhed i net og tjenester. Definitionen af en NUIK-tjeneste svarer indholdsmæssigt til den tilsvarende definition, der ved et samtidigt lovforslag fra Klima-, Energi- og Forsyningsministeriet foreslås indsat i teleloven. I lovforslagets øvrige bestemmelser anvendes det forkortede begreb "udbyder af NUIK-tjenester" ud fra et hensyn til læsbarheden af de enkelte bestemmelser i loven.

Lovforslagets definition af udbydere af nummeruafhængige interpersonelle kommunikationstjenester skal fortolkes i overensstemmelse med forarbejderne til den foreslåede bestemmelse i teleloven, og der henvises på den baggrund nærmere til Klima-, Energi- og Forsyningsministeriets samtidige lovforslag om ændring af teleloven og forarbejderne hertil.

For så vidt angår formuleringen "som normalt ydes mod betaling" henvises endvidere til betragtning 16 til EU's telekodeks, hvoraf det bl.a. fremgår, at i den digitale økonomi anser markedsdeltagerne i stigende grad oplysninger om brugerne for at have monetær værdi. Elektroniske kommunikationstjenester udbydes ofte til slutbrugeren, ikke kun mod penge, men i stigende grad og navnlig mod afgivelse af personoplysninger eller andre oplysninger. Begrebet betaling bør derfor også omfatte situationer, hvor slutbrugeren udsættes for reklamer som betingelse for at få adgang til en tjeneste, og situationer hvor tjenesteudbyderen omsætter personoplysninger, som vedkommende har indsamlet, i penge i overensstemmelse med forordning (EU) 2016/679.

3.4. Sikkerhed i net og tjenester

Region Syddanmark anfører, at med definitionen af sikkerhed i net og tjenester udvides sikkerhedsområdet til – ud over tilgængelighed, fortrolighed og integritet – også at omfatte autenticitet. Regionen finder, at der kunne være god mening i, at teleudbydere skal stille infrastruktur til rådighed, der generelt på nettet kan verificere brugeres autenti-

citet. Det vil dog være en meget stor ændring i forhold til, hvordan internettet fungerer i dag, idet der vil være store krav til håndtering af privatlivets fred og fortrolighed, herunder fortrolighed i forhold til brevhemmeligheden.

TI og IT-Branchen vurderer, at ændringen vil medføre, at teleoperatører i fremtiden eksempelvis skal rapportere til myndighederne, hvis data og informationssystemer mv. ikke er, hvad de foregiver at være, hvilket organisationerne finder rimeligt.

Med lovforslaget defineres sikkerhed i net og tjenester som net og tjenesters evne til på et givet fortrolighedsniveau at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af disse net og tjenester, lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net eller tjenester.

Det indebærer, at sikkerhedskravene i loven fremadrettet også vil omfatte sikring af, at data og informationssystemer mv. er, hvad de foregiver at være, forstået som sikring af data og informationssystemers ægthed eller originalitet. Ligeledes vil lovens underretningsforpligtelser også kunne angå tilfælde, hvor ægtheden eller originaliteten af data og informationssystemer mv. er påvirket eller risikerer at blive det.

Autenticiteten af net og tjenester vedrører således ikke verificering af brugeres autenticitet.

3.5. Sikkerhedshændelse

TI og IT-Branchen støtter den foreslåede definition og støtter desuden, at der ikke fokuseres på en potentiel, men en faktisk indvirkning på sikkerheden. TI og IT-Branchen gør opmærksom på, at graden af den faktiske negative påvirkning ikke kendes umiddelbart ved sikkerhedshændelsens begyndelse.

4. Bemyndigelser

DI Digital finder, at lovforslaget indeholder meget brede hjemler til senere at fastlægge krav i bekendtgørelser. Såfremt myndighederne ikke er parat til i loven at formulere kravene præcist allerede nu, ønsker branchen ifølge DI Digital som minimum en afgrænsning af hjemlerne, så alle kan se, hvilke grænser der gælder for de kommende bekendtgørelser.

