Fra: KS (svarer-ikke@dss.dep.no)
Sendt: 25.09.2018 16:36:09
Til: Postmottak FD
Kopi:

Emne: 2015/3139-254/FD V 3/ENWA - Høringsuttalelse fra KS - Høring - forskrifter til ny sikkerhetslov - via regjeringen.no
Vedlegg: Høringsuttalelse fra KS.pdf

Referanse:	2015/3139-254/FD V 3/ENWA
Høring:	Høring - forskrifter til ny sikkerhetslov
Levert:	25.09.2018 16:36
Svartype:	Med merknader
Kontakt avsender:	KS
Kontaktperson:	Anne Mette Dørum
Kontakt-e-post:	anne.mette.dorum@ks.no
Tittel:	Høringssvar - forskrifter til ny Sikkerhetslov
Uttalelse:	

Forsvarsdepartementet - FD

Postboks 8126 Dep.

0032 OSLO

Vår referanse: 15/00792-6

Arkivkode: X00 &00

Saksbehandler:	Anne Mette Dørum,
Deres referanse:	2015/3139-254/FD V 3/ENWA
Dato:	25.09.2018

Høringssvar - forskrifter til ny Sikkerhetslov

Vi viser til høringsnotat av 2. juli 2018 der Forsvarsdepartementet foreslår tre forskrifter til lov om nasjonal sikkerhet (sikkerhetsloven). Forskriftene regulerer henholdsvis:

- myndighetenes ansvar og roller for forebyggende sikkerhet
- virksomhetens arbeid med forebyggende sikkerhet
- klarering av personell og leverandører

I høringsnotatet foreslår departementet tre forskrifter:

- Forskrift om myndighetenes roller og ansvar for nasjonal sikkerhet (myndighetsforskriften)
  - Retter seg mot departementer, NSM og myndigheter med tilsynsansvar etter loven
- Forskrift om virksomhetens arbeid med forebyggende sikkerhet (virksomhetsforskriften).
  - Retter seg mot alle virksomheter som blir underlagt loven

- Forskrift om klarering av leverandører og personell (klareringsforskriften)
    - Retter seg mot klareringsmyndighetene som Sivil klareringsmyndighet og FSA og andre virksomheter som klarer personell Det vil primært være virksomhetsforskriften som er av betydning for kommuner og fylkeskommuner. Derfor omfatter høringsuttalelsen i hovedsak denne forskriften.

Bakgrunn

Lov om nasjonal sikkerhet (sikkerhetsloven) ble vedtatt av Stortinget 6. mars 2018, og i det vesentlige slik den ble fremmet av regjeringen i Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet (sikkerhetsloven)*. Proposisjonen baserte seg på anbefalingen fra det regjeringsoppnevnte sikkerhetsutvalgets utredning som forelå høsten 2016 i rapporten NOU 2016: 19 *Samhandling for sikkerhet.* Virkeområdet for ny sikkerhetslov er alle statlige, fylkeskommunale og kommunale organer. Loven vil også gjelde for leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser. Det vil si at loven får større betydning for sivil sektor enn dagens.

Hva er nytt i forslaget

Forslaget tar, i motsetning til mange andre lovforslag som berører IKT, hensyn til behov for standardisering og like regler for alle bransjer/sektorer så langt dette er mulig. For kommuner og fylkeskommuner som operert på tvers av sektorene, vil det være ønskelig at dette hensynet gis enda større vekt.

Forskriftene stiller krav til at forsvarlig sikkerhetsnivå skal oppnås gjennom en kombinasjon av menneskelige, elektroniske, fysiske og organisatoriske tiltak.

Med menneskelige tiltak menes ikke bare klarering og autorisasjon, men også tiltak som opplæring og bevisstgjøring av medarbeidere, og hvordan sikkerheten ivaretas både under ansettelse og avslutning av arbeidsforhold. Med elektroniske tiltak menes digitale/logiske tiltak. Dette kan være elektroniske alarm- og overvåkningssystemer av lokaler, men også tiltak gjort i IKT-systemer som brannmurer, passord og kryptering. Organisatoriske tiltak vil i all hovedsak dekkes av kravene til styringssystem for sikkerhet i virksomhetsforskriften.

Det er nytt at regelverket ikke bare omfatter informasjon og informasjonssystemer som er skjermingsverdige av hensyn til å beskytte informasjonens konfidensialitet, men at også informasjon og informasjonssystemer vil kunne være skjermingsverdige ut i fra i hvilken grad tap av integritet og tilgjengelighet vil kunne påvirke de grunnleggende nasjonale funksjonene. Dette vil medføre at flere informasjonssystemer og infrastrukturer, vil bli omfattet av regelverket.

Forskriftene åpner for at personer som bare skal gis tilgang til skjermingsverdige objekter og infrastruktur, kan gis adgangsklarering eller utvidet adgangsklarering. Videre er det gjort endringer når det gjelder hvem som fører kontroll med leverandører for sikkerhetsgraderte anskaffelser.

