Broadnet AS
Rolfsbuktveien 4
Postboks 1, Fornebu
NO-1330 Fornebu

Org NO 890 164 072 MVA

broadnet.no

Forsvarsdepartementet
Postboks 8126 Dep.
0032 Oslo

Vår referanse:
AS/MEJ

Mottakers referanse:
2015/3139-254/FD V 3/ENWA

Dato/Sted:
Fornebu, 1. oktober 2018

Antall vedlegg:
1

INNSPILL TIL HØRING AV FORSKRIFTER TIL NY SIKKERHETSLOV - BROADNET AS

1 Innledning

Broadnet AS ("**Broadnet**") viser til brev fra Forsvarsdepartementet ("**FD**") datert 2. juli 2018 hvor forslag til forskrifter til ny sikkerhetslov sendes på høring. Dette er en viktig regulering – både for samfunnet og for de offentlige og private virksomhetene som blir berørt. Vi takker derfor for muligheten til å kommentere på innholdet. Broadnet vil i dette høringssvaret redegjøre for vårt syn på forslaget til forskrifter slik det er beskrevet i høringsnotatet ("**Høringsnotatet**").

Broadnet er i korte trekk positiv til både innretningen på forskriftforslaget og detaljeringen av de kravene myndighetene ønsker å stille til de regulerte aktørene. Samtidig ser vi med bekymring på at forslaget ikke tar tak i to helt grunnleggende utfordringer med den relativt generelle hjemmelsloven. Det foreslåtte regelverket stiller ingen presise krav til hvordan myndighetene skal gå frem for å identifisere grunnleggende nasjonale funksjoner eller underlegger private og offentlige aktører det nye regelverket. Innholdet i de nye, funksjonelle kravene til forsvarlig sikkerhetsnivå er dessuten høyst uklart. Det foreslåtte regelverket pålegger heller ikke de involverte myndighetene å gi den veiledningen som er nødvendig for å etterleve kravene. Det krever ikke mange forskriftsendringer å rette opp de aktuelle forholdene. Skulle mot formodning det endelige regelverket lide av de samme svakhetene, vil det skape store utfordringer for både involverte myndigheter og de regulerte aktørene når sikkerhetsloven med forskrifter trer i kraft.

Broadnet vil i punkt 3 knytte noen overordnete kommentarer til både forskriftsarbeidet og de prinsippene som ligger til grunn for innholdet. I punkt 4 kommenterer Broadnet de særlige forholdene FD har tatt opp i høringsnotatet. Avslutningsvis vil vi i punkt 5 knytte noen merknader til konkrete bestemmelser som ikke er dekket av punkt 3 og 4.

Vedlegget til høringssvaret inneholder "råd om og vurderingar av korleis eit organ bør stille seg i ei sak, og som organet har innhenta til bruk for den interne saksførebuinga si", jf. offentleglova § 5. Det beskriver også sikkerhetstiltak og andre forhold som vil kunne lette gjennomføringen av straffbare forhold, jf. offentleglova § 24. Vi ber derfor om at innholdet unntas offentlighet, eventuelt at departementet utsetter innsyn til senere i saksbehandlingen jf. offentleglova § 5 ettersom dokumentet gir et misvisende bilde av saken inntil saksbehandlingen er avsluttet.

2 Kort om Broadnet

Broadnet er en norsk leverandør av bredbånds- og telekommunikasjonstjenester med et eget landsdekkende fibernett. Vi tilbyr overføringskapasitet, internettaksess og datakommunikasjonstjenester til sluttbruker- og grossistmarkedet. Kundene våre består av små, mellomstore og store bedrifter samt til offentlig sektor. I tillegg selger vi bredbåndstjenester til forbrukere gjennom vårt heleide datterselskap Homenet AS. Broadnet eier også PowerTech Information AS, Xfiber AS, DataGuard AS, Lynet AS og Kvantel AS. Dette høringssvaret inngis på vegne av alle selskapene.

Broadnet har hovedkontor på Fornebu i Oslo, 447 ansatte og er eid av oppkjøpsfondet EQT Infrastructure III.

Broadnet leverer samfunnskritisk infrastruktur. Vi har derfor vært underlagt sikkerhetsloven siden Samferdselsdepartementets ("**SD**")/FDs vedtak 25. mars 2008. Broadnet er også underlagt sektorspesifikke sikkerhetskrav knyttet til elektronisk kommunikasjon (såkalt ekom). Vi har derfor lang erfaring med både den praktiske etterlevelsen av regelverket og hvilke utfordringer de gjeldende reglene skaper for både regulerte aktører og offentlig myndighet. Dette omfatter også samspillet mellom de sektorovergripende og de sektorspesifikke sikkerhetskravene.

3 Broadnets overordnede kommentarer til forskriftsutkastet

3.1 Broadnet syn på arbeidsprosessen knyttet til operasjonalisering av sikkerhetsloven gjennom forskriftene

I punkt 2.1 i høringsnotatet redegjør FD for hvordan arbeidet med forskriftsutkastet har vært organisert som et prosjekt med prosjektmedarbeidere fra ulike offentlige virksomheter. Videre fremgår det på side 9 i høringsnotatet:

> "Departementene i referansegruppen og etatene i arbeidsgruppen har blitt oppfordret til å involvere private virksomheter og interesseorganisasjoner i sin sektor i arbeidet, og prosjektet

> har gjennom dette fått verdifulle innspill. Det ble 22. mars 2018 avholdt et informasjonsmøte hvor alle instanser som ble hørt i forbindelse med høringen av NOU 2016:19 var invitert, og hvor det ble åpnet for spørsmål og innspill til arbeidet.
>
> [...] Departementet mener at prosessen har gitt et godt grunnlag for å komme frem til en form og et nivå på bestemmelsene som gjør at forskriftene vil bidra til å bedre det forebyggende sikkerhetsarbeidet i alle samfunnssektorene."

I punkt 1 i høringsnotatet viser FD til at Regelverket forutsetter at det etableres gode arenaer for dialog mellom myndighetene og virksomheter som underlegges loven. Broadnet er positiv til intensjonen om å involvere de regulerte aktørene i arbeidet. Vi er samtidig bekymret for at dette har skjedd i mindre grad enn forutsatt. Dette bærer høringsnotatet preg av.

Slik vi opplever forskriftsprosessen så langt har arbeidsgruppen vært flinke til å invitere sektormyndigheter med som bidragsytere. Broadnet har dessuten hatt en løpende og god dialog med vårt sektortilsyn, Nasjonal kommunikasjonsmyndighet ("**Nkom**"), om innholdet i de ulike forslagene.

Broadnet er på overordnet nivå positive til at myndighetene ønsker å få på plass et moderne rammeverk for sikkerhet så fort som mulig. Når det er sagt har vi fra starten opplevd at fristene for å gi innspill har vært så korte at det har gått utover kvaliteten på tilbakemeldinger fra både sektormyndigheter og bransjen. Vi har blant annet vært tvunget til å prioritere strengt hvilke deler vi skulle kommentere og hvor grundig. Vi har heller ikke fått anledning til å utrede hvilke konsekvenser sentrale forpliktelser vil få for både bransjen og samfunnet.

Videre oppfatter vi at deler av innholdet preges av hastverksarbeid, noe som også gjenspeiler seg i innholdet. Formodentlig skyldes dette ønsket om at det nye regelverket skal tre i kraft 1. januar 2019. Vi mener dette er problematisk, både som følge av at virkeområdet utvides ganske betraktelig[1] og fordi sikkerhetsloven overlater til forskriftene å operasjonalisere en rekke sentrale forpliktelser.

Utfordringen med denne tilnærmingen er at det gjenstår en rekke uavklarte spørsmål som enten må løses gjennom presiseringer i den endelige forskriftsteksten eller etterfølgende veiledning fra departement, sikkerhets- og sektormyndigheter. Det sistnevnte alternativet skaper en rekke

[1] På side 29 i Høringsnotatet fremgår det at så mange som 20-30 nye virksomheter vil bli underlagt ny sikkerhetslov bare i ekomsektoren.

utfordringer for de virksomhetene som skal forsøke å etterleve kravene. Overgangen til svært overordnede, funksjonelle krav forsterker, heller enn løser, dette problemet.

Vi vil i dette høringssvaret belyse det vi mener er de mest sentrale avklaringspunktene. Broadnet ber i tillegg FD og andre relevante myndigheter til å involvere aktører i de ulike bransjene i langt større grad. Dette vil redusere samfunnets kostnader og bedre sikkerheten. Broadnet ber også om at de aktuelle avklaringene foreligger før departement og sikkerhetsmyndighet går videre med utpekingen av virksomheter og skjermingsverdige objekt/infrastruktur slik at det er mulig å etterleve de pålagte kravene.

3.2 Forskriften må sikre at myndighetene følger den lovpålagte prosedyren for å underlegge virksomheter sikkerhetsloven

Den nye sikkerhetsloven etablerer en kronologisk, og logisk, seks-stegs-prosedyre for å utpeke og klassifisere virksomheter samt identifisere avhengigheter som må beskyttes. Det er utfordrende lese innholdet i, og rekkefølgen på, de fem stegene direkte ut av de prosessuelle reglene og definisjonene i sikkerhetsloven kapittel 1 og 2. Utover supplerende informasjon om klassifiseringen av skjermingsverdige objekt og infrastruktur, gir de foreslåtte forskriftene samtidig ingen veiledning om prosessen.

