



Dato: 6. februar 2025
Kontor: Sikkerhed

KOMMENTERET OVERSIGT
over
høringssvar om forslag til lov om sikkerhed og beredskab i
telesektoren

Indhold

1. Høringen	2
1.1. Høringsperiode.....	2
1.2. Hørte myndigheder og organisationer mv.	2
2. Høringssvarene.....	4
2.1. Generelle bemærkninger til lovforslaget.....	4
2.2. Nærmere udmøntning i bekendtgørelser og behov for vejledning ...	4
2.3. Definitionen af et ledelsesorgan.....	6
2.4. Beredskabssituationer og andre ekstraordinære situationer	7
2.5. Sikkerhedsgodkendelser	8
2.6. Brud på persondatasikkerheden.....	10
2.6. Økonomiske- og administrative byrder	10
3. Lovforslaget i forhold til lovudkastet.....	12

1. Høringen

1.1. Høringsperiode

Et udkast til lovforslag har i perioden fra den 12. december 2024 til og med den 9. januar 2025 (28 dage) været sendt i høring hos en række myndigheder og organisationer mv.

Herudover blev udkast til lovforslag offentliggjort på Høringsportalen.

1.2. Hørte myndigheder og organisationer mv.

Nedenfor følger en alfabetisk oversigt over hørte myndigheder og organisationer mv.

Ud for hver høringspart er det ved afkrydsning angivet, om der er modtaget høringssvar, og om høringsparten i givet fald har haft bemærkninger til udkastet til lovforslag.

Oversigten omfatter herudover interessenter, som ikke er blandt de hørte myndigheder, organisationer mv., men på egen foranledning har sendt bemærkninger til udkastet til lovforslag. Sådanne interessenter er i oversigten markeret med *.

Høringspart	Høringssvar modtaget	Bemærkninger	Ingen bemærkninger
Advokatrådet	x	x	
Amnesty International			
Bauer Media			
Borch Teknik	x		x
Cibicom A/S			
Danmarks Radio			
Dansk Erhverv	x	x	
Danske Regioner	x		x
Datatilsynet	x	x	
DanPilot			

Den Danske Dommerforening			
DI Digital	x	x	
Domstolsstyrelsen			
Fibia A/S			
Forenede Danske Antenneanlæg			
GLOBALCONNECT A/S			
Hi3G Denmark ApS			
HORESTA			
Institut for Menneskerettigheder			
IT-Branchen	x	x	
IT-Politisk Forening			
Justitia			
KL			
Norlys			
Præsidenten for Vestre Landsret			
Præsidenten for Østre Landsret			
Retspolitisk Forening			
Rigsrevisionen	x		x
Rådet for Digital Sikkerhed	x	x	
Samtlige byretspræsidenter			
TDC A/S			
TeleDCIS			
Teleindustrien (TI)	x	x	
Telenor A/S			
Telia Company Danmark A/S			
TT-Netværket P/S			
TV DTT A/S			

2. Høringssvarene

Nedenfor er gengivet de væsentligste punkter i de modtagne høringssvar. Ministeriet for Samfundssikkerhed og Beredskabs bemærkninger til høringssvarene, herunder om der er foretaget ændringer i anledning af høringssvarene, er skrevet med kursiv.

Under pkt. 3 er det opsummeret, hvilke ændringer der er foretaget i forhold til det udkast, som har været i offentlig høring.

Samtlige høringssvar er vedlagt særskilt.

2.1. Generelle bemærkninger til lovforslaget

Der er blandt høringssvarerne generelt bred opbakning til lovforslaget, hvor høringssvarerne bl.a. anerkender behovet for at styrke indsatsen på området.

Ministeriet for Samfundssikkerhed og Beredskab har noteret sig høringssvarernes generelle bemærkninger til lovudkastet.

2.2. Nærmere udmøntning i bekendtgørelser og behov for vejledning

Dansk Erhverv, IT-Branchen, DI Digital, Rådet for Digital Sikkerhed og Teleindustrien bemærker, at 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 de endnu ikke kender indholdet af. Høringsspartener opfordrer i den forbindelse til, at Ministeriet for Samfundssikkerhed og Beredskab foretager en grundig inddragelse af alle interessenter i udarbejdelsen af udkast til bekendtgørelser. Høringssvarerne påpeger endvidere, at erhvervslivet har behov for, at visse af lovens begreber defineres nærmere i bekendtgørelser eller vejledningsmateriale. Dette omfatter lovforslagets definitioner af kritiske netkomponenter, risikostyring, IKT-produkter, -tjenester og -processer, og forpligtelsen til registrering af IP-intervaller.