Huawei finder, at væsentlige lovgivningsmæssige indgreb ikke bør implementeres ved sekundær lovgivning i form af bekendtgørelser, da

bekendtgørelser ikke er underlagt den samme parlamentariske proces som behandling af lovforslag i Folketinget med tilhørende offentlig høring. Huawei finder endvidere, at lovgivning via bekendtgørelser udgør en udfordring for den generelle regulatoriske transparens og gennemskuelighed, da det er svært at overskue reguleringen i en samling af sideordnede og delvist overlappende bekendtgørelser, der er forankret i generelle mandater i den overordnede lovgivning. Huawei oplyser, at virksomheden nøje følger implementeringen af EU's telekodeks i hele EU og kan konstatere, at størstedelen af medlemsstaterne har valgt at implementere direktivet direkte ved lov. Huawei opfordrer til, at relaterede bekendtgørelser udstedes hurtigst muligt og senest den 21. december 2020.

Region Nordjylland ønsker teksten i lovforslaget præciseret, således at relevante aktører ikke kan være i tvivl om omfatningsgraden af lovforslaget, da der ikke er nogen bekendtgørelser eller cirkulærer til at understøtte definitionerne i lovforslaget.

Lov om net- og informationssikkerhed er en rammelov, der i dag er udmøntet i fire bekendtgørelser. Af de fire bekendtgørelser indeholder to bekendtgørelser bestemmelser, der implementerer rammedirektivet og forsyningspligtdirektivet, der nu erstattes af EU's telekodeks. Det drejer sig om bekendtgørelse nr. 567 af 1. juni 2016 om informationssikkerhed og beredskab i net og tjenester og bekendtgørelse nr. 1256 af 27. november 2019 om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed.

Med lovforslaget justeres på baggrund af EU's telekodeks visse af de eksisterende rammer i loven, ligesom der tilføjes enkelte nye forpligtelser, som Center for Cybersikkerhed bemyndiges til at udmønte nærmere. Lovforslaget viderefører således den nuværende lovs grundlæggende struktur som rammelov. Det giver mulighed for, at de nærmere krav kan tilpasses udviklingen i teknologi, best practices og trusselsbilledet. Samtidig – og i denne sammenhæng mere afgørende – giver strukturen den bedste mulighed for at tage højde for anbefalinger fra EU's Agentur for Cybersikkerhed (ENISA), der bl.a. har til opgave at fremme medlemsstaternes samordning på området. Det forventes, at ENISA vil udgive anbefalinger vedrørende bl.a. sikkerhedskrav og underretningspligter i EU's telekodeks i slutningen af 2020.

De bekendtgørelser, der skal udmønte lovforslaget, vil i overensstemmelse med direktivets implementeringsfrist skulle udstedes med henblik på ikrafttrædelse den 21. december 2020.

5. Forvaltningsretlige principper samt behandling af personoplysninger

Datatilsynet forudsætter, at enhver eventuel behandling af personoplysninger foranlediget af udkastet til lovforslag sker under iagttagelse af reglerne i databeskyttelsesforordningen og databeskyttelsesloven.

Huawei opfordrer til, at der gives klar mulighed for at påklage CFCS' afgørelser efter de nye regler til en højere instans, og at der generelt sikres transparens i CFCS' afgørelser.

Det bemærkes, at databeskyttelsesforordningen ikke finder anvendelse for Center for Cybersikkerhed, idet forordningen ikke gælder for behandling af personoplysninger under udøvelse af aktiviteter, der falder uden for EU-retten, jf. forordningens artikel 2, stk. 2, litra a. Dette følger også af § 3, stk. 2, i lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven), som fastslår, at loven og databeskyttelsesforordningen ikke finder anvendelse på den behandling af personoplysninger, som udføres for eller af politiets og forsvarets efterretningstjenester.

Center for Cybersikkerheds behandling af personoplysninger er i stedet reguleret i lov om Center for Cybersikkerhed (CFCS-loven), jf. lovbekendtgørelse nr. 836 af 7. august 2019. I medfør af CFCS-loven gælder en række centrale persondataretlige principper for Center for Cybersikkerheds behandling af personoplysninger, ligesom der er fastsat særlige, skærpede regler for analyse, videregivelse og sletning af bestemte kategorier af oplysninger, inklusiv personoplysninger.

