Ministeriet for Samfundssikkerhed og Beredskab

E-mail til: mssb@mssb.dk

Sagsnr.: 2025-75

16. maj 2025

Høringssvar til høring over udkast til bekendtgørelser vedr. forslag til lov om sikkerhed og beredskab i telesektoren

Teleindustrien (TI), Dansk Erhverv (DE), DI Digital (DI) og IT-Branchen (ITB) skal indledningsvis takke for muligheden for at komme med bemærkninger til de fire bekendtgørelser, der skal udstedes i medfør af lov om sikkerhed og beredskab i telesektoren (L 142).

Høringssvaret er opdelt i en række generelle bemærkninger, og herefter gennemgås en række konkrete bemærkninger til hver enkelt af de fire bekendtgørelser.

Generelle bemærkninger

1.1. Ros til bekendtgørelsernes opdeling og sproglige udformning:
Medlemmerne fra TI, DE, DI og ITB vil gerne rose Ministeriet for Samfundssikkerhed og Beredskab (MSSB) for det gode arbejde, der er gjort med opsplitning af de tidligere bekendtgørelser og sammensætning af reglerne i nye bekendtgørelser. Den nye opdeling af emner virker gennemtænkt og meningsfuld, og det har ved gennemlæsning givet meget god mening. Ligeledes ser medlemmerne meget positivt på den sproglige oprydning og forenkling, der også er foretaget, eksempelvis i navngivningen af pligtsubjektet, der nu går under det mere mundrette ord *"teleudbyder"* i stedet for den tidligere term *"udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester*".

1.2. Bekendtgørelsen om sikkerhedsgodkendelse:
TI, DE, DI og ITB ser positivt på, at MSSB har lyttet til de udfordringer, som teleudbyderne har på dette område, og på den baggrund har udarbejdet en bekendtgørelse, der giver tydeligere regler på området. Der er dog en række bestemmelser, som TI, DE, DI og ITB mener, bør præciseres. Dette vil blive uddybet under de konkrete bemærkninger.

TI, DE, DI og ITB vil allerede her fremhæve, at bekendtgørelsesudkastet efter TI, DE, DI og ITB's opfattelse vil medføre flere anmodninger om sikkerhedsgodkendelse i fremtiden og herudover også, at bekendtgørelsen flere steder anvender begreber, der vil blive svært for medlemmerne at fortolke i praksis, medmindre reglerne tydeliggøres yderligere, og der udarbejdes vejledning om den praktiske anvendelse til teleudbyderne.

1.3. Behov for tydeliggørelse af, hvad definitionen af "kritiske netkomponenter, systemer og værktøjer" konkret omfatter:

Som TI, DE, DI og ITB også redegjorde for i høringssvaret til lovforslaget til lov om sikkerhed og beredskab i telesektoren, vil TI, DE, DI og ITB endnu en gang gerne understrege de store udfordringer, som medlemmerne har med at fastslå, hvilke "komponenter, systemer og værktøjer" der er kritiske i lovgivningens forstand, jf. definitionen af *"kritiske netkomponenter, systemer og værktøjer",* som TI, DE, DI og ITB kan konstatere er videreført ordret i de nye bekendtgørelser.

For at undgå gentagelser, henvises til TI, DE, DI og ITB's generelle bemærkninger i høringssvaret til lov om sikkerhed og beredskab i telesektoren (herefter høringssvaret til lovforslaget).

Definitionen er helt grundlæggende for, hvordan sikkerhedsområdet håndteres i en televirksomhed. TI, DE, DI og ITB vil gerne understrege, at for at opnå en ensartet fortolkning og forståelse af definitionen i branchen og dermed sikre et passende beskyttelsesniveau af den kritiske teleinfrastruktur, har teleudbyderne brug for tydeligere rammer og myndighedernes vejledning til, hvad definitionen mere konkret indebærer i praksis.

1.4. Ledelsesorganet i relation til de foreslåede regler:

Det fremgår af MSSB's høringsnotat, 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."*

Det betyder for teleudbydere omfattet af selskabsloven, at ledelsesorganet er bestyrelsen i selskaber, der både har en direktion og en bestyrelse, jf. selskabslovens § 5, nr. 4.