For informasjon som er sikkerhetsgradert eller objekter som er klassifisert etter gjeldende regelverk, vil kravet til sikringsnivå i utgangspunktet være det samme som i dag. Loven legger imidlertid opp til at avhengigheter skal kartlegges i større grad enn i dag. For virksomheter som andre virksomheter er avhengig av for å kunne fungere, vil ny sikkerhetslov kunne innebære et høyere klassifiseringsnivå og krav til høyere sikringsnivå. Departementet antar imidlertid at virksomhetene som utgangspunkt kan legge til grunn at et sikringsnivå som oppfyller gjeldende regelverk, også vil oppfylle nytt regelverk.

Det er ikke direkte nytt at sikkerhetsloven gis anvendelse i sivil sektor. Det gjør også gjeldende sikkerhetslov. Men den nye loven får større betydning for sivil sektor enn dagens.

Funksjonelle krav

Loven stiller krav om at virksomhetene skal gjennomføre de forebyggende sikkerhetstiltakene som må til for å gi et forsvarlig sikkerhetsnivå og redusere risikoen knyttet til sikkerhetstruende virksomhet. For at virksomhetene skal kunne oppnå et forsvarlig sikkerhetsnivå med sikkerhetstiltak som er tilpasset den enkelte virksomhet, informasjonen, informasjonssystem, infrastruktur og objekt virksomheten råder over og den trussel og risiko virksomheten er utsatt for, stiller forskriftene funksjonelle krav til sikring. Det innebærer at det ikke konkretiseres hvilke sikkerhetstiltak den enkelte virksomhet skal etablere, men at det stilles krav til hva sikkerhetstiltakene skal oppnå.

Det vil således være virksomhetene som må avpasse hvilke fysiske, elektroniske, menneskelige eller organisatoriske sikringstiltak, som er nødvendige for å oppnå et forsvarlig sikkerhetsnivå. Hva som er forsvarlig vil avhenge av hvor stor betydning informasjonen, informasjonssystemet, objektet eller infrastrukturen virksomheten skal beskytte, har for nasjonale sikkerhetsinteresser. Det vil også avhenge av hvilke trusler og risikoer disse verdiene til enhver tid er utsatt for og av hva som vil være kostnadseffektiv sikring.

Kravene i forskriftene vil på enkelte områder gi føringer om hvordan virksomheten systematisk skal gå frem for å sikre verdiene de rår over. Dette kan for eksempel gjelde prosesser som skal følges i sikkerhetsarbeidet og hva som skal vurderes i det forebyggende sikkerhetsarbeidet. Dette skal bidra til at virksomheter i ulike sektorer kommer frem til tilnærmet samme sikkerhetsnivå, men åpner for at det kan tas i bruk forskjellige tiltak. For eksempel kan det for én virksomhet være mest aktuelt å sikre et objekt med fysiske barrierer, mens en annen kan finne det mest kostnadseffektivt å sikre dette med elektronisk overvåkningssystem og vaktstyrker. Begge deler vil kunne ivareta grunnsikring for ulike objekter med samme klassifiseringsnivå.

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

Merknader til selve høringsdokumentet

Innretning av høringsnotatet

KS vil innledningsvis gi innspill til de mer generelle sidene ved forslaget (høringsnotatets kapittel 1-5). Deretter følger innspill til den enkelte forskrift (generelt og i tilknytning til den enkelte bestemmelse).

En generell merknad til hele lovteksten er at KS ikke i særlig grad ser spor av moderne sikkerhetsarkitektur i forslaget. Det er også lite spor av moderne informasjonsteknologi. Det kan virke som om dette utfordrende kompetanseområdet ikke i tilstrekkelig grad er vurdert. KS stiller også spørsmål ved om det er mulig å tenke seg et lovverk som er helt teknologinøytralt. Det er mulig utfordringer knyttet til «cyber space» bør omtales tydeligere, ettersom det er helt spesielle utfordringer på dette området.

Til høringsnotatets Kapittel 3 - Om forslaget

Høringsinnspill til pkt. 3.1 - Virkeområde

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Loven vil nå gjelde for virksomheter som behandler sikkerhetsgradert informasjon eller som råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for «grunnleggende nasjonale funksjoner». Som grunnleggende nasjonale funksjoner regnes:

1. De øverste statsorganers virksomhet, sikkerhet og handlefrihet

2. Forsvar, sikkerhet og beredskap
3. Forholdet til andre stater og internasjonale organisasjoner
4. Økonomisk stabilitet og handlefrihet
5. Samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet

Dette vil si at loven får større betydning for sivil sektor enn dagens. Det vil særlig være områdene som faller inn under punktene 2 og 5 over som vil berøre kommuner og fylkeskommuner.

NOU 2006:6 Når sikkerheten er viktigst/St.m. nr. 22 (2007–2008) nevnes flere eksempler på hva som er «samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende trygghet». For kommuner og fylkeskommuner er følgende mest aktuelle:

- Elektronisk kommunikasjon
- Kraft
- Vann og avløp
- Transport
- Bank og finans
- Matforsyning
- Kulturminner og symboler
- Helse-, sosial- og trygdetjenester
- Nød- og redningstjeneste
- Kriseledelse
- Miljøovervåkning
- Renovasjon

Slik departementet ser det, er det på det nåværende tidspunkt ikke nødvendig å forskriftsfeste ytterligere momenter som skal vektlegges i vurderingen av hvilke virksomheter loven skal gjelde for, utover de som allerede fremgår av Prop. 153 L (2016–2017), kapittel 6.4.

