



13. januar 2025

Til Ministeriet for Samfundssikkerhed og Beredskab

Sagsnr.: 2024/13723

Sendt pr. e-mail til: [mssb@mssb.dk](mailto:mssb@mssb.dk)

## Høringsvar til høring over udkast til lov om sikkerhed og beredskab i telesektoren

Indledningsvis skal TI, Dansk Erhverv, DI Digital, IT-Branchen og Rådet for Digital Sikkerhed (herefter høringssparterne) takke for muligheden for at afgive høringssvar til den nye lov om sikkerhed og beredskab i telesektoren. Høringssvaret er opdelt i en række generelle bemærkninger og en række konkrete bemærkninger.

### Generelle bemærkninger:

#### 1.1. Kort høringsfrist:

Nærværende udkast til lovforslag blev sendt i høring den 12. december 2024 med frist for at afgive høringssvar den 9. januar 2025. Høringssparterne finder det dybt problematisk, at et så omfangsrigt lovforslag fremsættes hen over en ferieperiode med frist kort tid efter nytår, da det lægger et unødigt stort pres på de omfattede televirksomheder, der på meget kort tid har skullet nå at forholde sig til et meget omfattende materiale.

Henset til den korte høringsfrist, vil høringssparterne gerne rose Ministeriet for Samfundssikkerhed og Beredskab (herefter "MSSB") for at have været så positivt indstillede på en tæt dialog med branchen. Høringssparterne imødeser en fortsat tæt dialog og håber, at MSSB også vil være lydhøre overfor branchens holdninger og indlæg i relation til de kommende bekendtgørelser. Høringssparterne opfordrer desuden helt generelt til, at der med fremsættelsen af bekendtgørelserne også videreføres en mere konsekvent begrebsanvendelse, så vi undgår unødigt "begrebsforvirring" f.eks. omkring tidsfrister som det er tilfældet i dag med begreberne "unødigt ophold", "ugrundet ophold" mv.

### 1.2. Erhvervsøkonomiske konsekvenser:

Det fremgår af lovforslagets side 207, at det ikke har været muligt at foretage en kvantificering af de erhvervsøkonomiske efterlevelsese- og administrative konsekvenser for erhvervslivet af de nye regler, men at det foreløbig vurderes, at der vil være efterlevelsesekonsekvenser for erhvervslivet på mindre end 10 mio. kr. og administrative konsekvenser på mindre end 4 mio. kr.

Høringsparterne ser frem til Erhvervsstyrelsens kommende konsekvensvurdering og minder i den forbindelse om, at det er et af de fire pejlemærker i den telepolitiske aftale, at *"[t]elepolitikken skal fremme, at rammerne for private investeringer på teleområdet er enkle, klare og forudsigelige, samtidig med at barrierer og byrder for private investeringer i den digitale infrastruktur reduceres"*. Ved implementering af de sektorspecifikke regler om sikkerhed og beredskab bør der derfor være særlig opmærksomhed på at undgå at øge byrderne for virksomhederne i telesektoren.

Det bemærkes i den forbindelse, at det er vanskeligt at foretage en reel vurdering af byrderne på baggrund af udkastet til lovforslaget i sig selv, da den væsentligste del af de specifikke krav til selskaberne vil blive fastsat i bekendtgørelser. Vurderingen bør derfor tage udgangspunkt i det markante udfaldsrum, myndighederne gives i forhold til at kunne pålægge byrder, hvis forslaget vedtages.

Høringsparterne har noteret, at der generelt må forventes et væsentligt større dokumentationsarbejde hos selskaberne samt væsentligt større indsats i forhold til assistance til myndighederne i forbindelse med hændelsesrapportering og tilsyn end det hidtil har været tilfældet. Disse opgaver forventes ikke at kunne varetages på tværs af sektoren indenfor de angivne, foreløbige estimater.

### 1.3. Bemyndigelseshjemler og kommende bekendtgørelser:

Det fremgår af lovforslaget, at meget af den konkrete regulering på området for sikkerhed i net og tjenester kommer til at blive udmøntet i bekendtgørelser, som vi endnu ikke kender indholdet af.

Høringsparterne havde gerne set, at bekendtgørelserne, særligt på baggrund af den lange forberedelse af lovforslagets fremsættelse, havde foreligget samtidig med udkastet til lovforslag, så helheden af den foreslåede regulering kunne være blevet vurderet samlet. Da dette ikke ses at være tilfældet, opfordrer høringsparterne til, at MSSB foretager en grundig inddragelse af alle interessenter i udarbejdelsen af udkast til bekendtgørelser, og herudover giver tilstrækkelig tid til, at det bliver en god høringsproces, når bekendtgørelsesudkastene skal i høring.