Dermed skal alle teleselskabers bestyrelsesmedlemmer fremover sikkerhedsgodkendes til HEM, jf. den foreslåede § 2, nr. 2, i bekendtgørelse om sikkerhedsgodkendelse af personer, som har funktioner inden for telesektoren, og bestyrelsen skal også godkende teleudbydernes rapport efter § 7 i bekendtgørelse om beredskab og krisestyring om beredskabsøvelser mv.

Ud fra en ansvarsbetragtning bør ledelsesansvar for, om lovgivningen er overholdt, pålægges dem, der til dagligt foretager dispositioner, der kan skade virksomheden eller andre, og det er i langt de fleste tilfælde direktionen. Det er derfor TI, DE, DI og ITB's medlemmers opfattelse, at mange af de opgaver, som NIS2-lovgivningen medfører, ligger bedst hos et eller flere direktionsmedlemmer eller alternativt i et udvalg, hvor enkelte bestyrelsesmedlemmer deltager eller lignende. TI, DE, DI og ITB forventer, at der vil være mulighed for, at bestyrelser kan uddelegere ansvar og opgaver til udvalg eller direktionsmedlemmer uden, at dette er på kant med reglerne.

Problemet med forståelsen af den ledelsesforankring, som NIS2 medfører, synes at eksistere i samtlige sektorer. SAMSIK har på den baggrund den 14. maj 2025 udgivet en vejledning kaldet "ledelsens rolle og opgaver", der adresserer nogle af disse spørgsmål. Imidlertid fremgår det af vejledningens side 4, at den ikke retter sig mod finans-, tele- og energisektorerne, da de har deres egen sektorspecifikke lovgivning. Men på netop dette område er det TI, DE, DI og ITB's opfattelse, at reglerne er ens, hvorfor MSSB bedes be- eller afkræfte, om teleudbyderne kan forholde sig til denne vejledning, eller om der påtænkes særskilt vejledning til telesektoren.

Konkrete bemærkninger

2.1. Udkast til bekendtgørelse om oplysnings- og underretningspligter vedrørende sikkerhed og beredskab i telesektoren:

2.1.1. Udvidelse af regimet for underretning af SAMSIK ved hændelser:
Det fremgår af både lovforslaget og den nye bekendtgørelses § 1, nr. 4, at den tidligere definition af, hvornår der er tale om en "beredskabssituation", bliver udvidet. Definitionen af "beredskabssituationer og andre ekstraordinære situationer" omfatter nu også større ulykker, katastrofer eller hændelser, hvor der er *risiko for* påvirkning af udbuddet af net og tjenester, modsat før, hvor begrebet dækkede over situationer, hvor det var nødvendigt at indføre særlige foranstaltninger.

Endvidere kan TI, DE, DI og ITB konstatere, at der med denne bekendtgørelses § 1, nr. 5, tillige indføres en helt ny definition af "internt beredskab", der lyder som følger: "*iværksættelse af særlige procedurer, processer og tiltag, der har til hensigt at håndtere en væsentlig hændelse, der ikke kan håndteres inden for teleudbyderens almindelige drift, herunder indkaldelse af ekstra eller særligt personel, etablering af særlige mødefora med leverandører, anvendelse af beredskabsplaner eller egentlig aktivering af krisestyringsplan".*

Samlet set er der derfor sket en udvidelse af, hvornår der er tale om en *"beredskabssituation",* og indført en tærskel for, hvornår en teleudbyder har aktiveret sit *"interne beredskab",* der også ligger lavere end den forståelse, som teleudbyderne tidligere har haft af begrebet "internt beredskab".

Medlemmerne skal derfor på baggrund af de nye regler ændre i deres processer for hændelsesrapportering. Det er her et uomtvisteligt faktum, at SAMSIK i fremtiden vil komme til at modtage flere straksunderretninger fra teleudbyderne. MSSB og SAMSIK har bekræftet, at dette også er hensigten, men TI, DE, DI og ITB vil dog stadig gerne gøre myndighederne opmærksomme på, at det nye underretningsregime vil blive mere byrdefuldt for teleudbyderne end det gamle regime. Både teleudbyderne og SAMSIK må således skulle forberede sig på at bruge flere ressourcer på at afsende, modtage og håndtere flere straksunderretninger i fremtiden.