De seks stegene kan i korte trekk beskrives på følgende måte:

1. Fagdepartementet identifiserer og kategoriserer grunnleggende nasjonale funksjoner ("GNF")

Den nye sikkerhetsloven er ikke altomfattende, men beskytter tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser. Det første steget i prosessen blir dermed å identifisere og kategorisere hvilke funksjoner som f.eks. påvirker de øverste statsorganers virksomhet eller Norges økonomiske stabilitet og handlefrihet (se sikkerhetsloven § 1-5 nr. 1. a) og d)). Det er fagdepartementene som er ansvarlige for å gjøre dette innenfor sin sektor (se sikkerhetsloven § 2-1 første ledd litra a)). For å unngå at loven

favner for vidt[2] må grensene for hva som er en GNF nødvendigvis trekkes opp etter gitt kriterier – i praksis bortfallets omfang, lengde i tid og geografiske nedslagsfelt.

2. Sikkerhetsmyndigheten og fagdepartementene harmoniserer GNF på tvers av beslektede sektorer

Når fagdepartementene har identifisert og kategorisert GNF innenfor sin sektor, må utpekingen avstemmes på tvers av beslektede sektorer for å sikre at verdikjeden henger sammen. Dette er en nødvendig forutsetning dersom sikkerhetsloven skal gi en tverrsektoriell beskyttelse av nasjonale sikkerhetsinteresser.[3] En harmonisering hvor likeartede bransjer underlegges likeartede forpliktelser både når det gjelder omfang og kostnadene forbundet med å oppfylle kravene. Det er fagdepartementene som har ansvar for denne oppgaven og den må gjøres før vi får videre.

3. Fagdepartementene identifisere virksomheter som har vesentlig betydning for GNF

Neste steg i prosessen er at fagdepartementene identifiserer og deretter utpeker de virksomhetene som har "vesentlig betydning" for GNF innenfor den enkelte sektor etter sikkerhetsloven § 2-1 b), jf. § 1-3 første ledd litra b) og c). Vesentlighetskravet innebærer at fagdepartementet må gjøre en reell vurdering av om vilkåret er oppfylt for den enkelte virksomhet. Som det fremgår av merknadene til bestemmelsen fører dessuten ikke en eventuell utpeking i seg selv til at virksomheten underlegges plikter etter sikkerhetsloven.[4]

4. Fagdepartementet fatter vedtak om at loven gjelder for virksomheter som har vesentlig betydning for GNF

Når fagdepartementet har gjennomført de tre første stegene er det i posisjon til å fatte vedtak om at loven gjelder for virksomheter som råder over informasjon, informasjonssystemer mv. eller driver aktivitet som har avgjørende betydning for GNF (sikkerhetsloven § 1-3 første ledd

[2] Dersom GNF defineres på en slik måte at den dekker bortfall av alle typer tjenester/produksjon uansett lengde og geografisk nedslagsfelt vil f.eks. et lokalt, kortvarig, strømbrudd på Lindesnes gis på samme linje som et langvarig utfall i hele Oslo og Akershus.

[3] Dette kommer til uttrykk i blant annet NOU 2016:19 punkt 2.1 og i beskrivelsen av sikkerhetsmyndighetens oppgaver i sikkerhetsloven § 2-2.

[4] Se Prop. 153 L (2016-2017) side 166.

litra b) og c)). Utpekingen må skje slik at likeartede selskaper underlegges de samme pliktene. Den bør heller ikke virke konkurransevridende.

5. Fagdepartementet klassifiserer skjermingsverdige objekter og infrastruktur som kan skade GNF og fatter vedtak om utpeking av virksomheter som råder over dette

Først når fagdepartementene har identifisert GNF og utpekt relevante virksomheter er de i posisjon til å utpeke skjermingsverdige objekter og infrastruktur etter sikkerhetsloven § 7-1. Det skyldes definisjonen av hva som inngår. I første ledd fremgår det:

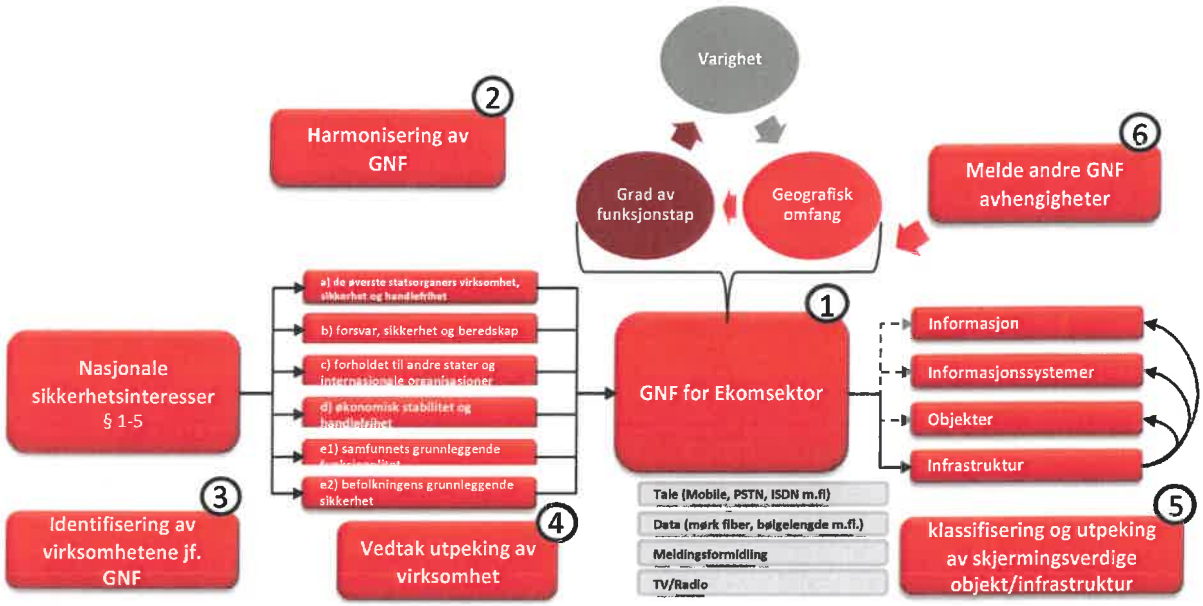
> "Objekter og infrastruktur er skjermingsverdige dersom det kan skade grunnleggende nasjonale funksjoner om de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse."

Slik Broadnet ser det, må de grunnleggende kriteriene for utpeking harmoniseres på tvers av sektorer. Dette sikrer en enhetlig praksis og likebehandling. Dette vil være dimensjonerende for hva som er et forsvarlig sikkerhetsnivå og derav også hvilke krav som deretter stilles til virksomhetenes håndtering. For at dette skal fungere på en tilsvarende harmonisert måte må det etableres vurderingskriterier og prosesser som sikrer at det blir sammenheng mellom utpeking av kritiske systemer innad i en sektor og på tvers av sektorer.

6. Utpekte virksomheter melder avhengigheter til andre virksomheter som skal beskytte GNF

Det siste steget går ut på at utpekte virksomheter melder avhengigheter til andre virksomheter som skal beskytte GNF. Dersom for eksempel et sykehus, en finanstjeneste eller et elkraftanlegg underlegges spesielle krav etter ny sikkerhetslov, må de ulike aktørene melde fra om dette til samtlige ekomleverandører i en anbudsprosess. Dette fører til at samtlige aktører som konkurrerer om leveransen blir informert om avhengigheten og kan ta høyde for dette ved prising og valg av tjeneste i tilbudet.

For ekomsektorens del kan seks-stegs-prosedyren illustreres på følgende måte:



Det er utfordrende lese innholdet i, og rekkefølgen på, de seks stegene direkte ut av de prosessuelle reglene og definisjonene i sikkerhetsloven kapittel 1 og 2. Utkast til forskrift om myndighetens roller og ansvar for nasjonal sikkerhet presisere dessuten i liten grad de enkelte stegene i prosessen. Dette gir i praksis de enkelte fagdepartement et bredt mandat til å selve definere prosessen.

Vi mener dette åpner for en svært ulikeartet prosess i de ulike sektorene. Broadnet ser dessuten med bekymring på at enkelte myndigheter allerede har foreslått prosesser som ikke følger de prosedyrene som følger av den vedtatte hjemmelsloven.

Samferdselsdepartementet ("**SD**") har startet prosessen med å kartlegge rammene for GNF gjennom en arbeidsgruppe. Både bransjen og sektortilsynet har blitt gitt mulighet til å komme med innspill. I møte med bransjen og departementet i august og september 2018 redegjorde sektormyndigheten for sitt foreløpige syn på det nye regelverket og den videre prosessen. Det så i denne forbindelse ut til at de involverte myndighetene og flere av de største tilbyderne av elektronisk kommunikasjon hadde en ulik forståelse av hvilken prosess den nye loven legger opp til, herunder identifiseringen av GNF, utpekingen av virksomheter basert på denne klassifiseringen samt utpekingen av skjermingsverdige objekt og infrastruktur.

Vedlegg: Brev fra Operatørene – vedrørende GNF datert 26. sep. 18

For det første vil fremgangsmåten resultere i at langt flere virksomheter, objekter og større deler av infrastrukturen underlegges loven enn det det er grunnlag for. Dette innebærer store kostnader uten at dette fremmer de sentrale formålene i loven og forarbeidene. Videre mener Broadnet for det andre at mangler ved prosessen vil føre til feilaktige beslutninger om hvilke GNF som bør beskyttes og hvorfor. Dette vil igjen påføre de regulerte virksomhetene og samfunnet store merkostnader i form av investeringer og ressursbruk knyttet til tiltak som ikke er nødvendige. Det vil også lede oss inn i en situasjon hvor det blir svært krevende for de ansvarlige fagdepartementene og de ulike virksomhetene (eiere av GNF-infrastruktur) å praktisere et harmonisert system for håndtering av avhengigheter.