Herudover er det for høringsparternes medlemmer positivt at kunne notere, at anvendelsesområdet, jf. den foreslåede § 1 i den nye lov om sikkerhed og beredskab i telesektoren, synes at omfatte alle relevante aktører i telesektoren. Det er vigtigt for konkurrenceevnen hos teleudbyderne, at de lovgivningsmæssige byrder, som denne nye

lovgivning medfører, hviler ligeligt på alle relevante aktørers skuldre, og høringsparterne håber derfor, at bekendtgørelserne også vil afspejle dette.

**1.4. Behov for tydeliggørelse af, hvilke krav, der skal stilles til teleudbydernes håndtering af ”kritiske netkomponenter, systemer og værktøjer”:**

Høringsparternes medlemmer er enige med MSSB i, at trusselsbilledet har ændret sig markant inden for de senere år, hvilket bl.a. også berøres af MSSB på side 151 i udkastet til lovforslag. Teleinfrastrukturen er uden tvivl kritisk infrastruktur i det danske samfund, og det faktum stiller store krav til sikkerheden hos teleudbyderne.

Høringsparterne støtter fuldt ud op om, at den danske teleinfrastruktur skal beskyttes bedst muligt. Men for at kunne løfte denne opgave, er det nødvendigt, at teleudbyderne får et tydeligere billede af, hvilke rammer og forventninger, der er fra myndighedernes side til teleudbydernes håndtering af den samfundskritiske teleinfrastruktur.

Først og fremmest er det for høringsparternes medlemmer med den gældende regulering en udfordring i sig selv at afgøre i praksis, hvilke komponenter, systemer og værktøjer, der er kritiske i lovgivningens forstand, jf. definitionen af ”kritiske netkomponenter, systemer og værktøjer” i § 1, nr. 3 i bekendtgørelse om sikkerhed i net og tjenester, jf. bekendtgørelse nr. 259 af 22. februar 2021. Definitionen er meget bred, hvilket medfører en vis usikkerhed om rækkevidden af definitionen. At der er usikkerhed om definitionens rækkevidde, medfører både en uensartet praksis på tværs af branchen og giver anledning til tvivl og forskellige opfattelser internt hos teleudbyderne.

Herefter, når den ovenstående udfordring er løst på bedst mulig vis, og en teleudbyder har afgjort, hvilke komponenter, systemer og værktøjer, der er kritiske i teleudbyderens virksomhed, opstår der et centralt spørgsmål om, hvordan de kritiske netkomponenter, systemer og værktøjer skal beskyttes og håndteres af teleudbyderen. I den forbindelse fremgår det f.eks. ganske klart af den eksisterende lovgivning, at CFCS skal underrettes, når en teleudbyder vil indgå en aftale med en leverandør om køb af kritiske netkomponenter, systemer og værktøjer mv. Men det fremgår omvendt ikke klart, om og i hvilket omfang, at fysisk eller logisk adgang til samfundskritisk teleinfrastruktur skal resultere i et krav om sikkerhedsgodkendelse. Endvidere fremgår det heller ikke klart, i hvilket omfang det f.eks. er muligt for en teleudbyder at outsource aktiviteter forbundet med kritiske netkomponenter, systemer og værktøjer. Disse udfordringer ses ikke løst med udkastet til lovforslag.

Tilsvarende rejser den foreslåede § 5 flere spørgsmål om fortolkning af de beskrevne krav til teleudbydernes sikkerhedsforanstaltninger. Eksempelvis om forståelse og definition af ’cyberhygiejnepraksisser’ (pkt. 7) samt definition og anvendelse af ”sikret tale-, video- og tekstkommunikation” (pkt. 10).

For at opnå en ensartet fortolkning og passende beskyttelse har teleudbyderne brug for tydeligere rammer og myndighedernes vejledning til, hvordan den kritiske teleinfrastruktur efter myndighedernes vurdering beskyttes bedst muligt. Høringsparterne ser NIS2- implementering som den perfekte mulighed for også at få nedbragt eksisterende uklarheder, som den gældende lovgivning indeholder.

#### 1.5. Hændelsesrapportering til både CSIRT og CFCS:

Det fremgår af side 158 i bemærkningerne til lovforslaget, at teleudbyderne skal foretage hændelsesrapportering til både CSIRT'en, som hører under Forsvarsministeriet og til CFCS, som hører under MSSB. I forlængelse heraf fremgår, at det forudsættes, at der vil være et tæt samarbejde mellem CFCS og CSIRT'en, og at en nærmere fastlæggelse af rammerne for dette vil kunne ske i en samarbejdsaftale.

Når der skal indrapporteres til to forskellige organer, er der en risiko for, at det kan blive uhensigtsmæssigt og unødigt bureaukratisk for virksomhederne, særligt hvis begge organer vender tilbage med opfølgende spørgsmål til rapporteringen o.lign. Det er derfor væsentligt, at myndighederne koordinerer området indbyrdes, og at indrapporteringsløsninger som 'virk.dk' og den efterfølgende kommunikation mellem myndigheden og den rapporterende virksomhed er overskuelig. En overskuelig proces kunne f.eks. ske således, at den samme indrapportering systemmæssigt sendes til begge organer uden at virksomheden skal indsende samme rapportering flere gange, samt at de to organer koordinerer indbyrdes om opfølgning.

