Nasjonal kommunikasjons-myndighet

Forsvarsdepartementet
Postboks 8126 Dep.
0032 OSLO

Vår ref.:1704851-19 - 005
Vår dato: 1.10.2018

Deres ref.: 2015/3139-254/FD V 3/ENWA
Deres dato: 2.7.2018

Saksbehandler: Svein Sundfør Scheie

Høringssvar - forskrifter til ny sikkerhetslov

Nasjonal kommunikasjonsmyndighet (Nkom) viser til brev fra Forsvarsdepartementet datert 2. juli 2018 om høring av forskrifter til ny sikkerhetslov.

Det er fremmet forslag til tre forskrifter til lov om nasjonal sikkerhet (sikkerhetsloven). Formålet med forskriftene er å regulere henholdsvis myndighetenes ansvar og roller for forebyggende sikkerhet, virksomhetens arbeid med forebyggende sikkerhet og klarering av personell og leverandører.

Nkom er tilsynsmyndighet for tilbydere av elektroniske kommunikasjonsnett- og tjenester etter lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven), herunder sikkerhets- og beredskapsplikter og kommunikasjonsvern. Nkom fører også tilsyn med skjermingsverdige objekter i ekomsektoren etter objektsikkerhetsbestemmelsene i gjeldende sikkerhetslov og Forskrift om objektsikkerhet. Objektsikkerheten i sektoren er dels regulert etter gjeldende sikkerhetslovs regime, og dels etter ekomloven § 2-10 og tilhørende forskrift om klassifisering og sikring av anlegg i elektroniske kommunikasjonsnett (klassifiseringsforskrifta).

Nkom kartlegger og gjennomfører tilsyn med Norges viktigste infrastruktur for elektronisk kommunikasjon. I tillegg gjennomfører Nkom risiko- og sårbarhetsanalyser (ROS-analyser) av kritisk infrastruktur med formål å identifisere konkrete tiltak som vil øke det nasjonale sikkerhets- og beredskapsnivået.

Nkom er positiv til at virkeområdet til loven og forskriftene gir et helhetlig nasjonalt perspektiv og en bred tverrsektoriell tilnærming til samfunnssikkerhet. Nkom mener forskriftenes tilnærming til funksjonelle krav og rettslige standarder vil bidra til at forebyggende sikkerhet kan utvikle seg i takt med samfunnet og endringer i risiko- og trusselbildet. Nkom støtter forslaget om å legge opp til en brukerrettet forskriftsstruktur som gir brukeren god oversikt over egne plikter og ansvar.

Nasjonal kommunikasjons-myndighet

Innholdsfortegnelse

Nasjonal kommunikasjons-myndighet

1 Nkoms overordnede kommentarer til forskriftene til ny sikkerhetslov

Bakgrunnen for det pågående forskriftsarbeidet er ny sikkerhetslov som ble vedtatt av Stortinget i mars 2018. Loven ble i det vesentlige vedtatt slik den ble fremmet av regjeringen gjennom Prop. 153 L (2016-2017) Lov om nasjonal sikkerhet (sikkerhetsloven). Proposisjonen baserte seg på anbefalingen fra det regjeringsoppnevnte sikkerhetsutvalgets utredning fra høsten 2016, NOU 2016:19 Samhandling for sikkerhet.

1.1 Forskriftenes formål og virkeområde

Forslaget til forskriftene har en funksjonell og overordnet tilnærming. Lovens systematikk er slik at departementene først skal identifisere de grunnleggende nasjonale funksjonene innen sitt ansvarsområde. Deretter skal departementene vurdere hvilken informasjon, informasjonssystemer, infrastruktur og objekter som er av avgjørende betydning for disse funksjonene og som dermed utpekes som skjermingsverdige.

Ny sikkerhetslov legger opp til at underlagte virksomheter selv er ansvarlig for at virksomheten har et forsvarlig sikkerhetsnivå. Det er, så langt det har vært hensiktsmessig, gitt gjennom funksjonelle krav i forskriftene. Funksjonelle krav vil si at det ikke gis detaljerte føringer for hva virksomheten skal iverksette av tiltak, men snarere at det er tydelig hva man ønsker å oppnå når det gjelder forsvarlig sikkerhetsnivå. Virksomhetene må balansere hvilke fysiske, elektroniske, menneskelige eller organisatoriske sikringstiltak som er nødvendige for å oppnå forsvarlig sikkerhetsnivå.

Kravene i forskriftene vil på enkelte områder gi føringer om hvordan virksomheten systematisk skal gå frem for å sikre verdiene de rår over. Nkom er generelt positive til at virkeområdet til loven og forskriftene gir et helhetlig nasjonalt perspektiv og en bred tverrsektoriell tilnærming til samfunnssikkerhet.

For ekomsektoren har den teknologiske utviklingen og økt globalisering medført nye eierstrukturer og samarbeidsformer som får betydning for grunnleggende nasjonale funksjoner.

Nasjonal kommunikasjonsmyndighet
Besøksadresse:
Nygård 1, Lillesand

Postadresse:
Postboks 93
4791 LILLESAND

Tel: 22 82 46 00
Fax: 22 82 46 40
firmapost@nkom.no

NO 974 446 871
www.nkom.no

Utviklingen medfører at det er en omfattende oppgave å ha en oppdatert oversikt over enkeltkomponentene i informasjonssystemer og infrastruktur, og å vurdere kritikaliteten av disse. Bruk av funksjonelle krav og rettslige standarder er grunnleggende for at forebyggende sikkerhet kan utvikle seg i takt med samfunnsutviklingen og endringer i risiko- og trusselbildet. Et funksjonelt regelverk stiller store krav til virksomhetens arbeid med forebyggende sikkerhet, og myndighetenes veiledning- og tilsynsarbeid for å oppnå et forsvarlig sikkerhetsnivå. Myndighetene har også et ansvar for at forsvarlighetsnivået blir harmonisert i egen sektor og på tvers av sektorene. Dette understreker viktigheten av en sektorvis tilnærming til sikkerhets slik ny sikkerhetslov og forskriftene legger opp til.

1.2 Om forslaget

Forsvarsdepartementet har i høringsforslaget beskrevet hvordan forslaget til forskriftene har en funksjonell overordnet tilnærming så langt det anses hensiktsmessig.

Den funksjonelle tilnærmingen innebærer en fleksibilitet for virksomheten som skal etterleve kravene, samtidig som den krever kompetanse for å komme frem til de rette sikringstiltakene. Nkom støtter en slik tilnærming.

Nkom vil understreke at den funksjonelle tilnærmingen gir Nasjonal sikkerhetsmyndighet og sektormyndighetene en grunnleggende viktig rolle med å gi råd og veiledning om hvordan bestemmelsene kan etterleves og hvordan tiltakene kan tilpasses sektorenes egenart. I mange tilfeller vil det være relevant for myndighetene å vise til standarder og andre normer for hvordan krav kan oppfylles.
Sektormyndighetene har i dag ansvar for oppfølging av sikkerhet ved utilsiktede hendelser. Nkom er positiv til at sektormyndighetene etter ny sikkerhetslov får ansvar også for oppfølging av sikkerhet ved tilsiktede hendelser fordi dette vil gi sektormyndigheten et helhetlig sikkerhetsansvar.

Et forsvarlig sikkerhetsnivå avhenge av en verdivurdering av informasjonen, informasjonssystemet, objektene og/eller infrastrukturen virksomheten råder over. Hvilke sikkerhetstiltak som iverksettes vil derfor avhenge av virksomhetens egenart, og virksomhetene må være bevist på og velge de sikringstiltakene som mest effektivt oppnår et forsvarlig sikkerhetsnivå.

Nkom mener at det er riktig å forskriftsfeste forsvarlighetsbegrepet. For ekomsektoren kom begrepet forsvarlighet inn i ekomregelverket etter en lovendring i ekomloven av 14. juni 2013 nr. 54, hvor ordlyden i ekomloven § 2-10 ble endret fra «Tilbyder skal tilby nett og tjenester med

nødvendig sikkerhet for brukerne, selv i situasjoner der nettet utsettes for ekstraordinære påkjenninger» til «Tilbyder skal tilby elektronisk kommunikasjonsnett og –tjeneste med forsvarlig sikkerhet for brukerne i fred, krise og krig.» I lovforarbeidene[1] ble det vist til Samferdselsdepartementets forslag om at sikkerheten i elektroniske kommunikasjonsnett- og tjenester ikke lenger skulle knyttes opp mot faktiske brukere, men mot en generell forsvarlighetsstandard for sikkerhet. Det ble foreslått at alle tilbydere skulle oppfylle samme forsvarlighetsstandard som et slags minstenivå for sikkerhet.

I lovforarbeidene ble det også presisert at forsvarlig sikkerhet forutsettes at nett og tjenester skal være tilgjengelige og at integriteten og konfidensialiteten skal beskyttes. Hva som for øvrig må anses for å være forsvarlig vil fremkomme gjennom markedspraksis, tilgjengelig teknologi og internasjonale krav2. Det er tilbyders ansvar at tjenestene som tilbys holder et forsvarlig sikkerhetsnivå

Nkom er positiv til at det i den nye sikkerhetsloven med forskrifter legges opp til bruk av en forsvarlighetsstandard som virksomhetene må oppfylle. Dette gir regelverket tilstrekkelig dynamikk og tilpasningsevne til å møte fortløpende endringer i samfunnet.

Nkom registrerer at det i høringsnotatet ikke er lagt opp til noen overgangsbestemmelser ved ikrafttredelse av forskriftene, men at det henvises til en rimelig frist for dette arbeidet. . Nkom er av den oppfatning at det er viktig at det er sektordepartementene som får ansvar,for å fastsette en rimelig frist for den enkelte virksomhet.

1.3 Inndeling i forskrifter

Forsvarsdepartementet har lagt opp til en brukerrettet forskriftsstruktur. Hensikten er her at virksomhetene som omfattes av ny lov skal kunne forholde seg til en enkelt forskrift for å identifisere egne plikter, og ikke opptil fem forskrifter slik situasjonen er i dag.

Nkom støtter forslaget om å legge opp til brukerrettet forskriftsstruktur. Flere samfunnsaktører- og funksjoner enn i dag vil kunne bli underlagt ny sikkerhetslov når denne trer i kraft. Begrepet «virksomheter» omfatter alle former for virksomheter, uavhengig av eierskap eller organisasjonsform. Ordlyden favner også ulike konstruksjoner av samarbeid mellom virksomheter som er involvert i verdikjeder som er av kritisk betydning i samfunnet. En

[1] Prop. 69 L 2012-2013 Endringer i ekomloven på side 33

[2] Prop. 69 L 2012-2013 Endringer i ekomloven på side 103

brukerrettet forskriftsstruktur vil bidra til at de virksomhetene som vil bli underlagt den nye sikkerhetsloven, lettere kan identifisere egne plikter og ansvar.

1.4 Hvordan oppnå et forsvarlig sikkerhetsnivå

Forsvarsdepartementet ber særlig om høringsinstansenes innspill på hvordan en virksomhet kan beskytte sine skjermingsverdige verdier på en slik måte at kravet til forsvarlig sikkerhetsnivå oppnås.

Nkom mener at det er viktig at loven og forskriftene etablerer en rettslig standard som trekker opp de ytre rammene for hvilket handlingsrom virksomhetene har for etablering av sikkerhetstiltak. En av målsetningene med loven er å lage et helhetlig robust regelverk for forebyggende sikkerhet, hvor hensynet til kostnadseffektive løsninger står sentralt. Slik Nkom ser det vil et forsvarlig sikkerhetsnivå for den enkelte virksomhet kunne variere avhengig av egne skjermingsverdige verdier og hvilket trussel- og risikonivå disse verdiene utsettes for. Nkom støtter derfor etablering av et funksjonelt regelverk istedenfor et tverrsektorielt detaljert kravsett, der virksomhetene gis tilstrekkelig handlingsrom for å oppnå et forsvarlig sikkerhetsnivå på en kostnadseffektiv måte.

Nkom vil påpeke at bruk av internasjonale anerkjente standarder i det forebyggende sikkerhetsarbeidet vil være til hjelp for virksomhetene for å oppnå et forsvarlig sikkerhetsnivå. Nkom foreslår på bakgrunn av dette at bruk av internasjonale anerkjente standarder i virksomhetenes forbyggende sikkerhetsarbeid forskriftsfestes.

Et funksjonelt regelverk forutsetter som nevnt at myndighetene gir god og rettidig veiledning. For å tilpasse et forsvarlig sikkerhetsnivå til den enkelte sektors behov for å beskytte skjermingsverdige verdier, mener Nkom det vil være nødvendig med sektorvis veiledning i tillegg til tverrsektoriell veiledning fra Nasjonal sikkerhetsmyndighet. Nkom foreslår at det forskriftsfestes en veiledningsplikt både for Nasjonal sikkerhetsmyndighet og utpekte sektortilsyn.

1.5 Objekt- og infrastruktursikkerhet

I høringsnotatet beskriver Forsvarsdepartementet at de finner det naturlig, tatt i betraktning kompleksiteten, å vurdere om det skal gis særlige regler for beskyttelse av infrastruktur etter at infrastruktur som omfattes av loven er utpekt og klassifisert. Forsvarsdepartementet ber om høringsinstansenes syn på om det bør gis mer detaljerte krav til sikring av infrastruktur.

Med et funksjonelt regelverk, med henvisning til rettslige standarder, mener Nkom at det er mindre nødvendig å gi ytterligere særlige regler for beskyttelse av infrastruktur. Vi viser til vår kommentar på forsvarlighetsnivå under punkt 1.4.

Skulle Forsvarsdepartementet likevel mene det vil være behov for et særlig regelverk for beskyttelse av infrastruktur, bør dette inngå i dette forskriftsarbeidet. Nkom mener at det er uheldig for forutsigbarheten for virksomhetene dersom særlig regelverk for infrastruktur blir implementert senere

Nkom har som tilsynsmyndighet hatt en sentral rolle i forbindelse med utpeking av objekter innenfor ekomsektoren etter dagens objektsikkerhetsforskrift. Nkom foreslår at tilsynsmyndighetenes ansvar i forbindelse med utpekingen av skjermingsverdige objekter og infrastruktur, forskriftsfestes.

Det er virksomhetene selv, i dialog med sektormyndigheten, som skal foreta skadevurderinger av egen virksomhet. Disse vurderingene gjøres på forhånd, og før departementet beslutter at objektet skal bli utpekt. Kosteffektive løsninger og redundans vil være viktige momenter når valg av sikringstiltak skal besluttes. Graden av redundans i en infrastruktur vil være en av flere momenter som påvirker sektordepartementets vurdering i forbindelse med klassifisering av skjermingsverdige objekter og infrastruktur etter myndighetsforskriften § 1 første ledd. For kritisk infrastruktur er redundans et viktig risikoreduserende tiltak for å sikre infrastrukturen. Nkoms erfaring med gjeldene sikkerhetslov er at redundans er et viktig moment når klassifisering av objekter utføresNkom har derfor foreslått at redundans forskriftsfestes som et vurderingskriterium.

1.6 Ordinær adgangsklarering og utvidet adgangsklarering

Forsvarsdepartementet foreslår to typer adgangsklarering, ordinær adgangsklarering og utvidet adgangsklarering, der sistnevnte er mer omfattende. Forsvarsdepartementet mener at denne todelingen legger til rette for rask og effektiv saksbehandling. Formålet med ordinær adgangsklarering er i hovedsak å forebygge terror. Ved utvidet adgangsklarering er formålet at kontrollen, i tillegg til terror, skal forebygge mot fremmedstatlig sabotasje og etterretning.

Nkom er positive til at det er inntatt en ny type klarering, adgangsklarering, og at denne forskriftsfestes. For laveste nivå av adgangsklarering er vurderingskriteriene lagt opp slik at det er mulig å adgangsklarere personell fra utlandet. Dette er viktig for ekomsektoren der det er behov for utenlandsk spesialkompetanse for å løse oppgaver knyttet til kritisk infrastruktur. Mye

samarbeid skjer på tvers av landegrensene, og da særlig i Norden. Nkom anser det som viktig at nordiske borgere kan få adgangsklarering på begge nivå, og at dette går klart frem av forskriftene.

1.7 Sikkerhetsklarering av utenlandske statsborgere

I forarbeidene til ny sikkerhetslov er følgende uttrykt om behovet for å kunne klarere utenlandske statsborgere uten tilknytning til Norge, jf. Prop. 153 L (2016-2017) pkt. 12.5.2 på s. 132:

«Det kan likevel være et særskilt behov for å klarere en utenlandsk statsborger uten tilknytning til Norge, eksempelvis dersom personen besitter særlig kompetanse som er av betydning for nasjonale sikkerhetsinteresser eller andre spesifikke nasjonale interesser. Ordlyden i departementets forslag gir tilstrekkelig handlingsrom til å kunne klarere personer som ikke har tilknytning til Norge, der særskilte grunner gjør dette nødvendig.»

I høringsnotatet erkjenner Forsvarsdepartementet at praktisering av gjeldende rett har vært for snever, og det foreslås derfor en forsiktig oppmyking av praksis, ved at handlingsrommet i ny sikkerhetslov § 8-7 benyttes i større grad. Dette vil i større grad muliggjøre klarering av utenlandske statsborgere, også de uten tilknytning til Norge.