2.1.2. Udvidelse og ny tilføjelse til § 3 om underretning om aftaleforhandlinger:
Generelt opfatter teleudbyderne bestemmelsen i § 3 som en bestemmelse, der primært retter sig mod en indkøbssituation, hvor teleudbyderen skal anskaffe sig nye komponenter, systemer eller værktøjer, der kan henføres under kategorien *"kritiske netkomponenter, systemer og værktøjer".* I den tidligere version af bestemmelsen fremgik det tydeligt, at bestemmelsen primært var målrettet disse situationer, og at teleudbyderen herudover også skulle underrette SAMSIK, inden teleudbyderen indgik aftaler om, at andre end teleudbyderen selv skulle varetage driften af de kritiske komponenter, systemer og værktøjer, dvs. bestemmelsen retter sig også mod aftaler om outsourcing o.lign.

Det bagvedliggende formål med bestemmelsen er, at SAMSIK skal have mulighed for at have et overblik over en teleudbyders varetagelse og drift af sine kritiske netkomponenter, systemer og værktøjer. Herudover skal SAMSIK også have mulighed for at

komme med sikkerhedsfaglige anbefalinger inden, at en kontrakt indgås, hvorfor forpligtelsen til at underrette træder i kraft ved påbegyndelse af aftaleforhandlinger.

Imidlertid ses den nye version af bestemmelsen at have fået en ny og ændret betydning. Det fremgår ikke længere tydeligt, at teleudbyderne skal underrette SAMSIK, inden der påbegyndes aftaleforhandlinger om køb af kritiske komponenter mv. Tværtimod er bestemmelsen opbygget således, at der fremhæves to tilfælde, hvor SAMSIK skal underrettes, nemlig ved:

1) aftaler om varetagelse af drift af de kritiske netkomponenter mv. og
2) ved væsentlige ændringer i teleudbyderens virksomhed, herunder fusioner, opkøb mv.

Baggrunden for denne ændring fremstår ikke tydeligt for teleudbyderne, og MSSB opfordres til at præcisere i bestemmelsen, at forpligtelsen først og fremmest vedrører indgåelse af aftaler om drift af kritisk infrastruktur samt anskaffelse af kritiske netkomponenter mv.

Særlige bemærkninger til § 3, stk. 1, nr. 2:
Det fremgår af § 3, stk. 1, nr. 2, at teleudbydere skal underrette SAMSIK forud for, at der indgås aftaler om væsentlige ændringer i teleudbyderens virksomhed, *herunder ved opkøb, fusioner og frasalg, der relaterer sig til teleudbyderens kritiske netkomponenter, systemer og værktøjer.*

Forpligtelsen er ny, og TI, DE, DI og ITB finder bestemmelsen uklar og potentielt enormt byrdefuld.

Det er på flere områder uklart for teleudbyderne, hvordan bestemmelsen skal forstås og fortolkes:

- Det er teleudbyderne, der er pligtsubjektet i bestemmelsen. Men teleudbyderne ejes for de fleste selskabers tilfælde af andre selskaber i forskellige ejerkonstruktioner. Ejerselskaberne, som kan være udenlandske selskaber, kan være flere led væk fra teleselskabet. Ejerne inddrager ikke nødvendigvis teleudbyderne i deres beslutninger om køb eller frasalg relateret til teleudbyderens virksomhed. Der er dermed ikke overensstemmelse mellem pligtsubjektet i bekendtgørelsen (teleudbyderen) og de selskaber, som i de fleste tilfælde indleder sådanne forhandlinger (ejerkredsen), og en teleudbyder vil i praksis ikke blive inddraget tids nok i en sådan sag til, at SAMSIK kan underrettes forudgående.

- Området for virksomheders opkøb, frasalg, fusioner etc. reguleres af andre regelsæt, herunder investeringsscreeningsloven og reglerne om sektorspecifik fusionskontrol, der jo netop er lavet til at favne meget lignende situationer. Ingen af disse regelsæt kræver forudgående underretning inden, at aftaleforhandlinger påbegyndes, og de indeholder også klare tærskelværdier for, hvornår og hvordan der skal underrettes. Derfor virker et krav om forudgående underretning inden, at aftaleforhandlinger påbegyndes, meget byrdefuldt.