#### **Konkrete bemærkninger:**

Nedenfor følger høringsparternes bemærkninger til de konkrete bestemmelser i lovforslaget.

##### 2.1. § 2, nr. 1: Definitionen af "Beredskabssituationer og andre ekstraordinære situationer":

Det fremgår af bemærkningerne på side 215 i lovforslaget, at den nye lov vil definere "Beredskabssituationer og andre ekstraordinære situationer", som: "*Situationer, hvor der allerede er, eller hvor der kan opstå større ulykker, katastrofer eller hændelser, herunder krise eller krig og hvor der er risiko for påvirkning af udbuddet af net og tjenester*". MSSB anfører i forlængelse heraf, at denne nye definition svarer til definitionen i den gældende lovgivning.

Imidlertid fremgår det af § 1, nr. 2 i bekendtgørelse om sikkerhed i net og tjenester, jf. bekendtgørelse 259 af 22. februar 2021, (herefter bekendtgørelse 259), at "Beredskabssituationer og ekstraordinære situationer" defineres som: "*Større ulykker, katastrofer eller hændelser, hvor det kan være nødvendigt at indføre særlige foranstaltninger vedrørende net og tjenester med henblik på at kunne opretholde samfundets funktioner*". Høringsparterne finder ikke, at disse to definitioner har et enslydende indhold.

Den nye definition udvider efter høringsparternes opfattelse området for, hvornår der er tale om en beredskabssituation, da definitionen med ordene "*hvor der kan opstå større ulykker*" og "*risiko for påvirkning[...]*" udvides til også at omfatte situationer, hvor en ulykke/hændelse/påvirkning endnu ikke rent faktisk er indtrådt eller foreligger.

Høringsparterne skal i den forbindelse understrege, at definitionen af, hvornår der er tale om en "beredskabssituation" er helt central for teleudbyderne af flere grunde. Som eksempler kan nævnes, at beredskabssituationer, hvor teleudbyderen aktiverer sit interne beredskab, medfører en række skærpede underretningspligter til CFCS, jf. kap. 5 i bekendtgørelse 259. Endvidere vedrører en stor del af teleudbydernes forpligtelser i "bekendtgørelse om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv.", jf.

bekendtgørelse 261 af 22. februar 2021, netop, hvad teleudbydere kan blive påbudt af CFCS i en beredskabssituation.

Det er således af stor betydning for høringsparternes medlemmer, at definitionen af en beredskabssituation kan omsættes, så den operationelt passer ind i teleudbydernes virksomhed. Og dette bliver sværere med den nye, bredere definition, hvor potentielle faktorer som noget nyt også skal medtages. Der vil være tale om en meget væsentlig udvidelse af forpligtelserne på udbydere, hvis definitionen udvides som foreslået.

Høringsparterne skal derfor henstille til, at den gældende formulering fastholdes i stedet for den foreslåede udvidelse.

Skulle MSSB se et behov for at benytte en udvidet definition i specifikke tilfælde, fx i relation til lovens kapitel 4 om beredskabs- og andre ekstraordinære situationer, bør definitionens udvidelse ske på en måde, så den kun vedrører CFCS' specifikke beføjelser i lovens kapitel 4. Og her bør det ydermere tydeliggøres, hvilke situationer, der hentydes til med ordene *"hvor der kan opstå større ulykker, katastrofer eller hændelser"* samt hvad der menes med *"risiko for påvirkning af udbuddet af net og tjenester"*.

## 2.2. § 5: Risikostyring:

Lovforslagets § 5, stk. 1 fastslår, at væsentlige og vigtige teleudbydere skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse udbydere anvender til deres operationer eller til at levere deres tjenester.

Bestemmelsen er en direkte implementering af artikel 21 i NIS2-Direktivet, men lader til at have væsentlig sammenhæng med de gældende bestemmelser om risikovurdering af *"risikoen for tab af tilgængelighed, autenticitet, integritet og fortrolighed i de net og tjenester, der udbydes"*, jf. bekendtgørelse 259, § 2, stk. 1 samt bekendtgørelsens § 9, som fastslår, at væsentlige erhvervsmæssige udbydere som en del af fastlæggelsen af risikovillighed i risikostyringsprocessen skal tage højde for, at udbydere i videst muligt omfang skal opretholde udbuddet af net og tjenester i beredskabssituationer og i andre ekstraordinære situationer med henblik på at sikre samfundets teleforsyning.