Nkom vil påpeke viktigheten av at klareringsmyndigheten innhenter råd fra sektormyndigheten når det gjelder vurderingen av om en person innehar en særlig kompetanse som gjør at det er særskilte grunner for sikkerhetsklarering Det er sektormyndigheten som er nærmest til å avklare kompetansebehov i egen sektor.

1.8 Økonomiske og administrative konsekvenser

Nkom viser til vårt høringssvar til ny sikkerhetslov, hvor vi påpekte at det medføre både administrative og økonomiske konsekvenser for den enkelte virksomhet innen ekomsektoren å bli underlagt ny sikkerhetslov. Det kan her nevnes organisasjonsmessige tilpasninger for å oppfylle krav til forebyggende sikkerhetsstyring med opplæring, analyse, rapportering mv., samt kostnader i forbindelse med fysiske og logiske sikringstiltak. For ekomsektoren som helhet vurderer Nkom at ny sikkerhetslov og tilhørende forskrifter ikke vil ha negative konsekvenser for nyetablering av aktører og den totale konkurransesituasjonen. En sikkerhetslov med forskrifter som gir sektormyndigheten ansvar for å tilpasse krav til næringen, vil gi økt tillitt til den overordnede sikkerheten innen ekomsektoren og overordnet sett være positivt for det norske ekommarkedet.

Sektoransvaret som vil tilfalle Nkom etter ny sikkerhetslov med tilsyn og utpeking av relevante virksomheter, objekter og infrastruktur, falle inn under vår kjernevirksomhet med ansvar for oppfølging av sikkerhet, beredskap og kommunikasjonsvern i ekomsektoren. Under forutsetning av tilstrekkelige ressurser vil ikke sektoransvaret etter ny sikkerhetslov med forskrifter få vesentlige administrative konsekvenser for Nkom.

1.9 Nkoms generelle kommentarer til forslag til forskrifter til ny sikkerhetslov

1.9.1 Skjermingsverdige informasjonssystemer

Nkom er positiv til at ny sikkerhetslov med forskrifter i større grad enn før søker å beskytte tilgjengelighet og integritet, i tillegg til konfidensialitet. Nkom mener imidlertid at høringsnotatet og forskriftene ikke i tilstrekkelig grad beskriver skjermingsverdig informasjonssystemer som ikke behandler gradert informasjon. Skjermingsverdige informasjonssystemer bør defineres i § 1 i virksomhetsforskriften, og Nkom foreslår at det tydeliggjøres i forskriften hvilke plikter som kun gjelder skjermingsverdige informasjonssystemer som ikke behandler gradert informasjon.

1.9.2 Sektorvis tilnærming

Nkom er som nevnt positiv til at oppfølging av ny sikkerhetslov med forskrifter i stor grad legges til utpekte sektormyndigheter, noe som medfører at sektormyndigheten får et helhetlig ansvar for sikkerhet,- både tilsiktede og utilsiktede hendelser.

Den teknologiske utviklingen og økt globalisering medfører nye utfordringer i flere sektorer, og nye eierstrukturer og samarbeidsformer vil få betydning i forhold til hvilke virksomheter og objekter som må anses å ha kritisk betydning for grunnleggende nasjonale funksjoner. Ovennevnte utvikling vil også medføre økt behov for spesialkompetanse som kan være vanskelig å finne i Norge. Nkom mener utviklingen understreker viktigheten av å ha en sektorvis tilnærming til gjennomføringen av ny sikkerhetslov med forskrifter ettersom det som nevnt er sektormyndigheten som er nærmest til å avklare utvikling og behov i egen sektor.

1.9.3 Hjemmelsgrunnlag for sikkerhetsklarering

I ekomsektoren har det vært en utfordring å finne hjemmelsgrunnlag for å sikkerhetsklarere personell som utfører kommunikasjonskontroll og anmodninger for fritak fra taushetsplikt som er gradert HEMMELIG og høyere for politiet og PST. Nkom viser i denne sammenheng til EOS-utvalgets rapport fra 2012 og 2013 hvor denne problemstillingen ble belyst. Kontroll- og konstitusjonskomiteen fulgte opp dette i sin innstilling hvor de fremmet følgende forslag:

«Stortinget ber regjeringen sikre at personer som er direkte involvert i arbeid for selskap som bistår ved utførelse av etterretnings-, overvåkings- og sikkerhetstjeneste, sikkerhetsklareres.»

Nkom ber Forsvarsdepartementet sikre at denne problemstillingen blir vurdert før forskriftene fastsettes.

1.9.4 Varsling til tilsynsmyndighet

Forskriftene inneholder flere bestemmelser om varsling til Nasjonal sikkerhetsmyndighet og departementene. Nkom mener at det er nødvendig at det forskriftsfestes en varslingsplikt også til de utpekte tilsynsmyndighetene. Det vil være vanskelig for tilsynsmyndighetene å utføre sitt ansvar innenfor forebyggende sikkerhet dersom disse ikke blir varslet.

1.9.5 Sikkerhetsgraderte anskaffelser

Regelverket for sikkerhetsgraderte anskaffelser er et viktig verktøy for å kunne sikre at leverandører som gis tilgang til skjermingsverdige objekter er sikkerhetsmessig til å stole på.

Globalisering og økt internasjonalisering av vare- og tjenestehandelen har ført til at eiere av kritisk infrastruktur, i større utstrekning enn tidligere, bruker utenlandske selskaper som leverandører til norsk kritisk infrastruktur.

Utstrakt bruk av utenlandske leverandører er potensielt problematisk fordi det kan medføre en forhøyet risiko for spionasje og sabotasje til skade for norske interesser.

En anskaffelse til en skjermingsverdig verdi vil kunne føre til økt risiko for sikkerhetstruende virksomhet mot verdien, ved at leverandører får tilgang til eller leverer komponenter til denne. Forskriftene stiller derfor krav til at virksomheten må opprettholde et forsvarlig sikkerhetsnivå ved anskaffelser til den skjermingsverdige verdien. Før en sikkerhetsgradert anskaffelse iverksettes, skal virksomheten inngå en sikkerhetsavtale med leverandøren. Det kan kun inngås sikkerhetsavtale med leverandører fra land Norge har sikkerhetsmessig samarbeid med.

Innenfor ekomsektoren er det i dag flere tilbydere som har utstyr levert fra utenlandske leverandører fra land Norge ikke har sikkerhetsmessig samarbeid med, noe som ikke er uproblematiske i forhold til vurderinger av risiko for spionasje og sabotasje mot norsk ekom-infrastruktur.

Nkom vil forøvrig påpeke viktigheten av en bred tilnærming til sikkerhet når myndighetene vurderer valg av leverandører og landtilhørighet. God diversitet mellom leverandørene til norske ekomnett- og tjenester vil også være med på å bidra til økt sikkerhet inne ekomsektoren.

Når det gjelder utstyrsleveranser vil Nkom påpeke at praksisen med følgetjeneste ikke vil være et like godt risikoreduserende tiltak i logiske systemer som i fysiske objekter. I fysiske objekter vil følgetjenesten kunne følge med på hva vedkommende gjør og gripe inn dersom vedkommende forsøker å gjøre noe ulovlig. Ved logisk tilgang fra leverandøren vil virksomheten ofte ikke ha tilstrekkelig kompetanse eller innblikk i hva vedkommende utfører til å ha mulighet til å forhindre ulovlig aktivitet.

Nkom støtter bestemmelsene i forskriftene om sikkerhetsgraderte anskaffelser og krav til sikkerhetsavtale. Nkom vil påpeke at det er viktig med god sektorkunnskap for å vurdere om det skal gjøres unntak fra kravet til sikkerhetsavtale med leverandører.

1.9.6 Unntakshjemmel

Unntakshjemmelen i virksomhetsforskriften § 19 åpner for at det i særlige tilfeller kan gis unntak fra kravene til sikkerhet som fremgår av virksomhetsforskriften. Forsvarsdepartementet skriver i høringsnotatet at det på nåværende tidspunkt er uklart hvordan kravene i virksomhetsforskriften vil treffe de ulike sektorene, og at det i enkelte tilfeller derfor kan være behov for å gjøre konkrete tilpasninger mellom ulike eksisterende sikkerhetsregimer som gjør det nødvendig å gjøre unntak fra kravene i forskriften. Både Nasjonal sikkerhetsmyndighet og sektortilsyn kan gi slike unntak. Nkom mener at unntakshjemmelen i § 19 i virksomhetsforskriften er helt nødvendig for å gi tilsynsmyndigheten et tilstrekkelig handlingsrom i oppfølgingen av virksomhetene og for å oppnå et forsvarlig sikkerhetsnivå i egen sektor.

2 Nkoms kommentarer til forskrift om myndighetenes roller og ansvar for nasjonal sikkerhet (myndighetsforskriften)

Forskrift om ansvar og myndighet for nasjonal sikkerhet (myndighetsforskriften)retter seg først og fremst mot departementene, Nasjonal sikkerhetsmyndighet og myndigheter som fører tilsyn etter ny sikkerhetslov med forskrifter. Myndighetsforskriften regulerer de overordnede roller, ansvar og oppgaver.

2.1 Departementets roller og oppgaver

2.1.1 Klassifisering av skjermingsverdige objekter og infrastruktur – til forskriftens § 1

Bestemmelsen regulerer departementenes og Nasjonal sikkerhetsmyndighets ansvar og myndighet til å utpeke, klassifisere og holde oversikt over skjermingsverdige objekter og infrastruktur. Bestemmelsen ses i sammenheng med Nasjonal sikkerhetsmyndighet og departementenes myndighet til å treffe enkeltvedtak etter ny sikkerhetslov § 2-1, første ledd bokstav c og § 2-2, første ledd bokstav e.

Utpeking og klassifisering av de skjermingsverdige objektene og infrastrukturen forutsetter at departementet først har identifisert grunnleggende nasjonale funksjoner. For å bestemme hvilke deler av objektene og infrastrukturene som skal klassifiseres og til hvilket nivå, må det vurderes hvilket tap man kan akseptere, hvor mye av funksjonen det gjelder (kapasitet), for hvor lenge (varighet), og i hvilken grad innholdet i funksjonens leveranse forringes (kvalitet), før det får konsekvenser av avgjørende betydning for grunnleggende nasjonale funksjoner.

Nkom støtter at man har brukt den metodiske tilnærmingen i KIKS-modellen3 for vurdering av samfunnskritiske funksjoner når det skal vurderes hvilken betydning objektet eller infrastrukturen har for grunnleggende nasjonale funksjoner. Modellenn gjør det mulig å etablere en overbygning for den sektorvise risikostyringen av kritisk infrastruktur og kritiske samfunnsfunksjoner. Arbeidet etter KIKS-modellen har to dimensjoner: etablering av et system for oppfølging av sikkerheten på overordnet nivå, og en tydeliggjøring av hvilke samfunnsfunksjoner som er å regne som kritiske.

Som nevnt innledningsvis er redundans et viktig risikoreduserende tiltak for å sikre infrastrukturen, og redundans vil således utgjøre et av de mest sentrale sikkerhetstiltakene hos virksomhetene. Redundans vil være et viktig vurderingskriterium som bør vektlegges ved en

[3] *Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner, DSB*

klassifisering av skjermingsverdige objekter og infrastruktur etter ny sikkerhetslov § 7-2. Nkom mener at grad av redundans bør forskriftsfestes som et vurderingskriterium og dermed tas inn som en bokstav c i bestemmelsen.

Nkom foreslår følgende endring i myndighetsforskriftens paragraf 1 bokstav c:
«i hvor stor grad redundans reduserer objektet eller infrastrukturens betydning for grunnleggende nasjonale funksjoner.»

Nkom mener samtidig at det også bør forskriftsfestes en ny bokstav d, om utpekte tilsynsmyndigheters ansvar til å gi vurderinger til klassifisering av skjermingsverdige objekter og infrastruktur innenfor eget ansvarsområder. Dette for å skape et helhetlig og balansert sikringsnivå i sektoren.

Nkom foreslår følgende endring i myndighetsforskriftens paragraf 1 ny bokstav d:
«sektormyndighetens vurdering av virksomhetens skadevurdering, jf. bokstav b.»

2.1.2 Bruk av adgangsklarering – til forskriftens § 2

Adgangsklareringsbestemmelsen er en ny type klarering jf. ny sikkerhetslov § 8-3. Hvor omfattende eller nær tilgangen til objektet eller infrastruktur må være for at den skal kunne begrunne krav om adgangsklarering, beror på en vurdering av i hvilken grad den tilgangen som gis gir mulighet til å utføre sikkerhetstruende virksomhet.

Nkom er positive til at adgangsklarering er tatt inn som en ny type klarering, og at denne forskriftsfestes. For laveste nivå av adgangsklarering er vurderingskriteriene lagt opp slik at det er mulig å adgangsklarere personell fra utlandet. Dette er særlig viktig for ekomsektoren der det kan være behov for utenlandsk spesialkompetanse for å løse oppgaver knyttet til kritisk infrastruktur. Mye samarbeid skjer her på tvers av landegrensene i Norden, og Nkom anser det som viktig at nordiske borgere kan få adgangsklarering på begge nivå. Dette bør gå klart frem av forskriftene.

Nkom foreslår et nytt ledd i § 1 i myndighetsforskriften som pålegger departementet og utpekt tilsynsmyndighet å gjøre en selvstendig vurdering av om det skal stilles krav til adgangsklarering i forbindelse med klassifisering av skjermingsverdige objekter og infrastruktur jf. virksomhetens plikt til å vurdere etter § 55 i virksomhetsforskriften. Nkom anser det som viktig at man forskriftsfester myndighetenes plikt til å gjøre denne vurderingen.

2.2 Nasjonal sikkerhetsmyndighets roller og ansvar

2.2.1 Iverksettelse av inntrengningstesting, kommunikasjons- og innholdskontroll og testing av sikkerhetstiltak – til forskriftens § 3

Bestemmelsen gir Nasjonal sikkerhetsmyndighet muligheten til å iverksette inntrengingstesting, kommunikasjons- og innholdskontroll og testing av sikkerhetstiltak når virksomhetens leder ber om det. En anmodning om at slike tester mv. blir gjennomført innebærer imidlertid ikke en plikt for Nasjonal sikkerhetsmyndighet om å iverksette.

Nkom støtter bestemmelsens utforming og ser viktigheten av at det skal inngås en avtale mellom Nasjonal sikkerhetsmyndighet og virksomheten om omfang og gjennomføring av inntrengingstesting, kommunikasjons- og innholdskontroll og testing av sikkerhetstiltak.

2.2.2 Iverksettelse av tekniske sikkerhetsundersøkelser – til forskriftens § 4

I likhet med § 3 foreslås det i § 4 at også tekniske undersøkelser (TSU) kan iverksettes av Nasjonal sikkerhetsmyndighet når virksomhetens leder ber om det. Det skal inngås en avtale med virksomheten om hvilket personell som skal stå for undersøkelsen, og hva undersøkelsen skal omfatte. Nkom støtter bestemmelsens utforming og at inngåelse av avtale forskriftsfestes i likhet med § 3. Nkom mener det vil være hensiktsmessig å få til en henvisning etter bestemmelsens første setning hvor det henvises til § 5-5 i ny sikkerhetslov der TSU er definert.

2.2.3 Fellesregler for tekniske sikkerhetsundersøkelser, inntrengningstesting, testing av sikkerhetstiltak og kommunikasjons- og innholdskontroll av informasjonssystemer – til forskriftens § 5

Bestemmelsen angir fellesregler for at resultater fra undersøkelser, testing og kontroller skal rapporteres til virksomheten og den myndigheten som fører tilsyn etter loven. Videre peker den på at informasjonen ikke skal identifisere enkeltpersoner som har begått eventuelle sikkerhetsbrudd, samt at hovedregelen er en tre måneders sletteplikt. Nkom mener bestemmelsen er viktig for å skape tillitt mellom den enkelte virksomhet og Nasjonal sikkerhetsmyndighet/myndighetene.

2.2.4 Bruk av tredjepart til å utføre tekniske sikkerhetsundersøkelser, inntrengingstesting, testing av sikkerhetstiltak og kommunikasjon- og innholdskontroll av informasjonssystemer – til forskriftens § 6

Bestemmelsen regulerer Nasjonal sikkerhetsmyndighets mulighet til å utpeke virksomheter til å utføre tekniske sikkerhetsundersøkelser, inntrengingstesting, testing av sikkerhetstiltak og kommunikasjon- og innholdskontroll av informasjonssystemer.

Nkom ser at det vil kunne bli behov for at flere enn Nasjonal sikkerhetsmyndighet kan utføre slike undersøkelser, tester og kontroller nå som virkeområdet utvides, og er positive til at man forskriftsfester en unntaksbestemmelse. Nkom mener at en utpeking av virksomheter bør skje gjennom en åpen og transparent konkurranse etter fastsatte kriterier.

2.2.5 Om kryptosikkerhetstjenester – til forskriftens § 7

Bestemmelsen beskriver den rolle og det ansvaret Nasjonal sikkerhetsmyndighet har når det gjelder kryptosikkerhetstjenester. Bestemmelsen bidrar også til å ivareta Norges forpliktelser overfor NATOs regelverk gjennom å beskrive og plassere ansvar for konkrete roller som de enkelte medlemsland skal ivareta. Nkom har ingen kommentarer til bestemmelsen, og er således enig i det som er anført.