På bakgrunn av dette ber Broadnet om at FD tar inn prosessuelle regler i den endelige forskriften som reflekterer de stegene vi har beskrevet over. Bestemmelsene må både presisere hvilken prosedyre fagdepartementene skal følge og tydeliggjøre de enkelte stegene i prosessen. Vi ber også om at FD pålegger de involverte myndighetene å fullføre hvert sted før de går videre til neste. Det kan også være hensiktsmessig å sette frister for blant annet identifiseringen og kategoriseringen av GNF. I tillegg må slike prosessuelle regler stille krav om at fagdepartementene publiserer retningslinjer, veileder e.l. som konkretiserer hva som er GNF innen den enkelte sektor slik at det er enkelt for de regulerte virksomhetene å identifisere avhengigheter mv.

3.3 Forskriften må gi forutsigbarhet om innholdet i de funksjonelle kravene til et forsvarlig sikkerhetsnivå

Både den nye sikkerhetsloven og utkast til forskrift om virksomhetens arbeid med forebyggende sikkerhet legger opp til gjennomgående bruk av funksjonelle handlingsnormer i form av et forsvarlighetskrav ("forsvarlig sikkerhetsnivå"). Broadnet slutter seg til FDs egen beskrivelse av både fordeler og ulemper med denne tilnærmingen:[5]

> "Funksjonelle krav gir virksomhetene som underlegges loven stor grad av fleksibilitet med tanke på hvordan virksomheten sikrer den informasjon, informasjonssystemene, infrastrukturen eller objektene den råder over. Samtidig forutsetter funksjonelle krav sikkerhetsfaglig kompetanse for å kunne komme frem til de mest hensiktsmessige sikkerhetstiltakene. NSM og sektormyndighetene med tilsynsansvar, vil derfor ha en viktig rolle med å gi råd og veiledning om hvordan bestemmelsene kan etterleves og hvordan tiltakene kan tilpasses en sektors egenart. Det vil i mange tilfeller være mulig for myndighetene å peke på standarder og andre

[5] Høringsnotatet side 13.

> normer for hvordan krav kan oppfylles. Forslaget til forskrifter skal gjennom begrepsbruk og oppbygning av bestemmelsene legge til rette for at disse kan etterleves gjennom å legge anerkjente standarder til grunn."

Broadnet er positiv til den fleksibiliteten forsvarlighetskravet gir bransjen. Når det er sagt, forutsetter funksjonelle sikkerhetskrav at både tilsynsmyndigheter og de regulerte aktørene er i stand til å tolke seg frem til innholdet i handlingsnormen ut fra tilgjengelige rettskilder, eventuelt supplert med retningslinjer og veileder. Det er ikke mulig slik forskriftene er utformet per nå sett i sammenheng med sikkerhetsloven. Verken ordlyd eller forarbeider gir nærmere veiledning om hvilke konkrete tiltak en tilbyder må gjennomføre for å tilfredsstille kravet om "forsvarlig sikkerhetsnivå", utover opplistingen av relevante momenter.

Slik Broadnet ser det gir for eksempel "forsvarlig sikkerhetsnivå" anvisning på en målestokk som ligger utenfor loven. Rettsanvenderen må benytte alminnelig rettslig metode for å klarlegge hvilken rettslig standard som er relevant for å fastlegge innholdet i handlingsnormen samt yttergrensene for vurderingen.

Vi vil for det første peke på at det verken fremgår av lov, forskriftstekst eller merknadene til bestemmelsene at regulerte aktører vil oppfylle kravene gjennom å legge anerkjente og egne standarder til grunn. Det fremgår heller ikke av forskriftsteksten at dette er et moment som skal tas i betraktning.[6]

Til sammenlikning går sikkerhetsutvalget inn på dette i langt større detaljer i NOU 2016: 19, men da under de generelle beskrivelsene av de grunnleggende krav til sikkerhet på side 144:

> "Utvalget har derfor anbefalt som et generelt og gjennomgående krav at virksomhetene skal iverksette de sikkerhetstiltak som er nødvendige for å oppnå et forsvarlig sikkerhetsnivå.
>
> [...]
>
> At sikkerhetsnivået skal være forsvarlig er en rettslig standard som trekker opp de ytre rammene for hvilket handlingsrom virksomhetene har for etablering av sikkerhetstiltak. Hva som vil utgjøre et forsvarlig sikkerhetsnivå for den enkelte virksomhet, og på de enkelte fagfeltene loven dekker, vil måtte vurderes opp mot hva som anses som god faglig praksis på de enkelte fagområdene, herunder informasjons- og informasjonssystemsikkerhet, objekt- og infrastruktursikkerhet og personellsikkerhet. Den nærmere grensedragningen bør, slik utvalget

[6] Forutsetningen er kun nevnt andre steder i høringsnotatet.

> ser det utvikles i samarbeid mellom Sikkerhetsmyndigheten og de aktuelle sektormyndighetene. Dette vil også gi mulighet til å kunne gjøre sektorspesifikke tilpasninger der det er behov".

Sektorlovgivningen går også lengere i å beskrive innholdet i forsvarlighetsstandarden innenfor sitt virkeområde. Blant annet pålegger ekomloven § 2-10 første ledd aktører å oppfylle en forsvarlighetsstandard. I dette tilfellet har lovgiver selv beskrevet hvilken målestokk "forsvarlig sikkerhet for brukerne i fred, krise og krig" skal måles mot. I merknadene til bestemmelsen på side 103 i Prop. 69L (2012-2013) fremgår det at "nett og tjenester skal være tilgjengelige, og at integriteten og konfidensialiteten beskyttes. Videre uttaler lovgiver:

> "Hva som for øvrig må anses for å være forsvarlig vil fremkomme gjennom markedspraksis, tilgjengelig teknologi og internasjonale krav. Det er tilbyders ansvar at tjenestene som tilbys holder et forsvarlighetsnivå. Men myndigheten kan gjennom vedtak presisere dette nivået, jf. første ledd fjerde punktum."

Selv om heller ikke ekomloven § 2-10 første ledd gir de regulerte aktørene tilstrekkelig forutsigbarhet om innholdet i handlingsnormen, er det mulig å utlede de ytre rammene av direkte av rettskildene.

Slik Broadnet ser det pålegger, for det andre, verken sikkerhetsloven eller de foreslåtte forskriftene tilsynsmyndighetene i den enkelte sektor å utarbeide veiledere, retningslinjer e.l. De tre forskriftene utdyper heller ikke det generelle kravet i den nye sikkerhetsloven § 2-2 d) til at sikkerhetsmyndigheten skal "gi informasjon, råd og veiledning om forebyggende sikkerhetsarbeid og krav til tiltak". Etter sin ordlyd er det uansett uklart om regelverket pålegger NSM å presisere innholdet i forsvarlighetsstandarden. Vi går nærmere inn på behovet for en forskriftsbasert veiledningsplikt i punkt 3.4 under.

I denne forbindelse vil vi også slutte oss til de forutsetningene FD selv fremhever som en grunnstein i Høringsnotatet:

> "Departementet bemerker at regelverkets funksjonelle innretning gjør det nødvendig at det utarbeides veiledere av Nasjonal sikkerhetsmyndighet og myndigheter med sektoransvar i de aktuelle sektorene."

Broadnet har de siste to årene selv erfart hvilke konsekvenser uklare handlingsnormer kombinert med mangelfull veiledning i forkant av en hendelse kan få for alle involverte parter. For at det nye regelverket skal fungere tilfredsstillende i tiden fremover er det en avgjørende forutsetning at både regulerte virksomheter, sikkerhetsmyndigheter og tilsynsmyndigheter forholder seg til de samme handlingsnormene. Dette gjør det også mulig for at konkurrerende aktører stilles overfor like krav.

På bakgrunn av dette ber Broadnet om at FD presiserer de endelige forskriftene ved å klargjøre at etterlevelse av anerkjente standarder er et tungtveiende moment i vurderingen av om sikkerhetstiltakene er forsvarlige og at sikkerhets- og/eller tilsynsmyndigheter skal veilede om slike standarder i tråd med det som fremgår i punkt 3.4 under. Vi ber også om at forskriften kobler forsvarlighetsstandarden til markedspraksis, tilgjengelig teknologi i den bransje det gjelder og/eller andre momenter som er relevante for å fastlegge rammene for handlingsnormen.

3.4 Forskriften bør pålegge både sikkerhetsmyndigheten og tilsynsmyndigheten en proaktiv veiledningsplikt om de konkrete handlingsnormene

Broadnet har over beskrevet hvorfor aktiv veiledning fra både sikkerhetsmyndighet og tilsynsmyndighet hva sikkerhetsloven med forskrifter krever er avgjørende for at aktører i ulike bransjer skal kunne etterleve regelverket.

Broadnet har i de senere år gjort seg en rekke erfaringer som tilsynsobjekt som vi mener er nyttig og relevant å trekke erfaringer fra i denne sammenheng. Som det fremgår over er vårt overordnete inntrykk at kapasitet, kompetanse og profesjonalitet varierer i for stor grad mellom de ulike tilsynsorganene. Dersom sikkerheten skal bedres gjennom nytt regelverk, mener vi det er behov for en lagt mer koordinert innsats mellom sektorspesifikke og sektorovergripende tilsyn, felles minimumskrav til det offentliges oppfølging av krav i lov og forskrift, proaktiv rådgivning/veiledning om de konkrete handlingsnormene og at det må gjennomføres tiltak for å sikre en uavhengig og objektiv oppfølging av regelverket. Det er også viktig at de ulike tilsynsorganene gis tilstrekkelige midler til å tilegne seg nødvendig kapasitet og kompetanse for å utføre sin oppgave på en profesjonell måte.