Selvom bestemmelsen i lovforslaget, som tager udgangspunkt i direktivet, er ny for teleudbydere, vil det være hjælpsomt, hvis MSSB kan oplyse, hvorvidt der ses at være tale om ændring i forhold til de gældende regler om risikostyring. For at sikre en god og ensartet implementering af den foreslåede bestemmelse, skal høringsparterne henstille til MSSB, at der udarbejdes vejledning eller lignende om den ønskede risikostyring af net- og informationssystemer, der anvendes til udbydernes operationer.

## 2.3. § 6: Begrebet *"ledelsesorgan"* og dette organs forpligtelser:

Det fremgår af lovforslagets § 6, stk. 1, at teleudbydernes ledelsesorganer skal godkende og føre tilsyn med de foranstaltninger til risikostyring, som teleudbyderen skal have, jf. lovforslagets § 5. Herudover skal ledelsesorganerne deltage i relevante kurser om risikostyring mv., jf. forslaget § 6, stk. 2.

Det materielle indhold af forpligtelserne svarer i det store hele til NIS2-Direktivets artikel 20 og giver derfor efter høringsparternes opfattelse alene anledning til følgende bemærkninger:

Ved første øjekast på § 6 er det meget vanskeligt for høringsparternes medlemmer at afklare, hvilken personkreds, der skal henføres under begrebet "ledelsesorgan". Høringsparterne ønsker derfor, at MSSB forholder sig direkte til indholdet af dette begreb, således at vi sikrer en ensartet implementering på tværs af branchen, men også på tværs af sektorerne i Danmark. Konkret ønsker høringsparternes medlemmer en afklaring af, hvorvidt der ved ansvarligt ledelsesorgan lægges vægt på funktion fremfor ledelsesniveau.

Som baggrund kan kort nævnes, at høringsparternes medlemmers organisationer er bygget op på meget forskellig vis. Det faglige ledelsesansvar for fysisk sikkerhed, telesikkerhed, cybersikkerhed mv. kan være placeret mange forskellige steder både vertikalt og horisontalt inden for organisationerne, og derfor kan det hurtigt blive en svær øvelse at fastlægge, hvilken personkreds, der hentydes til med den foreslåede § 6. Det er et tungt ansvar at skulle føre tilsyn med sin egen organisations overholdelse af de foranstaltninger til risikostyring, som hjemles i § 5, og derfor bør det fremstå mere klart for teleudbyderne, hvor dette ansvar skal placeres, så organisationen kan indrettes og evt. tilpasses derefter.

I forlængelse af ovenstående bør MSSB også overveje, om det bør præciseres, at ledelsesorganets opfyldelse af sin tilsynsforpligtelse forudsætter en passende tildeling af centrale sikkerhedsroller og en uafhængig rapporteringskanal for at være effektiv. Med andre ord kan det være vanskeligt at 'føre tilsyn med sig selv' internt i en virksomhed, hvis ikke der laves det rette set up, og det bør ikke være muligt at indrette sin organisation på en måde, gør § 6 illusorisk

#### 2.4. § 7: IKT-produkter, -tjenester og -processer:

Det fremgår af den foreslåede § 7, at Ministeren for samfundssikkerhed og beredskab kan fastsætte regler om, at væsentlige og vigtige teleudbydere skal anvende særlige IKT-produkter, -tjenester og -processer, som er certificeret i henhold til en europæisk cybersikkerhedscertificeringsordning for at påvise overensstemmelse med bestemte krav i § 5, stk. 1, eller regler om krav til foranstaltninger fastsat i medfør af § 5, stk. 3.

Bestemmelsen er en direkte implementering af artikel 24, stk. 1, i NIS2-Direktivet, og er således helt ny for teleudbyderne. Høringsparternes medlemmer er dog usikre på rækkevidden af bestemmelsen, der potentielt virker meget omfattende. Herudover er der flere forhold, der endnu ikke fremstår helt klart, f.eks. hvad tidsrammen er for efterlevelse af et fremtidigt påbud om at benytte bestemte IKT-produkter, -tjenester eller -processer, hvordan en europæisk cybersikkerhedscertificeringsordning helt konkret kommer til at se ud og virke i praksis m.v.

Endvidere fremgår det af bemærkningerne på side 230, at EU-Kommissionen kan vedtage delegerede retsakter på dette område, når "der er identificeret utilstrækkeligt cybersikkerhedsniveau". Det er efter høringsparternes opfattelse uklart, om og hvordan EU-Kommissionen i fremtiden har tænkt sig at håndtere denne bemyndigelse.

2.5. § 8, stk. 1: Registrering af IP-intervaller:

Det fremgår af den foreslåede § 8, stk. 1, at teleudbyderne skal registrere sig hos CFCS og udlevere en række bestemte 'pligtoplysninger', herunder IP-intervaller. Bestemmelsen stammer direkte fra NIS2-Direktivet og giver efter høringsparternes opfattelse også meget god mening i udgangspunktet.