Departementet ber likevel om høringsinstansenes syn på om det bør fremgå ytterligere momenter i forskriftene, og i så fall hvilke. Departementet ser at en slik momentliste vil kunne bidra til å klargjøre virkeområde til loven, og vil vurdere om det er behov for at det tas inn ytterligere momenter i forskriftene i forbindelse med høringsrunden.

KS' merknad

Kommuner og fylkeskommuner har et meget vidt fagfelt og skal forhold seg til mange departementer. Mye av kommunenes infrastruktur og mange av deres informasjonssystemer betjener tjenester som er underlagt forskjellige departementer og derigjennom flere direktorater. Ettersom kommuner og fylkeskommuner er integrerte virksomheter, vil IT-infrastruktur, fellesløsninger og fagsystem ofte brukes på tvers av de sektorgrenser som finnes i staten. Det vil derfor være en stor utfordring hvis departementer og direktorater i sine vurderinger vektlegger «like hensyn» ulikt.

KS foreslår at forskriften tar inn mer detaljert veiledning om hvilke momenter som skal vektlegges når departementene skal avgjøre hvilke informasjonssystemer og hvilken infrastruktur som skal omfattes av loven. Dette for å unngå forskjeller i krav som stilles til en og samme infrastruktur / ett og samme informasjonssystem.

Høringsinnspill til pkt. 3.2 – Inndeling i forskrift

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

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

entydige.

KS' merknad

KS går ut fra at det rent pedagogisk vil være en fordel om alle bestemmelsene samles i en forskrift. Det som berøres i de tre forskriftene, henger nøye sammen. En oppdeling vil kunne innebære at viktig informasjon i en forskrift, ikke oppdages av aktører som normalt forholder seg primært til en annen forskrift.

Det antas også at det vil være enklere å vedlikeholde en forskrift enn tre. Herunder at risikoen for utilsiktede forskjeller, vil være mindre om alt reguleres i en og samme forskrift.

Opprettholdes valget med tre forskrifter oppfattes korttitlene som allerede er brukt av departementet i høringsnotatet, som tilstrekkelig entydige.

Til høringsnotatets Kapittel 4 – Omtale av enkelte særskilte temaer

Høringsinnspill til pkt. 4.1 – Objekt- og infrastruktursikkerhet

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Departementet erkjenner at infrastrukturer ofte er svært komplekse, og kjennetegnes av lange og uoversiktlige verdikjeder, som kan gjøre det vanskeligere å sikre en infrastruktur enn et objekt.

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

KS' merknad:

KS mener at mer detaljert regulering av hvilke krav som stilles til infrastruktur, vil kunne gjøre det enklere for kommuner og fylkeskommuner å etterleve loven.

I tilfelle slike regler gis, er det viktige at disse gis på en måte som er forståelig for de som skal praktisere regleverket. Reglene bør gi gode føringer over tid, og kravene bør være teknologinøytrale og robuste over tid. Det er også viktig at alle generelle krav samles på et sted, og at kun virksomhetsspesifikke krav reguleres på «fagdepartementsnivå».

Et noe større detaljeringsnivå vil også kunne lette offentlige myndigheters forhandlinger med leverandører ved anskaffelse av infrastruktur. Noe klarere krav vil også kunne ha positive effekter i oppfølgning av kontrakten.

En annen positiv effekt av å samle generelle krav på et sted, er at det vil gjøre det enklere for leverandørene å standardisere sine løsninger. Felles generelle krav vil også redusere kostnader ved sektorspesifikke tilpasninger hos kunder som operer innenfor flere sektorer. Totalt vil dette kunne gi betydelige kostnadsreduksjoner både for kunder og leverandører.

Høringsinnspill til pkt. 4.5/4.5.1 – Klarering av utenlandske statsborgere

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Departementet mener at § 8-7 gir tilstrekkelige føringer for den helhetsvurderingen klareringsmyndigheten skal gjøre, og har derfor ikke sett det som nødvendig at det gis ytterligere bestemmelser om selve vurderingen i forskrift, utover §§ 14 og 16 i klareringsforskriften, om personhistorikk og tilknytning. Departementet har bedt om høringsinstansenes

innspill på om det er behov for en bestemmelse som konkretiserer vurderingstemaene ytterligere, og vil vurdere en slik bestemmelse i lys av høringsinnspillene.

Det følger av ny sikkerhetslov § 8-7 at

«En person som har utenlandsk statsborgerskap, kan etter en konkret helhetsvurdering få klarering, dersom det ikke er rimelig grunn til å tvile på at personen er sikkerhetsmessig skikket. I tillegg til forholdene i § 8-4 skal det i vurderingen legges vekt på hjemlandets sikkerhetsmessige betydning, personens tilknytning til hjemlandet og tilknytningen til Norge.

Ved klarering av en person med utenlandsk statsborgerskap, skal det vurderes særskilt om bruk av vilkår, som for eksempel stillingsklarering, kan være et risikoreduserende tiltak.»

KS' merknad:

KS mener at lovens bestemmelser og de foreslåtte bestemmelsene i klareringsforskriften §§ 14 og 16 som tilstrekkelige.