Broadnet har også lang erfaring med å aktivt søke veiledning og råd fra relevante myndigheter innenfor IKT-sikkerhet. Tilbakemeldingene har ofte vært svært generelle, til dels mangelfulle og ikke tilpasset den operative virkeligheten for en ekomaktør. I enkelte tilfeller er anmodninger besvart svært sent, eller ikke i det hele tatt.

Som nevnt stiller vi oss bak FDs uttalelse om at dette også er forutsetning for den funksjonelle tilnærmingen både lovgiver og FD har valgt. Til tross for dette inneholder utkastet til nye forskrifter ingen klare plikter for de involverte myndighetene til å proaktivt gi slik veiledning slik at det er kun er minimumsstandarden i § 2-2 d) i ny sikkerhetslov og forvaltningslovens alminnelige regler som gjelder. Det synes heller ikke å få noen konsekvenser for andre enn den regulerte virksomheten dersom relevante myndigheter skulle unnlate å gi den forutsatte veiledningen.

Det blir en utfordring for de virksomhetene som underlegges sikkerhetsloven ettersom det i praksis tillater at tilsynsmyndighetene etablerer "fasiten" for godt sikkerhetsarbeid i etterkant av et tilsyn eller

hendelse – heller enn i forkant. Broadnet mener regelverket må pålegge både sikkerhetsmyndigheter og tilsynsmyndigheter en klart plikt til å utarbeide og å offentliggjøre slik veiledning. Dette bør skje innen nærmere angitte frister fra det nye regelverket trer i kraft. For å sikre at dette følges opp, bør eventuelle håndhevelse forutsette at slik veiledning har blitt gitt i tråd med de forskriftbaserte kravene

I lys av dette ber Broadnet om at de endelige forskriftene pålegger tilsynsmyndigheter en entydig plikt til å på eget initiativ gi nødvendig veiledning om forsvarlighetsstandarden mv. innenfor egen sektor. Dette bør omfatte informasjon om hvilket etablerte standarder som er relevante for de ulike bransjer. Regelverket bør stille krav til hvordan og hvor raskt dette skal skje og fastsette konkrete frister for å oppfylle kravet. Det er også en fordel om forskriften operasjonaliserer den veiledningsplikten som fremgår av sikkerhetsloven § 2-2 d). Videre ber Broadnet om at den endelige forskriften også etablerer prosedyrer for hvordan regulerte virksomheter kan anmode om veiledning som går utover forvaltningslovens minimumskrav fra tilsynsmyndigheter – og hvilken betydning råd, veiledning mv. får for etterlevelsen.

3.5 Forskriften bør stille krav til at godkjente tilsynsmyndigheter har tilstrekkelig kompetanse og ressurser til å utføre tilsynsoppgaven

Broadnet mener det er betydelige svakheter ved dagens organisering på sikkerhetsområder, særlig når det gjelder ekom og IT (IKT-sikkerhet).

Vi har frem til nå opplevd de ulike myndighetenes oppfølging som fragmentert og lite koordinert. Det er dessuten merkbare forskjeller i kapasitet, profesjonalitet og kompetanse. Dette fører til at de regulerte aktørene møter ulike krav og forventninger, noe som i seg selv er egnet til å svekke IKT-sikkerhet. Arbeid med sikkerhet krever langsiktige og forutsigbare rammer for alle aktørene for å investere i gode teknologiske løsninger, etablere robuste prosesser og bygge god kultur med riktig kompetanse. Vi er derfor bekymret for konkrete eksempler på at offentlige myndigheter tilsynelatende lar kortsiktige politiske hensyn og medieoppslag påvirke både prioritering og oppfølgingen av sikkerhetsarbeidet på IKT-området - noe som tidvis har gått på bekostning av sikkerhet. Utkastet til forskrift ser ikke ut til å løse denne typen utfordringer. Broadnet savner en mer presis regulering av samspillet mellom sikkerhetsmyndighet og tilsynsmyndighet - særlig når det gjelder det forebyggende sikkerhetsarbeidet.

Vi ser det som positivt at forskriften stille kvalitative krav til de etater og tilsyn som kan få i oppgave å følge opp det nye regelverket innenfor sin sektor. Når det er sagt, savner vi en forskriftbasert plikt for de offentlige organene som har blitt utpekt til å opprettholde både kompetanser og ressurser. Det er uheldig både for samfunnet og de regulerte aktørene.

Som en del av dette bør forskriften også stille krav til hvordan utpekte tilsynsmyndigheter utøver rollen. Vi har i de senere årene gjort oss en rekke erfaringer som tilsynsobjekt. Vårt inntrykk er at ulike myndigheter har ulik tilnærming til hvordan de utfører tilsynsoppgaven. Profesjonaliteten varierer også. Det fremstår dessuten ikke alltid som om tilsynsmyndighetene er tilstrekkelig uavhengige og objektive.

Dersom det nye regelverket skal sikre økt sikkerhet, særlig i det digitale domenet, mener vi derfor de endelige forskriftene bør stille visse minimumskrav basert på mønsterpraksis for tilsyn. Etter modell fra for eksempel Konkurransetilsynet bør det for eksempel være et organisatorisk skille mellom den delen av forvaltningsorganet som gir veiledning og råd om forebyggende sikkerhet, og den som fører tilsyn med at kravene blir fulgt.

Dette synes å være i tråd med det FD selv uttaler på side 44 i Høringsnotatet[7]:

> "For å sikre en mest mulig uavhengig og objektiv kontroll av styringssystemet følger det av tredje ledd at personer med kontrollerende roller ikke bør være de samme som har styrende eller utøvende roller i det forebyggende sikkerhetsarbeidet."

Broadnet ber på bakgrunn av det som fremgår over at FD i den endelige forskriften pålegger sektortilsyn å opprettholde nødvendig kompetanse og ressurser innenfor de områdene loven dekker. Om mulig bør forskriften også stille faglige krav til sektormyndighetenes sikkerhetsarbeid. Dette vil også gjøre det lettere for NSM å gripe inn raskt der tilsyn med sikkerhetsloven med forskrifter svikter. I tillegg mener Broadnet at forskriften bør stille prosessuelle krav til hvordan relevante myndigheter organiserer og utfører tilsynsvirksomheten.

3.6 Forskriften bør tydeliggjøre kravet til kompetanse hos regulert virksomhet som gjennomfører anskaffelser

På side 20 i NOU 2016:19 fremgår det:

> "Utvidelsen av lovens virkeområde gjør det også nødvendig med en mer funksjonell tilnærming til beskyttelse av slike objekter og infrastruktur. Det primære ansvaret for å sikre at objektene og infrastrukturen har et forsvarlig sikkerhetsnivå, tilligger den enkelte virksomhet. Også på dette området må det være en forutsetning at tiltakenes kostnader står i et rimelig forhold for

[7] Det samme fremgår også på side 120 i NOU 2016:19: "En forutsetning for en tilfredsstillende gjennomføring av forebyggende sikkerhet for å sikre grunnleggende nasjonale funksjoner, er at det etableres et system hvor roller, ansvar og plikter er avklart og tilstrekkelig definert."

til den sikkerhetsmessige effekten som oppnås. Ved vurderingen av hva som er forsvarlig, vil virksomhetene også måtte se hen til gjensidige avhengigheter og deres rolle i understøttelsen av en grunnleggende nasjonal funksjon".

Dette innebærer blant annet at det er eieren av skjermingsverdig objekter og/eller infrastruktur som er ansvarlig for å melde avhengigheter til andre virksomheter og fagdepartementet. Denne plikten gjelder både private og offentlige virksomheter.

Broadnet har erfart at de regulerte aktørene ikke tar inn over seg at det er de som er ansvarlig for å etablere et forsvarlig sikkerhetsnivå etter sikkerhetsloven og annen regulering (som for eksempel ekomlovgivningen). Anbudsinvitasjonen verken informerer eller stiller krav på dette området. Dette er uheldig. Selv om både Broadnet og andre tilbydere forsøker å gi råd om forebyggende sikkerhet mv. av eget initiativ, har innkjøperen ingen plikt til å følge opp. Det virker dessuten som om viljen til å betale for sikkerhet er begrenset.

Vi etterlyser på bakgrunn av dette en presisering i forskriften som tydeliggjør at den regulerte virksomheten er ansvarlig for å informere om sikkerhetslovens krav i anbudsprosessen og tar høyde for dette ved utarbeidelsen av anbudsinvitasjoner mv.

3.7 Forskriftens krav og definisjoner bør harmoniseres og presiseres

I et samfunnsperspektiv krever forebyggende sikkerhet i cyberdomenet at man på tvers av sektorer, private og offentlige virksomheter forholder seg til samme standarder og med lik risikoforståelse. Det er positivt at sikkerhetsmyndighetene tillegges et tydelig ansvar for harmonisering, rådgivning og oppfølging på tvers, samtidig er det viktig at man i lovforslaget tillegger sektormyndighetene et tydelig krav om å legge til rette for harmonisering av IKT-sikkerhetskrav på tvers av sektorspesifikk lovgivning.

Vi er enig i at det ikke bør være en lovbestemt plikt med forhåndsgodkjenning av ugraderte systemer. Hvis det allikevel blir besluttet en slik forhåndsgodkjenning for enkelte ugraderte systemer er det viktig at denne prosessen blir lettfattelig og at det finnes standarder for ugraderte systemer/systemgrupper.

Broadnet ber FD om å revidere forslaget i lys av dette.