Dog forholder det sig sådan i praksis, at det for teleudbyderne vil være en meget stor administrativ opgave løbende at skulle registrere og ajourføre sine IP-ranges, sådan som det de facto bliver tilfældet med den nye § 8.

Derfor skal høringsparterne opfordre MSSB til at implementere et nemt og lempeligt set up, så teleudbydernes administrative byrde med registrering af IP-ranges bliver så lille som muligt. Høringsparternes medlemmer deltager gerne i denne proces, da de har en stor interesse i at sikre, at forpligtelserne de pålægges i medfør § 8, bliver så lette at løfte i praksis som muligt.

2.6. §§ 8, stk. 5, nr. 2, og 9, stk. 2: Begreberne "væsentlige dele af udbyderens net", "alvorlige driftsforstyrrelser" og "betydelig skade":

Det fremgår af lovforslagets § 8, stk. 5, nr. 2, at der skal udstedes en bekendtgørelse, hvorefter teleudbyderne skal underrette CFCS inden, at der indgås aftaler om "**væsentlige dele af udbyderens net**". Høringsparterne finder i det store hele, at der er tale om en videreførsel af den gældende bekendtgørelse om oplysnings- og underretningspligter vedr. sikkerhed i net og tjenester, jf. bekendtgørelse 1414 af 30. november 2023.

Det er dog i den forbindelse vigtigt for høringsparternes medlemmer, jf. også vores generelle bemærkning ovenfor om tydeligere rammer, at understrege, at det kan være en stor udfordring i praksis for teleudbyderne at skulle foretage en vurdering af, hvad der kan siges at være "*en væsentlig del af udbyderens net*".

Ligeledes fremgår det af forslaget § 9, stk. 2, der vedrører, hvornår en hændelse er væsentlig, at: "*En hændelse anses for at være væsentlig, hvis den 1) har forårsaget eller er i stand til at forårsage **alvorlige driftsforstyrrelser** af net eller tjenester eller økonomiske tab for den berørte udbyder, eller 2) har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage **betydelig** fysisk eller ikke fysisk **skade***" (Høringsparternes fremhævelse).

Definitionen stammer fra NIS2-Direktivets artikel 23, stk. 3, og er dermed ny for teleudbyderne. Det er høringsparternes opfattelse, at også denne definition kan resultere i en svær vurdering af, hvornår en hændelse er *væsentlig*.

Høringsparterne skal derfor på baggrund af ovenstående opfordre MSSB til at udarbejde vejledninger, formålsbeskrivelser eller lignende, der kan støtte teleudbyderne i fortolkningen. Og herudover opfordres MSSB også til i den nye bekendtgørelse at indsætte tærskelværdier for, hvornår en hændelse er væsentlig, sådan som det er tilfældet i dag, jf. § 8 i bekendtgørelse 1414 af 30. november 2023.

Det overordnede formål bør være, at bestemmelserne får et indhold, der kan indarbejdes i den mere operationelle del af teleudbydernes virksomhed og herudover, at vejledninger mv. kommer til at danne grundlag for en mere ensartet forståelse og praksis på tværs af telebranchen, hvilket ikke altid ses i dag.

2.7. § 9: Undtagelse for aktindsigt

Høringsparterne har med tilfredshed noteret, at det foreslås at undtage teleudbydernes underretninger om hændelser og trusler fra aktindsigt og at bemyndige CFCS til at fastsætte regler om undtagelse fra aktindsigt vedr. selskabernes underretninger til CFCS fx om aktivering af beredskab.

Høringsparterne finder det væsentligt, at det sikres, at følsomme oplysninger om sårbarheder i teleudbydernes net mv. ikke kommer til uvedkommendes kendskab, herunder i forbindelse med en evt. deling af oplysninger mellem relevante myndigheder.

2.8. § 14: Beredskabs- og andre ekstraordinære situationer:

§ 14, stk. 1:

Bestemmelsen viderefører indholdet af § 5, stk. 3 i den tidligere lov om sikkerhed i net og tjenester. Bestemmelsen er udmøntet i bekendtgørelse 261 om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer (herefter BEK 261).

Ud fra ordlyden af bestemmelsen vil det kunne forstås, at det er CFCS der prioriterer hvilke beredskabsaktører, der kan opnå prioritet i et netværk. Da der er tale om en videreførelse af de gældende regler, forstår høringsparterne, at det således stadig er mobilselskaberne, jf. § 9 i BEK 261, der via brancheaftaler sikrer, at beredskabsaktørerne får forrang i forhold til brug af mobilnettet i beredskabssituationer og i andre ekstraordinære situationer eller at CFCS påbyder udbyderen at etablere en sådan sikring.

Da der er tale om en videreførelse af reglerne, er det høringsparternes forventning, at de nye regler ikke vil ændre den eksisterende brancheaftale.