2.2.6 Register over avgjørelser om personklarering – til forskriftens § 8

Bestemmelsen er en videreføring av gjeldende personellforskrift § 4-7, hvor det fremgår at hver enkelt klareringsmyndighet skal føre register over egne klareringsavgjørelse, og at Nasjonal sikkerhetsmyndighet i tillegg skal føre et sentralt register over alle klareringsavgjørelser som er foretatt. I mangel av en god og tilgjengelig elektronisk løsning som autorisasjonsansvarlig kan benytte seg av for å registrere autorisasjonsstatus, har man valgt å angi at registeret kan inneholde informasjon om autorisasjonsstatus, når den er tilgjengelig.

Nkom er positiv til at det forskriftsfestes at klareringsstatus kan utleveres til autorisasjonsansvarlig. Det er viktig for virksomhetene å ha en lett tilgjengelig oversikt over eget personell og klareringsstatus. Videre anser Nkom det som hensiktsmessig at det forskriftsfestes deling med PST når nasjonale sikkerhetsinteresser krever, det slik departementet har gjort i tredje ledd.

2.2.7 Register over leverandørklareringer og sikkerhetsgraderte anskaffelser – til forskriftens § 9

Bestemmelsen omhandler Nasjonal sikkerhetsmyndighets plikt til å føre et sentralt register over alle leverandørklareringer og inngåtte avtaler om sikkerhetsgraderte anskaffelser. Bestemmelsen tydeliggjør hvilke opplysninger om leverandørklareringer registeret skal inneholde, samt en plikt til oppdragsgiver om årlig å sende en oversikt over egne sikkerhetsgraderte anskaffelser til klareringsmyndigheten og Nasjonal sikkerhetsmyndighet.

Nkom støtter en regulering av et sentralt register. Nkom mener at det kunne vært formålstjenlig å innta i bestemmelsen en hjemmel for å få utlevering av klareringsstatus, eksempelvis følgende: «opplysninger om klareringsstatus kan utleveres til virksomheter underlagt sikkerhetsloven ved tjenstlig behov.»

2.2.8 Utlevering av opplysninger om klarering og personkontroll til andre staters myndigheter eller internasjonale organisasjoner – til forskriftens § 10

Bestemmelsen åpner opp for at Nasjonal sikkerhetsmyndighet på forespørsel kan opplyse fremmed stat eller internasjonale organisasjoner om en person er gitt sikkerhetsklarering og for hvilken sikkerhetsgrad. Bestemmelsen setter samtidig begrensninger for hva det kan opplyse om, av hensyn til personvernet.

Nkom støtter en slik videreføring av tydelig hjemmel når det gjelder håndtering av personopplysninger i forbindelse med klareringssaker. Dette er viktig med tanke på den enkeltes personvern og rettssikkerhet.

2.2.9 Unntak fra krav om sikkerhetsklarering og autorisasjon – til forskriftens § 11

Bestemmelsen gir Nasjonal sikkerhetsmyndighet mulighet for i særlige tilfeller å gjøre unntak fra kravet om klarering etter ny sikkerhetslov § 8-1, og unntak fra kravet i klareringsforskriften § 26.

Nkom ser det som fornuftig å ha en unntaksbestemmelse, da spesielt med tanke på andre ledd hvor det skal vurderes om behovet for tilgang er større enn risikoen som manglende klarering eller samtykke vil innebære for nasjonale sikkerhetsinteresser. Nkom støtter Forsvarsdepartementets merknader til bestemmelsen om at unntakene skal praktiseres snevert og kun brukes i særlige tilfeller.

2.3 Nasjonal responsfunksjon og nasjonalt varslingssystem for digital infrastruktur (VDI)

2.3.1 Utøvelse av nasjonalt responsfunksjon for alvorlige digitale angrep og nasjonalt varslingssystem for digital infrastruktur – til forskriftens § 12

Kritisk infrastruktur blir mer og mer avhengig av IKT og Internett, og dette utgjør en stor sårbarhet. Hensikten med VDI er å innhente, analysere og dele informasjon om angrep mot kritisk infrastruktur. Dette oppnås blant annet gjennom utplassering av sensorer i et representativt utvalg virksomheter som innehar kritisk infrastruktur eller informasjon. Informasjon fra sensorene bidrar til en nasjonal evne til tidlig deteksjon og verifikasjon av koordinerte og målrettede angrep. Når angrep mot vår mest kritiske infrastruktur inntreffer, bidrar slik informasjon til bedre analyse og håndtering av angrep på nasjonalt nivå.

Bestemmelsen fastsetter at det er Nasjonal sikkerhetsmyndighet som skal drive responsfunksjonen og varslingssystemet for digital infrastruktur. Denne oppgaven ligger til Nasjonal sikkerhetsmyndighet i dag, og ny sikkerhetslov § 2-4 har ikke ment å innebære noen materiell endring fra gjeldende sikkerhetslov. Nkom støtter at det er Nasjonal sikkerhetsmyndighet som skal drive VDI.

Nkom bemerker at påleggsbestemmelsen er tatt bort fra tidligere utkast til bestemmelsen. Nkom mener at det bør reguleres inn en påleggskompetanse og at denne bør legges til sektormyndigheten som har den nødvendige kjennskap til virksomhetene i egen sektor. Videre mener Nkom at den myndighet som pålegger tilknytning til VDI, må dekke kostnadene ved slikt pålegg.

2.3.2 Informasjonsbehandling og –deling – til forskriftens § 13

Bestemmelsen gir Nasjonal sikkerhetsmyndighet hjemmel til å dele informasjon med partene i Felles cyberkoordineringssenter (FCKS) når dette er av betydning for å sikre nasjonale sikkerhetsinteresser. FCKS er et samarbeid mellom Etterretningstjenesten, Kripos, Nasjonal sikkerhetsmyndighet og PST, og ble opprettet for å styrke evnen til å motvirke truslene i det digitale rom. Hensikten med bestemmelsen er å sikre informasjonsflyt mellom de hemmelige tjenestene og på den måten bidra til å oppfyllet formålet med FCKS.

Nkom støtter bestemmelsen og er enig i at en slik koordinering er grunnleggende viktig for å sikre nasjonale sikkerhetsinteresser. Nkom mener at bestemmelsen bør inneholde et nytt andre

ledd der Nasjonal sikkerhetsmyndighet gis hjemmel til å dele informasjon med de sektorvise responsmiljøene (SRM), og virksomheter tilknyttet VDI. Nkom anser det som viktig at sektormyndigheten får tilgang til den informasjonen som VDI-sensorene gir.

Nkom foreslår nytt andre ledd til myndighetsforskriftens paragraf 13:
«Nasjonal sikkerhetsmyndighet kan dele informasjon med sektorvise responsmiljøene og virksomheter tilknyttet VDI når delingen er innenfor lovens formål og avtale er inngått etter virksomhetsforskriften § 56 andre ledd.»

2.4 Tilsyn

Nkom er som nevnt positive til at myndighet med sektoransvar skal føre tilsyn etter ny sikkerhetslov. Sektormyndighetene vil med dette få ansvaret for både tilsiktede og utilsiktede hendelser, og få ansvar for en helhetlig sikkerhetsstyring av sektoren.
Nkom mener at det er nødvendig å forskriftsfeste sektormyndighetens adgang til å utarbeide sektorspesifikke veiledninger og metoder. Sektormyndighetens veiledninger må bygge på Nasjonal sikkerhetsmyndighets generelle veiledninger og basere seg på sektorspesifikk kunnskap. Nkom mener at tilsynsmyndighetens veiledningsrolle bør inngå som en del av samarbeidsavtalen mellom sikkerhetsmyndighet og tilsynsmyndighet.

Nkom forslår på bakgrunn av dette en ny bokstav i til myndighetsforskriften § 15:
«sektormyndighetens ansvar for veiledning i egen sektor.»

2.4.1 Tildeling av tilsynsansvar – til forskriftens § 14

Tildeling av tilsynsansvar reguleres i ny sikkerhetslov § 3-1. Nasjonal sikkerhetsmyndigheten skal påse at det føres tilsyn med virksomheters gjennomføring av kravene til forebyggende sikkerhet etter loven.

Nkom er positive til hybridmodellen som blir innført med ny sikkerhetslov, der den utøvende funksjonen overfor virksomhetene i praksis ivaretas av sektormiljøene. Lovens virkeområde stiller krav til oppdaterte vurderinger av hele verdikjeder i den enkelte sektor i langt større grad enn etter gjeldende regelverk. Nkom mener derfor at en slik funksjonsdeling mellom Nasjonal sikkerhetsmyndighet og sektorene er den mest effektive løsning for gjennomføring av lovens krav med forskrifter.

Nkom støtter bestemmelsens klargjøring av det overordnede ansvaret som tillegges sikkerhetsmyndigheten når det kommer til rådgivning og informasjon til sektorene, og det å holde en tverrsektoriell oversikt over faktisk praktisering av loven. Dette vil være til god støtte når sektormyndighetene skal gi veiledning i egen sektor.

Videre støtter Nkom det helhetlige ansvaret som tillegges den sektormyndighet som får et tilsynsansvar med å følge opp ny sikkerhetslovs i egen sektor. Dette innebærer ansvar til å gi råd, veiledning og informasjon til virksomhetene. Her vil samarbeidsavtalen mellom Nasjonal sikkerhetsmyndighet og sektormyndighetene bli et viktig verktøy for hvordan oppgavene fordeles for å unngå dobbeltarbeid og unødvendig dublering av kompetansemiljøer.

Nkom mener at forskriftens § 14 første ledd er overflødig og dekkes av ny sikkerhetslov § 3-1 andre ledd.

2.4.2 Avtale om samarbeid mellom Nasjonal sikkerhetsmyndighet og andre myndigheter med tilsynsansvar – til forskriftens § 15

Bestemmelsen regulerer samhandlings- og koordineringsplikten mellom Nasjonal sikkerhetsmyndighet og relevante sektormyndigheter. Nkom støtter forslaget om at det etableres samarbeidsavtaler mellom Nasjonal sikkerhetsmyndighet og andre myndigheter med tilsynsansvar. Nkom foreslår en endring av bestemmelsens tredje ledd for å forskriftsfeste at samarbeidsavtalen bør revideres regelmessig.

Nkom foreslår følgende endring av tredje ledd i myndighetsforskriften § 15:
«Departementet har ansvar for at det inngås samarbeidsavtale mellom Nasjonal sikkerhetsmyndighet og myndigheten som tildeles tilsynsansvar. Avtalen skal revideres regelmessig.»

Nkom er enig i at Nasjonal sikkerhetsmyndighet bør ha et overordnet ansvar for å sikre grunnleggende kriterier for tilsyn og opplæring til tilsynspersonell ettersom flere samfunnsaktører- og funksjoner enn i dag vil kunne bli underlagt ny sikkerhetslov. På enkelte fagområder vil det ikke være hensiktsmessig å bygge opp egen kompetanse på enkelte spesialområder hos sektormyndighetene, eksempelvis på kryptosikkerhet. Nkom er positive til at Forsvarsdepartementet vurderer at sektormyndighetene på enkelte fagområder kan inngå en avtale om at Nasjonal sikkerhetsmyndighet bidrar med forberedelse og gjennomføring av tilsyn.

Videre vil Nkom understreke viktigheten av at sektormyndigheten får nødvendig sikkerhetsinformasjon og trusselinformasjon fra de hemmelige tjenestene for å kunne ivareta sitt ansvar som tilsynsmyndighet. Forsvarlig risikohåndtering krever god kjennskap til både verdiene som skal beskyttes, sårbarheter og trusselbildet.

Nkom etablerte i 2014 sikkerhetsforum for elektronisk kommunikasjon, «Ekomsikkerhetsforum». Forumet består av Nkom, representanter for utvalgte ekomtilbydere, Nasjonal sikkerhetsmyndighet (NSM), Politiets sikkerhetstjeneste (PST) og Etterretningstjenesten (ETJ). Møter i forumet gjennomføres med faste intervaller og ved behov, og hovedmål er å være en felles arena for tillitsbasert utveksling av informasjon som kan gi tilbyderne et godt grunnlag for egne risikoanalyser og risikohåndtering. Risikoanalyser omfatter aktørbaserte villede hendelser. Erfaringene med Ekomsikkerhetsforum så langt er at forumet gir både tilbyderne og EOS-tjenestene god og relevant trusselinformasjon for det forebyggende sikkerhetsarbeidet, og at det er et godt instrument for sektormyndigheten både ved oppfølging av sektorspesifikke sikkerhetsbestemmelser, sektorens tilsynsansvar og i forhold til sikkerhetsloven.

Nkom ser at det er nødvendig at det etableres samarbeidsforum for tilsynsvirksomheter som nevnt i høringsnotatet. Nkom deltar i samhandlingsarena for tilsyn som ledes av Nasjonal sikkerhetsmyndighet, og ser viktigheten av å videreutvikle denne arenaen, og av å kunne ha en løpende dialog for å harmonisere og sikre rett kvalitet på tilsyn på tvers av sektorene.

2.4.3 Tilsynsmyndighet for leverandører i sikkerhetsgraderte anskaffelser – til forskriftens § 16

Bestemmelsen regulerer Nasjonal sikkerhetsmyndighets tilsynsansvar med norske leverandører i sikkerhetsgraderte anskaffelser. Bakgrunnen for dette er at mange leverandører ikke kan kategoriseres inn under en definert sektor når de er leverandører til ulike oppdragsgivere. Nkom er enige i at det vil være et enklere og mer forutsigbart regime at Nasjonal sikkerhetsmyndighet som hovedregel skal være tilsynsmyndighet overfor alle disse leverandørene.

2.4.4 Om tilsyn med virksomheter underlagt lov om nasjonal sikkerhet – til forskriftens § 17

Bestemmelsen omhandler tilsynsmyndighetens ansvar for tilsyn med virksomheter underlagt ny sikkerhetslov. Nkom er enig i de generelle prinsippene for gjennomføring av tilsyn med virksomheter underlagt ny sikkerhetslov.

Nkom mener at ordlyden i myndighetsforskriften andre ledd bør endres for å gjøre bestemmelsen mer klar. Det foreslås derfor en endring lik den som står i høringsnotatet: «Tilsyn skal gjennomføres planlagt, systematisk og regelmessig, og følge et program som er utarbeidet på bakgrunn av risiko og vesentlighet.»

Nkom støtter at det benyttes en internasjonal anerkjent standard for tilsynsmetodikk. En slik standard kan for eksempel være ISO 19011. Standarden er vel etablert og anerkjent, og det finnes mange opplæringsprogrammer for innføring i denne.

2.4.5 Rapport etter tilsyn – til forskriftens § 18

Bestemmelsen regulerer tilsynsmyndighetens plikt til å utarbeide en foreløpig rapport som skal forelegges virksomheten til uttalelse. Videre fastsettes det en plikt til å utarbeide en endelig rapport som skal sendes virksomheten og Nasjonal sikkerhetsmyndighet. Nkom mener bestemmelsen er viktig for at Nasjonal sikkerhetsmyndighet skal kunne ivareta sine tverrsektorielle oppgaver, og ha kjennskap til sikkerhetstilstanden også i de sektorene hvor det er utpekt sektormyndigheter med tilsynsansvar.

2.4.6 Tvangsmulkt – til forskriftens § 19

Bestemmelsen gir hjemmel til å ilegge en virksomhet som har overtrådt loven en engangsmulkt eller løpende mulkt. Vedtak om tvangsmulkt skal kunne påklages, jf. lovens § 11-2. Nkom har pr. i dag mulighet til å ilegge tvangsmulkt og andre typer sanksjoner for å påse etterlevelse av ekomregelverket. En forutsetning for bruk av sanksjoner er klare regler om forholdsmessighet og klagerett.

Nkom er enig i at muligheten til å ilegge mulkt er et viktig verktøy for tilsynsmyndigheten. Nkom vil imidlertid påpeke at det er viktig at hjemmelsgrunnlaget fremgår tydeligere i forskriften.. Bestemmelsen om tvangsmulkt bør derfor endres til å gjelde både tvangsmulkt og overtredelsesgebyr. Nkom viser til ekomforskriften § 10-3 hvor en slik opplisting av sanksjonshjemler er listet opp.

Videre fremgår det av bestemmelsen at tilsynsmyndighet kan frafalle påløpt tvangsmulkt. Det er imidlertid ikke nevnt noe om når en slik frafallelse kan være aktuelt. Nkom stiller spørsmål om det bør være opp til hver enkelt tilsynsmyndighet å etablere en praksis på dette.

2.5 Andre bestemmelser

2.5.1 Melding om erverv av kvalifisert eierandel i virksomhet underlagt sikkerhetsloven – til forskriftens § 20

Bestemmelsen regulerer hva en melding om erverv av kvalifisert eierandel i virksomhet underlagt ny sikkerhetslov skal inneholde. Nkom mener det vil være hensiktsmessig å flytte denne bestemmelsen inn i virksomhetsforskriften ettersom det er virksomheten som skal sende melding.