3.8 Behov for å presisere ytterligere rettssikkerhetsgarantier ved ileggelse av overtredelsesgebyr

Den nye sikkerhetsloven § 11-3 gir tilsynsmyndigheten kompetanse til å pålegge en virksomhet overtredelsesgebyr for nærmere angitte overtredelser. Etter det Broadnet kan se inneholder ikke de foreslåtte forskriftene ytterligere prosedyrer eller skranker for bruk av denne sanksjonsmekanismen. Vi

mener det kan gi utilsiktede resultater og at det er problematisk med tanke på tilsynsobjektenes rettssikkerhet.

Formålet med overtredelsesgebyret er å påføre et onde som en reaksjon fra samfunnet på en overtredelse av lovpålagte plikter. Overtredelsesgebyr etter sikkerhetsloven § 11-3 regnes ikke som formell straff etter Grunnloven § 96. Det er likevel snakk om en sanksjon med "strafferettslig karakter" etter Den europeiske menneskerettighetskonvensjonen ("**EMK**")[8]. Dette innebærer blant annet at rettsikkerhetsgarantiene i artikkel 7 kommer til anvendelse slik at det stilles strengere krav til både bevis og klarheten i rettsgrunnlaget, noe Høyesterett har bekreftet i flere avgjørelser.

På bakgrunn av dette etterlyser Broadnet to grunnleggende endringer i de foreslåtte forskriftene.

For det første mener vi at forskriftene selv må angi hvilke konkrete bestemmelser tilsynsmyndigheten kan sanksjonere med overtredelsesgebyr. Per nå fremgår det av sikkerhetsloven § 11-3 at gebyret kan ilegges ved overtredelse bestemmelser gitt i medhold av "§§ 3-4, 4-3, 4-4, 4-5, 5-2, 6-2, 6-3, 7-3, 9-2 første ledd, 9-4 første ledd første punktum eller § 9-4 andre ledd første eller andre punktum". På flere punkter er det ikke opplagt hvilke forskriftskrav som er hjemlet i de ulike paragrafene. I ytterste konsekvens kan rettsgarantiene beskrevet over føre til at tilsynsmyndighetene må avstå fra å sanksjonere overtredelser fordi det ikke er klart hvilke handlingsnormer som er belagt med "straff".[9] Slik Broadnet ser det, kan dette enkelt løses ved å ta inn en ny forskriftsbestemmelse som oppsummerer hvilke konkrete paragrafer tilsynsmyndigheten kan sanksjonere med overtredelsesgebyr. Et eksempel på dette er ekomforskriften § 10-3 andre ledd.

For det andre mener Broadnet at forskriften må fastsette et øvre tak for størrelsen på overtredelsesgebyret. De fleste sektorregelverk angir de rammene tilsynsmyndighetene må forholde seg til ved ileggelse av sanksjoner. Slik sikkerhetsloven og forskriftene er utformet per nå, kan myndighetene

---

[8] Se også Ot.prp.nr. 72 (2006 – 2007) side 42 er lovgiver understreker at "overtredelsesgebyr er et tyngende virkemiddel med et strafferettslig preg."

[9] Se blant annet Høyesteretts uttalelse i Rt. 2009 side 780 punkt 21: "For at det hjemmelskrav som følger av EMK artikkel 7, skal være tilfredsstilt, må det fremgå av straffebestemmelsens ordlyd, eventuelt supplert med de presiseringer som måtte følge av rettspraksis, hvilke handlinger eller unnlatelser som rammes, se for eksempel dom 25. mai 1993 i saken Kokkinakis mot Hellas avsnitt 52, dom 22. november 1995 i saken S.W. mot Storbritannia avsnitt 34-36, dom 22. november 1995 i saken C.R. mot Storbritannia avsnitt 32-34 og storkammerdom 15. november 1996 i saken Cantoni mot Frankrike avsnitt 29."

i teorien sanksjonere et regelbrudd med et gebyr som tilsvarer 100 % av virksomhetens omsetning. Vi antar det ikke er tilsiktet. Slike bøtenivåer ville dessuten være uholdbare. Vi ber derfor om at FD tar inn en bestemmelse som angir maksimalsatsen, f.eks. som en andel av virksomhetens årlige brutto omsetning. Det finnes mange eksempler på hvordan dette kan formuleres. Forskrift til utmåling og lemping av overtredelsesgebyr etter konkurranseloven fastsetter f.eks. en øvre ramme på " inntil 10 prosent av foretakets omsetning (§ 2, andre ledd).[10] Personopplysingsloven § 26, jf. personvernforordningen åpner til sammenlikning for et gebyr på inntil 4 %, mens ekomforskriften benytter en samme på inntil 5 %.

3.9 Forskriften bør regulere forholdet mellom kravene i sikkerhetsforskriften og sektorspesifikke sikkerhetskrav

Den eksisterende objektssikkerhetsforskriften regulerer i § 1-3 forholdet mellom kravene i sikkerhetsregelverket og dem som følger av sektorlovgivningen. Her fremgår det:

> "Der det finnes relevante og tilstrekkelige bestemmelser innenfor sektorlovgivningen, og det er etablert tilsynsorgan, går disse foran bestemmelsene i denne forskriften."

Forarbeidene til sikkerhetsloven utdyper vurderingstemaet:[11]:

> "Sikring mot tilsiktede hendelser må derfor sees i sammenheng med de tiltak som er nedfelt i særlovene. Sikkerhetstiltakene bør derfor tilpasses den enkelte sektor. Sektorlovgivningen - der den gir bestemmelser om konkrete sikkerhetstiltak mot tilsiktede hendelser - skal derfor etter departementets syn legges til grunn ved implementering av forebyggende tiltak. Der sektorlovgivningen ikke gir denne type bestemmelser, eller bestemmelsene som er gitt (åpenbart) ikke tilfredsstiller sikkerhetslovens norm for beskyttelse av skjermingsverdige objekter, vil ytterligere tiltak måtte implementeres, slik at de funksjonelle standarder som sikkerhetsloven stiller blir ivaretatt.
>
> På objektsikkerhetsområdet kan flere sektorer i samfunnet vise til sikkerhetsbestemmelser nedfelt i lov eller forskrift som helt eller delvis kan sies å omfatte de sikkerhetshensyn som sikkerhetsloven på objektsikkerhetsområdet også søker å ivareta. På de områder slike hensyn fullt ut er ivaretatt i sektorbestemmelsene, vil sikkerhetsloven stå tilbake for disse.

[10] https://lovdata.no/dokument/SF/forskrift/2013-12-11-1465
[11] Se Ot.prp.nr. 21 (2008 – 2009) side 31.

> Der hensyn delvis er ivaretatt gjennom sektorbestemmelsene, vil sikkerhetsloven som tverrsektoriell standard virke reparerende, slik at det helhetlige, tverrsektorielle nasjonale sikkerhetsbehovet knyttet til defensiv forebygging av spionasje, sabotasje og terrorhandlinger, blir ivaretatt. Eksempler på sektorer med et «security»-regelverk finnes innen luftfarten, sjøfarten og kraftforsyningen." [våre understrekninger]

Disse kildene gir både myndigheter og regulerte virksomheter verdifull og nødvendig veiledning av forholdet mellom sikkerhetsloven med forskrifter. Dette er en grunnleggende forutsetning for at de regulerte virksomhetene skal kunne etterleve reguleringen.

Broadnet må, i likhet med de fleste andre aktører, forholde seg til sikkerhetsrelaterte krav i en rekke lover og forskrifter. Dette kommer i tillegg til sikkerhetsloven med forskrift. For vår del må vi for eksempel også etterleve de sektorspesifikke reglene om kommunikasjonsvern i ekomloven med forskrifter samt de kravene til informasjonssikkerhet som følger av personopplysningsloven og personvernforordningen.

Vår erfaring er at det i praksis kan oppstå motstrid mellom de ulike regelsettene ettersom lovgiver kun i noen får tilfeller har vurdert de ulike handlingsnormene opp mot hverandre. Det er samtidig ikke gitt at de tradisjonelle motstridsprinsippene[12] løser slike konflikter, blant annet fordi det er uklart hvilket regelverk som er mest spesielt. Denne uklarheten åpner tidvis også for at tilsynsmyndighetene velger å håndheve det regelverket de selv mener er mest hensiktsmessig ut fra vikarierende motiver som f.eks. hvilket regelsett som åpner for strengest sanksjoner.

Etter det Broadnet kan se inneholder verken den nye sikkerhetsloven eller de foreslåtte forskriftene bestemmelser som regulerer forholdet mellom sikkerhetsregelverket og sikkerhetskrav i andre regelverk. Dette er en svakhet.

FD erkjenner utfordringen så langt gjelder objektssikkerhet i forarbeidene til den nye sikkerhetsloven:[13]

> "Når det gjelder objektsikkerhet viser departementet til at dagens objektsikkerhetsforskrift har en bestemmelse som innebærer at sektorregelverket går foran forskriftens krav, så framt sektorregelverket har relevante og tilstrekkelige bestemmelser og det er etablert tilsynsorgan. Det er imidlertid ikke til å unngå en viss grad av overlappende regelverk. Dette er ikke noe særegent knyttet til forebyggende sikkerhetsarbeid. Departementet mener

[12] Lex specialis, lex superior og lex posterior.
[13] Se Prop. 153 L (2016-2017) side 81.

> sikkerhetsmyndigheten og sektormyndighetene, sammen med virksomhetene, i den videre operasjonaliseringen av kravene, vil måtte ta hensyn til alle regelverk som stiller krav til sikkerhet."