DI Digital og Rådet for Digital Sikkerhed anfører, at det fremgår af lovforslaget, at dele af den konkrete regulering på området efterfølgende vil blive udmøntet i bekendtgørelser, hvor lovforslaget herunder indeholder en række ministerbemyndigelser med mulighed for at ”fastsætte nærmere regler”. DI Digital og Rådet for Digital Sikkerhed bemærker, at dette skabere en vis fleksibilitet hos myndighederne, men gør det ligeledes svært at gennemskue omfanget, rækkevidden og proportionaliteten af krav og forpligtelser, som herved skaber usikkerhed for virksomheder i telesektoren. DI Digital og Rådet for Digital Sikkerhed opfordrer i den forbindelse til, at interessenter fra branchen involveres i udarbejdelsen af disse samt at der planlægges en tilstrækkelig lang frist når disse sendes i høring. Endelig bemærker DI Digital og Rådet for Digital Sikkerhed, at for at indfri lovforslagets ambitioner ses generelt et behov for klare definitioner og vejledning, herunder for at sikre, at implementeringen ikke øger byrderne for virksomheder i telesektoren.

Ministeriet for Samfundssikkerhed og Beredskab bemærker, at der med lovforslaget bl.a. lægges op til, at visse af lovens krav udmøntes nærmere i bekendtgørelser. Det gælder bl.a. de foreslåede bestemmelser i §§ 5, stk. 3 (foranstaltninger), 7, stk. 4 og 5 (underretnings- og oplysningspligter) og 8, stk. 4 (væsentlige hændelser). Formålet med muligheden for at fastsætte nærmere regler i bekendtgørelser er bl.a. at sikre, at der i nødvendigt omfang hurtigere kan gennemføres ændringer på baggrund af eksempelvis den teknologiske udvikling eller ændringer i trusselsbilledet.

Ministeriet for Samfundssikkerhed og Beredskab er enig i vigtigheden af, at der sker en tæt inddragelse af alle relevante interessenter i forbindelse med udarbejdelsen af bekendtgørelserne.

Endvidere har Ministeriet for Samfundssikkerhed og Beredskab noteret sig høringsparternes ønske om klare definitioner og vejledningsmateriale som supplement til lovudkastet. Ministeriet bemærker i den forbindelse, at Styrelsen for Samfundssikkerhed vil udarbejde vejledningsmateriale, som uddyber lovens krav og definitioner nærmere. Styrelsen for Samfundssikkerhed vil i den

forbindelse så vidt muligt sikre, at branchen inddrages i forbindelse med udarbejdelsen af vejledningsmaterialet.

I forlængelse heraf bemærker Ministeriet for Samfundssikkerhed og Beredskab, at det er blevet præciseret i lovforslaget, at teleudbydere i overensstemmelse med forvaltningslovens § 7 i fornødent omfang vil kunne få vejledning og bistand fra Styrelsen for Samfundssikkerhed. Det indebærer bl.a. bistand til nærmere forståelse af lovens krav, definitioner mv.

2.3. Definitionen af et ledelsesorgan

Dansk Erhverv, IT-Branchen, DI Digital, Rådet for Digital Sikkerhed og Teleindustrien bemærker, at det fremgår af lovforslagets § 6, stk. 1, at teleudbydernes ledelsesorganer skal godkende og føre tilsyn med de foranstaltninger til risikostyring, som teleudbyderen skal have, samt at ledelsesorganerne skal deltage i relevante kurser om risikostyring mv., jf. forslaget § 6, stk. 2.

DI Digital og Rådet for Digital Sikkerhed anfører, at lovforslaget stiller krav til, at foranstaltninger godkendes af teleudbyderens ledelsesorgan, ligesom der i § 6, stk. 2, stilles krav til, at ledelsesorganet skal deltage i relevante kurser om styring af informationssikkerhedsrisici og tilskynde til, at tilsvarende kurser tilbydes til udbyderens øvrige ansatte. Høringsparterne bemærker i den forbindelse, at det ikke præciseres yderligere, hvilken enhed eller personkreds, begrebet ledelsesorgan dækker over.