Nkom ser ikke behov for ytterligere forskriftsfesting av eierskapskontroll ettersom vi mener ny sikkerhetslov § 10-2 og § 10-3 er tilstrekkelig klare.

2.5.2 Oppnevning av advokater etter sikkerhetsloven § 8-15 – til forskriftens § 21

Nkom støtter Forsvarsdepartementets forslag med at det er Forsvarsdepartementet som oppnevner advokater, og at sikkerhetsklarering og autorisasjon foretas av Sivil klareringsmyndighet (SKM).

3 Nkoms kommentarer til forskrift om virksomhetens arbeid med forebyggende sikkerhet (virksomhetsforskriften)

Forskriften regulerer virksomhetens plikt til å sikre sine skjermingsverdige verdier. Forskriften stiller krav til virksomhetens styringssystem for sikkerhet som utgjør rammen for hvordan virksomheten oppfyller kravene til forebyggende sikkerhet. Videre stilles det generelle krav til beskyttelse av skjermingsverdige verdier og spesifikke krav for de konkrete verdiene.

3.1 Sikkerhetsstyring

3.1.1 Definisjoner - til forskriftens § 1

Forsvarsdepartementet har foreslått en innledende paragraf med definisjoner av begreper som er sentrale i loven. Nkom er enig i at en slik bestemmelse som utgangspunkt har en stor nytteverdi. For å sikre at regelverket forblir funksjonelt mener Nkom imidlertid det er viktig å ha en balansert tilnærming til hvor mange definisjoner det er behov for og hvor utfyllende disse skal være.

I forskriften er det benyttet enkelte begreper som ikke er klart definert. Nkom mener det er hensiktsmessig å definere de mest sentrale begrepene innledningsvis slik at etterfølgende bestemmelser kan utformes enklere og mer presist.

Nkom mener at følgende begreper bør defineres i virksomhetsforskriften § 1:

- skjermingsverdig informasjon
- skjermingsverdige informasjonssystemer som ikke behandler gradert informasjon
- skjermingsverdig informasjonssystemer som behandler gradert informasjon
- styringssystem for sikkerhet

Det bør i enda større grad gjøres tydelig hvilke bestemmelser som gjelder for skjermingsverdige informasjonssystemer som ikke behandler gradert informasjon og hvilke bestemmelser som gjelder for skjermingsverdige informasjonssystemer som behandler graderte informasjon.

3.1.2 Styringssystem for sikkerhet - til forskriftens § 2

Et velfungerende styringssystem for sikkerhet utgjør rammen for hvordan virksomheten oppfyller kravene til en helhetlig forebyggende sikkerhet. Nkom er positive til at bestemmelsen i

forskriften tydeliggjør virksomhetenes plikt til å ha et styringssystem som i større grad skal sikre et helhetlig forebyggende sikkerhetsarbeid.

3.1.3 Styringsdokument for det forebyggende sikkerhetsarbeidet - til forskriftens § 3
Bestemmelsen regulerer krav om at styringsdokument for det forebyggende sikkerhetsarbeidet skal være forankret hos virksomhetens leder.

Nkom er positiv til at krav om styringsdokument konkretiseres i forskriften. Nkom foreslår at det forskriftsfestes at virksomhetens leder også har ansvar for å vurdere selskapets skjermingsverdige verdier i forhold til å avgjøre hvilke deler av ny sikkerhetslov med forskrifter som er gjeldende for den aktuelle virksomheten.

Med bakgrunn i det foreslår Nkom ny litra d i virksomhetsforskriften § 3 som tydeliggjør virksomhetens leders ansvar i forhold til å ha oversikt over virksomhetens skjermingsverdige verdier:
«virksomhetens skjermingsverdig verdier.»

3.1.4 Sikkerhetsmål - til forskriftens § 4
Sikkerhetsmål skal omfatte ledelsens beslutning om hvordan eksterne og interne krav skal oppnås. Sikkerhetsmålene må inngå som en del av virksomhetens totale målsetning og være faktisk målbare. Det kreves god planlegging og evaluering av gjennomførte tiltak for å kunne måle om virksomheten har et forsvarlig sikkerhetsnivå.

Nkoms erfaring med tilsyn har vært at det er nødvendig med tydelig dokumentasjonskrav i forbindelse med virksomhetenes vurderinger knyttet til risiko og skjermingsverdige verdier. Det anbefales derfor en kobling mellom sikkerhetsmål og dokumentasjonskrav i ny sikkerhetslov § 4-4 første ledd i denne bestemmelsen.

Nkom foreslår et nytt andre ledd i virksomhetsforskriften § 4:
«Sikkerhetsmål skal beskrives i henhold til dokumentasjonskravet i sikkerhetslovens § 4-4 første ledd.»

3.1.5 Roller og ansvar i det forebyggende sikkerhetsarbeidet - til forskriftens § 5
Bestemmelsen stiller krav til at det forebyggende sikkerhetsarbeidet fordeles på nødvendige roller i virksomheten. Det stilles ikke spesifikke krav til hvilke roller som skal etableres eller at

det skal etableres en sikkerhetsorganisasjon, noe som er naturlig sett i lys av at ny sikkerhetslov får et bredt nedslagsfelt med alt fra små virksomheter til store konsern.

Det er viktig at det forebyggende sikkerhetsarbeidet forankres hos virksomhetens leder og Nkom er derfor positiv til at dette tydeliggjøres i regelverket.

Nkom mener at det bør tilføyes et dokumentasjonskrav til det forebyggende sikkerhetsarbeidet i virksomheten. Et slikt dokumentasjonskrav vil være med på å bidra til en bevisstgjøring av virksomhetens verdier, samt at ansvar og myndighet for forebyggende sikkerhet gjøres kjent i virksomheten.

3.1.6 Ressurser og kompetanse - til forskriftens § 6

Bestemmelsen setter krav om nok personell og økonomiske ressurser til å gjennomføre sikkerhetstiltakene.

Nkom er positive til at det stilles overordnet krav om tilstrekkelige ressurser til å forvalte og utvikle det forebyggende sikkerhetsarbeidet, og ikke kun for styringssystemet som tidligere foreslått.

Når det gjelder bestemmelsens bokstav a mener Nkom at det må stilles krav om gyldig legitimasjon for å sikre at ikke enhver form for identifikasjonspapir godtas. Det vises i den sammenheng til hvitvaskingsforskriften §§ 5 og 6.

Nkom foreslår å endre bokstav a i virksomhetsforskriften § 6 til:
«har bekreftet identiteten sin med gyldig legitimasjon.»

3.1.7 Tiltak ved sikkerhetstruende virksomhet, avvik og kompromittering av sikkerhetsgradert informasjon - til forskriftens § 7

Bestemmelsen fastsetter funksjonelle krav til hvordan en virksomhet skal håndtere sikkerhetstruende virksomhet og avvik.

Nkom støtter bestemmelsens innhold og er positive til at det henvises til § 4-5 i ny sikkerhetslov, som informerer om varslingskjeden ved sikkerhetsbrudd. Imidlertid er bestemmelsens første ledd noe vanskelig å lese da ordet «virksomhet» er brukt i ulike sammenhenger i forskriften. Nkom mener at begrepet «sikkerhetstruende virksomhet» med fordel kan byttes ut med

«sikkerhetstruende aktivitet». Dersom dette ikke gjøres foreslår Nkom at ordlyden «den enkelte virksomhet» inntas i bestemmelsen for å bedre skille mellom «sikkerhetstruende virksomhet» og «virksomheten».

Nkoms forslag til endring av virksomhetsforskriften § 9 første ledd er følgende:
«Ved sikkerhetstruende virksomhet eller avvik fra styringssystemet for sikkerhet skal den enkelte virksomhet gjennomføre umiddelbare tiltak for å redusere skadeomfanget og tiltak som gjenoppretter sikkerhetstilstanden. Det skal rapporteres internt og til andre som er berørt av den sikkerhetstruende virksomheten. Den enkelte virksomhet skal vurdere konsekvensene av den sikkerhetstruende virksomheten eller avviket.»

3.1.8 Evaluering og øvelser - til forskriftens § 8

Denne bestemmelsen er en presisering av ny sikkerhetslovs bestemmelser om evaluering og øvelser og stiller krav til at virksomheten regelmessig skal evaluere hvorvidt sikkerhetsmålene nås.

I ny sikkerhetslov er det fastslått krav om «regelmessig» gjennomføring av øvelser. I forskriftsteksten er imidlertid ordlyden «jevnlig evaluere» foreslått. Nkom mener at det bør brukes samme betegnelse i forskriften som i loven for å hindre uklarhet som kan oppstå ved ulik begrepsbruk om samme type krav. Videre mener Nkom at begrepet «regelmessig» er bedre enn «jevnlig» når det gjelder å fastsette ønskelig frekvens på evaluering og øvelser.

Nkoms forslag til endring av virksomhetsforskriften § 9 første ledd er følgende:
«Virksomheten skal regelmessig evaluere om kravet til forsvarlig sikkerhetsnivå er oppfylt, jf. § 4, og minst en gang i året evaluere om styringssystemet for sikkerhet er egnet til å sørge for at kravet oppfylles.

Virksomheten skal regelmessig gjennomføre øvelser for å kontrollere effekten av sikkerhetstiltakene i en normalsituasjon, og av tiltakene som er planlagt ved økt trusselnivå. Er virksomheten avhengig av andre virksomheter for å fungere slik den skal, skal øvelsen regelmessig inkludere de andre virksomhetene.

Resultatet av evalueringer og øvelser skal inngå i virksomhetens leders årlige gjennomgang, jf. § 9.»

3.1.9 Virksomhetens leders gjennomgang av det forebyggende sikkerhetsarbeidet - til forskriftens § 9

Bestemmelsen regulerer at virksomhetens leder skal evaluere det forebyggende sikkerhetsarbeidet. Nkom støtter forslaget om at ansvar for internrevisjon legges på virksomhetens leder og at det må gjennomføres årlig. I flere anerkjente standarder om kvalitet, som for eksempel ISO 9001 for kvalitetsledelse, stilles det krav om kontinuerlig forbedring. Nkom mener at tilsvarende krav bør nedfelles i forskriftsbestemmelsen for å sikre en kontinuerlig forbedring av sikkerhetsnivået hos den enkelte virksomhet.

3.1.10 Dokumentasjon om styringssystemet for sikkerhet - til forskriftens § 10

Nkom er svært positiv til at forskriften har egen bestemmelse om krav til dokumentasjon. Det vil gjøre forskriften mer brukervennlig for virksomhetene og gi en god oversikt over hvilke bestemmelser som stiller krav til dokumentasjon.

3.1.11 Forslag til ny paragraf om virksomhetenes opplysningsplikt

Nkom foreslår at virksomhetens opplysningsplikt til tilsynsmyndighetene klargjøres og forskriftsfestes i virksomhetsforskriften. Dette for å ha en klar og tydelig hjemme for tilgang til nødvendig informasjon for utføring av lovpålagte tilsynsoppgaver. Nkom har hatt god erfaring med kravet til opplysningsplikt i ekomregelverket.

Nkom forslår at en ny paragraf inntas i virksomhetsforskriften som fastslår virksomhetenes opplysningsplikt:
«Myndigheten kan kreve opplysninger som er nødvendige for gjennomføre lovpålagte tilsynsoppgaver. Taushetsplikt etter annen lovgivning, pålegg eller avtale, er ikke til hinder for opplysningsplikten. Opplysningene kan kreves utlevert skriftlig eller muntlig innen en fastsatt frist. Virksomheten kan kreve begrunnelse for pålegget om å utlevere informasjon.»

3.2 Generelle krav til beskyttelse av skjermingsverdige verdier

3.2.1 Plikt til å vurdere risiko - til forskriftens § 11

Bestemmelsen regulerer virksomhetens plikt til risikovurdering. Forsvarsdepartementet har valgt å legge samme forståelse av risikobegrepet som i ISO 31000 om risikostyring. Målet er at virksomheten skal ha et forsvarlig sikkerhetsnivå.

Nkom er generelt positive til bestemmelsens innhold men har likevel noen forslag til endringer I bestemmelsens første ledd for å få en presisering av formålet.

Nkom bemerker at det er en gjentakelsesfeil i virksomhetsforskriften § 11 andre ledd.

Videre følger det av bestemmelsens andre ledd at det «minst årlig» skal vurderes behov for å gjennomføre en ny helhetlig vurdering av risiko. Nkom mener at det er tilstrekkelig med krav om at virksomheten "regelmessig" vurderer behovet for risikovurderinger. En slik formulering gir virksomheten den nødvendige fleksibiliteten i forhold til behov, størrelser og ressurser.

I bestemmelsen siste ledd er virksomheter pliktig til å gi en oversikt til sitt departement om avhengigheter til andre virksomheter. I ny sikkerhetslov § 4-2 fjerde ledd er det fastslått at tilsynsmyndigheten skal gi råd og veiledning i forbindelse med vurderinger av risiko. For å understreke systematikken i loven med kobling mellom råd/veiledning i forbindelse med virksomhetenes risikohåndtering, er det viktig at tilsynsmyndighet også får en oversikt over virksomhetenes risikohåndtering. Informasjon om avhengigheter mellom virksomhetene vil være nyttig å ha for tilsynsmyndighetene for å kunne gi nyttige og aktuelle råd og veiledning til virksomhetene.

Med bakgrunn i ovennevnte foreslår Nkom følgende endringer i virksomhetsforskriften § 11:
«Virksomheten skal med utgangspunkt i sin vurdering av risiko identifisere, analysere og evaluere risikoreduserende tiltak for å oppnå et forsvarlig sikkerhetsnivå jf. § 4. Når virksomheten vurderer risikoen, skal den ta hensyn til:

a) hvilken sikkerhetstruende virksomhet de skjermingsverdige verdiene kan bli utsatt for
b) hvilke sårbarheter som er knyttet til de skjermingsverdige verdiene
c) i hvilken grad virksomheten er avhengig av andre virksomheter for å fungere som den skal.

Virksomheten skal regelmessig vurdere behovet for å for å gjennomføre en ny helhetlig vurdering av risiko.

Dersom endringer planlegges, gjennomføres eller inntreffer, skal virksomheten vurdere hvilken risiko endringene medfører.

Virksomheten skal sende en oversikt over hvilke virksomheter den er avhengig av for å fungere som den skal, jf. ny sikkerhetslov § 4-2, til det departement som er ansvarlig for det forebyggende sikkerhetsarbeidet i sektoren, eller det departement som har fattet vedtak om at

virksomheten skal omfattes av loven. Virksomheten skal også sende denne oversikten til Nasjonal sikkerhetsmyndighet og utpekt tilsynsmyndighet.»

3.2.2 Plikt til å håndtere risiko - til forskriftens § 12

Bestemmelsen slår fast at virksomheten skal håndtere risiko for å oppnå et forsvarlig sikkerhetsnivå. Det er fastsatt flere ulike alternativer for risikohåndtering, hvor risiko kan håndteres helt eller delvis. Forsvarsdepartementet har bedt høringsinstansenes syn på innretningen til § 12 i virksomhetsforskriften.

Som påpekt i våre generelle kommentarer mener Nkom at henvisning til § 12 i forskriften som igjen viser tilbake til §§ 20, 32, 45 og 53 er unødvendig kompliserende. Nkom foreslår derfor at plikt til å håndtere risiko for å oppnå et forsvarlig sikkerhetsnivå bør inntas direkte i bestemmelsen om forsvarlig sikkerhetsnivå jf. §§ 20, 32, 45 og 53. Etter Nkoms mening er dette forslaget, rent lovteknisk, en bedre løsning da alle plikter vil stå i bestemmelsen og ikke må hentes ut fra ulike steder i forskriften.

Videre mener Nkom at det bør stilles krav om hyppigheten til vurdering av risikohåndtering. Et slikt krav vil føre til at virksomhetene må ha oppdaterte vurderinger av risikohåndtering. Det er også viktig at det oppstilles krav til dokumentasjon for risikohåndtering slik at virksomhetene får grunnlag for en kontinuerlig forbedring av eget arbeid. Dokumentasjonskrav vil også bygge opp under virksomhetens mulighet til å dokumentere et forsvarlig sikringsnivå.

Nkom mener at bruk av anerkjente standarder i virksomhetens forbyggende sikkerhetsarbeid bør forskriftsfestes. Anerkjente standarder vil være et nyttig verktøy for å sikre at virksomhetene når et forsvarlig sikkerhetsnivå.

Nkom foreslår ny tekst til virksomhetsforskriften § 12:
«Virksomheten skal kontinuerlig håndtere risiko for å oppnå forsvarlig sikkerhetsnivå. Virksomhetens håndtering av risiko skal dokumenteres og skal inngå som en del av virksomhetens leders årlige gjennomgang av forebyggende sikkerhetsarbeid.

Dersom virksomheten oppfyller kravene i relevante anerkjente internasjonale standarder for håndtering av risiko kan dette bidra til å dokumentere forsvarlig sikkerhetsnivå i virksomheten.»

3.2.3 Grunnsikringstiltak, påbyggingstiltak og tiltak for skadebegrensning og gjenopprettelse - til forskriftens § 13

Bestemmelsen stiller krav om at det skal være en sammenheng mellom virksomhetens risikovurdering og kravene til håndtering av risiko og for beskyttelse av informasjon, informasjonssystem, objekt eller infrastruktur.