  Teleudbyderne vil i den forbindelse gerne opfordre MSSB til at undersøge, om formålet med bestemmelsen kan opnås ved at koble SAMSIK op på et af de eksisterende regimer for myndighedsunderretning, eksempelvis således, at SAMSIK orienteres om teleudbyderes opkøb, salg og fusioner gennem Erhvervsstyrelsen eller konkurrencemyndighederne. En sådan løsning ville lette byrden hos den enkelte teleudbyder, da denne dermed ikke skal underrette flere forskellige myndigheder i

disse situationer.

- Det er uklart, hvordan en "væsentlig ændring" skal forstås i mere selskabsretlig forstand. Er det enhver ændring i ejerskab over teleudbyderen eller kun ved ændringer i ejerskab, der tillige indebærer en ændring i, hvem der har kontrol over teleudbyderen? Hvis førstnævnte mod forventning er tilfældet, skal børsnoterede teleudbydere underrette SAMSIK hver gang, der frasælges eller opkøbes et større antal aktier i televirksomheden, og det kan næppe være hensigten.

- Hvis formålet med bestemmelsen er at sikre særlig opmærksomhed på opkøb af mindre selskaber med kritisk infrastruktur, som har et lavere sikkerhedsniveau og dermed vil udgøre en sikkerhedsrisiko, når dette selskabs systemer mv. integreres i teleudbyderens systemer mv., er det ikke efter TI, DE, DI og ITB's opfattelse nødvendigt med et krav om forudgående underretning for, at SAMSIK kan foretage denne vurdering og varetage dette hensyn. I det tænkte tilfælde, hvor et mindre selskab med kritisk infrastruktur erhverves, kunne et krav om, at SAMSIK blev underrettet i forbindelse med den endelige aftaleindgåelse, være tilstrækkeligt til at varetage det bagvedliggende hensyn. Desuden opnås der i praksis først viden om potentielle sikkerhedsrisici på et langt senere tidspunkt end ved de første, spæde aftaleforhandlinger.

- Det fremgår af bestemmelsen, at både det overdragende selskab og det modtagende selskab skal underrette SAMSIK. Af hensyn til en effektiv administration og lavest mulige administrative byrde bør forpligtelsen til underretning af SAMSIK kun placeres på én af parterne, fx den part, som køber et selskab/dele af et selskab på samme måde, som anmeldelsespligten i investeringsscreeningsloven påhviler den investerende/ købende part.

TI, DE, DI og ITB foreslår på den baggrund, at de to områder for henholdsvis aftaleindgåelse om indkøb og drift af kritiske netkomponenter mv. og de selskabsmæssige overdragelser opdeles i to separate bestemmelser. For de selskabsmæssige overdragelser skal underretningen ske senere i processen, og det skal fastlægges, om det er overdragende eller modtagende selskab, der er pligtsubjektet.

2.1.3. <u>§ 14 om aktindsigt:</u>
Det fremgår af § 14, at der ikke er aktindsigt i underretninger efter §§ 2 og 3, § 5, stk. 1 og 3, §§ 6 og 7. Herved omfattes straksunderretningerne i §§ 11-13 ikke af undtagelsen for aktindsigt, og straksunderretningerne er heller ikke undtaget fra aktindsigt i medfør af reglerne i lov om sikkerhed og beredskab i telesektoren.

Af sikkerhedsmæssige hensyn opfordrer TI, DE, DI og ITB til, at det sikres, at der ikke kan gives aktindsigt i oplysninger og underretninger om aktivering og de-aktivering af en teleudbyders interne beredskab. Kan §§11-13 ikke undtages fra aktindsigt, bør SAMSIK som minimum foretage en høring af den berørte teleudbyder, hvis der modtages en anmodning om aktindsigt i underretninger og oplysninger vedrørende det interne beredskab, så udbyderen har mulighed for at begrunde eventuelle ønsker om at få sensitive informationer undtaget fra aktindsigt.