Broadnet mener uklarhetene i regelverket gjør handlingsnormene lite forutsigbare. Dessuten er det lite heldig at det blir opp til sektormyndighetene og tilsynsmyndighetene selv å beslutte hvilket normsett aktørene skal forholde seg til. Vi mener det er en oppgave for lovgiver og departement å avklare dette i forkant. Uten forskriftsbaserte rammer, blir det dessuten opp til de involverte myndighetenes selv å beslutte om de ønsker å involvere de regulerte aktørene i denne grenseoppgangen. I mangel av forskriftsbestemmelser om forholdet mellom regelsettene, fratas uansett de berørte partene mulighetene til å utfordre operasjonaliseringen.

Vi ber om at FD i den endelige forskriften:

a) tar inn en bestemmelse som regulerer forholdet mellom sikkerhetsloven med forskrifter og sikkerhetskrav i andre regelverk og eventuell motstrid, og

b) presiserer bestemmelsen på en slik måte at vurderingen av hvilket normsett de regulerte virksomhetene skal forholde seg til ikke overlates til tilsynsmyndighetene.

4 Broadnets kommentarer til de særlige forholdene der departementet har bedt om innspill

4.1 Broadnets syn på strukturen i forskriftsforslaget

På side 11 i Høringsnotatet ber FD om høringsinstansenes syn på antall forskrifter og strukturen i forskriftene:

> "Departementet vurderer hvorvidt bestemmelsene i myndighetsforskriften skal flyttes til en av de to andre forskriftene, eller til en egen instruks for de myndighetsorganene loven gjelder for. Departementet vurderer også om alle bestemmelsene i forskriftene skal samles i én forskrift. Departementet ber om høringsinstansenes innspill på om forslaget til inndelingen i forskrifter er hensiktsmessig, og særlig på om det er mer hensiktsmessig med en eller to forskrifter. Departementet ber også om innspill til offisielle korttitler på forskriftene for å sikre at de er tilstrekkelig entydige."

Broadnet kan ikke se at det har noen materiell betydning om de relevante bestemmelsene samles i én felles forskrift eller om FD beholder tre som i forslaget. Vi er videre enige i at det er behov for entydige korttitler, uten at vi har konkrete forslag til ordlyd.

4.2 Broadnets syn på detaljering av krav til objekts- og infrastruktursikkerhet

På side 13 i Høringsnotatet etterlyser departementet innspill på detaljeringsgraden:

> " Departementet ser derfor at kan være hensiktsmessig å i større grad detaljregulere sikring av infrastruktur. Departementet vil vurdere å gi ytterligere detaljkrav for sikring av infrastruktur når infrastrukturen er utpekt, og regelverket har fått virke over noe tid. Departementet ber høringsinstansenes syn på om det bør gis mer detaljerte krav til sikring av infrastruktur, og i så fall hvilke krav som bør stilles."

Som det fremgår i punkt 3.3 - 3.4 mener Broadnet at forskriftskravene i sin nåværende form er så generelle at det i seg selv gjør det utfordrende å etterleve det nye regelverket. *Vi mener derfor både at FD bør detaljere kravene i forskriften og pålegge relevante myndigheter en tydelig plikt til å gi konkret veiledning om hvordan virksomhetene skal innrette seg. Broadnet viser i denne forbindelse til det vi har sagt over.*

Utydelige handlingsnormer kombinert med strenge sanksjoner er et rettssikkerhetsproblem. Det fremmer dessuten verken en enhetlig praksis eller økt sikkerhet i det norske samfunnet. *Broadnet mener derfor at de mer detaljerte kravene må på plass før forskriften trer i kraft, eventuelt ved at ikrafttredelsen utsettes. Kun dersom dette ikke er mulig bør FD legge opp til å revidere detaljkravene i etterkant.*

Uavhengig av om FD presiserer kravene til forsvarlig sikkerhet, mener Broadnet at departementet bør definere begrepet "infrastruktur". Dette er et nytt uttrykk. Verken sikkerhetsloven eller forskriften inneholde noen utfyllende definisjon. Grensene for hva som kan sies å være "infrastruktur" er dessuten utydelig, særlig i de mer digitaliserte sektorene som ekomsektoren. Samtidig er begrepet svært sentralt ved utpekingen og kategoriseringen av GNF. Det kan med andre ord få store utslag dersom FD venter med å detaljere innholdet ytterligere til etter utpekingen av objekt mv

4.3 Broadnets syn på behovet for å konkretisere vurderingstemaet ved klarering av utenlandske statsborgere

FD etterlyser på side 19 i Høringsnotatet innspill på om det er behov for en bestemmelse som konkretiserer vurderingstemaet ved klarering av utenlandske statsborgere:

> "Departementet mener at § 8-7 gir tilstrekkelige føringer for den helhetsvurderingen klareringsmyndigheten skal gjøre, og har derfor ikke sett det som nødvendig at det gis ytterligere bestemmelser om selve vurderingen i forskrift, utover §§ 14 og 16 i klareringsforskriften, om personhistorikk og tilknytning. Departementet ber imidlertid om høringsinstansenes innspill på om det er behov for en bestemmelse som konkretiserer vurderingstemaene ytterligere, og vil vurdere en slik bestemmelse i lys av høringsinnspillene."

Broadnet er avhengig av tilgang til kvalifisert arbeidskraft både fra land hvor Norge har og ikke har sikkerhetsavtale med for å sikre tilgjengelighet av tjenester og nett. Det er et underskudd på både kompetanse og kapasitet i Norge. Det er derfor helt nødvendig å benytte utenlandske statsborgere som et supplement til norsk personell.

Vår erfaring er at klareringsmyndighetene per i dag legger urimelig stor vekt på tilknytningen til Norge ved vurdering av personell med utenlandsk statsborgerskap. Broadnet har blant annet en rekke eksempler på at klareringsmyndigheten har avslått søknader om dispensasjon for å autorisere nordiske statsborgere til BEGRENSET basert på dette kriteriet alene. Dette er uholdbart, særlig ettersom en slik sjablonmessig praksis ikke er egnet til å fremme sikkerheten i det norske samfunn.

Broadnets foreslår i lys av dette at prosedyrene ved adgangsklarering, utvidet adgangsklarering og fastsettelse av sikkerhetsklareringsnivå til BEGRENSET harmoniseres med det kravene som stilles til KONFIDENSIELT. Vi ber også FD å vurdere om det i slike tilfeller er mulig å for eksempel gi midlertidige sikkerhetsklareringer eller adgangsklarer med f.eks. 1 års gyldighet som et kompenserende tiltak frem til det foreligger tilstrekkelig personhistorikk, jf. klareringsforskriften § 22. Slik Broadnet ser det burde det være mulig å åpne for en "[...] gyldighet inntil 5 år".

4.4 Broadnets syn på behovet for unntaksbestemmelse for å gi utenlandske statsborgere tilgang til skjermingsverdige objekter og informasjon

På side 22 i Høringsnotatet fremgår det:

> "Departementet ser at § 8-7 i utgangspunktet vil dekke behovet for å kunne gi utenlandsk personell tilgang til sikkerhetsgradert informasjon og skjermingsverdige objekter og infrastruktur av hensyn til behovet for kompetanse, uten at dette i for stor grad går på bekostning av behovet for kontroll med personellet av hensyn til nasjonale sikkerhetsinteresser. Departementet ber derfor om høringsinstansenes syn på behovet for og hensiktsmessigheten av den unntaksbestemmelsen som er foreslått i myndighetsforskriften § 11, og vil vurdere bestemmelsen i lys av høringsinnspillene".

Broadnet støtter forslaget. En slik unntaksbestemmelse er allerede en nødvendighet i ekomsektoren. Både vi, og andre aktører, er avhengige av få tilgang til utenlandsk personell, med høy- eller spesialkompetanse på blant annet utstyr, programvare og tjenester som inngår i skjermingsverdig verdier eller GNF. Vi forventer at dette behovet også kommer til å øke i takt med digitaliseringen av andre sektorer slik som olje- og gass, finans og kraft. Når det er sagt mener vi den foreslåtte forskriften ikke ivaretar samfunnets behov på området fullt ut ettersom unntaket er for snevert.

Broadnet foreslår derfor at FD i den endelige forskriften åpner for å gi midlertidige eller tidsbegrensete unntak fra kravet om sikkerhetsklarering for utenlandske personell på gitte vilkår. Alternativt bør regulerte virksomheter gis mulighet til å gi utenlandske statsborgere tidsbegrenset autorisasjon forutsatt adekvate, kompenserende sikkerhetstiltak. Det kan f.eks. omfatte utvidet logging eller reduserte tilgangsrettigheter basert på virksomhetens forutgående vurdering av risiko og skadepotensiale.

Slike tidsbegrensete eller midlertidig autorisasjoner bør for eksempel kunne gis i situasjoner hvor det er snakk om helt eller delvis bortfall av en GNF-funksjon som påvirker nasjonale sikkerhetsinteresser. Samtidig bør FD stille krav i forskriften til myndighetenes tidsbruk når de behandler søknader om slike dispensasjoner ("hasteprosedyre"). For å kunne ivareta samfunnets behov for tilgjengelighet og robusthet må behandlingstiden være svært kort.

4.5 Broadnets syn på krav til varslingsplikten anskaffelser til skjermingsverdige informasjonssystem, objekter eller infrastruktur

På side 24 i Høringsnotatet ber FD om det er behov for ytterligere forskriftsbestemmelser knyttet til varsling ved anskaffelser:

> "Departementet har foreløpig ikke funnet det nødvendig med ytterligere forskriftsbestemmelser knyttet til varslingsplikten i loven § 9-4, utover hva et varsel til myndighetene skal inneholde, jf. virksomhetsforskriften § 18. Det er særlig lagt vekt på at det er de enkelte departementene som har ansvaret for det forebyggende sikkerhetsarbeidet i de ulike samfunnssektorene, og det kunne være behov for å gjøre avveininger knyttet til risiko som er tilpasset behovene i den enkelte sektor.
>
> Departementet antar at det vil være mer hensiktsmessig at myndigheter med sektoransvar lager veiledere med momenter som kan vektlegges i vurderingen. Departementet ber om høringsinstansenes innspill på om det er nødvendig med ytterligere forskriftsbestemmelser knyttet til denne bestemmelsen."