Center for Cybersikkerheds afgørelser i medfør af net- og informationssikkerhedsloven kan påklages som led i almindelig administrativ rekurs. Det ændrer lovforslaget ikke ved. Lovforslaget ændrer endvidere ikke på, at Center for Cybersikkerhed i medfør af CFCS-loven i alle afgørelsessager konkret skal vurdere, om det er muligt at anvende forvaltningslovens principper om partens aktindsigt, partshøring og begrundelse mv.

6. Minimumskrav til sikkerhed i net og tjenester samt anvendelse af internationale standarder

DI Digital opfordrer til, at lovforslaget henviser til, at minimumskrav i videst muligt omfang skal basere sig på internationale standarder. Herved vil implementeringen også være mere direktivnær. DI Digital henviser til, at det fremgår af direktivets artikel 40, at procedurer og stan-

darder skal lægge sig op ad internationale standarder. Samtidig bør den brede hjemmel afgrænses, så det fremgår, at der vil blive taget højde for, at indgrebet skal være mindst muligt indgribende.

Huawei henviser til, at det fremgår af artikel 40, stk. 1, i EU's telekodeks, at en medlemsstat skal træffe "[…] passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for på passende vis at styre risiciene for sikkerheden i net og tjenester". Direktivets artikel 40, stk. 5, uddyber henvisningen til tekniske og organisatoriske foranstaltninger ved at specificere, at udgangspunktet for sådanne foranstaltninger "[…] i videst muligt omfang baseres på europæiske og internationale standarder". Huawei anfører, at virksomheden er overbevist om, at eventuelle risici adresseres bedst muligt ved at fastsætte kriterier, som er målbare og verificerbare. Huawei opfordrer derfor til at tage europæiske og internationale standarder for sikkerhed i 5G i betragtning ved udformning af lovgivningen, herunder lave specifikke henvisninger til standarder såsom Network Equipment Security Assurance Scheme og Security Assurance Specifications. Dermed sikres stabile rammer for en ensartet og skræddersyet tilgang til sikkerhedsrevisioner samtidig med, at strenge sikkerhedsstandarder afkræver et højt niveau af engagement fra operatører og leverandører. Huawei henleder opmærksomheden på, at trusselsbilledet er i konstant forandring, og at en etablering af eller henvisning til "god skik" eller "internationale standarder eller krav" vil hjælpe leverandører med at overholde kravet om at kunne identificere "betydelige trusler". ENISA opfordrer ligeledes til brugen af en god skik-standard i identificeringen af trusler.

TI og IT-Branchen finder det rimeligt, at der stilles krav til kryptering både på teleoperatørniveau og blandt nye typer af tjenesteudbydere. TI og IT-Branchen anmoder dog om særlig forsigtighed og proportionalitet i overvejelserne herom, da vidtgående (system)krav kan udgøre væsentlige ekstraomkostninger for udbyderne. TI og IT-Branchen gør opmærksom på, at fremtidens mobile teknologier, herunder 5G, har kryptering af data mellem mobilnetværkets radio access netværk og mobil core-systemet indbygget som standard. TI og IT-Branchen oplyser i øvrigt, at kryptering allerede er fuldt implementeret i risikostyringen for danske teleudbydere, men har ikke kendskab til, hvorledes kryptering anvendes for udbydere af NUIK-tjenester.

Region Nordjylland finder, at der mangler informationer om, hvilke minimumskrav til sikkerhed, der vil blive fastlagt af CFCS, og at der er tale om en carte blanche til CFCS om, hvilke krav der vil blive stillet.

Lov om net- og informationssikkerhed har siden lovens ikrafttrædelse i 2015 indeholdt en bemyndigelse i lovens § 3, stk. 1, til at Center for Cybersikkerhed inden for nærmere rammer kan fastsætte minimums-

krav til informationssikkerhed i net og tjenester. Bemyndigelsen er udmøntet i bekendtgørelse nr. 567 af 1. juni 2016 om informationssikkerhed og beredskab i net og tjenester, og kravene er således velkendte for de danske teleudbydere, som er omfattet af loven i dag.

Med lovforslaget vil lovens § 3, stk. 1 – ligesom en række andre bestemmelser – fremadrettet også gælde for udbydere af NUIK-tjenester. Derudover videreføres bestemmelsen med visse sproglige justeringer som konsekvens af ændringer af lovens terminologi.