Det forventes at virksomheten skal ha en helhetlig plan for hva som skal gjøres dersom barrierene ikke fungerer. Virksomhetene skal etablere grunnsikringstiltak, påbyggingstiltak, skadebegrensnings tiltak og tiltak for gjenopprettelse som er nødvendig for å håndtere risiko for å oppnå forsvarlig sikkerhet. Nkom mener at bestemmelsen bør utformes på samme måte som i § 14 i virksomhetsforskriften.

Nkom foreslår følgende ny tekst til § 13 i virksomhetsforskriften:
«Grunnsikringstiltakene kan være en eller kombinasjon av følgende:
a) fysiske, elektroniske, menneskelige eller organisatoriske barrierer (barrierer)
b) systemer som skal oppdage og varsle om aktiviteter eller hendelser (deteksjon)
c) systemer og rutiner for å avklare aktiviteter og hendelser og bakgrunnen for dem (verifikasjon)
d) oppfølging av uønskede aktiviteter og uønskede hendelser (reaksjon)

3.2.4 Prinsipper ved valg og utforming av sikkerhetstiltak - til forskriftens § 14

Bestemmelsen fastsetter at valg og utforming av sikkerhetstiltak skal foretas i henhold til opplistede prinsipper. De opplistede prinsippene er en videreføring av prinsipper for informasjonssikkerhet og Nkom er enig i at dette er gode sikkerhetsprinsipper som kan anvendes generelt for sikring av alle skjermingsverdige verdier.

Av pedagogiske årsaker anbefaler Nkom at begreper som beskriver prinsippene kommer på slutten av setningen. Nkom mener videre at dokumentasjonskrav bør nedfelles i bestemmelsen og foreslår ny setning i siste ledd.

Nkom foreslår følgende endring av tekst til § 14 i virksomhetsforskriften:
«Når virksomheten velger ut og utformer sikkerhetstiltak, skal den vurdere prinsippene om

a. Sikkerhetsrelevante funksjoner skal ikke ha mer funksjonalitet eller kompleksitet enn strengt nødvendig for å utføre sin tilsiktede oppgave (Minimalisme).

b. Brukere og funksjoner skal bare tildeles rettigheter som er strengt nødvendige (Minste privilegium).
c. Sikkerhetsrelevante funksjoner skal ha ekstra kapasitet for å tåle overbelastning og utstyrssvikt (Redundans).
d. Flere sikkerhetsfunksjoner skal ivareta samme sikkerhetsbehov (forsvar i dybden).
e. Sikkerhetsfunksjoner skal ikke ha unødige avhengigheter til andre sikkerhetsområder (Selvbeskyttelse).
f. Flyt av aktiva, herunder bevegelse av informasjon og personell, skal skje etter fastsatte kriterier som er underlagt sentral kontroll (Kontrollert flyt av aktiva).
g. Balansert styrke. Nivået til sikkerhetsfunksjoner som ivaretar samme behov skal være tilnærmet like.

Sikkerhetstiltakene skal være samordnet slik at de ikke fragmenteres eller dupliseres unødvendig.

Virksomheten skal ikke bruke mer inngripende sikkerhetstiltak enn det som fremstår som nødvendig for å håndtere den aktuelle risikoen. I vurderingen av hva som er nødvendig, skal virksomheten særlig ta hensyn til enkeltpersoners rettssikkerhet og personvern. Når sikkerhetstiltaket kan gripe inn i enkeltpersoners rettssikkerhet eller personvern, skal virksomheten kunne dokumentere vurderingen. Vurderingen av sikkerhetstiltakene etter forrige ledd skal dokumenters.*»*

3.2.5 Krav om bruk av evaluerte produkter og tjenester - til forskriftens § 15

Bestemmelsen oppstiller krav om at det er evaluerte produkter og tjenester som skal benyttes når virksomheten velger sikkerhetstiltak i forhold til skjermingsverdig informasjon og informasjonssystem.

Nkom vil påpeke at dette kravet er svært utfordrende for ekomsektoren. Eksempelvis kan styringssystemer til enkelte ekomtilbydere bli utpekt som et skjermingsverdig informasjonssystem, og etter den foreslåtte § 15 bestemmelsen vil da enkelte ekomtilbydere måtte bruke evaluerte produkter/systemer og tjenester som er sikkerhetsevaluert av et organ som er godkjent av Nasjonal sikkerhetsmyndighet.

Bestemmelsens andre ledd beskriver at evaluering skal sikre tillitt til at produktet eller tjenesten har den funksjonalitet som er nødvendig for å sikre det aktuelle graderingsnivået. Nkom er enig i den presiseringen, men mener at det vil være riktig å tilføye «klasseringsnivå» i tillegg til graderingsnivå.

Nkom foreslår følgende endring til virksomhetsforskriftens § 15 siste ledd:
«Evalueringen skal gi tillit til at produktet eller tjenesten har den funksjonaliteten som er nødvendig for å sikre det aktuelle graderingsnivået eller klassifiseringsnivået. Evalueringen skal bestå av metodisk utvikling og testing, og være etterprøvbar.»

3.2.6 Evaluering av produkter og tjenester - til forskriftens § 16

Bestemmelsen går nærmere inn på hvem som skal evaluere produkter og tjenester. Det er fremsatt referanser til to ulike type sikkerhetsevalueringsregimer. Det er en «eller» bestemmelse og Nkom mener at det i kommentarene til bestemmelsen i høringsnotat bør utdypes nærmere når de ulike regimene skal anvendes. Gjeldende ordlyd åpner for fritt valg av sikkerhetsevalueringsregime.

Nkom vil bemerke at det vil kunne være behov for sektorvis kompetanse når evaluering av produkter og tjenester skal gjennomføres. Utpekt tilsynsmyndighet bør derfor ha mulighet på lik linje med Nasjonal sikkerhetsmyndighet å godkjenne evalueringer av produkter og tjenester innenfor egen sektor.

Videre mener Nkom at det er viktig at det er tydelig skille mellom hvilke bestemmelser som gjelder skjermingsverdige informasjonssystem som behandler gradert informasjon og de som ikke behandler gradert informasjon. Nkom anbefaler derfor at § 15 deles i to. En del for skjermingsverdig informasjonssystemer som ikke behandler gradert informasjon og en del for skjermingsverdig informasjonssystemer som behandler gradert informasjon.

3.2.7 Krav til sikkerhet i anskaffelser - til forskriftens § 17

Denne bestemmelsen pålegger virksomheten ansvaret for at krav til forsvarlig sikkerhet i anskaffelser ivaretas. Nkom viser til Digital sårbarhetsutvalgs rapport angående digitale verdikjeder og utfordringene knyttet til dette. Utfordringene til digitale verdikjeder gjør at det er viktig at virksomheten kan undersøke og kontrollere sikkerheten hos sine underleverandører. Nkom støtter gjeldende ordlyd og er positive til bestemmelsens siste setning som gir virksomheten en plikt til å avtalefeste en rett til å undersøke at leverandøren ivaretar sikkerheten i anskaffelsen.

3.2.8 Varslingsplikt om anskaffelser til skjermingsverdig informasjonssystem, objekt og infrastruktur til forskriftens § 18

I denne bestemmelsen nedfelles det at virksomheten har varslingsplikt om anskaffelser til skjermingsverdig informasjonssystem, objekt og infrastruktur. Nkom mener at bestemmelsen er tydelig og godt formulert, og vil påpeke at denne varslingsplikten er dyptgående diskutert i både høringsnotatet til forskriftene og i forarbeidene til ny sikkerhetslov.

3.2.9 Unntak fra sikkerhetskrav - til forskriftens § 19

Bestemmelsen er en generell unntaksbestemmelse som fastslår at Nasjonal sikkerhetsmyndighet kan gjøre unntak fra sikkerhetskrav i denne forskriften. Andre ledd gir sektortilsyn adgang til å gi unntak etter første ledd fra de sikkerhetskravene som ikke gjelder for beskyttelse av sikkerhetsgradert informasjon. Nkom mener det er riktig at sektortilsyn får en dispensasjonsadgang for å sikre fleksibilitet og nødvendig handlingsrom i sin myndighetsutøvelse.

3.3 Beskyttelse av skjermingsverdig informasjon

3.3.1 Forsvarlig sikkerhetsnivå for skjermingsverdig informasjon - til forskriftens § 20

Bestemmelsen stiller krav til hva som vil være et forsvarlig sikkerhetsnivå for sikring av skjermingsverdig informasjon. Dette innebærer at informasjonen skal beskyttes slik at den ikke med enkle midler kan endres, gå tapt, gjøres utilgjengelig eller bli kjent for uautoriserte personer.

Nkom er positive til en funksjonell tilnærming i høringsnotatets redegjørelse for «enkle midler» og at det vil være vurdering av risiko som vil være avgjørende for hvilke tiltak som vil inngå i begrepet «enkle midler».

Nkom støtter forslaget og er enig i terskelen som settes for forsvarlig sikkerhetsnivå for skjermingsverdig informasjon. Nkom mener at det er en viktig presisering at beskyttelse av konfidensialitet, integritet og tilgjengelighet må ses i sammenheng, og at det skal foretas en avveiing knyttet til disse nøkkelbegrepene.

3.3.2 Destruering av dokumenter og lagringsmedier med sikkerhetsgradert informasjon - til forskriftens § 21

Bestemmelsen er en videreføring av gjeldende forskriftsbestemmelser om tilintetgjøring og metoder for tilintetgjøring. Nkom er positive til videreføring av bestemmelsen og at kravet er mer funksjonelt beskrevet enn tidligere.

3.3.3 Evakuering og ekstraordinær destruering i nødsituasjoner - til forskriftens § 22

Denne bestemmelsen er en videreføring av tidligere bestemmelser om evakuering og ekstraordinær tilintetgjøring i nødsituasjoner. Nkom er positive til at kravet i foreslått bestemmelse er mindre detaljert enn dagens bestemmelser. Det sentrale er at virksomheten har en plan for evakuering og tilintetgjøring av skjermingsverdig informasjon i nødsituasjoner.

3.3.4 Utlevering av sikkerhetsgradert informasjon til fremmede stater og internasjonale organisasjoner - til forskriftens § 23

Dette er en videreføring av gjeldende bestemmelser. Det skal fremgå av en sikkerhetsavtale mellom statene hva den enkelte stat er forpliktet til.

Nkom støtter forslaget og synes det er riktig at det er sikkerhetsavtalen som er utgangspunktet for hvordan myndigheten, virksomheten eller en internasjonal organisasjon i en annen stat skal behandle sikkerhetsgradert informasjon. Videre er Nkom positive til at det legges opp til unntak for særlige tilfeller hvor det er i Norges interesse å utlevere informasjonen.

3.3.5 Korresponderende sikkerhetsgrader - til forskriftens § 24

Bestemmelsen regulerer at utenlandsk sikkerhetsgradert informasjon sikres på samme måte som tilsvarende norsk sikkerhetsgradert informasjon. Nkom er positiv til bestemmelsen og mener at det er viktig med et konkret krav til prosedyrer for å sikre fremtidig informasjonsdeling mellom landene.

3.3.6 Kryptering - til forskriftens § 25

Denne bestemmelsen regulerer kryptering av sikkerhetsgradert informasjon som er lagret hos virksomheten, som sendes ut av område virksomheten kontrollerer og om sikring av kryptomateriell.

Nkom er generelt positive til bestemmelsen og at det forutsettes at de krav som er stilt i denne bestemmelsen skal ses i sammenheng med bestemmelsene i kapittel 2, 3, 5 og 6 for å få en

helhetlig sikring av kryptomateriell. Det sentrale er at kryptomateriell skal sikres i tråd med verdien på informasjonen som materiellet er ment å beskytte.

3.4 Sikkerhetsgradering og merking

3.4.1 Merking av dokumenter og lagringsmedier som inneholder sikkerhetsgradert informasjon - til forskriftens § 26

Bestemmelsen regulerer krav til sikkerhetsgradering og merking av de graderte dokumentene, og er i stor grad en videreføring av gjeldende bestemmelse. Nkom er positiv til at bestemmelsen har en funksjonell tilnærming og Nkom er enig med Forsvarsdepartementet i at det ikke er nødvendig med et eksplisitt krav om at journaler ikke skal sikkerhetsgraderes høyere enn nødvendig.

3.4.2 Sikkerhetsgradering ut over 30 år - til forskriftens § 27

Bestemmelsen er videreføring av gjeldende sikkerhetslov hvor regelen er at sikkerhetsgradering skal tidsbegrenses. Det innebærer at informasjon ikke skal sikkerhetsgraderes for lengre tid enn det som er nødvendig. Nkom er enig i videreføring av bestemmelsen.

3.4.3 Omgradering av sikkerhetsgradert informasjon - til forskriftens § 28

Bestemmelsen er videreføring av gjeldende sikkerhetslov. Nkom støtter presiseringen som angår når virksomheten skal vurdere om den sikkerhetsgraderte informasjonen skal gis et høyere eller lavere nivå eller skal avgraderes.

3.4.4 Hvem som kan omgradere - til forskriftens § 29

Denne bestemmelsen er en videreføring av § 2-11 i forskrift om informasjonssikkerhet og fastsetter at omgradering kan skje av virksomheten som har utstedt informasjonen, en virksomhet overordnet denne eller Nasjonal sikkerhetsmyndighet.

Nkom mener at ordlyden «virksomhet overordnet denne» ikke er tilstrekkelig dekkende. I flere av sektorene, og særlig i ekomsektoren, er virksomhetene underlagt sikkerhetsloven et privat rettssubjekt. Nkom mener at utpekte tilsynsmyndighet bør ha mulighet til å omgradere informasjon som private rettssubjekt har utstedt i egen sektor. Det er ikke en naturlig tolkning av ordlyden, slik den er fremsatt i forslag til virksomhetsforskriften, at en myndighet vil være «virksomhet overordnet» et privat rettssubjektet. Nkom foreslår derfor at ordlyden endres til at det er sektormyndigheten for virksomheten som kan omgradere.

Nkom foreslår en endring av virksomhetsforskriften § 29 som følgende:
«Bare virksomheten som har utstedt informasjonen, en virksomhet overordnet denne, Nasjonal sikkerhetsmyndighet eller utpekt tilsynsmyndighet kan omgradere informasjon med norsk sikkerhetsgradering. Informasjon med utenlandsk sikkerhetsgradering kan bare omgraderes av den staten eller organisasjonen som har utstedt informasjonen, eller etter samtykke fra den.»

3.4.5 Plikt til å informere om behov for eller avgjørelse om omgradering - til forskriftens § 30

I denne bestemmelsen videreføres krav til at virksomheten skal underrette utsteder dersom sikkerhetsgraderingen er feil. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

3.4.6 Prosedyrer ved henvendelse om innsyn etter offentleglova eller forvaltningsloven - til forskriftens § 31

Bestemmelsen angir regler for prosedyrer ved henvendelse om innsyn og er en videreføring av gjeldende forskriftsbestemmelse innen informasjonssikkerhet. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

3.5 Beskyttelse av informasjon gradert KONFIDENSIELT eller høyere

3.5.1 Forsvarlig sikkerhetsnivå for informasjon gradert KONFIDENSIELT eller høyere - til forskriftens § 32

Bestemmelsen omhandler krav til forsvarlighetsnivå for sikring av gradert informasjon.
Nkom er generelt positive til bestemmelsen og støtter Forsvarsdepartementets forslag om krav til etablering av tiltak som gjør det mulig å oppdage om en trusselaktør har fått tak i informasjon gradert KONFIDENSIELT. For sikkerhetsnivå HEMMELIG mener Nkom at det er riktig å oppstille krav om at virksomheten skal ha etablerte tiltak som gjør at kompromittering skal kunne oppdages i tide. Videre støtter Nkom forslaget om at kombinasjon av barrierer, deteksjon, verifikasjon og reaksjon er gode virkemidler for å hindre at uautoriserte personer kan få tilgang til informasjon gradert STRENGT HEMMELIG.

3.5.2 Sending av informasjon gradert KONFIDENSIELT eller høyere - til forskriftens § 33

I denne bestemmelsen har Forsvarsdepartementet foreslått en reell innstramming i forbindelse med sending av informasjon gradert KONFIDENSIELT eller høyere.

Denne innstrammingen vil være rimelig sett i forhold til oppmykingen av kurertjenesten i § 43, hvor det ikke lenger stilles krav om godkjenning fra Nasjonal sikkerhetsmyndighet.

3.5.3 Pakking av informasjon gradert KONFIDENSIELT eller høyere - til forskriftens § 34

Bestemmelsen angir krav til pakking av informasjon gradert KONFIDENSIELT eller høyere og er i all hovedsak videreføring av gjeldende rett. Nkom støtter at bestemmelsen er blitt mer funksjonsbasert enn tidligere.

3.5.4 Krav til oversikt over informasjon gradert KONFIDENSIELT eller høyere - til forskriftens § 35

Denne bestemmelsen regulerer at virksomheten skal ha oversikt over informasjon gradert KONFIDENSIELT eller høyere. Selv om bestemmelsen er en videreføring av gjeldende krav, er det ikke gitt detaljerte krav om beskrivelse av journalføring. Nkom støtter denne innretning da det sentrale er at virksomheten til enhver tid har oversikt over selve informasjonen og ikke selve journalføringen.