Høringsnotatet punkt 4.6.4 dekker både graderte og ugraderte informasjons- og kommunikasjonssystemer, og kontroll- og styringssystemer. Begge kategorier er relevante for GNF eller kritiske infrastruktur.

Broadnet har (på lik linje med andre ekomtilbydere) systemer som er utdaterte og utenfor leverandørens vedlikeholds program. Disse systemene kan være i bruk for virksomhet som har identifisert avhengigheter til GNF. Dette innebærer at det nødvendig med en overgangs ordning eller fritak for eksisterende teknologier og systemer.

Virksomhetens risiko- og sårbarhetsanalyser må danne grunnlaget for å angi hvilke informasjonssystemer eller infrastruktur som skal beskyttes etter sikkerhetsloven. Det er utfordrende å fastslå hvilke konsekvenser varslingsplikten vil få før dette er gjennomført.

Broadnet foreslår derfor at FD legger opp til å revidere varslingsplikten når dette steget er gjennomført.

4.6 Broadnets syn på forskriftens ikrafttredelse

I Høringsnotatet fremgår det på side 26:

> "Departementet mener i utgangspunktet at det følger av den alminnelige forvaltningsretten at virksomhetene skal gis en rimelig frist for å oppfylle kravene i regelverket. Departementet ser likevel at det kan være hensiktsmessig med en egen bestemmelse som regulerer hvilke momenter som skal vurderes når det settes en konkret frist for at hvert enkelt informasjonssystem, infrastruktur eller objekt oppnår et forsvarlig sikringsnivå. Departementene ber om høringsinstansenes innspill, og vil vurdere en slik bestemmelse i lys av høringsrunden."

Gjeldende objektsikkerhetsregelverk trådte i kraft 1. januar 2011. I forskriftens § 5-2 ble det fastsatt en overgangsbestemmelse. Her fremgår det at sikkerhetstiltak skulle gjennomføres innen tre år fra ikrafttredelse. Bestemmelsen åpnet også for å utsette fristen med ytterligere ett år etter godkjennelse fra NSM.

Den nye Sikkerhetsloven med forskrifter medfører en utvidelse av virkeområdet sammenliknet med den eksisterende reguleringen. Den dekker både flere virksomheter og stiller også flere, og mer inngripende krav. Overgangen til et fullt ut funksjonelt regelverk innebærer også at arbeidsbyrden for den enkelte virksomhet øker. Tidsfristene må reflektere det som fremgår over.

I forslaget til § 1 første ledd bokstav a og b er det angitt kriterier som departementene eller NSM skal legge vekt på ved klassifisering av skjermingsverdige objekter og infrastruktur. Bestemmelsen må ses i

sammenheng med de kriteriene som skal vektlegges for virksomhetenes skadevurdering etter forslaget til virksomhetsforskriften § 52 første ledd bokstav a til e.

Broadnet kan ikke se at dette er tilstrekkelig. Vi ber om at det i tillegg gis frister som, som et minimum, er like langt som dem som ble gitt i forbindelse med innfasingen av dagens regelverk. Dersom den endelige forskriften utelukkende gjør dette til en skjønnsmessig vurdering, må momentene konkretiseres og presiseres på en slik måte at det resulterer i liknende, realistiske tidsrom.

4.7 Departementenes beslutning av klareringsnivå

På side 32 etterlyser Høringsnotatet innspill på kriteriene for beslutning av klassifiseringsnivå etter sikkerhetsloven § 7-1:

> "I forslaget til § 1 første ledd bokstav a og b er det angitt kriterier som departementene eller NSM skal legge vekt på ved klassifisering av skjermingsverdige objekter og infrastruktur. Bestemmelsen må ses i sammenheng med de kriteriene som skal vektlegges for virksomhetenes skadevurdering etter forslaget til virksomhetsforskriften § 52 første ledd bokstav a til e. Departementet ber om høringsinstansenes syn på om ovennevnte kriterier er tilstrekkelige for at departementene skal kunne beslutte et klassifiseringsnivå etter sikkerhetsloven § 7-1".

Broadnet har i punkt 3.2 beskrevet hvor viktig en tydelig definering og kategorisering av GNF i de enkelte sektorer er for å identifisere skjermingsverdig eller kritisk infrastruktur. Virksomhetsforskriften § 52 reflekterer ikke disse utfordringene.

Broadnet foreslår på bakgrunn av dette at forskriftene i tillegg stiller tydelig krav hvordan departementene definerer og kategoriserer GNF, harmoniserer utpekingen mv. og gjennomfører de andre stegene vi har beskrevet i punkt 3.2 over.

4.8 Nasjonal sikkerhetsmyndighets roller og ansvar

På side 33 i Høringsnotatet fremgår det:

> "Bruk av tredjepart til å utføre tekniske sikkerhetsundersøkelser, inntrengingstesting, testing av sikkerhetstiltak og kommunikasjon- og innholdskontroll av informasjonssystemer. Departementet ber høringsinstansenes syn på om bestemmelsen gir tilstrekkelige føringer for å benytte tredjeparter til disse oppgavene, og ønsker særlig tilbakemelding på om det bør fremgår ytterligere kriterier, og i så fall hvilke, som bør fremgå av forskrift for bruk av tredjeparter i disse tilfellene".

Dagens ordning fungerer etter vårt syn tilfredsstillende. Men det er behov for å tydeliggjøre roller og ansvar.

Broadnet støtter adgangen til å bruke tredjeparter til å utføre eller bistå med å "tekniske tester og undersøkelser" for de generiske systemer, løsninger eller plattformer. Forskriftene bør åpne for at NSM deler informasjon om akkrediterte tredjeparter til virksomheter med kompetanse på de områdene som tredjepart dekker. Videre mener vi at det bør etableres egen ekspert gruppe for relevante sektorer i regi av NSM eller NorCERT der formålet er å kunne dele og samhandle om sektorspesifikke forhold. Dette gjør det også mulig for aktørene å dra nytte av NSMs spesialkompetanse, f.eks. knyttet til Tempest. De prosessuelle reglene bør for øvrig harmoniseres med §§ 14-17 i virksomhetsforskriften.

Så lenge ovennevnte mål nås, mener Broadnet det er underordnet om informasjonsutvekslingen reguleres gjennom nye forskriftskrav eller kommer i stand på andre måter.

4.9 Broadnets syn på krav om å melde erverv av kvalifisert eierandel

FD ber på side 40 i Høringsnotatet om innspill til bestemmelsen om melding av erverv:

> "Departementet ber om høringsinstansenes innspill til bestemmelsen, og vil vurdere behovet for ytterligere bestemmelser om eierskapskontroll i lys av høringsinstansenes innspill. Departementet vil også vurdere om det er mer hensiktsmessig at bestemmelsen fremgår av virksomhetsforskriften."

En rekke av de virksomhetene som underlegges den nye loven har et operativt behov for å kunne benytte utenlandske statsborgere i styret. Dette sikrer blant annet diversitet og nødvendig kompetanse. Broadnet kan ikke se at Høringsnotatet belyser dette forholdet.

Vi ber FD om å vurdere denne utfordringen og ta høyde for dette i den endelige forskriften.

4.10 Broadnet mener departementet må konkretisere det funksjonelle kravet til forsvarlig sikkerhetsnivå

FD etterlyser på side 42 innspill til kravet om et forsvarlig sikkerhetsnivå:

> "Departementet ber særlig om høringsinstansenes innspill på denne innretningen for hvordan en virksomhet kan beskytte sine skjermingsverdige verdier på en slik måte at kravet til forsvarlig sikkerhetsnivå oppnås."

Broadnet mener den eksisterende beskrivelsen av det funksjonelle kravet til et forsvarlig sikkerhetsnivå er ufullstendig. Vi støtter fullt og helt en konkretisering av forskriften på dette punktet.

I ekomsektoren har det tatt myndighetene nesten fem år å sette i gang en prosess med tilbyderne for å konkretisere innholdet i handlingsnormen. Dette taler med styrke for at detaljeringen må skje gjennom den endelige forskriften fra den trer i kraft. Dette kan ikke etterlates til etterfølgende veiledning fra sikkerhetsmyndighet, tilsynsmyndigheter eller en fremtidig revisjon.

Broadnet har utdypet vårt forslag i punkt 3.3 over. Vi viser til det som fremgår her.

4.11 Broadnets syn på godkjenning av oppbevaringsenheter

På side 59 i Høringsnotatet fremgår det:

> "Departementet har ikke foreslått nærmere regulering av godkjenning av oppbevaringsenheter. Det vil være opp til NSM hvilke krav som skal stilles til oppbevaringsenheter som skal godkjennes for oppbevaring av informasjon på de forskjellige graderingsnivåene. Departementene ber om høringsinstansenes innspill på om dette er en hensiktsmessig innretning, og hvorvidt det finnes anerkjente standarder eller metoder som bør ligge til grunn for godkjenning av oppbevaringsenheter."

Broadnet støtter at grunnprinsippene i gjeldene regulering av oppbevaringsenheter videreføres. Videre mener vi at forskriften må stille tydelige krav til sikkerhetsmyndigheter slik at det tas høyde for utvikling av oppbevaringsenheter og at dette harmoniseres med andre relevante standarder. Sikkerhetsmyndigheter må lage oversikt over godkjente oppbevaringsenheter som revideres hvert 3 eller 5 år.