Det fremgår af bemærkningerne til den foreslåede bestemmelse, at den nærmere udmøntning forudsættes at ske under hensyntagen til de relevante fortolkningsbidrag i EU's telekodeks. Det drejer sig navnlig om betragtning 94, hvoraf det bl.a. følger, at de sikkerhedsforanstaltninger, som udbyderne forpligtes til at træffe, bør tage hensyn til overholdelse af internationale standarder, samt artikel 40, stk. 1, om, at det kan være relevant at anvende kryptering som foranstaltning til at forhindre og minimere virkningen af sikkerhedshændelser. Det konstateres i den forbindelse i bemærkningerne til bestemmelsen, at der i vidt omfang er tale om foranstaltninger, som allerede i dag er omfattet af bemyndigelsen i § 3, stk. 1.

Det bemærkes i øvrigt, at det ikke med bestemmelsen er hensigten, at der skal stilles teknologispecifikke (system)krav til kryptering.

Forsvarsministeriet finder det ikke på nuværende tidspunkt proportionalt at pålægge udbydere at anvende bestemte standarder. Der findes således forskellige anerkendte internationale standarder, og det vil kunne være ganske byrdefuldt for en virksomhed – der eventuelt er en del af en større, international koncern – at blive pålagt at anvende en bestemt standard fastlagt af myndighederne, herunder skifte fra én standard (som er fælles for koncernen) til en anden.

7. Påbud om konkrete foranstaltninger

DI Digital, Huawei, Region Nordjylland, Region Sjælland, Region Syddanmark samt TI og IT-Branchen finder, at den foreslåede § 3, stk. 3, er for bredt formuleret. Høringsparterne opfordrer til, at det nærmere defineres, hvornår der er tale om en "betydelig trussel", og at det afgrænses nærmere, hvilke konkrete foranstaltninger der kan påbydes med hjemmel i bestemmelsen, herunder de nærmere regler, der vil blive udstedt af CFCS.

DI Digital påpeger i den forbindelse, at påbudsmuligheden i sig selv er et stort indgreb i virksomhedernes ret til selv at imødegå trusler, og at krav fra CFCS kan være omkostningstunge og indgribende. DI Digital

opfordrer til, at man enten bliver meget mere klar på, hvad man vil stille af materielle krav, eller at man alternativt fastsætter, at CFCS skal tage vidtgående hensyn til proportionalitetsprincippet og således stille krav om mindst mulige indgribende foranstaltninger.

Huawei finder, at der som minimum bør fastsættes en tærskel for, hvornår en trussel kan kvalificeres som "betydelig", inden den resulterer i et påbud fra CFCS.

Region Sjælland anfører, at regionen er stærkt bekymret for, om lovforslaget giver CFCS hjemmel til beføjelser og mandater, der i sidste ende kan føre til indgriben i regionernes selvstændige myndighedsudøvelse samt registreredes og borgernes rettigheder. Det er Region Sjællands opfattelse, at CFCS med lovforslaget vil få mulighed for, ved identifikation af en betydelig trussel, at prioritere handlinger i regionernes it-infrastruktur uden involvering af regionale prioriteringer, kompetencer og indsigt. Det er ifølge regionen problematisk, hvis lovforslaget giver hjemmel til, at cybersikkerhed fra centralt hold kan prioriteres over patientsikkerheden. Region Sjælland finder det desuden bekymrende, at der lægges op til, at påbud skal ske uden retskendelse.

Region Nordjylland og Region Sjælland ser behov for at præcisere, hvorledes et påbud tænkes ophævet, når trusselsbilledet ændrer sig.

TI og IT-Branchen finder, at domstolene bør afsige kendelse om påbuddet, hvis foranstaltningerne indebærer begrænsninger i grundlæggende rettigheder. TI og IT-Branchen er bekymrede over det upræcise omfang af bestemmelsen og finder, at CFCS tillægges en næsten ubegrænset mulighed for at kræve, at konkrete udbydere foretager potentielt særdeles indgribende og omkostningstunge foranstaltninger.

Der foretages med bestemmelsen, som foreslås indsat som lovens § 3, stk. 3, en direktivnær implementering af artikel 41, stk. 1, i EU's telekodeks. Ordlyden af bestemmelsen er således formuleret meget tæt op ad direktivets krav. Det er beskrevet nærmere i bemærkningerne til bestemmelsen, hvordan den forudsættes udmøntet.