Høringsinnspill til pkt. 4.5.4 – Unntak fra krav om sikkerhetsklarering i særskilte tilfeller

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

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

KS' merknad:

KS vurderer det slik at i noen få tilfeller kan være behov for et slikt unntak.

Det antas at det kan være hensiktsmessig at bestemmelsen utvides med noen flere kriterier for hva som skal inngå i vurderingen for om unntak skal gis. Dette for å lette praktiseringen av bestemmelsen for kommuner og fylkeskommuner.

Høringsinnspill til pkt. 4.6 – Krav til sikkerhet i anskaffelser/pkt. 4.6.4 – Varslingsplikt

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

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

KS' merknad:

KS antar at bruken av veiledere her kan være hensiktsmessig. En slik fremgangsmåte legger til rette for raskere oppdatering ved endringer i risikobildet. Også her vurderes det som hensiktsmessig at det legges opp til en veileder med generelle krav, det vil si at bare fastsettelse av områdespesifikke momenter overlates til det enkelte departement. Dette for å gjøre det enklest mulig for de som skal forholde seg til flere statlige sektorer – slik tilfellet er i kommuner og fylkeskommuner – å gjenbruke risikovurdering/sikringstiltak, så langt mulig, på de områder hvor risikobildet/sikringsbehovet er likt for alle sektorer.

Høringsinnspill til pkt. 4.7 - Ikrafttredelse

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Det foreslås at loven trer i kraft og forskriftene fastsettes fra 1. januar 2019.

Departementene skal fatte enkeltvedtak om hvilke virksomheter loven skal gjelde for, jf. sikkerhetsloven § 1-3. Virksomhetene vil da ha behov for tid til å tilpasse seg kravene i lov og forskrifter. Hvor mye tid virksomheten trenger for å tilpasse seg vil imidlertid være individuelt. Det er derfor naturlig at det som del av vedtaket om at sikkerhetsloven skal gjelde for virksomheten også fastsettes hvor mye tid virksomheten får til å tilpasse seg kravene til sikring av den informasjon, informasjonssystem, infrastruktur eller objekt virksomheten råder over. Departementet vurderer hvorvidt det er nødvendig med en bestemmelse som fastsetter kriterier som skal vektlegges når fristen for oppfyllelse skal settes.

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

KS' merknad:

KS mener at det er hensiktsmessig med en egen bestemmelse som regulerer hvilke momenter som skal vurderes når det settes en konkret frist for at hvert enkelt informasjonssystem, infrastruktur eller objekt oppnår et forsvarlig sikringsnivå.

KS vil påpeke at det må tas hensyn til at de kostnader som vil påløpe for å tilpasse seg regelverket, vil være betydelige for kommuner og fylkeskommuner. Det må derfor sikres at det avsettes tilstrekkelig midler i statsbudsjettet, slik at kommuner og fylkeskommuner gis faktisk økonomisk mulighet til å oppfylle kravene på en god måte. Skal disse midlene tas over kommunenes ordinære budsjetter, er det stor risiko for at det ikke er tilstrekkelig midler til å gjennomføre tiltakene på den måten som forventes. Å sikre et økonomisk forsvarlig grunnlag for tilpasning til nytt regelverk, blir særlig viktig når man ser hen til de komplekse infrastrukturer som i dag finnes i offentlig sektor og særlig i kommunal sektor. Kompleksiteten gjør at svakheter og sårbarheter som ikke utbedres hos en statlig virksomhet, en kommune eller fylkeskommune, lett vil kunne få konsekvenser for det totale risikobildet.

Høringsinnspill til kapitel 5 - Økonomiske og administrative konsekvenser

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Departementet påpeker at den nye sikkerhetsloven med forskrifter vil innebære betydelige utgifter for de virksomhetene som blir underlagt loven. Samtidig påpeker departementet at de nye kravene vil kunne spare så vel den enkelte virksomhet som samfunnet som helhet, for kostbare konsekvenser som følge av alvorlige sikkerhetsbrudd.

KS' merknad:

KS mener at en forsvarlig gjennomføring av kravene i ny sikkerhetslov med forskrifter, er av stor betydning for samfunnssikkerhet, bevaring av demokratiet, utvikling av digitale løsninger og innbyggernes sikkerhet og velferd. Det vil derfor være av stor betydning at kommunal sektor tilføres nødvendige midler over statsbudsjettet slik at de har økonomisk mulighet til å oppfylle kravene. I motsatt fall vil manglende implementering kunne undergrave prosessen med å sikre infrastruktur og informasjonssystemer. Dette som følge av at kontaminering i et system/en del av en infrastruktur, vil kunne kontaminere andre informasjonssystemer/andre deler av infrastrukturen uavhengig av forvaltningsnivå.

På samme måte er det viktig at NSM og andre som er ansvarlig for veiledere, instrukser og generell veiledning og kontroll, tilføres tilstrekkelige midler slik at virksomhetene får den bistanden de trenger for å kunne gjennomføre kravene i loven på en god måte.