Advokatrådet bemærker, at der med lovforslaget lægges op til, at medlemmerne af ledelsesorganet skal deltage i relevante kurser om styring af informationssikkerhedsrisici og tilskynde til at tilsvarende kurser tilbydes til udbyderens øvrige ansatte, og at denne forpligtelse af strafbelagt. Advokatrådet opfordrer til, at det i lovforslaget behandles nærmere, om f.eks. et medlem af ledelsesorganet, der ikke konkret har ansvar for eller indblik i cybersikkerhedsmæssige forhold hos teleudbyderen, kan holdes strafferetlig ansvarlig, såfremt medlemmet har deltaget i beslutninger eller dispositioner som medlem

af ledelsesorganet, der efterfølgende viser sig at have ført til en overtrædelse af kravene i § 6.

Lov om aktie- og anpartsselskaber, jf. lovbekendtgørelse nr. 1168 af 1. september 2023 (selskabsloven), definerer i § 5, nr. 4, 'det centrale ledelsesorgan' som a) bestyrelsen i selskaber, der har en direktion og en bestyrelse, b) direktionen i selskaber, der alene har en direktion og c) direktionen i selskaber, der både har en direktion og et tilsynsråd. Selskabsloven finder dog alene anvendelse for aktie- og anpartsselskaber, jf. lovens § 1, stk. 1.

Lov om visse erhvervsdrivende virksomheder, jf. lovbekendtgørelse nr. 249 af 1. februar 2021 (LEV-loven), definerer i lovens § 4 a, nr. 2, en ledelse, som 'medlemmer af bestyrelse, direktion eller et tilsvarende ledelsesorgan'.

LEV-loven finder anvendelse for enkeltmandsvirksomheder, interessentskaber, kommanditselskaber, andelsselskaber (andelsforeninger) samt andre selskaber og foreninger med begrænset ansvar, som ikke er omfattet af selskabsloven, lov om erhvervsdrivende fonde eller §§ 133-154 i lov om forvaltere af alternative investeringsfonde m.v., jf. LEV-lovens § 1, stk. 2.

Ministeriet for Samfundssikkerhed og Beredskab har bl.a. på baggrund af de indkomne høringssvar foretaget en præcisering af begrebet 'ledelsesorgan', således at der nu af de specielle bemærkninger til lovforslagets § 6 bl.a. fremgår, at begrebet 'ledelsesorgan' i NIS 2-direktivet skal forstås i overensstemmelse med definitionerne af henholdsvis det centrale ledelsesorgan i selskabslovens § 5, nr. 4, og ledelsen i LEV-lovens § 4 a, nr. 2.

2.4. Beredskabssituationer og andre ekstraordinære situationer

Dansk Erhverv, IT-Branchen, DI Digital, Rådet for Digital Sikkerhed og Teleindustrien bemærker, at det fremgår af bemærkningerne på side 215 i høringversionen af 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”. Høringsparterne fremhæver i den forbindelse, at det fremgår af bemærkningerne, at definition svarer til definitionen i den gældende lovgivning, hvilket ikke er korrekt.

Ministeriet for Samfundssikkerhed og Beredskab bemærker, at der i forhold til definitionen ”beredskabssituationer og andre ekstraordinære situationer” er tale om en videreførelse af den gældende definition af beredskabssituationer og andre ekstraordinære situationer, dog således, at definitionen udvides til også at omfatte situationer, hvor der potentielt kan opstå større katastrofer eller hændelser, og hvor det kan være nødvendigt at indføre særlige foranstaltninger vedrørende net og tjenester med henblik på at kunne opretholde samfundets funktioner. I lyset af det aktuelle trusselsbillede har udvidelsen til formål at udvide Styrelsen for Samfundssikkerheds handlemuligheder i beredskabssituationer og i andre ekstraordinære situationer.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 2, nr. 1.

2.5. Sikkerhedsgodkendelser

Dansk Erhverv, IT-Branchen, DI Digital, Rådet for Digital Sikkerhed og Teleindustrien bemærker, at der bør skabes et lovgivningsmæssigt regime for sikkerhedsgodkendelser, der indeholder tydelige og gennemskuelige krav for teleudbyderne. Det fremhæves endvidere, at høringsparterne gerne ser, 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 teleudbyderne får sikkerhedsgodkendt.