2.2. Udkast til bekendtgørelse om beredskab og krisestyring i telesektoren:

Samlet set er mange af bestemmelserne i denne bekendtgørelse en videreførsel af den gældende lovgivning. TI, DE, DI og ITB kan herudover konstatere, at bekendtgørelsens begreber er opdaterede og gjort mere tidssvarende, hvilket er positivt.

2.2.1. Håndtering af klassificerede oplysninger, § 5, nr. 3:
Det fremgår af § 5, nr. 3, at væsentlige teleudbyderes krisestyringsplan bl.a. skal indeholde følgende: "*3) En procedure for modtagelse og håndtering af oplysninger, herunder klassificerede informationer fra SAMSIK om en beredskabssituation eller anden ekstraordinær situation.*"

TI, DE, DI og ITB er klart over, at dette krav ikke er nyt, men det fremstår uklart, hvordan dette krav skal håndteres i praksis. TI, DE, DI og ITB antager, at der med bestemmelsen menes, at teleudbyderne skal have et set up, der er i stand til at håndtere "klassificeret information", sådan som det er beskrevet i sikkerhedscirkulæret. I sikkerhedscirkulæret stilles der strenge krav til opbevaring af klassificeret information og henset til, at sikkerhedscirkulæret er en interministeriel forskrift og således møntet på myndighedernes håndtering, vil teleudbyderne gerne have vejledning fra myndighederne i, hvordan det forventes, at klassificeret information håndteres og opbevares. Det fremstår endvidere uklart, hvilket klassifikationsniveau som myndighederne forventer, at teleudbyderne skal være i stand til at kunne håndtere.

2.2.2. Prioritering af telefoni via dataforbindelser, § 9:
TI, DE, DI og ITB forstår bestemmelsen som en helt ny bestemmelse, der giver SAMSIK mulighed for at påbyde teleudbyderne at etablere en prioriteringsordning, der giver forrang til beredskabsaktører via dataforbindelser som f.eks. bredbåndstelefoni. Bestemmelsen erstatter det gamle kapitel 2 i bekendtgørelse nr. 261 om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer.

TI, DE, DI og ITB ser positivt på bestemmelsen, idet der er tale om en lempelse af reglerne i tråd med den teknologiske udvikling, hvorefter mobiltelefoni er det mest benyttede kommunikationsmiddel.

Endvidere ser TI, DE, DI og ITB også positivt på, at forpligtelsen til at etablere sikret adgang i fastnettet er udgået særligt henset til, at ordningen siden sin indførsel aldrig har været i brug.

TI, DE, DI og ITB hører dog gerne SAMSIK's eller MSSB's bemærkninger til, om og hvordan myndighederne forventer at benytte påbudsmuligheden i § 9.

2.2.3. Prioritering af adgang i mobilnet, § 10:
TI og SAMSIK har været i dialog om denne bestemmelse i lang tid, og med denne bekendtgørelse foreligger der nu den fornødne hjemmel til at fortsætte arbejdet. De tekniske specifikationer for løsningen er fuldt afklaret i en teknisk arbejdsgruppe mellem teleudbyderne og SAMSIK, men der mangler fortsat en udarbejdelse af en brancheaftale på dette område.

2.3. Udkast til bekendtgørelse om risikostyring og sikkerhed i telesektoren:

Bekendtgørelsen er i meget vidt omfang en videreførsel af regler fra den gældende bekendtgørelse om sikkerhed i net og tjenester, jf. bekendtgørelse nr. 259 af 22. februar 2021, og TI, DE, DI og ITB har ikke fundet anledning til at afgive konkrete bemærkninger til denne.

2.4. Udkast til bekendtgørelse om sikkerhedsgodkendelser i telesektoren

TI, DE, DI og ITB's bemærkninger til denne bekendtgørelse er opdelt i generelle bemærkninger og i konkrete bemærkninger til de specifikke bestemmelser i bekendtgørelsen:

2.4.1. Generelle bemærkninger til den nye bekendtgørelse:

Som nævnt ser TI, DE, DI og ITB meget positivt på, at der nu arbejdes med at gøre området for sikkerhedsgodkendelser lettere at håndtere for teleudbyderne. Bekendtgørelsen forsøger at opstille nogle mere faste regler for, hvilke roller i televirksomheden, som myndighederne har en forventning om, bliver sikkerhedsgodkendt.