Til utkast til forskrift om myndighetens roller og ansvar for nasjonal sikkerhet

Generelle høringsinnspill til «Utkast til forskrift om myndighetens roller og ansvar for nasjonal sikkerhet» (myndighetsforskriften)

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Departementet vil vurdere hvorvidt bestemmelsene i forskrift om myndighetenes roller og ansvar for nasjonal sikkerhet (myndighetsforskriften), isteden skal fremgå av en egen instruks for departementene og etatene, og hvorvidt noen av bestemmelsene skal flyttes til virksomhets- eller klareringsforskriften.

KS' merknad:

KS mener det er hensiktsmessig at de tre foreslåtte forskriftene samles i en forskrift.

Når det gjelder spørsmålet om deler av bestemmelsene i myndighetsforskriften isteden skal fremgå av en instruks, bør det gjøres en avveining mellom hensynet til at regelverksarbeider skal underlegges en demokratisk prosess og behovet for rask oppdatering av krav på dette området som følge av den raske utviklingen i trusselbildet. KS mener derfor at de mer sentrale punktene i forskriften bør være i forskrifts form. Samtidig kan det være hensiktsmessig av de deler av regelverket som kan trenge hurtige endringer som følge av endringer i trusselbildet gis som instruks.

Dersom departementet konkluderer med regulering gjennom instruks, er det viktig at de generelle reglene for å sikre IKT sikkerhet samles i en og samme instruks. Dette for å sikre like og helhetlige regler i alle sektorer, så langt som overhode mulig. Dette er særlig av betydning for kommunal sektor, som har oppgaver og plikter innenfor de aller fleste sektorene som er underlagt forskjellige departement.

Kapittel 1. Departementenes roller og oppgaver

Nedenfor følger KS' innspill: på aktuelle bestemmelser som departementet har bedt om høringsinstansenes syn på, samt ytterligere noen bestemmelser som KS finner grunn til å gi innspill på.

Høringsinnspill til pkt. 6.1.1 - § 1 Klassifisering av skjermingsverdige objekter og infrastruktur

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Departementet ber om høringsinstansenes syn på om de foreslåtte kriterier i myndighetsforskriften, jf. virksomhetsforskriften er tilstrekkelige for at departementene skal kunne beslutte et klassifiseringsnivå etter

sikkerhetsloven § 7-1.

Det fremgår av forslaget til myndighetsforskrift at det «*skal de legge vekt på i hvor stor grad grunnleggende nasjonale funksjoner er avhengig av objektet eller infrastrukturen virksomhetens skadevurdering, jf. virksomhetsforskriften § 52»*

Det fremkommer av utkastet til virksomhetsforskrift § 52, at virksomheten i vurderingen av kritikalitet skal legge vekt på:

- *hvilke konsekvenser det vil få for grunnleggende nasjonale funksjoner dersom objektets eller infrastrukturens funksjon faller bort eller reduseres*
- *hvor lenge objektet eller infrastrukturen kan være satt ut av funksjon før det får betydning for grunnleggende nasjonale funksjoner*
- *i hvilken grad objektets eller infrastrukturens funksjon kan gjenopprettes eller erstattes*
- *hvilken grad rettstridig overtakelse av objektet- eller infrastrukturen kan påvirke befolkningens grunnleggende sikkerhet.*

KS' merknad:

KS stiller spørsmål til om såpass åpne kriterier vil kunne medføre store ulikheter i de ulike departementenes klassifisering, jf. innspillene over til kap. 3.1 i høringsnotatet. Det er mulig departementene har behov for mer detaljerte kriterier for å kunne gjennomføre en god og forsvarlig klassifisering. Samtidig bør det tas hensyn til at for mye detaljering raskt vil kunne bli «foreldet».

KS ber derfor departementet vurdere om det bør åpnes for at NSM gir nærmere instrukser og veiledere på dette området. Særlig i forhold til skjermingsverdig infrastruktur, vil det være NSM som er den nærmest til å se det totale risikobildet og derigjennom ha forutsetninger for å bistå departementene på en god måte for å sikre helhetlige prosesser og løsninger. En slik fremgangsmåte vil trolig også sikre at NSMs kompetanse kan videreføres til departementene og virksomhetene på en effektiv måte.

Kapittel 3. Nasjonal responsfunksjon og nasjonalt varslingssystem for digital infrastruktur

Høringsinnspill til pkt. 6.3.1 - § 12 Utøvelse av nasjonal responsfunksjon for alvorlige digitale angrep og nasjonalt varslingssystem for digital infrastruktur

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

NSM skal drive responsfunksjonen og varslingssystemet for digital infrastruktur (VDI). I dag skjer tilknytning til VDI etter avtale. Ettersom det er et klart behov for bedre VDI dekning for å gi en bedre oversikt over digitale angrep mot sentrale virksomheter, vurderer departementet at NSM skal gis mulighet til å pålegge VDI tilknytning for de virksomhetene som blir underlagt loven. Departementet ber om høringsinstansenes syn på en slik påleggskompetanse, og eventuelt hvilke rammer en slik påleggskompetanse bør ha.

KS' merknad:

KS anser at det for å sikre komplekse infrastruktur som f.eks. involverer så vel statlige organer som kommuner og fylkeskommuner, vil være ønskelig at NSM gis myndighet til å pålegge bruk av VDI. Se for øvrig innspill under «Høringsinnspill til pkt. 7.9.2 - § 56 Tilknytning til varslingssystemet for digital infrastruktur».