DI Digital og Rådet for Digital Sikkerhed anfører, at de finder det uklart, hvem der er omfattet af lovforslagets krav om

sikkerhedsgodkendelser, herunder om leverandører ligeledes skal godkendes.

Fiberalliancen anfører, at det af lovforslagets § 17 fremgår, at medarbejdere hos teleudbydere samt repræsentanter for disse udbydere skal sikkerhedsgodkendes af Center for Cybersikkerhed (nu Styrelsen for Samfundssikkerhed).

Med den foreslåede § 16, stk. 1, lægges der op til, at medarbejdere hos væsentlige og vigtige teleudbydere og repræsentanter for disse udbydere skal sikkerhedsgodkendes af Styrelsen for Samfundssikkerhed, når 1) det er nødvendigt i forhold til den pågældendes adgang til klassificeret information eller til de funktioner, som den pågældende skal varetage, eller 2) den pågældende varetager kontakten til Styrelsen for Samfundssikkerhed i relation til beredskabet i henhold til regler, der er udstedt i medfør af § 13, stk. 3.

Som det fremgår af den foreslåede § 16, stk. 2, vil der blive fastsat regler om ansøgninger vedrørende sikkerhedsgodkendelser, herunder betingelser for indgivelse af sådanne ansøgninger samt meddelelse og tilbagekaldelse af sikkerhedsgodkendelser i en bekendtgørelse. Det fremgår af de specielle bemærkninger til § 16, at dette bl.a. omfatter administrative krav i forbindelse med indgivelse af en ansøgning, krav om afmelding, hvis en person ikke længere har en funktion, som forudsætter en sikkerhedsgodkendelse, og bestemmelser om, at afgørelsen tilbagekaldes, hvis en person ikke længere opfylder kravene til godkendelsen.

Ministeriet for Samfundssikkerhed og Beredskab har i den forbindelse noteret sig, at høringsparterne har udtrykt et ønske om nærmere konkretisering af personkredsen, der vil være omfattet af kravet om sikkerhedsgodkendelser. Som det fremgår ovenfor er ministeriet enig i vigtigheden af, at der sker en tæt inddragelse af alle relevante interessenter i forbindelse med udarbejdelsen af bekendtgørelserne.

2.6. Brud på persondatasikkerheden

Datatilsynet bemærker, at det fremgår af databeskyttelseslovens § 1, stk. 3, at regler om behandling af personoplysninger i anden lovgivning, som ligger inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger, går forud for reglerne i denne lov, og at der er fastsat sådanne særregler i telelovens § 8, stk. 2, nr. 2. Disse regler forpligter udbydere af offentlige tilgængelige elektroniske kommunikationsnet og -tjenester til at underrette Digitaliseringsstyrelsen (tidligere Erhvervsstyrelsen) om brud på persondatasikkerheden, når bruddet opstår i relation til udbuddet af sådanne tjenester.

Ministeriet for Samfundssikkerhed og Beredskab har tilrettet lovforslaget i overensstemmelse med Datatilsynets bemærkninger, således at det nu fremgår, at anmeldelser af brud på persondatasikkerheden skal ske til Digitaliseringsstyrelsen og ikke Datatilsynet.

Der henvises i øvrigt til lovforslagets pkt. 3.8.3.2.

2.6. Økonomiske- og administrative byrder

Dansk Erhverv, IT-Branchen, DI Digital, Rådet for Digital Sikkerhed og Teleindustrien bemærker, 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.

DI Digital og Rådet for Digital Sikkerhed henleder opmærksomheden på, at lovforslagets krav om, at teleudbydere uden unødigt ophold underretter Center for Cybersikkerhed (nu Styrelsen for Samfundssikkerhed) og CSIRT'en om enhver væsentlig hændelse, medfører unødige administrative byrder, da teleudbydere skal underrette flere instanser. I tilfælde af væsentlige hændelser, der netop

har karakter af kritiske samfundssituationer, er det ikke effektivt at skulle bruge tid på at underrette flere steder, men derimod at allokere virksomhedens ressourcer til at bidrage til at løse den pågældende situationen. Høringsparterne ser derfor, at underretningerne til Center for Cybersikkerhed (nu Styrelsen for Samfundssikkerhed) og CSIRT'en sker via én fælles digital indgang, som sikrer, at virksomheden kun skal foretage én samlet underretning, som derefter fordeles til relevante myndigheder.