§ 14, stk. 2:

Det fremgår af bestemmelsen, at CFCS kan fastsætte regler om, at væsentlige og vigtige teleudbydere skal sikre, at de foretagne prioriteringer gennemføres i net og tjenester.

Hvis bestemmelsen udmøntes i en bekendtgørelse, vil høringsparterne i den proces opfordre til, at de berørte parter inddrages så tidligt som muligt.

I bemærkningerne til bestemmelsen, side 249, står (Høringsparternes fremhævnning):

*”Der kan desuden med hjemmel i bestemmelsen fastsættes regler om, at væsentlige teleudbydere og vigtige teleudbydere 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 væsentlige teleudbydere og vigtige teleudbydere skal prioritere reetablering af bestemte dele af en udbyders beskadigede infrastruktur.”**

Ovenstående fremhævelse skaber bekymring i telebranchen, da det indikeres, at teleselskaberne kan pålægges uforudsete omkostninger ved påbud om reetablering af infrastruktur, som kan ligge udover selskabernes egen planlægning.

Det er således vigtigt at udmøntningen af bestemmelsen ikke er for vidtrækkende og at teleselskaberne skal have med indflydelse på prioriteringsordningerne, som udarbejdes af CFCS.

#### § 14, stk. 3:

Bestemmelsen bemyndiger CFCS til at fastsætte regler om at teleudbydere skal underrette CFCS i tilfælde hvor beredskabet aktiveres. Der er tale om en delvis videreførelse af § 5, stk. 2 i lov om sikkerhed og tjenester.

Der kan således fastsættes nærmere regler om underretning. Der står imidlertid i bemærkningerne til bestemmelsen, på side 250, at:

*”MSSB finder det henset til vurderingen af det aktuelle trusselsniveau mod telesektoren væsentligt at opretholde det nuværende sikkerhedsniveau i telesektoren.”*

Dette afsnit står for sig selv og høringsparterne kan ikke se koblingen til reglerne om underretning. Høringsparterne beder derfor ministeriet om en uddybende forklaring af, hvorledes vurderingen af det aktuelle trusselsniveau og opretholdelsen af det nuværende sikkerhedsniveau hænger sammen med regler om hvordan underretninger skal foretages.

#### § 14, stk. 4:

Den foreslåede bestemmelse er en uændret videreførelse af § 5 a i lov om sikkerhed i net og tjenester. Bemyndigelsen til at fastsætte regler er ikke udmøntet i dag.

Der refereres i bemærkningerne til at udbydere i alvorlige nødsituationer skal ’træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne.’ Der refereres i denne forbindelse til art. 108, 2. pkt. i teledirektivet (EU 2018/1972) som skal ses i sammenhæng med art. 110 i samme direktiv.

Art. 110 i teledirektivet pålægger medlemsstater at indføre et offentligt varslingsystem. I Danmark blev det system til via en kontrakt mellem Forsvarets Materiel- og Indkøbsstyrelsen (herefter FMI) og mobilsekskaberne og er kendt som S!RENEN. Hjælpen til implementeringen af S!RENEN findes i telelovens § 62.

Der står bl.a. i art. 108 at: *”Medlemsstaterne sikrer, at udbydere af talekommunikationstjenester træffer alle nødvendige foranstaltninger til at sikre uafbrudt adgang til beredskabstjenester og uafbrudt transmission af offentlige advarsler.”*

Denne ordlyd er ikke implementeret i teleloven, men er omfattet af kontrakten mellem FMI og mobilsekskaberne, som blev indgået i stedet for at myndighederne skulle udstede en bekendtgørelse.

Kontrakten mellem FMI og mobiloperatørerne består af to aftaler:

- En hovedaftale om implementeringen af systemet og
- En driftsaftale om driften af systemet

Der blev valgt en kontrakt i stedet for at udstede en bekendtgørelse fordi, at der er tale om en yderst teknisk implementering i den kritiske infrastruktur, som krævede dialog mellem parterne. Dette er svært at udmønte i en bekendtgørelse. Herudover må slutbrugerne jf. telelovens § 62, 2. pkt. ikke pålægges udgifter i forbindelse med modtagelse af advarslerne, samt at mobiloperatørerne heller ikke pålægges omkostninger ved implementeringen jf. telelovens § 62, stk. 2.

FMI afholdt derfor omkostningerne til implementeringen af systemet samt afholder omkostningerne til driften af systemet.

Kontrakten indeholder flere bilag med krav til den tekniske implementering, test, opetid, redundans, kravspecifikationer, beskrivelser af hardware og software etc. Alle disse tekniske dialoger blev foretaget, fordi systemet skulle bygges redundant og derved til at sikre uafbrudt transmission af advarslerne. Herudover er der i kontrakten givet FMI beføjelser til at sikre systemet og iværksætte tiltag for at sikre at systemet fungerer ved katastrofer. Det indebærer den net-tekniske sikkerhed, men også mulighed for fysisk sikkerhed som f.eks. vagter på bestemte lokationer, for at opretholde systemets funktionalitet.