TI, DE, DI og ITB kan dog efter gennemlæsning af bekendtgørelsesudkastet konstatere, at bekendtgørelsen vil medføre væsentligt flere anmodninger om sikkerhedsgodkendelser, hvilket vil øge presset på et i forvejen meget presset område med høj sagsbehandlingstid. Dette faktum er i sig selv bekymrende.

Ved siden af de øgede antal sikkerhedsgodkendelsesanmodninger, som den nye bekendtgørelse vil medføre, vil TI, DE, DI og ITB gerne fremhæve følgende problematiske forhold:

1. Den mellemliggende periode mellem ansøgning og godkendelse:
   De lange sagsbehandlingstider medfører, at der er en stor gruppe personer, som befinder sig i en mellemliggende periode, hvor de endnu ikke er sikkerhedsgodkendt på trods af, at de varetager en rolle, hvor det er påkrævet. For denne periode vil teleudbyderne gerne have MSSB's angivelse af en forventet og helst garanteret sagsbehandlingstid, da det giver teleudbyderne mulighed for at indrette sig efter denne sagsbehandlingstid. Derudover bør MSSB angive, hvordan teleudbyderne kan forholde sig i perioden inden, at sikkerhedsgodkendelsen er opnået, så udbyderen får mulighed for at fortsætte varetagelsen af opgaver under ventetiden.

2. Udenlandsk arbejdskraft:
   Udviklingen i Danmark i de senere år har skabt en stigende efterspørgsel på medarbejdere med specialiserede kompetencer inden for en række områder, herunder nicheviden om teleinfrastruktur og systemer. Derfor er det vigtigt for teleudbyderne, at de kan rekruttere den nødvendige kvalificerede arbejdskraft uden for landets grænser både i form af ansatte internt i virksomhederne og ved at lægge opgaver hos leverandører beliggende i udlandet. For disse to grupper er det væsentligt, at de også kan sikkerhedsgodkendes, hvis de varetager en rolle, der kræver sikkerhedsgodkendelse.

   TI, DE, DI og ITB anerkender, at det stiller langt større krav til sagsbehandlingen, når der skal indhentes oplysninger fra myndigheder i andre lande til brug for sikkerhedsgodkendelsessagen. TI, DE, DI og ITB opfordrer dog til, at myndighederne opsætter så klare rammer som muligt for dette område, da det er en stor udfordring i praksis.

3. Søsterselskaber i andre nordiske lande:
   Flere af medlemmerne har nordiske søsterselskaber. Heri ligger der en specifik udfordring i, om det er i overensstemmelse med reglerne, hvis en svensk sikkerhedsgodkendt medarbejder drifter/reparerer/ændrer i nogle systemer, der befinder sig i Danmark og omvendt. For disse teleselskaber udrulles ofte de samme systemer og den samme form for infrastruktur, hvorfor dette spørgsmål er relevant for dem at få afklaret.

4. Mitigerende foranstaltninger:
   TI, DE, DI og ITB hører gerne myndighedernes vurdering af, om og i givet fald hvilke mitigerende foranstaltninger, der kan træde i stedet for en sikkerhedsgodkendelse i den mellemliggende periode.

5. Behov for forenkling af systemet
   Endelig vil TI, DE, DI og ITB gerne opfordre til, at hele systemet for sikkerhedsgodkendelser moderniseres og forenkles, hvor det er muligt. TI, DE, DI og ITB opfordrer til, at systemet ændres, så en sikkerhedsgodkendelse følger den person, der er sikkerhedsgodkendt, og dermed ikke bortfalder, når en person skifter stilling mellem kritiske sektorer eller mellem teleudbydere. I dag skal den modtagende virksomhed igangsætte en ny anmodning om sikkerhedsgodkendelse, fordi godkendelsen netop ikke følger personen.