3.5.5 Soneinndeling for informasjon gradert KONFIDENSIELT eller høyere - til forskriftens § 36

Inndeling i avgrensende soner er av grunnleggende betydning for å kunne ivareta kravene til sikring på en hensiktsmessig måte. Bestemmelsen regulerer krav til etablering av soneinndeling for informasjon gradert KONFIDENSIELT eller høyere og er således lemping av tidligere regelverk. Nkom støtter forslaget med bakgrunn i blant annet at NATO ikke stiller krav til soner for NATO RESTRICTED. Krav til både tilgangskontroll og autorisasjon for BEGRENSET jf. prinsippet om minste privilegium og ny sikkerhetslov § 8-1 gjelder fremdeles.

3.5.6 Kontrollert sone - til forskriftens § 37

Bestemmelsen er en videreføring av gjeldende bestemmelse i sikkerhetsloven og omhandler kontrollerte områder som er beskyttet og sperret av. Disse fungerer som en buffersone mellom område med allmenn ferdsel og hvor det behandles gradert informasjon. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

3.5.7 Beskyttet sone - til forskriftens § 38

Bestemmelsen omhandler krav til beskyttet sone som skal ha en fysisk avgrensning der sikkerhetstruende virksomhet skal kunne oppdages. Bestemmelsen er i all hovedsak

videreføring av gjeldende rett. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

3.5.8 Sperret sone - til forskriftens § 39

Denne bestemmelsen regulerer soner hvor adgang gir direkte tilgang til gradert KONFIDENSIELT eller høyere. Bestemmelsen fastsetter at disse sonene skal sperres og beskyttes, men gir ingen detaljerte krav til hvordan det skal beskyttes. Nkom er enig i at det ikke bør gis et detaljerte krav til hvordan disse sonene skal beskyttes i og med at kravet til tilstrekkelig god sikring ivaretas gjennom de generelle kravene for beskyttelse av informasjon gradert KONFIDENSIELT eller høyere.

3.5.9 Behandling av informasjon gradert KONFIDENSIELT eller høyere - til forskriftens § 40

Denne bestemmelsen stiller krav til at informasjon gradert KONFIDENSIELT eller høyere skal behandles i beskyttet eller sperret sone. Unntak fra hovedregelen kan gjøres dersom en etter en risikovurdering finner det tilrådelig og det iverksettes kompenserende tiltak som ivaretar informasjonens konfidensialitet, integritet og tilgjengelighet. Nkom er generelt positive til bestemmelsens innhold og mener at den fremstår som tydelig og helhetlig.

3.5.10 Særlige krav for informasjon gradert HEMMELIG eller høyere - til forskriftens § 41

Bestemmelsen regulerer særlige krav til dokumenter eller lagringsmedier med informasjon gradert HEMMELIG eller høyere. Nkom mener at det fremgår tydelig av bestemmelsen at det sentrale er at virksomheten til enhver tid har oversikt over hvem som har informasjonen slik at denne ikke kommer på avveie. Dette kommer også frem i andre ledd som omhandler krav til destruering av informasjon gradert HEMMELIG eller STRENGT HEMMELIG.

3.5.11 Rapportering av informasjon gradert STRENGT HEMMELIG - til forskriftens § 42

Bestemmelsen omhandler rapportering av informasjon gradert STRENGT HEMMELIG og er videreføring av § 4-39 i forskrift om informasjonssikkerhet. Nkom er enig i denne videreføringen.

3.5.12 Krav til forsendelse med kurer - til forskriftens § 43

Bestemmelsen er delvis videreføring av tilsvarende krav i gjeldende forskrift. Nkom støtter høringsnotatets forslag om at det ikke er nødvendig at Nasjonal sikkerhetsmyndighet skal godkjenne virksomheter som utfører kurerposttjeneste så lenge virksomheter utfører dette i samsvar med de øvrige kravene i bestemmelsen.

3.5.13 Beskyttelse av rom og lokaler for tale gradert KONFIDENSIELT eller høyere - til forskriftens § 44

Denne bestemmelsen omhandler krav til beskyttelse av rom og lokaler for gradert tale KONFIDENSIELT eller høyere og er i all hovedsak videreføring av gjeldende regelverk. Bestemmelsen må ses i sammenheng med kravene i kapittelet om styringssystem for sikkerhet og bestemmelsene i §§ 37-41 om etablering og behandling av informasjon i soner, noe Nkom er positive til.

Nkom synes det er positivt at bestemmelsen har en mer funksjonell tilnærming enn tidligere slik at regelverket kan tilpasses virksomhetene og den teknologiske utviklingen.

3.6 Beskyttelse av skjermingsverdige informasjonssystemer

3.6.1 Generell merknad til kapittel 6

Det er viktig at regelverket settes opp på en slik måte at virksomheter enkelt kan finne frem til de bestemmelsene som omhandler det enkelte emnet. Nkom mener at Kapittel 6 burde struktureres bedre. . Det er for eksempel ikke tydelig hvilke bestemmelser som gjelder skjermingsverdige informasjonssystemer som behandler gradert informasjon og hvilke som gjelder for informasjonssystemer som ikke behandler gradert informasjon.

Nkom mener at det bør komme tydeligere frem hvilke bestemmelser som gjelder behandling av all skjermingsverdig informasjon og hvilke bestemmelser som gjelder behandling av gradert informasjon og kritisk infrastruktur. Nkom foreslår således at kapittel 6 deles opp i tre deler for å gi en bedre oversikt over hvilke krav som gjelder de ulike informasjonskategoriene.

Nkom foreslår følgende struktur i virksomhetsforskriften kapittel 6:

1. Generelle bestemmelser om informasjonssystemer.
2. Bestemmelser som går spesifikt på informasjonssystemer som behandler informasjon om kritisk infrastruktur.
3. Bestemmelser som går spesifikt på informasjonssystemer som behandler gradert informasjon.

3.6.2 Forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer - til forskriftens § 45

Bestemmelsen oppstiller krav om at virksomheten skal ha et forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer og hva som skal til for å få skjermingsverdige informasjonssystem godkjent jf. § 48.

Bestemmelsens bokstav a til e er en gjentakelse av § 6-2 i ny sikkerhetslov med noen få justeringer som etter Nkoms mening ikke er mer utdypende eller oppklarende. Videre kan en opplisting oppfattes som uttømmende. Det bør inntas «blant annet» eller «minst» for å presisere at listen ikke er uttømmende.

Paragraf 45 fremstår som mindre tydelig enn ny sikkerhetslov § 6-2 når det gjelder prinsippene konfidensialitet, integritet og tilgjengelig (KIT). Nkom foreslår derfor å gjøre bestemmelsen enklere ved å fjerne bokstavene a til e og kun ha med en henvisning til ny sikkerhetslov § 6-2. Med en slik endring gjøres bestemmelsen mer funksjonell.

Videre foreslår Nkom at bokstav f og g beholdes, men omskrives til eget ledd i bestemmelsen.

Nkom foreslår følgende endring til virksomhetsforskriften § 45:
«Som en del av risikohåndteringen skal virksomheten registrere bruk, misbruk og forsøk på misbruk av informasjonssystemet, tjenester og data. Virksomhetene skal systematisk kontrollere at sikkerhetstiltakene er korrekt implementert og ivaretar sikkerheten på en effektiv og hensiktsmessig måte.»

Som pekt på innledningsvis mener Nkom at henvisning til § 12 i forskriften som viser tilbake til §§ 20, 32, 45 og 53, er unødvendig kompliserende. Nkom foreslår derfor at plikt til å håndtere risiko for å oppnå et forsvarlig sikkerhetsnivå bør inntas direkte i bestemmelsen om forsvarlig sikkerhetsnivå jf. §§ 20, 32, 45 og 53. Etter Nkoms mening er dette forslaget,en bedre løsning fordi alle plikter da vil stå samlet i denne bestemmelsen.

3.6.3 Plikt til å sørge for godkjenning av skjermingsverdige informasjonssystemer - til forskriftens § 46

Bestemmelsen fastsetter at virksomheten skal sørge for at informasjonssystemer som skal behandle sikkerhetsgradert informasjon er godkjent før det tas i bruk. Videre skal andre skjermingsverdige informasjonssystemer være godkjent så fort som praktisk mulig.

Virksomheten er selv ansvarlig for å oppnå et forsvarlig sikkerhetsnivå. Virksomheten har som en del av dette en plikt til å sørge for godkjenning av skjermingsverdige informasjonssystemer. Nkom foreslår å forskriftsfeste at virksomheter får en plikt til å fremlegge en samsvarsvurderingsrapport basert på ny sikkerhetslovs krav, internasjonale anerkjente standarder og veiledning gitt av myndighetene. Samsvarsvurderingsrapporten må være utstedt av et akkreditert samsvarsorgan. Denne rapporten skal inngå som en del av myndighetens vurderingsgrunnlag for godkjenning.

Tilsvarende innretning finner man i myndighetsforskriften § 6, som regulerer bruk av tredjepart til å utføre tekniske undersøkelser for å vurdere om virksomheten som søker er sikkerhetsmessig skikket til godkjenning. Disse undersøkelsene foregår etter anerkjente internasjonale standarder for godkjenning. Tilsvarende regel finnes for godkjenning av tillittstjenester, jf. lov om tillitstjenester art 20 nr. 1.

Nkom er innforstått med at innføring av en slik godkjenningsregime kan forhøye kostnadene noe for tilbyderne, men mener dette ligger klart innenfor tilbydernes plikt til å få sine skjermingsverdige informasjonssystemer godkjent. Videre mener Nkom at bruk av akkreditert tredjepart, som foretar undersøkelser etter anerkjente internasjonale standarder, føre til mer forutsigbarhet for tilbyderne..

Nkom foreslår følgende siste ledd til virksomhetsforskriften § 46:
«Virksomheten må for godkjenning av skjermingsverdig informasjonssystem fremlegge en samsvarsvurderingsrapport utstedt av et akkreditert samsvarsorgan.»

Nkom er klar over at det er utfordrende å regulere godkjenningens omfang og detaljeringsgrad på en slik måte at den treffer alle type virksomheter i alle sektorer. Desto viktigere er det at bestemmelsen utformes åpent for å gi tilstrekkelig handlingsrom for nødvendige tilpasninger.

Når det gjelder dekning av kostnader for godkjenning mener Nkom at det er virksomheten som må dekke disse.

3.6.4 Godkjenningsmyndighet - til forskriftens § 47

Bestemmelsen regulerer hvem som skal godkjenne skjermingsverdige informasjonssystemer. Det er lagt opp til at virksomhetene i all hovedsak selv skal godkjenne sine skjermingsverdige informasjonssystemer.

Nkom mener at det ikke er hensiktsmessig å legge godkjenningsmyndigheten til Nasjonal sikkerhetsmyndighet for godkjenning av skjermingsverdige informasjonssystemer for alle de ulike sektorene. En slik godkjenningsmyndighet bør ligge hos sektormyndigheten som har god kjennskap til virksomhetene og deres utfordringer og har en regelmessige dialog med disse.

Videre mener Nkom at bestemmelsens andre ledd er uklar og ikke helt henger sammen med resten av bestemmelsen. Nkom viser til våre kommentarer til § 46 og mener det vil være mer oversiktlig om bestemmelsen utformes på en slik måte at det er tydelig skille mellom skjermingsverdig informasjonssystemer som behandler gradert informasjon og de som ikke gjør det.

Nkom er positive til at departementene kan bestemme at godkjenning av skjermingsverdige informasjonssystemer etter andre ledd kan gjøres av myndighet med tilsynsansvar. Særlige kompetanse og tette dialogen med virksomheten vil være sentralt i et effektivt godkjenningsregime.

3.6.5 Godkjenningen - til forskriftens § 48

Denne bestemmelsen omhandler hva godkjenning av skjermingsverdig informasjonssystem er og hva det vil bety for virksomhetene.

Nkom er enig med Forsvarsdepartementet om at en godkjenning ikke må oppfattes som en garanti for at kravet til forsvarlig sikkerhetsnivå er oppfylt. Hensikten med bestemmelsen er at godkjenningen skal være en formell bekreftelse på identifisering, erkjennelse og tilfredsstillende håndtering av risiko og at tiltak er kontrollert. Nkom mener at disse elementene kommer godt frem i bestemmelsen.

Når det gjelder spørsmål om bestemmelsen er tilstrekkelig knyttet til de krav som er oppstilt i virksomhetsforskriftens § 45, mener Nkom at det vil være en fordel med referanse til denne bestemmelsen for å synliggjøre tilknytningen.

3.6.6 Godkjenningens varighet - til forskriftens § 49

Bestemmelsen regulerer lengden på godkjenningen og at det ved vesentlige endringer skal foretas en regodkjenning. Nkom støtter krav til regodkjenning ved vesentlige endringer slik dette er formulert med en tilstrekkelig fleksibilitet i forhold til den enkelte virksomhet.

3.6.7 Midlertidig brukstillatelse - til forskriftens § 50

Bestemmelsen åpner for at det skal være mulig å gi midlertidig brukstillatelse ved særlig behov. Særlige behov er i høringsnotatet avgrenset til de tilfeller hvor de prosessuelle kravene ikke er oppfylt. Nkom er enig i en slik avgrensning. Midlertidig brukstillatelse bør ikke benyttes som et smutthull for lemping av sikkerhetskravene til godkjenning.

Bestemmelsen andre ledd gir Nasjonal sikkerhetsmyndighet myndighet til å dispensere fra kravene i første ledd. Nkom stiller spørsmål til nødvendigheten av bestemmelsens andre ledd ettersom vi mener dette dekkes godt av den generelle dispensasjonsbestemmelsen i § 19. Dersom bestemmelsen likevel beholdes vil det være mer naturlig om dispensasjonsadgangen gis til godkjenningsmyndigheten (sektormyndighetene) fremfor Nasjonal sikkerhetsmyndighet.

3.6.8 Sammenkobling av informasjonssystemer som behandler sikkerhetsgradert informasjon - til forskriftens § 51

Bestemmelsen pålegger virksomheten en plikt til å ha et eget informasjonssystem for sammenkobling av informasjonssystemer som behandler sikkerhetsgradert informasjon på høyeste nivå. Dette kravet er til en viss grad videreføring av forskrift om informasjonssikkerhet § 5-8 og Nkom støtter videreføringen av dette.

3.7 Beskyttelse av skjermingsverdig objekt og infrastruktur

3.7.1 Skadevurdering i forbindelse med klassifisering av skjermingsverdig objekt eller infrastruktur - til forskriftens § 52

Bestemmelsen stiller krav til at virksomheten utarbeider en skadevurdering i forbindelse med klassifisering av skjermingsverdig objekt eller infrastruktur. Nkom er enig at det må være krav om utarbeidelse av en skadevurdering slik at myndigheten får tilstrekkelig grunnlag for å klassifisere objektet eller infrastruktur, og fastsette hvilke sikkerhetstiltak som må iverksettes for å oppnå forsvarlig sikkerhet. Nkom mener at denne skadevurderingen også må deles med tilsynsmyndigheten, da den vil være sentral i deres veiledning og tilsynsrolle overfor virksomheten.

Nkom foreslår følgende endring i virksomhetsforskriften § 52 andre ledd:
«Skadevurderingen skal sendes til det departement som har utpekte skjermingsverdige objektet eller infrastrukturen, utpekt tilsynsmyndighet og nasjonal sikkerhetsmyndighet, jfr. myndighetsforskriften § 1.»

3.7.2 Forsvarlig sikkerhetsnivå for klassifiserte objekter og infrastruktur - til forskriftens § 53

Bestemmelsen regulerer hvordan virksomheten skal oppnå forsvarlig sikkerhet for klassifiserte objekter og infrastruktur. Bestemmelsen er en forlengelse av plikten til å vurdere og håndtere risiko i forskriften § 11 og § 12. Nkom er enig i bestemmelsen og mener den er funksjonell utformet med en god tilnærming til hvordan virksomheten skal oppnå forsvarlig sikkerhet for klassifiserte objekter og infrastruktur.

3.7.3 Bruk av sikringsstyrker - til forskriftens § 54

Bestemmelsen regulerer bruk av sikringsstyrker fra politiet og Forsvaret til beskyttelse av et objekt eller infrastruktur ved behov. Dersom sikringsstyrker blir tatt i bruk fastsettes det en plikt for virksomheten å tilrettelegge og utarbeide plan for bruk av sikringsstyrkene i samarbeid med politiet eller Forsvaret. Nkom er positive til bestemmelsen og mener det er riktig at det er virksomheten som har plikt til å tilrettelegge og lage en plan for bruk av sikringsstyrker.

3.7.4 Behovet for bruk av adgangsklarering - til forskriftens § 55

Bestemmelsen regulerer bruk av adgangsklarering dersom det ikke vil være mulig å redusere risikoen tilstrekkelig ved hjelp av andre egnede tiltak. Nkom mener at en vurdering av adgangsklarering hører naturlig inn under bestemmelsen om skadevurderingen jf. § 52. Nkom foreslår derfor å innlemme denne bestemmelsen som eget ledd i § 52.

3.8 Nasjonalt varslingssystem for digital infrastruktur

3.8.1 Tilknytning til varslingssystemet for digital infrastruktur - til forskriftens § 56

Bestemmelsen er en videreføring av dagens system med frivillig tilknytning til varslingssystem for digital infrastruktur (VDI).