Det er derfor høringsparternes klare forståelse, at teledirektivets art. 108 og art. 110 er fuldt implementeret i teleloven og i kontrakten med FMI.

Høringsparterne mener derfor, at § 14, stk. 4 allerede er implementeret i dansk ret, og at bestemmelsen bør udgå.

Vælges det at beholde bestemmelsen, skal der med reference til telelovens § 62, stk. 2 fremgå, at mobiloperatørerne får refunderet udgifter afholdt i forbindelse med systemet.

Høringsparterne har nedenfor med blå/fed skrift indsat ordlyden fra telelovens § 62, stk. 2 og en omskrivning af bestemmelsen bør se således ud:

*”Stk. 4. Ministeren for samfundssikkerhed og beredskab kan fastsætte regler om, at udbydere, som i medfør af lov om elektroniske kommunikationsnet og -tjenester skal udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer, skal træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne. **Det sikres, at udbydere refunderes nødvendige, dokumenterede udgifter, som udbydere har afholdt i forbindelse med udvikling, etablering og drift af den tekniske løsning, der anvendes til udsendelse af offentlige advarsler.**”*

§ 14, stk. 5:

Der er tale om en videreførelse af indholdet i § 5, stk. 4 i lov om sikkerhed i net og tjenester.

I bemærkningerne til bestemmelsen står slutteligt:

*”Det forudsættes, at udbydere 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.”*

Høringsparterne henviser til sine bemærkninger til § 14, stk. 4, at staten afholder omkostninger til etablering og drift af det offentlige varslingsystem.

#### 2.9. § 17: Sikkerhedsgodkendelser:

Det fremgår af bemærkningerne til lovforslaget (side 256), at den foreslåede § 17 om sikkerhedsgodkendelser delvist viderefører indholdet af den gældende § 6, stk. 1, i lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021.

Ordlyden i bestemmelsen er ændret, så det tydeliggøres, at der er 2 grundlæggende tilfælde, hvor det er relevant at vurdere, om en medarbejder eller repræsentant for teleudbyderen skal sikkerhedsgodkendes i regi af denne lovgivnings regler.

Det ene kriterie vedrører sikkerhedsgodkendelse, når *”det er nødvendigt i forhold til den pågældendes adgang til klassificeret information eller til de funktioner, som den pågældende skal varetage.”* Det andet kriterie vedrører sikkerhedsgodkendelse, når *”den pågældende varetager kontakten til Center for Cybersikkerhed i relation til beredskabet i henhold til regler, der er udstedt i medfør af § 14, stk. 3”.*

Hvad angår anden del af det første kriterie om *”funktioner, som den pågældende skal varetage”*, har høringsparternes medlemmer meget vanskeligt ved at indsnævre den relevante personkreds ud fra denne bestemmelses ordlyd. Allerede i dag volder den løse formulering i den gældende § 6, stk. 1, om sikkerhedsgodkendelse stort besvær for teleudbydere. Støttes den nye ordlyd i § 17 ikke op af yderligere og mere detaljeret regulering, eller alternativt vejledninger fra myndighederne, vil disse vanskeligheder fortsætte.

Der skal på den ene side naturligvis være en vis margin i lovgivningen til, at teleudbydere selv kan indstille medarbejdere eller repræsentanter til sikkerhedsgodkendelse, såfremt teleudbyderen vurderer, at den pågældende medarbejder varetager en så kritisk eller central funktion i virksomheden, at det er nødvendigt at sikkerhedsgodkende vedkommende.

Men denne margin kan også være for stor, og det er netop det, der er tilfældet i dag.

Den brede margin kan resultere i, at der enten sendes et for lille eller for stort antal anmodninger om sikkerhedsgodkendelse ind til CFCS og PET. Sendes der for lille et antal anmodninger, giver det ikke den ønskede personalesikkerhed på tværs af branchen. Sendes der omvendt et for stort antal, vil det lægge et pres på myndighedernes sagsbehandlingstid af ansøgningerne. Der ses p.t. enormt lange sagsbehandlingsperioder på op til 12-14 måneder, hvilket ikke er rimeligt i forhold til at sikre udbydere gode rammevilkår for at varetage sikkerhedsmæssigt følsomme opgaver. Endvidere medfører den brede margin, at området vurderes forskelligt på tværs af teleudbydere, hvilket skaber tvivl og dårlige sager mellem teleudbydere i praksis. Endelig kan en bred margin i lovgivningen gøre det svært for

teleudbydere at sikre sig, at der stilles de fornødne kontraktuelle krav om sikkerhedsgodkendelse i kontrakter med andre teleudbydere, leverandører m.v.