Ministeriet for Samfundssikkerhed og Beredskab bemærker, at det bl.a. fremgår af lovforslagets pkt. 6 om økonomiske og administrative konsekvenser for erhvervslivet mv., at de samlede administrative omkostninger for erhvervslivet er over 4 mio. kr. Det har dog ikke været muligt at gennemføre en AMVAB-måling af konsekvenserne forud for fremsættelsen af lovforslaget i Folketinget. Denne vil derfor blive foretaget ex post efter lovforslagets ikrafttræden.

Det fremgår endvidere af lovforslaget, at det ikke har været muligt at foretage en kvantificering af de erhvervsøkonomiske konsekvenser for erhvervslivet forud for den offentlige høring. Det vurderes foreløbigt, at lovforslaget medfører øvrige efterlevelseskonsekvenser for erhvervslivet på mindre end 10 mio. kr. De erhvervsøkonomiske konsekvenser for erhvervslivet vil blive kvantificeret nærmere af Ministeriet for Samfundssikkerhed og Beredskab snarest muligt efter lovens ikrafttræden.

Ministeriet for Samfundssikkerhed og Beredskab bemærker, at det fremgår af den foreslåede bestemmelse i § 30, at ministeren for samfundssikkerhed og beredskab kan fastsætte regler om digital kommunikation, herunder om anvendelsen af bestemte it-systemer og særlige digitale formater samt digital signatur eller lignende.

Som nærmere beskrevet i lovforslagets pkt. 3.3.1., indgives underretninger om hændelser i dag via selvbetjeningsløsningen virk.dk. Når teleudbydere indgiver en hændelsesunderretning på virk.dk, fordeles denne automatisk til Styrelsen for Samfundssikkerhed (tidligere Center for Cybersikkerhed).

Ministeriet for Samfundssikkerhed og Beredskab forventer, at hændelsesunderretningen fremover på tilsvarende vis vil foregå via selvbetjeningsløsningen virk.dk, og at hændelsesunderretningen efter indgivelsen automatisk vil blive fordelt til de myndigheder og/eller sektorer, der er angivet som modtager af indberetningen.

3. Lovforslaget i forhold til lovudkastet

I forhold til det udkast til lovforslag, der har været i offentlig høring, indeholder det fremsatte lovforslag følgende indholdsmæssige ændringer:

- Afgørelseskompetencen i den foreslåede § 3, stk. 2, ændres således, at der for de i bestemmelsens nr. 1-5 nævnte teleudbydere ikke skal træffes en afgørelse af Styrelsen for Samfundssikkerhed, men at teleudbyderen selv skal vurdere, om den er omfattet de oplyste kriterier. Ændringen skal navnlig ses i lyset af den tilsvarende ordning i forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven). Det bemærkes, at kriterierne i bestemmelsens nr. 1-5 vil blive udmøntet nærmere i en bekendtgørelse, ligesom de vil blive suppleret af vejledningsmateriale. Der henvises til den foreslåede bestemmelse i § 3, stk. 2, og bemærkningerne hertil.
- I den foreslåede § 13 er der blevet tilføjet et stk. 6 og 7 vedrørende teleudbyderes forpligtelser i beredskabssituationer og andre ekstraordinære situationer. Bestemmelserne er en videreførelse af gældende ret og er indsat i loven på grund af kravenes indgribende karakter.
- Begreberne 'kommercielt formål' og 'ikke accessorisk del af virksomheden' er blevet beskrevet nærmere i bemærkningerne til den foreslåede bestemmelse i § 3, stk. 1.
- Foranstaltningerne efter den foreslåede § 5, stk. 1, er blevet uddybet nærmere. Der henvises til bemærkningerne til den foreslåede § 5, stk. 1.
- Kriterier for at anse en hændelse for væsentlig efter den foreslåede § 8, stk. 3, er blevet uddybet. Der henvises til bemærkningerne til den foreslåede § 8, stk. 3.

Herudover er der foretaget ændringer af sproglig, redaktionel og lovteknisk karakter.