Nkom bemerker at påleggsbestemmelsen er tatt bort fra tidligere utkast til bestemmelsen. Nkom mener at det bør reguleres inn en påleggskompetanse og den bør ligge hos sektormyndigheten.

Nkom mener at den myndighet som pålegger tilknytning til VDI også må dekke kostnadene ved dette.

3.8.2 Virksomhetens rett til innsyn - til forskriftens § 57

Bestemmelsen regulere virksomhetens rett til innsyn i hvordan kapasitetene for deteksjon og sårbarhetsreduksjon som brukes i virksomheten er konfigurert og i dataen som Nasjonal sikkerhetsmyndighet mottar fra virksomhetens kapasiteter. Nkom støtter bestemmelsen om innsynsrett da det vil gi den nødvendige åpenhet rundt Nasjonal sikkerhetsmyndighets bruk av varslingssystemet.

3.9 Personellsikkerhet

3.9.1 Generell merknad til kapittel 9

Nkom mener at det bør forskriftsfestes at autorisasjonsansvarlig skal være autorisert for høyeste nivå som vedkommende kan autoriserer andre til. For å skape troverdighet til autorisasjonsprosessen bør det ikke være mulig å gi noen høyere tillitt (autorisasjon) enn det en selv er blitt gitt.

3.9.2 Vilkår for å gi autorisasjon - til forskriftens § 58

Bestemmelsen regulerer vilkår for å gi autorisasjon og er basert på gjeldene forskrift om personellsikkerhet § 5-2. Nkom ber Forsvarsdepartementet vurdere om det kunne være hensiktsmessig å forskriftsfeste en opplisting av vilkår.

I arbeidet med klarering og autorisasjon av personell har Nkom erfart at det har vært utfordrende for virksomheter å benytte seg av personopplysningsblankett ved autorisasjon for BEGRENSET. Nkom mener at det er viktig at den enkelte avgir en egenerklæring når de skal autoriseres for BEGRENSET. Nkom ber derfor Forsvarsdepartementet vurdere å forskriftsfeste en slik adgang til å innhente opplysninger på et eget skjema eller at personopplysningsblanketten kan brukes.

3.9.3 Autorisasjonssamtale - til forskriftens § 59

Bestemmelsen regulerer hva autorisasjonsansvarlig skal berøre i autorisasjonssamtalen og tilsvarer i hovedsak gjeldende forskrift om personellsikkerhet § 5-5. Nkom er positive til bestemmelsen og mener dette skaper en forutsigbarhet overfor den som skal autoriseres.

3.9.4 Autorisasjon av autorisasjonsansvarlig hos leverandøren - til forskriftens § 60

Bestemmelsen regulerer oppdragsgiverens plikt til å autorisere den autorisasjonsansvarlige hos leverandøren og henviser til det tillitsforholdet som må avklares mellom oppdragsgiver og autorisasjonsansvarlig hos leverandøren. Nkom har ingen kommentarer til denne bestemmelsen, og er enig i det som er anført.

3.9.5 Autorisasjon av utenlandske statsborger - til forskriftens § 61

Bestemmelsen fastsetter autorisasjonsansvarliges plikt til å innhente samtykke fra klareringsmyndigheten dersom utenlandske statsborgere skal autoriseres for BEGRENSET. Nkom har ingen kommentarer til bestemmelsen, og er enig i det som er anført.

3.9.6 Nødautorisasjon - til forskriftens § 62

Bestemmelsen fastsetter at en person ved nødrett kan autoriseres uten å ha nødvendig klarering. Bestemmelsen er utledet av gjeldende forskrift om personellsikkerhet § 5-3, der annet ledd ikke er videreført. Nkom er enig i Forsvarsdepartementets vurdering av å ikke videreføre § 5-3 andre ledd, men vil understreke viktigheten av at utpekt tilsynsmyndighet også varsles ved nødautorisasjon.

Nkom foreslår å endre virksomhetsforskriften § 62:
«Ved nødrett, jf. straffeloven § 17, kan en person autoriseres uten å ha nødvendig klarering. Virksomheten skal uten ugrunnet opphold varsle klareringsmyndigheten, Nasjonal sikkerhetsmyndighet og utpekt tilsynsmyndighet om hvilke personer som har nødautorisasjon, og på hvilket nivå denne autoriasjonen er gitt.»

3.9.7 Oversikt over personell med autorisasjon - til forskriftens § 63

Bestemmelsen regulerer autorisasjonsansvarliges plikt til å ha oversikt over personell som er autorisert. Nkom har ingen kommentarer til bestemmelsen, og er således enig i det som er anført.

3.9.8 Dokumentasjon på autorisasjon - til forskriftens § 64

Bestemmelsen fastsetter et dokumentasjonskrav på at en person er autorisert og vilkår som stilles til dokumentasjonen. Nkom har ingen kommentarer til bestemmelsen, og er enig i det som er anført.

3.9.9 Nedsettelse, suspensjon og tilbakekallelse av autorisasjon - til forskriftens § 65

Bestemmelsen regulerer hvilke krav som stilles til dokumentasjon dersom autorisasjonsansvarlig skal vurderer om en autorisasjon skal endres eller tilbakekalles. Bestemmelsen tilsvarer i hovedsak gjeldende forskrift om personellsikkerhet § 5-8 om ufordelaktige autorisasjonsavgjørelser.

I bestemmelsens første ledd siste setning står det at avgjørelsen ikke kan påklages. Nkom mener at Forsvarsdepartementet bør vurdere hvordan rettsikkerheten til den enkelte kan ivaretas når det gjelder autorisasjon for BEGRENSET. For autorisasjon for nivåene høyere enn BEGRENSET er rettsikkerheten ivaretatt med bestemmelsens tredje ledd, hvor det fremgår at dersom klareringsmyndigheten opprettholder klareringen kan autorisasjonsansvarlig ikke tilbakekalle, nedsette eller suspendere autorisasjonen på grunnlag av de innmeldte opplysningene.

3.9.10 Begrunnelse og dokumentasjon ved forespørsel om klarering – til forskriftens § 66

Bestemmelsen fastsetter krav til begrunnelse og dokumentasjon ved forespørsel om klarering fra autorisasjonsansvarlig. Hensikten med bestemmelsen er å unngå at det bes om klarering og igangsettes personkontroll i tilfeller der det ikke foreligger et behov.

Nkom mener det bør fremkomme tydelig i denne bestemmelsen eller i klareringsforskriften § 5 - hva som er «tilstrekkelig begrunnelse». Slik det står i dag, er det merknadene til virksomhetsforskriften § 66 som angir hva som er tilstrekkelig. Nkom antar at dette uansett vil måtte presiseres i en veiledning utarbeidet av Nasjonal sikkerhetsmyndighet..

3.9.11 Merking av personopplysninger for klarering og autorisasjon - til forskriftens § 67

Bestemmelsen er utledet av gjeldende forskrift om personellsikkerhet § 6-2 som viser til at er et dokument sikkerhetsgradert skal det i tillegg merkes i samsvar med ny sikkerhetslov § 5-3. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

3.9.12 Beskyttelse av personopplysninger for klarering og autorisasjon - til forskriftens § 68

Bestemmelsen regulerer autorisasjonsansvarliges plikt til å utpeke personell i virksomheten som kan få tilgang til opplysninger merket PERSONKONTROLL. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

3.9.13 Bevaring og kassasjon av opplysninger i saker om autorisasjon og klarering - til forskriftens § 69

Bestemmelsen fastsetter at autorisasjonsansvarlig uten ugrunnet opphold skal kassere eller returnere dokumenter med personopplysninger som er innhentet for autorisasjon eller klarering av søkere – dersom personer ikke blir tilsatt, engasjert eller opptatt på skoler eller kurs. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

3.10 Sikkerhetsgraderte anskaffelser

3.10.1 Vurdering av graderingsnivået for ulike deler av en sikkerhetsgradert anskaffelse - til forskriftens § 70

Bestemmelsen er i stor grad en videreføring av § 2-1 i forskrift om sikkerhetsgraderte anskaffelser med noen få justeringer. Den mest sentrale endringen er at vurdering av graderingsnivået skal skje for de ulike stadiene av sikkerhetsgraderte anskaffelser. Nkom støtter denne tilnærmingen. For at riktige sikkerhetstiltak skal kunne brukes på riktig stadiet er det viktig at oppdragsgiver tidlig i anskaffelsesprosessen fastsetter graderingsnivået på dokumentene i prosessen.

3.10.2 Krav til sikkerhetsavtalen etter sikkerhetsloven § 9-2 når leverandøren skal ha sikkerhetsgradert informasjon eller tilgang til skjermingsverdig objekt eller infrastruktur i eller fra sine egne lokaler - til forskriftens § 71

Bestemmelsen regulerer krav til sikkerhetsavtalen mellom virksomheten og leverandøren når leverandøren skal ha sikkerhetsgradert informasjon eller tilgang til skjermingsverdig objekt eller infrastruktur i eller fra sine egne lokaler. Nkom støtter Forsvarsdepartementets forslag til kravene i bestemmelsens bokstav a til g.

3.10.3 Unntak fra krav om sikkerhetsavtale etter sikkerhetsloven - til forskriftens § 9-2 og § 72

Bestemmelsen regulerer de tilfeller hvor det ikke er behov for sikkerhetsavtale fordi tilgang til sikkerhetsgradert informasjon, skjermingsverdige objekter eller infrastruktur gis under oppsyn av en representant for virksomheten.

Nkom er generelt positive til bestemmelsen, men mener at det bør stilles krav om at den som skal holde oppsyn har tilstrekkelig autorisasjon og klarering for den informasjonen eller det informasjonssystem, infrastruktur eller objekt leverandøren får tilgang til.

3.10.4 Tilbakelevering av sikkerhetsgradert informasjon – til forskriftens § 73

Bestemmelsen regulerer tilbakelevering av sikkerhetsgradert informasjon, og at dette skal skje uten unødig opphold dersom vedkommende ikke tildeles kontrakt. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

3.10.5 Krav om leverandørklarering - til forskriftens § 74

Bestemmelsen regulerer krav til leverandørklarering for å sikre forsvarlig sikkerhetsnivå under anskaffelsen. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

3.10.6 Leverandører med lokaler utenfor norsk jurisdiksjon og utenlandske leverandører - til forskriftens § 75

Bestemmelsen stiller krav til leverandørklarering for leverandører med lokaler utenfor norsk jurisdiksjon og utenlandske leverandører. Nkom støtter Forsvarsdepartementets forslag og mener bestemmelsen gir god oversikt over de krav som skal gjelde for forsvarlig sikkerhetsnivå under anskaffelsen.

3.10.7 Forespørsel om leverandørklarering - til forskriftens § 76

Bestemmelsen tydeliggjør at det er oppdragsgiveren, og ikke leverandøren, som skal be om en leverandørklarering. Bakgrunnen for bestemmelsen er at det er oppdragsgiver som er nærmest til å begrunne behovet for klareringen. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

3.10.8 Oversikt over sikkerhetsgraderte anskaffelser - til forskriftens § 77

Bestemmelsen fastsetter at oppdragsgiveren skal føre oversikt over egne sikkerhetsgraderte anskaffelser. Bestemmelsen må sees i sammenheng med myndighetsforskriften § 9, som beskriver Nasjonal sikkerhetsmyndighetens plikt til å føre et sentralt register over sikkerhetsgraderte anskaffelser og klareringsavgjørelser basert på oversikten. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

3.10.9 Til § 78 Prosedyrer for besøk fra utlandet - til forskriftens § 78

Bestemmelsen er i hovedsak en videreføring av forskrift om sikkerhetsgraderte anskaffelser § 4-3. Det er i de sikkerhetsavtaler som utarbeides med andre stater og internasjonale organisasjoner vanlig med avtalevilkår om prosedyrer for besøk mellom partene. Hensikten er å kunne kontrollere at de besøkende har et legitimt behov for besøket, at de er den de gir seg ut for og at de har tilstrekkelig klarering. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

3.11 Avsluttende bestemmelser

Nkom registrerer at det ikke er lagt opp til noen overgangsbestemmelser ved ikrafttredelse av forskriftene, men at det vises til en «rimelig frist». Nkom mener det er viktig at det er departementene som får ansvar for å fastsette hva som vil være en rimelig frist for virksomhetene i egen sektor. Videre er det viktig at bestemmelsen om «rimelig frist» gjøres gjeldende både for eksisterende virksomheter, hvor det eventuelt kommer nye krav og plikter, og nye virksomheter som blir underlagt sikkerhetsloven. Nkom har ingen ytterligere kommentarer til de avsluttende bestemmelsene i virksomhetsforskriften.

I arbeidet med klarering og autorisasjon av personell har Nkom erfart at det har vært utfordrende for virksomheter å benytte seg av personopplysningsblankett ved autorisasjon for BEGRENSET. Nkom mener at det er viktig at den enkelte avgir en egenerklæring når de skal autoriseres for BEGRENSET. Nkom ber derfor Forsvarsdepartementet vurdere å forskriftsfeste en slik adgang til å innhente opplysninger på et eget skjema eller at personopplysningsblanketten kan brukes.

4 Nkoms merknader til forskrift om klarering av personell og leverandører (klareringsforskriften)

Klareringsforskriften omhandler klarering av personell og leverandører.

4.1 Generelle bestemmelser om sikkerhetsklarering og adgangsklarering

4.1.1 Klareringsmyndighet – til forskriftens § 1

Bestemmelsen fastsetter hvem som er klareringsmyndighet, samt at det i enkeltsaker kan avtales hvem av klareringsmyndighetene som skal være klareringsmyndighet. Når det gjelder bestemmelsens fjerde ledd tilsvarer den forskrift om personellsikkerhet § 4-1 og fastsetter at den som utøver klareringsmyndighet må ha klarering for det høyeste klareringsnivået vedkommende skal gis fullmakt til å fatte vedtak om. Nkom er enig i forskriftsfesting av føringen om at den som utøver klareringsmyndighet må ha klarering for det høyeste klareringsnivået vedkommende skal fatte vedtak om.

4.1.2 Definisjoner – til forskriftens § 2

Bestemmelsen definerer hvem som er å anse som nærstående og enkelte undergrupper av nærståendebegrepet. Forsvarsdepartementet har valgt å definere dette for å unngå forskjellsbehandling og for å oppnå forutsigbarhet og åpenhet om hvem som kontrolleres i klareringssaker.

Nkom ser det som positivt at det defineres hvem som er å anse som nærstående. Nkom mener også at det bør tilføres en bokstav d, der annen nær tilknytning beskrives. Personkontrollseksjonen hos Nkom har ved flere anledninger behandlet saker hvor en slik definisjon ville forenklet vurderinger og saksbehandling. Nkom har i arbeidsgruppemøtene med forskriftene foreslått at det ses hen til habilitetsreglene i forvaltningsloven for definisjon og/eller beskrivelse av begrepet «annen nær tilknytning».

4.1.3 Forholdet mellom adgangsklarering og sikkerhetsklarering – til forskriftens § 3

Bestemmelsen beskriver forholdet mellom adgangsklarering og sikkerhetsklarering. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

4.1.4 Hvem som kan be om klarering – til forskriftens § 4

Bestemmelsen slår fast at autorisasjonsansvarlig i virksomheter som er underlagt ny sikkerhetslov, kan be klareringsmyndigheten om klarering av personell. Nkom støtter at det fremgår tydelig hvem som kan be om klarering.

4.2 Personkontroll

4.2.1 Kontroll og avvisning av forespørsel om personkontroll – til forskriftens § 5

Bestemmelsen regulerer en plikt for klareringsmyndigheten til å kontrollere at forespørselen om klarering er tilstrekkelig begrunnet og dokumentert.

Nkom mener det bør fremkomme tydeligere, enten i klareringsforskriften § 5 eller i virksomhetsforskriften § 66, hva som er å anse for «tilstrekkelig begrunnelse». En tydeliggjøring vil gi bedre grunnlag for etablering av en enhetlig praksis.

4.2.2 Personer som inngår i personkontrollen – til forskriftens § 6

Bestemmelsen regulerer hvilke personer som inngår i personkontrollen. Ny sikkerhetslovs utvidelse av begrepet «nærstående» medfører at det kan utføres personkontroll overfor en videre krets av personer. Bestemmelsens andre ledd fastsetter i hvilke tilfeller det kan gjennomføres personkontroll av andre nærstående enn de som er angitt i første ledd, Nkom har i utøvelsen av klareringsmyndighet sett behovet for å utvide hvilke nærstående det kan utføres personkontroll av og støtter Forsvarsdepartements forslag.

4.2.3 Sikkerhetsklarering – krav til egenopplysninger – til forskriftens § 7

Bestemmelsen er ny og regulerer de plikter og krav private rettssubjekter vil få ved innmelding av opplysninger fra den som skal sikkerhetsklareres.

Forsvarsdepartementet har i merknader til forskriften opplyst at de vil vurdere om det er hensiktsmessig å kreve at den som skal klareres selv må gi opplysninger eller om det er tilstrekkelig at klareringsmyndighet innhenter opplysninger fra offentlige registre. Nkom anser det som viktig at den som skal klareres gir opplysninger om seg selv. En slik «egenmelding» gir klareringsmyndigheten mulighet til å kontrollere pålitelighet, lojalitet og dømmekraft ved å sammenligne skjemaet den enkelte fyller ut opp mot opplysninger fra offentlige registre.