En indskrænkning af bestemmelsens rammer vil således indebære en risiko for, at direktivet ikke implementeres korrekt og tilstrækkeligt. Forsvarsministeriet har dog på baggrund af høringssvarene tilføjet i bemærkningerne til bestemmelsen, at det forudsættes, at de konkrete foranstaltninger, som Center for Cybersikkerhed kan påbyde i medfør af de nærmere regler, der udstedes herom, i videst muligt omfang vil være baseret på anerkendte internationale standarder eller tilsvarende.

Det bemærkes endvidere, at påbud fra Center for Cybersikkerhed under alle omstændigheder vil skulle være proportionale, og at påbud kun kan opretholdes, så længe grundlaget for påbuddet fortsat er til stede.

Der vil ikke med den foreslåede bestemmelse være hjemmel til at gøre indgreb i grundlæggende rettigheder i grundlovens forstand, og det ville dermed være en markant nyskabelse, såfremt påbudsmuligheden blev underlagt et krav om retskendelse. Det er således heller ikke tilfældet, når myndighederne på eksempelvis fødevareområdet eller arbejdsmiljøområdet giver påbud efter den relevante lovgivning om at bringe forhold i orden. Der er med den foreslåede bestemmelse alene tale om, at Center for Cybersikkerhed kan påbyde en udbyder at tage de nødvendige skridt til at håndtere en sikkerhedshændelse eller en betydelig trussel om en sikkerhedshændelse – hvilket udbyderen i forvejen har pligt til – såfremt udbyderen ikke gør dette i rette tid og af egen drift.

8. Underretning om sikkerhedshændelser

TI og IT-Branchen finder det relevant, at udbydere på det danske marked pålægges at informere Center for Cybersikkerhed om sikkerhedshændelser, og organisationerne anerkender, at de foreslåede ændringer af lovens § 4, nr. 3, er udtryk for direktivimplementering. TI finder dog, at tilføjelsen af "uden unødigt ophold" er en signifikant stramning af bestemmelsen i forhold til i dag, hvor fristen er 14 dage. TI opfordrer til, at 14-dages fristen fastholdes ved udmøntning af bestemmelsen i bekendtgørelsen. TI og IT-Branchen er desuden særligt bekymret over tilføjelsen af en ny § 4, nr. 4, om at udbydere generelt i alle tilfælde skal underrette offentligheden ved sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester. TI og IT-Branchen er bekymret over at skulle informere offentligheden om sikkerhedshændelser, der måtte være forsvarligt håndteret, idet der vil være risiko for, at dette kan skabe unødig utryghed. Derudover er TI og IT-Branchen bekymret over, at offentliggørelse af information om sikkerhedstrusler kan anspore hackere til at gå målrettet mod en udbyder eller en sektor, der har været ramt. TI og IT-Branchen finder, at udbyderen bør partshøres med mindre det af tidsmæssige grunde er umuligt.

Med lovforslaget videreføres lovens eksisterende § 4, stk. 3 og 4, med visse justeringer.

Forsvarsministeriet anerkender, at der med tilføjelsen af "uden unødigt ophold" til lovens § 4, stk. 3, sker en skærpelse af fristen for udbydernes underretning af Center for Cybersikkerhed om sikkerhedshændelser. Tilføjelsen følger dog direkte af artikel 40, stk. 2, i EU's telekodeks,

og den nuværende 14-dages frist vurderes dermed ikke at kunne opretholdes.

Der er ikke med lovens § 4, stk. 4, tale om – hverken i dag eller efter lovforslaget – at udbydere i alle tilfælde skal underrette offentligheden ved sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester. I medfør af bestemmelsen kan Center for Cybersikkerhed efter en konkret vurdering i det enkelte tilfælde påbyde en udbyder at underrette offentligheden. Det vil fortsat være en forudsætning, at det godtgøres, at det vil være i offentlighedens interesse, at sikkerhedshændelsen offentliggøres, jf. bemærkningerne til bestemmelsen.