   Endvidere opfordrer TI, DE, DI og ITB til, at myndighederne i højere grad accepterer hinandens sikkerhedsgodkendelser. Som tingene er i dag, skal den samme person ofte have sikkerhedsgodkendelse til samme klassifikationsniveau hos flere forskellige myndigheder, f.eks. tre sikkerhedsgodkendelser til FE HEM, PET HEM og SINE HEM. Der skal således både foretages anmodninger og fornyelser af de tre typer af sikkerhedsgodkendelse til denne samme person, hvilket er unødigt byrdefuldt for både virksomheder og myndigheder.

Endelig skal TI, DE, DI og ITB understrege, at medlemmerne altid står til rådighed for en dialog med myndighederne om dette område. TI, DE, DI og ITB ser fortsat et stort behov for yderligere vejledning og dialog på området.

2.4.2. Konkrete bemærkninger til bekendtgørelsen om sikkerhedsgodkendelse:

2.4.3. Kapitel 1 om den omfattede personkreds:
Det fremgår af kapitel 1 i bekendtgørelsen, hvilke roller der kræver sikkerhedsgodkendelse til hhv. FORTROLIGT og HEM.

Nedenfor gennemgås rollerne og TI, DE, DI og ITB's bemærkninger:

§ 1, nr. 1: "Personer, der arbejder med håndteringen af væsentlige hændelser":
Det fremgår af § 2, nr. 6 i lovforslaget til lov om sikkerhed og beredskab i telesektoren, at håndtering af hændelser defineres som følgende:

"6) *Håndtering af hændelser: Enhver handling og procedure, der tager sigte på at forebygge, opdage, analysere og inddæmme eller at reagere på og reetablere sig efter en hændelse."*

Personkredsen, der arbejder med hændelser, er således meget bredt defineret i lovforslaget, hvilket får den konsekvens, at mange roller skal sikkerhedsgodkendes i relation til denne bestemmelse.

§ 1, nr. 2: "Personer, der arbejder med driftskontinuitet, herunder backup-styring og reetablering efter en katastrofe og krisestyring":
For disse roller fører en fortolkning til, at en stor del af teleudbydernes "kontorpersonale", der arbejder med området på et mere strategisk plan, f.eks. ved at skrive politikker eller krisestyringsplaner, ville blive omfattet.

§ 1, nr. 3: "Personer, der har adgang til at foretage ændringer i kritiske netkomponenter, systemer og værktøjer…":
Ved gennemlæsning af den foreslåede § 1, nr. 3, har TI, DE, DI og ITB bemærket, at bestemmelsen retter sig mod roller, der kan *foretage ændringer* i kritiske netkomponenter, systemer og værktøjer. Roller med læseadgang er der omvendt ikke fokus på. Derfor må reglen umiddelbart fortolkes og forstås således, at medarbejdere og eksterne konsulenter (herunder medarbejdere hos outsourcede partnere) gerne må have indsigt i og tilgå kritiske systemer så længe, at der alene er tale om at *læse* informationer. Informationer kunne være data såsom informationer omkring systemer og kritiske netkomponenter, herunder netværksdiagrammer, kapacitetsdata, informationer om opbygningen af infrastrukturen, løsninger og design. Denne sondring synes ikke hensigtsmæssig ud fra et sikkerhedsfagligt perspektiv, og TI, DE, DI og ITB hører gerne, om ovenstående fortolkning er korrekt.

§ 1, nr. 4: "Personer, der har særlig betroede roller og ansvar i forbindelse med anskaffelser vedrørende kritiske netkomponenter, systemer eller værktøjer, som er omfattet af underretningsforpligtelser i medfør af bekendtgørelse om underretning":
Denne personkreds er vanskelig at fastlægge og involverer medarbejdere fra indkøbsafdelinger, kommercielle, tekniske og juridiske afdelinger m.fl. Det er derfor svært definérbart, hvem der har en "særligt betroet rolle" i en indkøbsproces.

Hvis formålet med bestemmelsen er at adressere "insidertruslen" i en indkøbsproces og dermed retter sig mod den persongruppe, der kan påvirke eller træffe beslutning om, hvilken leverandør der vælges, bør dette tydeliggøres i bestemmelsen, så den ikke rammer andre grupper uden teknisk indsigt i det produkt, der erhverves, f.eks. jurister, der konciperer og forhandler aftalevilkår og priser.