Broadnet ser utfordringer med at sikkerhetsmyndigheten ikke er underlagt slik plikt, de dette medfører at sikkerheten svekkes over tid. Broadnet mener også det er utfordrende å opprettholde kompetanse og tilgjengelig reservedeler på eldre oppbevaringsenheter. I tillegg må forskriften åpne for godkjenning av oppbevaringsenheter eller skap med Tempest-egenskaper for å kunne følge den teknologiske utviklingen for lav graderte løsninger.

4.12 Broadnets syn på plikten til å gi egenopplysninger

På side 78 i Høringsnotatet står det:

> "Departementet vil vurdere om det er hensiktsmessig å kreve at den som klareres skal måtte gi slike opplysninger eller om det er tilstrekkelig at klareringsmyndighet innhenter slike

> opplysninger fra offentlige registre. I sistnevnte tilfeller kan det tenkes at klareringsmyndigheten bare ber den som skal klareres om opplysninger der disse ikke kan innhentes fra registre. På den andre siden er det å be om å få slike opplysninger fra den som klareres en måte å kunne kontrollere påliteligheten til den som skal klareres. Et alternativ til å gi en uttømmende liste er en generell plikt til å opplyse om forhold som den klarete antar er av betydning for om han eller hun er sikkerhetsmessig skikket knyttet til lovens § 8-4 fjerde ledd. Departementet ønsker høringsinstansenes innspill på hvordan plikten til å gi egenopplysninger bør reguleres."

Broadnet ønsker at sikkerhetsklareringsprosessen gjennomføres på en harmonisert måte og basert på korrekte faktum. Vi støtter forslaget så lenge det foreslåtte kravet til egenopplysninger fører til bedre vurderinger og/eller en mer effektiv prosess.

4.13 Broadnets kommentarer til vurderingsgrunnlaget for tilknytning til andre stater

På side 81 i Høringsnotatet fremgår det:

> "Bestemmelsen tilsvarer materielt sett gjeldende forskrift om personellsikkerhet § 3-3 tredje ledd. Hensikten er å regulere at klareringsmyndighetene benytter samme relevante og autorative kilde som grunnlag for å vurdere tilknytning til andre stater. Bestemmelsen forutsetter at NSM fortsatt utarbeider konkrete personellsikkerhetsmessige vurderinger av andre stater. Departementet ber om høringsinstansenes innspill på bestemmelsen, herunder om momentene i tilknytningsvurderingen bør fremgå tydeligere av forskriftene."

Broadnet ønsker sikkerhetsklarering prosessen gjennomføres på en enhetlig og basert på faktum. *Hvis krav til egenopplysninger medfører bedre vurdering og samtidig mer effektiv prosess støtter Broadnet at det stille krav til egenopplysninger.*

4.14 Broadnets kommentarer til vurderingsgrunnlaget for tilknytning til andre stater

I Høringsnotatet fremgår det på side 81:

> "Bestemmelsen tilsvarer materielt sett gjeldende forskrift om personellsikkerhet § 3-3 tredje ledd. Hensikten er å regulere at klareringsmyndighetene benytter samme relevante og autorative kilde som grunnlag for å vurdere tilknytning til andre stater. Bestemmelsen forutsetter at NSM fortsatt utarbeider konkrete personellsikkerhetsmessige vurderinger av andre stater. Departementet ber om høringsinstansenes innspill på bestemmelsen, herunder om momentene i tilknytningsvurderingen bør fremgå tydeligere av forskriftene."

Broadnet ønsker forutsigbarhet om sikkerhetsklarering for andre staters borgere, samt en presisering av hvilke stater Norge har tettere samarbeid eller et sikkerhetspolitisk samarbeid med (f.eks. Norden og EØS-land). *Broadnet foreslår at FD i den endelige forskriften stiller krav til at NSM deler slik informasjon med regulerte virksomheter.* Utover det har ikke Broadnet innspill til forslaget om å fjerne bestemmelsene i kapittel 4.

4.15 Broadnets syn på videreføring av bestemmelsene i kapittel 4 om autorisering av utenlandske statsborgere for BEGRENSET

På side 84 i Høringsnotatet skriver FD:

> "Departementet ser at de bestemmelsene som foreslås i kapittel 4 kan bli i overkant omstendelige å gjennomføre i praksis, tatt i betraktning den risiko autorisering av personell for BEGRENSET innebærer for nasjonale sikkerhetsinteresser. Departementet ber derfor om høringsinstansenes innspill, og vil vurdere etter høringsrunden hvorvidt det er hensiktsmessig å videreføre bestemmelsene i kapittel 4. Et alternativ er at virksomhetene blir gjort kjent med NSMs vurdering av andre stater, jf. § 16."

Broadnets erfaringer tilser at dagens prosesser er meget omstendelig og tidskrevende. Vi støtter derfor forslaget om deling av "NSMs vurdering av andre stater" til virksomheter underlagt sikkerhetsloven.

5 Broadnets kommentarer til de konkrete bestemmelsene i forskriftsutkastet

5.1 Behov for innføring av konkrete saksbehandlingsfrister

Den nye sikkerhetsloven stiller krav til at virksomheter som er omfattet av loven må innhente ulike former for godkjenning og forhåndsgodkjennelser fra sikkerhetsmyndigheten.
Eksempler på dette er krav om personkontroll i sikkerhetslovens § 8-5, sikkerhetsavtale og § 9-2, leverandørkontroll. I tillegg har §§ 9-3 og 9-4 regler om varslingsplikt ved anskaffelser til informasjon, objekt og infrastruktur.

Virksomheter som eier og drifter infrastruktur har til enhver tid behov for personell og nettverkskomponenter for oppgradering, utvidelse, drift og feilretting. Dersom prosedyren skal fungere i praksis må det innføres en ramme for hvor lenge den ansvarlige myndighet kan bruke for behandling av søknadene. Lang saksbehandlingstid hos offentlige myndigheter er ikke forenelig med vår operasjonelle

hverdag. Broadnet ber om at det tas inn krav til saksbehandlingsfrister for de ulike bestemmelsene som krever godkjenning fra myndighetene slik at det er forutsigbarhet for alle parter.
Når det gjelder sikkerhetslovens §9-4 er det særlig bruk for retningslinjer i forskriftene om hvilke kriterier som gjelder for at anskaffelsen kan nektes gjennomført. Bestemmelsen legger opp til at allerede signerte avtaler må termineres og det er må settes en grense slik at et vedtak kommer før partene har innrettet seg og avtalen er gjennomført.

5.2 Virksomhetsforskriften

5.2.1 Broadnets kommentarer til § 11 – Plikt to å vurdere risiko

Regulert virksomheter er avhengig av informasjon om avhengigheter både hos andre aktører i samme bransje og hos andre aktører i andre bransjer for å kunne etterleve reglene. Dersom f.eks. et sykehus underlegges sikkerhetsloven fordi den driver aktiviteter som er relevante for en GNF, må den informere aktørene som leverer bredbåndstilgangen om dette slik at de kan ivareta den tverrsektorielle dimensjonen.

Virksomhetsforskriften § 11 pålegger regulerte virksomheter en plikt til å vurdere risiko. Den tverrsektorielle dimensjonen er likevel ikke nevnt eksplisitt utover at bestemmelsen pålegger aktøren å sende departementet en oversikt over virksomheter den er avhengig av.

Broadnet foreslår på bakgrunn av dette at FD presisere at virksomheten på selvstendig grunnlag også skal vurdere risikoen knyttet til GNF-avhengigheter, både mot andre aktører i samme bransje og mot andre aktører i andre bransjer. En slik plikt må avstemmes mot varslingsplikten i virksomhetsforskriften § 52 tredje ledd.

5.2.2 Broadnets kommentarer til § 52 - Skadevurdering i forbindelse med klassifisering av skjermingsverdig objekt eller infrastruktur

Broadnet støtter forslaget i virksomhetsforskriften § 52 om å pålegge de regulerte virksomhetene en plikt til å vurdere hvilke skadefølger "skadeverk, ødeleggelse eller rettstridig overtakelse" vil få. NOU 2016:19 understreker hvor viktig det er å fange opp både et "helt" og et "delvis" funksjonstap. På side 68 fremgår det blant annet:

> "Konsekvensene av helt eller delvis bortfall av en samfunnsfunksjon er avhengig av graden av kritikalitet eller nødvendighet for samfunnet eller befolkningen, graden av resiliens og redundans i systemene som understøtter den aktuelle funksjonen, samt annen beredskap for

gjenopprettelse eller skadebegrensning. Her vil også avhengigheter mellom den aktuelle samfunnsfunksjonen og andre samfunnsfunksjoner være avgjørende for hvor omfattende konsekvensene av bortfall vil være. Konsekvensene vil også kunne variere avhengig av klima og andre naturfenomener, samt samfunnsmessige forhold"

Dette kommer ikke tydelig frem i forslaget til § 52. *Broadnet foreslår derfor at FD presisering av at vurderingen må dekke både et "helt" og et "delvis" funksjonstap som følge av "skadeverk, ødeleggelse eller rettstridig overtakelse". Videre ber vi om at bestemmelsen endres slik at den også tar høyde for kompenserende tjenester.*

6 Avslutning

Broadnet stiller gjerne til et møte for å redegjøre nærmere for innholdet i vårt høringssvar. Ta gjerne kontakt med Anurag Shukla per e-post (Anurag.Shukla@broadnet.no) eller telefon nr. +47 982 22 614 for å avtale møte eller dersom FD skulle ha spørsmål til våre kommentarer.

Med vennlig hilsen

Broadnet AS

Per Morten Torvildsen

Styreleder

Anurag Shukla

Sikkerhetssjef

Vedlegg