Til første ledd bokstav i foreslår Nkom å stryke «særlig» og bare la det stå «Tilknytning til andre stater […]». Endringen senker terskelen for å opplyse om tilknytning til andre stater.

Nkom ber Forsvarsdepartementet vurdere å bytte ut «grunn til å frykte» med «grunn til å tro». Personell som skal sikkerhetsklareres vil lettere kunne forholde seg til «grunn til å tro», enn uttrykket «grunn til å frykte».

4.2.4 Adgangsklarering – krav til egenopplysninger – til forskriftens § 8
Bestemmelsen er ny og regulerer hvilke egenopplysninger som skal gis i forbindelse med adgangsklarering. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

4.2.5 Registre for personkontroll ved sikkerhetsklarering – til forskriftens § 9
Bestemmelsen regulerer hvilke registre Nasjonal sikkerhetsmyndighet kan innhente og videreformidle til klareringsmyndigheten for personkontroll ved sikkerhetsklarering.
Nkom har ingen kommentar til bestemmelsen og er således enig i det som er anført.

4.2.6 Registre for personkontroll ved adgangsklarering – til forskriftens § 10
Bestemmelsen er utledet av forskriften § 9, men med færre registre, da det er færre registre som vil være relevant for vurderingsgrunnlaget for adgangsklarering. Nkom har ingen kommentar til bestemmelsen og er således enig i det som er anført.

4.2.7 Innhenting av personkontrollopplysninger fra andre stater – til forskriftens § 11
Bestemmelsen regulerer Nasjonal sikkerhetsmyndighets mulighet til å innhente tilsvarende opplysninger som i forskriftens §§ 9 og 10 fra andre staters myndigheter. Nkom har ingen kommentar til bestemmelsen og er således enig i det som er anført.

4.2.8 Behandlingsansvarliges plikter ved utlevering av opplysninger – til forskriftens § 12
Bestemmelsen regulerer den behandlingsansvarliges plikter ved utlevering av opplysninger. Bestemmelsen må sees i sammenheng med ny sikkerhetslovs § 8-4 niende ledd. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

4.2.9 Utlevering og bruk av opplysninger fra etterretnings- og arbeidsregistre ved politiet og Politiets sikkerhetstjeneste – til forskriftens § 13
Bestemmelsen er ny og regulerer bruk av opplysninger fra registre hos politiet og Politiets sikkerhetstjeneste. Bestemmelsen søker å ivareta hensynet til operative og forebyggende behov hos politiet/PST og Nasjonal sikkerhetsmyndighet/klareringsmyndighetene. Nkom vil

understreke at det er positivt at hensynet til operative og forebyggende behov hos politiet og PST ivaretas.

4.2.10 Personhistorikk – til forskriftens § 14

Bestemmelsen regulerer krav om personhistorikk, som må være innfridd for at en personkontroll for sikkerhetsklarering/adgangsklarering, samt klarering av personer som har oppholdt seg i utlandet, kan anses å være tilfredsstillende. Bestemmelsens fjerde ledd gir en mulighet til å gjøre unntak fra kravet om personhistorikk dersom årsaker til dette i stor grad veier opp for risikoen ved å klarere personen. Vurderingen skal være basert på en konkret helhetsvurdering.

Etter bestemmelsens andre ledd vil en personkontroll for adgangsklarering anses å være tilfredsstillende når det foreligger personkontrollopplysninger for de siste fem årene. Nkom støtter en slik femårsregel for tilfredsstillende personkontroll ved adgangsklarering.

Til bestemmelsens fjerde ledd ser Nkom at det er tatt inn noen nye momenter sammenlignet med nåværende forskrift om personellsikkerhet § 3-7, siste ledd. Dette anser Nkom som positivt, da det gis noe utvidelse av unntaksbestemmelsen. Bestemmelsens femte ledd mener Nkom bør utdypes i forhold til hvilke momenter som skal vektlegges i en helhetsvurdering.

4.3 Prosessen for sikkerhetsklarering og adgangsklarering

4.3.1 Vurderingsgrunnlaget for adgangsklarering – til forskriftens § 15

Bestemmelsen regulerer hvilke forhold som skal vektlegges i vurderingen av adgangsklarering og ved utvidet adgangsklarering etter ny sikkerhetslov § 8-4. Hensikten med bestemmelsen er å få frem at formålet med adgangsklarering i hovedsak omhandler forebygging mot forberedelser til og forsøk på terror. Avgrensningen er ikke absolutt, dersom tilknytning til spionasje eller sabotasje for fremmes stat likevel skulle fremkomme, kan også det vektlegges.

Nkom er positive til at man har delt adgangsklarering inn i to nivåer, men mener at den utvidede adgangsklareringen ikke bør begrenses til norske borgere, men også bør omfatte borgere fra de nordiske landene. Det vises her til våre tidligere kommentarer knyttet til nordisk samarbeid og næringsvirksomhet.

4.3.2 Vurderingsgrunnlaget for tilknytning til andre stater – til forskriftens § 16

Bestemmelsen regulerer hvilke forhold klareringsmyndigheten skal vektlegge som grunnlag for å vurdere tilknytning til andre stater. Materielt sett tilsvarer bestemmelsen gjeldende forskrift om

personellsikkerhet § 3-3 tredje ledd. Bestemmelsen forutsetter at Nasjonal sikkerhetsmyndighet fortsatt utarbeider konkrete personellsikkerhetsmessige vurderinger av andre stater.

Innen ekomsektoren er det som nevnt utstrakt bruk av utenlands kompetanse på tvers av landegrensene, og da særlig innen Norden. Nkom foreslår at det tas inn et nytt ledd til forskriften §16, eventuelt ny §16a, der det fremkommer at det i vurderingen av klarering av utenlandske statsborgere uten tilknytning til Norge bør legges avgjørende vekt på sektormyndighetenes vurdering om det foreligger særlige grunner for å gjennomføre sikkerhetsklarering.

4.3.3 Klareringsintervju – til forskriftens § 17

Bestemmelsen regulerer hva som menes med klareringsinterviu, hva formålet med dette er, og en dokumentasjonsplikt. Videre regulerer bestemmelsen hvilke plikter den som innkalles til et klareringsintervju har. Bestemmelsen tilsvarer gjeldende bestemmelse i forskrift om personellsikkerhet § 4-2, men med enkelte endringer. Begrepet «sikkerhetssamtale» er erstattet med «klareringsintervju».

Nkom er enig i begrunnelsen til Forsvarsdepartementet for endring av begrepet sikkerhetssamtale til klareringsintervju, Nkom er positive til forslaget om at bisitter må være innmeldt på forhånd, og at bisitter skal undertegne en taushetserklæring.

4.3.4 Vurdering om lavere klareringsnivå kan gis og bruk av vilkår – til forskriftens § 18

Bestemmelsen regulerer muligheten for klareringsmyndigheten å gi lavere klareringsnivå dersom klareringsnivå ikke kan gis for det nivå autorisasjonsansvarlig har bedt om. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

4.3.5 Karantene før ny klareringsvurdering – til forskriftens § 19

Bestemmelsen regulerer en karantenetid dersom klareringsmyndigheten ikke innvilger klarering i samsvar med det den autorisasjonsansvarlige har bedt om. Personen kan da ikke vurderes på nytt før den gitte karantenetida har utløpt. Bestemmelsen tilsvarer i all hovedsak gjeldende bestemmelse i forskrift om personellsikkerhet § 4-4 andre ledd, men enkelte endringer er gjort i ordlyden, eksempelvis har uttrykket «observasjonstid» blitt erstattet med «karantene».
Nkom støtter at uttrykket «observasjonstid» har blitt erstattet med «karantenetid».

4.3.6 Melding om klareringsavgjørelse – til forskriftens § 20

Bestemmelsen regulerer klareringsmyndighetens plikt til å gi melding om klareringsavgjørelser til autorisasjonsansvarlig og til Nasjonal sikkerhetsmyndighet, og tilsvarer gjeldende bestemmelser i forskrift om personellsikkerhet § 4-4 første og tredje ledd, med presisering om at både eventuell karantene og vilkår skal følge meldingen.

Nkom støtter bestemmelsens utforming og er positiv til at det kreves tillatelse for at opplysninger fra PST/etterretnings- og arbeidsregistre fra politiet kan inngå i melding til person som gis delvis avslag/avslag.

4.3.7 Innsyn i klareringssak – til forskriftens § 21

Bestemmelsen regulerer klareringsmyndighetens plikt til å i hvert enkelt tilfelle be om tillatelse når det gjelder innsyn i opplysninger fra Politiets sikkerhetstjeneste eller etterretnings- og arbeidsregistre fra politiet. Bestemmelsens første ledd er ny, mens andre ledd er utledet av gjeldende sikkerhetslov § 25 a. Nkom støtter bestemmelsen, men mener det vil være hensiktsmessig å forskriftsfeste at det ikke gis innsyn i suspensjonssaker, ettersom dette ikke er en avgjørelse om klarering jfr. ny sikkerhetslov § 8-14.

4.3.8 Gyldighetstid for sikkerhetsklarering og adgangsklarering – til forskriftens § 22

Bestemmelsen regulerer en gyldighetstid på fem år for sikkerhetsklarering og adgangsklarering. Nkom har ingen kommentar til bestemmelsen og er således enig i det som er anført.

4.3.9 Betydningen av forhold som ble vurdert ved en tidligere klareringsavgjørelse – til forskriftens § 23

Bestemmelsen slår fast at forhold som har vært vurdert ved tidligere klareringsavgjørelser ikke alene kan danne grunnlag for helt eller delvis avslag på en ny forespørsel. Bestemmelsen tilsvarer gjeldende bestemmelse i forskrift om personellsikkerhet § 4-8. Nkom vil peke på at det kan være en utfordring dersom trusselvurderingen knyttet til land vedkommende har en tilknytning til, har endret seg

4.3.10 Bevaring, kassasjon og avlevering av dokumenter i klareringssaker – til forskriftens § 24

Bestemmelsen regulerer Nasjonal sikkerhetsmyndighets plikt til å fastsette en instruks om bevaring, kassasjon og avlevering av dokumenter i saker om personkontroll og klarering. Bestemmelsen er foreslått forskriftsfestet da Forsvarsdepartementet ser nødvendigheten av å

fastsette bestemmelser om bevaring, kassasjon og avlevering av dokumenter i klareringssaker. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

4.3.11 Dekking av kostnader ved klarering – til forskriftens § 25

Bestemmelsen regulerer klareringsmyndighetens plikt til å dekke kostnadene ved klarering, med mindre annet er avtalt med klareringsansvarlig. Bestemmelsen tilsvarer gjeldende bestemmelser i forskrift om personellsikkerhet § 6-11. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført..

4.4 Samtykke til å autorisere utenlandske statsborgere for BEGRENSET

4.4.1 Samtykke til å autorisere utenlandske statsborgere for BEGRENSET – til forskriftens § 26

Bestemmelsen regulerer klareringsmyndighetens plikt til å samtykke til autorisasjon før en utenlandsk statsborger kan autoriseres for BEGRENSET. Bestemmelsen er ny og formålet med bestemmelsen er å unngå at det gis tilgang til gradert informasjon i større grad enn hva det strengt tatt er behov for, og at det ikke gis autorisasjon uten at risikoen knyttet til etterretningstrusselen fra personellets hjemland er vurdert. Bestemmelsene i kapittel fire skal også sikre at klareringsmyndigheten har oversikt over utenlandsk personell som skal gis tilgang til BEGRENSET informasjon. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

4.4.2 Egenopplysninger – til forskriftens § 27

Bestemmelsen regulerer hvilke opplysninger klareringsmyndigheten kan kreve av utenlandske statsborgere for avgjørelse om tillatelse for autorisasjon fro BEGRENSET. Opplysningene som innhentes skal være egnet til å vurdere risikoen forbundet med å gi den utenlandske statsborgeren tilgang til BEGRENSET informasjon. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

4.4.3 Saksbehandling og avgjørelse av forespørsel om tillatelse til autorisasjon – til forskriftens § 28

Bestemmelsen regulerer klareringsmyndighetens saksbehandling og avgjørelse av forespørsel om samtykke til å autorisere en utenlandsk statsborger for BEGRENSET. Bestemmelsen skal legge til rette for at autorisasjon gis på bakgrunn av klareringsmyndighetens tilgang til Nasjonal sikkerhetsmyndighets personellsikkerhetsmessige landvurderinger, og autorisasjonsansvarliges vurdering av personellet, slik at samtykke gis på bakgrunn av en helhetlig forståelse av risikoen

forbundet med å gi tilgang til BEGRENSET informasjon. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

4.5 Leverandørklarering

4.5.1 Klareringsmyndighet for leverandørklarering – til forskriftens § 29

Bestemmelsen regulerer hvem som er klareringsmyndighet for leverandørklarering. Praksis for sikkerhetsavtaler mellom stater er at det legges opp til at statenes sikkerhetsmyndigheter bare skal kontrollerer leverandører som holder til på statens eget territorium. Av den grunn er også leverandørklareringsmyndigheten lagt til sikkerhetsmyndigheten i staten der leverandøren holder til. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

4.5.2 Egenopplysninger fra leverandøren – til forskriftens § 30

Bestemmelsen regulerer leverandøren som skal klareres sin plikt til å samtykke til å bli kontrollert og gi egenopplysninger bestemt av Nasjonal sikkerhetsmyndighet. Bestemmelsen forskriftsfestes for å oppnå en effektiv saksbehandling og forutsigbarhet om hvilke opplysninger leverandøren skal gi til klareringsmyndigheten. Da private rettssubjekter ikke kan pålegges å gi opplysninger på en bestemt måte uten at det er fastsatt i lov eller forskrift har Forsvarsdepartementet foreslått en ny bestemmelse i første ledd om at leverandøren skal benytte et skjema fastsatt av Nasjonal sikkerhetsmyndighet. Nkom støtter bestemmelsens utforming, og ser positivt på den forutsigbarhet bestemmelsen gir i forhold til hvilken informasjon som skal gis i forbindelse med klarering.

4.5.3 Vurderingsgrunnlaget for leverandørklarering – til forskriftens § 31

Bestemmelsen regulerer hvilke krav leverandøren må oppfylle i ny sikkerhetslov og virksomhetsforskriften, samt hvilke kriterier som vektlegges i vurderingen av om leverandørklareringen skal gis. Bestemmelsen tilsvarer bestemmelsene i gjeldende forskrift om sikkerhetsgraderte anskaffelser § 3-2. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

4.5.4 Kilder for leverandørkontroll – til forskriftens § 32

Bestemmelsen regulerer hvilke registre klareringsmyndigheten kan innhente opplysninger om leverandøren fra. Det er en ny bestemmelse som vil bidra til økt forutsigbarhet og til å unngå usaklig forskjellsbehandling i saksbehandlingen da det går tydelig frem av bestemmelsen hvilke typer registre som kontrolleres.

Nkom støtter bestemmelsens utforming, og ser på det som positivt å forskriftsfeste hvor opplysninger kan innhentes fra

4.5.5 Kontroll av om leverandøren oppfyller sikkerhetskravene – til forskriftens § 33

Bestemmelsen regulerer klareringsmyndighetens plikt til å kontrollere at leverandøren oppfyller kravene i ny sikkerhetslov og virksomhetsforskriften. En slik kontroll skal foretas før vedtak om leverandørklarering gis. Kravet i gjeldende forskrift om kontroll av sikkerhetsgraderte anskaffelser hver 18. måned, er ikke videreført. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

4.5.6 Tilbakekall av leverandørklarering – til forskriftens § 34

Bestemmelsen regulerer en tilbakekallelse av leverandørklareringen dersom leverandøren ikke retter avvik innen en fastsatt frist. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

4.5.7 Leverandørklareringens gyldighetstid – til forskriftens § 35

Bestemmelsen fastsetter at leverandørklareringen kan vare i inntil fem år og tilsvarer gjeldende forskrift om sikkerhetsgraderte anskaffelser § 3-1. Nkom har ingen kommentarer til bestemmelsen og er således enig i det som er anført.

4.5.8 Registrering av klareringsavgjørelser – til forskriftens § 36

Bestemmelsen fastsetter at avgjørelser skal registreres i det sentrale registeret over leverandørklareringer. Nkom er enig i bestemmelsen med en tydelig henvisning til myndighetsforskriften § 9, hvor det fremkommer at det er Nasjonal sikkerhetsmyndighet som skal føre register over klareringsavgjørelsene.

4.6 Særbestemmelser for domstolene

Nkom har ingen kommentarer til bestemmelsene og er således enig i det som er anført.

Nasjonal kommunikasjons-myndighet

4.7 Avsluttende bestemmelser

Nkom har ingen kommentarer til bestemmelsene og er således enig i det som er anført.

Med hilsen

Elisabeth Aarsæther
direktør

Elise K. Lindeberg
avdelingsdirektør

Dokumentet er godkjent elektronisk og ekspedert uten underskrift

Kopi Samferdselsdepartementet, Postboks 8010 Dep., 0030 OSLO