§ 2, nr. 2: "Personer, der er del af ledelsesorganet i væsentlige teleudbydere":
Da ledelsesorganet skal fortolkes og forstås i overensstemmelse med de selskabsretlige regler, betyder det, at bestyrelserne hos teleudbyderne skal være HEM-godkendte. Omvendt er der ingen krav til direktionen, som reelt er den ledelse, der har ansvaret for virksomhedens daglige drift. TI, DE, DI og ITB betragter denne bestemmelse som udfordrende, jf. også kommentarerne ovenfor under 1.4.

§ 2, nr. 3: "Personer, der arbejder med risikoanalyse og informationssikkerhed i væsentlige enheder":
Der er rigtig mange roller, der arbejder på et mere strategisk plan med risikoanalyse og informationssikkerhed hos de væsentlige teleudbydere, f.eks. ved at udarbejde politikker, rådgive om regelforståelse, foretage interne kontroller af informationssikkerhedsniveauet eller mere generelt arbejde med "risk management" m.fl.

2.4.4. Ansøgninger om sikkerhedsgodkendelse, jf. § 8:
Det følger af § 8, at teleudbyderne skal udpege én kontaktperson for sikkerhedsgodkendelser, som SAMSIK skal underrettes om. TI, DE, DI og ITB skal her bemærke, at det er sårbart kun at have én kontaktperson, da det skaber udfordringer, hvis vedkommende er fraværende, f.eks. grundet ferie eller sygdom. TI, DE, DI og ITB vil derfor opfordre til, at MSSB præciserer bestemmelsen, så det i stedet bliver muligt at udpege flere kontaktpersoner eller stedfortrædere, da det vil lette samarbejdet mellem teleudbyderen og SAMSIK.

2.4.5. Påbud i relation til sikkerhedsgodkendelser, jf. § 9:
Den foreslåede § 9 giver SAMSIK mulighed for at give påbud om sikkerhedsgodkendelse af personale, der ikke er omfattet af §§ 1-4, og som har adgang til kritiske netkomponenter, systemer og værktøjer, hvis det er af væsentlig samfundsmæssig betydning.

Henset til den lange sagsbehandlingstid, kan det have store konsekvenser for teleudbyderen, hvis en medarbejder med kort eller ingen varsel fratages muligheden for at varetage sin funktion, indtil vedkommende er blevet sikkerhedsgodkendt. For at minimere påbuddets negative indvirkning bør sagsbehandlingen overstås hurtigst muligt i sådanne særlige tilfælde, og SAMSIK bør som minimum angive den forventede sagsbehandlingstid, så teleudbyderen kan indrette sig derefter.

2.4.6. Ansøgninger om forlængelse af sikkerhedsgodkendelse, § 10, stk. 6:
Det fremgår af § 10, stk. 6, 2. pkt., at: *"Er ansøgningen om forlængelse af en sikkerhedsgodkendelse indgivet inden fristen nævnt i 1. pkt., kan ansøgningen efter anmodning herom tillægges opsættende virkning."*

Det vil altid være i en teleudbyders interesse, at ansøgninger om forlængelse tillægges opsættende virkning, da det netop betyder, at personen må fortsætte sit arbejde under den gældende sikkerhedsgodkendelse, indtil en afgørelse om fornyelse er truffet.

Derfor virker det som et unødvendigt administrativt skridt, at der kræves en særskilt anmodning fra teleudbyderen om, at en ansøgning skal tillægges opsættende virkning. I praksis vil teleudbyderne sandsynligvis løse denne problematik ved at indsætte en standardtekst i alle ansøgninger om forlængelse, hvori der vil stå, at der ønskes opsættende virkning, såfremt fornyelsen ikke foreligger inden udløb af den gældende sikkerhedsgodkendelse. MSSB kunne på den baggrund overveje at fjerne teksten *"efter anmodning herom"* og i stedet blot fastslå, at ansøgninger, der er indgivet rettidigt, tillægges opsættende virkning.

Med venlig hilsen

Jakob Willer	Poul Noer	Anders S. Skovbakke	Troels Johansen
Direktør	Fagchef for telepolitik	Konsulent	Chefkonsulent
Teleindustrien	Dansk Erhverv	DI Digital	IT-Branchen