9. Informering af brugere om beskyttelsesforanstaltninger mv.

Region Nordjylland anfører, at det i praksis vil være yderst vanskeligt at informere alle brugere på eksempelvis gæstenetværk på hospitaler om en potentiel sikkerhedshændelse, og at der må gives plads til individuelle vurderinger af impactet for de relevante netværk. Regionen finder, at det må anses for værende på grænsen af gældende lovgivning at logge så mange detaljer om enheder på eksempelvis gæstenetværk, at en bruger kan entydigt identificeres. Regionen anser derfor kravet for urimeligt.

TI og IT-Branchen anfører, at organisationerne har svært ved at gennemskue, hvorledes teleudbydere skal kunne informere en specifik (gruppe af) forbrugere, der f.eks. anvender sikkerhedsmæssigt kompromitterbart udstyr, f.eks. en ukurant WiFi-router, når denne type information ikke er kendt af teleudbyderen. TI og IT-Branchen anerkender dog også intentionen med forslaget. TI og IT-Branchen finder det usikkert, om der i medfør af bestemmelsen skal etableres nye funktioner i virksomheden og opfordrer til, at det præciseres, hvorledes det forventes, at udbyderne kan designe et system, der kan håndtere kravet. En eventuel løsning bør være omkostningseffektiv og proportional i forhold til den ønskede effekt.

Den foreslåede bestemmelse indebærer, at de omfattede udbydere skal informere deres potentielt berørte brugere om mulige beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som brugerne kan træffe i tilfælde af en særlig og betydelig trussel om en sikkerhedshændelse i udbyderens net og tjenester. I visse tilfælde skal udbyderne endvidere informere brugerne om selve truslen.

Det er således en forudsætning, at der er tale om en særlig og betydelig trussel, og at brugerne selv kan foretage sig noget for at beskytte sig mod eller afhjælpe truslen om en sikkerhedshændelse.

Det er ikke hensigten med bestemmelsen, at udbyderne skal indsamle eller opbevare yderligere oplysninger om deres brugere til opfyldelse af forpligtelsen. Ligeledes indebærer bestemmelsen ikke, at udbyderne skal udvikle nye systemer specifikt til understøttelse af forpligtelsen.

10. Øvrige bemærkninger

Region Nordjylland anser det for usikkert, om offentlige instanser vil være omfattet af definitionen af udbydere af NUIK-tjenester, hvorfor regionen ikke mener, at det er korrekt, at implementering kan ske under eksisterende bevillingsmæssige rammer.

TI og IT-Branchen har forståelse for og støtter, at den eksisterende § 3, stk. 3, om at traditionelle teleudbydere kan pålægges forpligtelser ved hensyn af væsentlig samfundsmæssig betydning, videreføres som § 3, stk. 4, med de mindre, foreslåede sproglige præciseringer. TI og IT-Branchen påpeger desuden, at omkostningerne for erhvervslivet ved lovforslaget er usikre og virker særdeles underestimerede henset til usikkerhederne om lovforslagets rækkevidde.

Der er ved vurderingen af omkostningerne for erhvervslivet taget udgangspunkt i erfaringerne med net- og informationssikkerhedsloven fra 2015, herunder omkostningerne forbundet med loven. Udgifterne som følge af lovforslaget for de traditionelle teleudbydere, som er omfattet af loven i dag, vurderes på den baggrund at have et meget begrænset omfang. Det skyldes, at der med lovforslaget kun foretages ganske få ændringer af eksisterende krav og ganske få tilføjelser af nye krav, som kan indebære merudgifter for disse udbydere. Som det fremgår af Forsvarsministeriets bemærkninger til høringssvarene ovenfor, er de nye forpligtelser i medfør af lovforslaget i en række tilfælde af væsentlig mindre omfang og rækkevidde end det umiddelbart antages af høringsparterne.

For udbydere af NUIK-tjenester, der med lovforslaget som noget nyt bliver omfattet af reguleringen, forventes det – også i lyset af erfaringerne med de samme krav, der allerede i dag gælder for de traditionelle teleudbydere – at omkostningerne vil være beskedne.

Det er i lovforslaget præciseret, at i det omfang stat, kommuner og regioner udbyder offentligt tilgængelige elektroniske kommunikationsnet og -tjenester eller NUIK-tjenester, vil de krav, der efter lovforslaget stilles til udbydere af disse net og tjenester, også omfatte stat, kommuner og regioner. Det vil kunne medføre økonomiske og administrative konsekvenser i samme omfang som for private udbydere.