Samlet set er det høringsparternes opfattelse, at der bør skabes et lovgivningsmæssigt regime for sikkerhedsgodkendelser, der indeholder tydelige og gennemskuelige krav for teleudbydere, også set i lyset af det ovenfor beskrevne afsnit 1.4. om det generelle behov for tydeligere rammer. Herudover bør det på myndighedssiden sikres tilstrækkelige ressourcer til at håndtere sagsbehandlingen af anmodningerne, så der kan skabes det ønskede niveau af sikkerhedsgodkendelse med en rimelig sagsbehandlingstid.

Høringsparterne ser gerne, at teleudbydernes mulighed for at få sikkerhedsgodkendt centrale medarbejdere efter eget skøn bevares, mens det herudover fremgår klart af enten bekendtgørelser, vejledninger eller andet, hvilken personkreds, som myndighederne har en klar forventning om, at teleudbydere får sikkerhedsgodkendt.

Høringsparterne hilser det desuden velkomment, at MSSB har planer om at udstede nærmere regler for ansøgning og afgørelser om sikkerhedsgodkendelser, samt meddelelse om og tilbagekaldelse af afgørelser om sikkerhedsgodkendelser. Det praktiske og administrative arbejde med sikkerhedsgodkendelser fylder meget hos både myndigheder og teleudbydere. Derfor vil en forenkling af de administrative krav og processer uden tvivl være en stor hjælp i praksis.

Endelig er der et ønske hos flere af høringsparternes medlemmer om, at MSSB sammen med sine nordiske søstermyndigheder vil kigge på, om der i fremtiden kan etableres en løsning, hvor en sikkerhedsgodkendelse i ét nordisk land nemmere kan bruges/overføres til et andet nordisk land.

#### 2.10. § 21: Tilsyn

Det fremgår af den foreslåede § 21, stk. 1, at CFCS som led i sit tilsyn bl.a. kan "foretage kontrol på stedet og eksternt tilsyn, herunder stikprøvekontroller". Det er ikke beskrevet i bemærkningerne til bestemmelsen, hvad begrebet "eksternt tilsyn" dækker over i forhold til de øvrige nævnte tilsynsmuligheder med kontrol på stedet og stikprøvekontroller.

Høringsparterne beder MSSB om at uddybe beskrivelsen af denne type tilsyn enten i bestemmelsen, dens bemærkninger eller i en vejledning.

Det fremgår videre af den foreslåede bestemmelses stk. 3, at CFCS kan stille nærmere krav om, hvordan og i hvilken form oplysninger, som skal afgives af udbydere skal afgives. Det nævnes i bemærkningerne, at oplysningerne kan kræves udleveret på en bestemt måde, på et bestemt sprog og i en bestemt form, samt at der fx kan stilles krav om indtastning på en hjemmeside eller brug af et bestemt skema.

Det bør tilføjes i bemærkningerne til bestemmelsen, at denne beføjelse skal anvendes på baggrund af dialog med den berørte part samt med behørig hensyntagen til den potentielle byrde særlige krav til form, sprog osv. kan pålægge virksomheden, der skal afgive oplysningerne. Der bør i størst muligt omfang tages hensyn til, hvordan oplysningerne lettest

muligt kan stilles til rådighed af virksomheden, da ændring af formater, systemer osv. kan indebære en væsentlig omkostning.

2.11. § 23: Håndhævelsesforanstaltninger

Det fremgår af den foreslåede bestemmelses stk. 1, nr. 1, at CFCS bl.a. bemyndiges til midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de tjenester, teleudbyderen leverer. Bemærkningerne til bestemmelsen fastslår, at bestemmelsen forudsættes ikke at blive anvendt, før CFCS har fastsat nærmere regler om, hvilke certificeringer og godkendelser, som bestemmelsen finder anvendelse på.

Høringsparterne hilser denne detaljering af bestemmelsen velkommen og ser frem til dialog i forbindelse med CFCS' udarbejdelse af disse nærmere regler, da det ikke er muligt at tage stilling til konsekvensen af denne bestemmelse før de nærmere regler er fastsat.

2.12. § 33: Bøder

MSSB bemærker i forbindelse med sanktionsbestemmelsen i § 33, at det foreslås, at der ikke anvendes administrative bøder, men at bøder udstedes og udmåles i det almindelige straffeprocessuelle system. Høringsparterne støtter denne tilgang, som svarer til dansk praksis i øvrigt.

Høringsparterne står naturligvis til rådighed for en uddybning af høringssvaret og besvarelse af eventuelle spørgsmål.

Med venlig hilsen

Poul Noer  
Fagchef for telepolitik  
Dansk Erhverv

Troels Johansen  
Chefkonsulent  
IT-B Branchen

Anders S. Skovbakke  
Konsulent  
DI Digital

Claus Hjorth  
Sekretariatschef  
Rådet for Digital Sikkerhed

Jakob Willer  
Direktør  
Teleindustrien