Kapittel 4. Tilsyn

Generelle høringsinnspill til pkt. 6.4 - Kapittel 4 – «Tilsyn»

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Til kapittelet om tilsyn, bemerker departementet at flere av disse bestemmelsene snarere kan gis gjennom instruks fremfor forskrift. Departementene ber høringsinstansene om deres synspunkter på innholdet i bestemmelsene og ønsker også synspunkter på om det er noe av dette som bør stå i forskrift av hensyn til forutberegnelighet for de som blir gjenstand for tilsyn.

Forskriftens forslag til regler om tilsyn, overlater langt på vei til NSM og andre myndigheter som gis tilsynsmyndighet å regulere ansvarfordelingen seg imellom i avtale.

KS' merknad:

Som påpekt av departementet antas det at hensynet til forutberegnelighet for virksomhetene som blir underlagt tilsyn, tilsier at bestemmelsen om tilsyn bør stå i forskriften.

KS ber departementet vurdere om det er hensiktsmessig at ansvarfordelingen mellom NSM og andre tilsynsmyndigheter i så stor grad bare skal skje gjennom avtale. KS stiller spørsmål ved om en slik fremgangsmåte gir tilstrekkelig sikkerhet for at ansvar faktisk blir entydig fordelt.

I de samarbeidsprosjektene og tiltakene på tvers av statlig og kommunal sektor som KS kjenner til, er ansvarsfordeling ikke i tilstrekkelig grad tydeliggjort mellom forvaltningsnivåene. Dette vil f.eks. kunne innebære at «ingen» sitter med det samlede ansvaret for totalrisikoen for den komplekse infrastrukturen som prosjektet eller tiltaket leverer. KS frykter en tilsvarende ansvarspulverisering kan bli et resultat av den forslåtte regulering av ansvarsforhold på tilsynsområdet.

Kapittel 5. Andre bestemmelser

Høringsinnspill til pkt. 6.5.1 - § 20 Melding om erverv av kvalifisert eierandel i virksomhet underlagt sikkerhetsloven

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Departementet har ikke sett det hensiktsmessig å regulere nærmere hvordan den konkrete vurderingen om stans av erverv skal gjøres, herunder hvilke momenter som skal vektlegges i vurderingen, da bestemmelsen regulerer svært ulike typetilfeller. Departementet viser til momentene i merknaden til § 10-3, og vil bemerker at utgangspunktet for vurderingen vil være størrelsen på det økonomiske tapet for virksomheten, og i hvilken grad stans av ervervet vil ha negative konsekvenser for norske næringsinteresser, holdt opp mot den risiko ervervet innebærer for nasjonale sikkerhetsinteresser.

KS' merknad:

KS har ingen innsigelser til § 20 når det gjelder hva som skal inngå i meldingen om erverv av kvalifisert eierandel, dvs. erverv av andel e.l. som innebærer kontroll (evt. negativ kontroll) over selskapet.

KS påpeker likevel at det er behov for nærmere regulering av hvordan virksomhetene som er underlagt loven skal forhold seg til beslutning om stans av erverv i praksis, herunder hvordan virksomhetene skal forholde seg hvis det gjennomføres et erverv i strid med pålegget.

Til utkast til forskrift om virksomhetens arbeid med forebyggende

sikkerhet

Høringsinnspill til pkt. 7.1.1 - Forsvarlig sikkerhetsnivå

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Virksomheten skal *vurdere risiko* knyttet til oppnåelsen av sikkerhetsmålene. Med grunnlag i vurderingen av risiko skal virksomheten *håndtere risiko*. Dette kan skje i form av å vurdere passende sikkerhetstiltak og fastsette hvilke sikkerhetstiltak som skal benyttes, samt iverksette og evaluere tiltakene.

På mange andre områder er det imidlertid ikke gitt slike konkrete krav. Det er derfor nødvendig at virksomhetene som råder over de skjermingsverdige verdiene, konkretiserer hva som anses forsvarlig for sine verdier.

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

KS' merknad:

KS er enige i at det ikke er hensiktsmessig å detaljregulere hva som er nødvendige tiltak for å oppnå sikkerhetstiltakene i lov eller forskrift.

Samtidig ser KS et behov for at f.eks. NSM utarbeider fortløpende konkrete veiledere som oppdateres forløpende ut fra endringer i risikobilde, teknologi m.m. Slike veiledere kan med hell deles i to deler, dels generelle krav til tiltak på hvert enkelt risikonivå og dels mer bransjespesifikke krav der det er særlig behov for dette.

En slik ordning vil kunne redusere mangelfull sikring som følge av manglende kompetanse, redusert risiko for kontaminering fra et system /en infrastruktur til et / en annen, vil åpne for en større grad av standardisering og vil kunne være nyttige verktøy i en anskaffelsesprosess. En slik standardisering vil også gjøre det lettere for leverandørene å tilpasse seg regelverket. Dette vil igjen medføre reduserte kostnader for virksomhetene som anskaffer infrastruktur og informasjonssystemer.

Kapittel 1. Sikkerhetsstyring

Høringsinnspill til pkt. 7.2.1 - § 1 Definisjoner

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Departementet ber om høringsinstansenes syn på om definisjonene i bestemmelsen er nødvendig, og på om det er andre begreper som bør defineres.

KS' merknad:

KS forslår at det i denne bestemmelsen også henvises til definisjonene i lovens § 1-5. Videre forslås det at følgende andre begreper som benyttes i forskriften også defineres:

- Sikkerhetstruende virksomhet
- Sårbarheter
- Avhengigheter
- Sikkerhetsmål
- Grunnsikringstiltak
- Påbyggingstiltak
- Tiltak for skadebegrensning
- Tiltak for gjenopprettelse

- Lagringsmedier

Høringsinnspill til pkt. 7.2.2 - § 2 Styringssystem for sikkerhet

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Forskriften stiller krav til at virksomheten skal ha et styringssystem for sikkerhet, uten at det stilles nærmere krav til hva et slikt system skal inneholde.

KS' merknad:

KS er enige i at innholdet i et styringssystem ikke defineres i forskriften. Det stilles dog spørsmål til om det bør stilles noen minimumskrav til hva som bør inngå i styringssystemet, utover det som foreløpig fremkommer av forskriftenes § 2, alternativt om det bør stilles krav til bruk av anerkjente standarder for slike styringssystemer.

Høringsinnspill til pkt. 7.2.7 - § 7 Tiltak ved sikkerhetstruende virksomhet, avvik og kompromittering av sikkerhetsgradert informasjon

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Begrepet «sikkerhetstruende virksomhet» benyttes gjennomgående i forskriften. Begrepet er definert i loven som «tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser», jf. § 1-5 nr. 4. Departementet har vurdert om det skal benyttes et annet begrep av pedagogiske årsaker, men har foreløpig funnet det mest hensiktsmessig å benytte samme begrep som i loven. Departementet ber om høringsinstansenes syn på bruken av begrepet «sikkerhetstruende virksomhet».

KS' merknad:

KS opplever at det er hensiktsmessig å gjenbruke begrepet, men stilles spørsmål til om begrepet, ut fra pedagogiske hensyn, bør defineres også i forskriften evt. om forskriften bør henvises til definisjonen i loven.

Kapittel 2. Generelle krav til beskyttelse av skjermingsverdige verdier

Høringsinnspill til pkt. 7.3.1 – § 11 Plikt til å håndtere risiko

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Det fremkommer av bestemmelsen at:

«*Virksomheten skal minst årlig vurdere behovet for å gjennomføre en ny helhetlig vurdering av risiko» Dersom endringer planlegges, gjennomføres eller inntreffer, skal virksomheten vurdere hvilken risiko endringene medfører.*

KS' merknad:

KS foreslår at forskriften bør suppleres med et krav til at en slik vurdering også må gjøres ved endringer i det eksterne trusselbildet.

Høringsinnspill til pkt. 7.3.2 - § 12 Plikt til å håndtere risiko

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Bestemmelsen pålegger virksomhetene å håndtere risiko for å oppnå et forsvarlig sikkerhetsnivå.

Bestemmelsen henviser til øvrige bestemmelser i forskriften som stiller krav til risikohåndtering; § 20 (skjermingsverdig informasjon) og § 32 (gradert informasjon), og § 45 og § 53 (konfidensialitet, integritet og tilgjengelighet for henholdsvis informasjonssystemer og infrastruktur).

Det påpekes at det sentrale er ikke er *på hvilken måte* risiko håndteres, men *at* den håndteres på en slik måte at virksomheten oppnår et forsvarlig sikkerhetsnivå. Departementet ber om høringsinstansenes syn på denne innretningen.

KS' merknad:

KS oppfatter det som hensiktsmessig at ansvaret for risikohåndtering entydig legges på virksomheten og hva dette innebærer for de forskjellige kategoriene skjermingsverdige verdier som vernes av loven beskrives nærmere i tilknytning til reguleringen av den enkelte kategori.

Kapittel 3. Beskyttelse av skjermingsverdig informasjon og Kapittel 4. Sikkerhetsgradering og merking

KS har ingen ytterligere innspill til de enkelte bestemmelser i disse kapitlene.

Kapittel 5. Beskyttelse av informasjon gradert KONFIDENSIELT eller høyere

Høringsinnspill til pkt. 7.6.8 - § 38 Beskyttet sone

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Bestemmelsen gir føringer for opprettelse av beskyttet sone og kontroll med tilgang til slike soner. Departementet har ikke foreslått nærmere regulering av godkjenning av oppbevaringsenheter. Det vil være opp til NSM hvilke krav som skal stilles til oppbevaringsenheter som skal godkjennes for oppbevaring av informasjon på de forskjellige graderingsnivåene. Departementene ber om høringsinstansenes innspill på om dette er en hensiktsmessig innretning, og hvorvidt det finnes anerkjente standarder eller metoder som bør ligge til grunn for godkjenning av oppbevaringsenheter.

KS' merknad:

KS opplever at bestemmelsen i begrenset grad tar hensyn til hvordan dokumentasjon i dag skapes og lagres. Det meste av dokumentasjon skapes og arkiveres elektronisk. F.eks. skapes papirdokumenter normalt gjennom bruk av PC og printer. Slik denne bestemmelsen er foreslått, stilles det ikke noen krav eller føringer til hvordan elektronisk dokumentfremstilling- og lagring skal håndteres, herunder om det kan være behov for endringer i NOARK standarden. KS kan heller ikke se spor av moderne sikkerhetsarkitektur og lite spor av moderne informasjonsteknologi.

Kapittel 6. Beskyttelse av skjermingsverdige informasjonssystemer og Kapittel 7. Beskyttelse av skjermingsverdig objekter og infrastruktur

KS har ingen ytterligere innspill til de enkelte bestemmelser i disse kapitlene.

Kapittel 8. Nasjonalt varslingssystem for digital infrastruktur

Høringsinnspill til pkt. 7.9.2 - § 56 Tilknytning til varslingssystemet for digital

infrastruktur

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Varslingssystem for digital infrastruktur er opprettet for å ivareta nasjonale sikkerhetsinteresser. Varslingssystemets primærfunksjon er ikke å håndtere virksomhetens risiko, men å detektere og varsle om alvorlige hendelser som kan ha betydning for nasjonale sikkerhetsinteresser. Gjennom dette vil NSM imidlertid også varsle virksomheten om hendelser av betydning for virksomhetens risiko.

Bestemmelsen er en videreføring av dagens system med frivillig tilknytning til varslingssystemet for digital infrastruktur (VDI/NorCERT). Departementet ser imidlertid nærmere på muligheten for NSM til å kunne pålegge tilknytning til VDI. Slik departementet ser det bør alle virksomheter som underlegges loven være tilknyttet VDI, for å gi best mulig oversikt over digitale angrep mot virksomheter som er underlagt loven. Departementet ber om høringsinstansenes syn på en slik påleggskompetanse, og eventuelt hvilke rammer en slik påleggskompetanse bør ha.

KS' merknad:

KS opplever at dagens komplekse infrastrukturer medfører et økt behov for varslingssystemer for digital infrastruktur. Kommuner og fylkeskommuner har et bredt tjenestespekter og tilknyttes offentlige infrastrukturer som f.eks. Norsk Helsenett. Mange av disse infrastrukturene er igjen koblet sammen med infrastrukturer etablert av store internasjonale leverandører.

De komplekse digitale infrastrukturene medfører risiko for at kontaminering i en del av infrastrukturen, kan medføre kontaminering av hele infrastrukturen. Departementets forslag om at NSM gis hjemmel til å pålegge tilknytning til VDI, må på denne bakgrunn være et godt initiativ for å øke sikkerheten.

KS ser også behovet for at det for infrastrukturer som blir pålagt tilslutning til VDI, etableres mekanismer som sikrer at tilknytning av nye systemer eller sammenkobling mot andre infrastrukturer, underlegges kontroll/godkjenningsprosedyrer. Herunder at NSM oppstiller relevante minstekrav for slik tilslutning.

Når det gjelder avtalen som skal inngås mellom NSM, virksomheten og evt. sektorspesifikke hendelseshåndteringssystem, anbefales det å benytte standardiserte avtaler hvor det stilles tilnærmet like krav til prosedyrer, behandling av personopplysninger, taushetsbelagt informasjon og gradert informasjon, varsling m.m.

Det bør også settes minimumskrav til hva som skal inngå i sikkerhetsavtaler og databehandleravtaler med leverandørene. Kravene bør så langt mulig være sektornøytrale.

En slik standardisering vil bidra til økt informasjonssikkerhet og til å lette virksomhetenes forhandlinger med leverandørene. Standardiseringen vil også kunne gjøre det enklere for leverandørene å tilpasse seg kravene som stilles.

Kapittel 9. Personellsikkerhet og Kapittel 10. Sikkerhetsgraderte anskaffelser

KS har ingen innspill til bestemmelsene i dette kapitlet.

Kapittel 11. Avsluttende bestemmelser

Høringsinnspill til pkt. 7.11.10 Til § 80 Overgangsregler

Oppsummering av forslaget i høringsnotatet/departementets bemerkninger:

Bestemmelsen gir overgangsregler i for dem som har vært omfattet at den gamle loven.

KS' merknad:

KS vil påpeke behovet for at det også inntas overgangsregler for nye virksomheter som blir omfattet av loven. Dette gjelder både virksomheter som blir omfattet av loven som følge av den pågående kartlegging av hvilke virksomheter som nå skal underlegges loven og enkeltvirksomheter som i fremtiden blir lagt inn under loven.

Det er viktig at fristene i overgangsreglene gir virksomhetene en reell mulighet til å oppfylle kravene på en forsvarlig måte. Det er også viktig at det sikres at virksomhetene som blir underlagt loven, tilføres nødvendige midler for å kunne gjennomføre nødvendige endringer. Dette gjelder særlig der fristene for å gjennomføre lovens krav, som følge av raske endringer i risikobildet, blir svært korte.

Det vises også til hva som er sagt ovenfor under «Høringsinnspill til pkt. 4.7 - Ikrafttredelse»

Til utkast til forskrift om klarering av leverandører og personell

KS har ingen innspill til de enkelte bestemmelser i dette utkastet.

Med hilsen

Kristin Weidemann Wieland

Områdedirektør

Line Richardse

Avdelingsdirektør

Vedlegg: -