**Fra:** Odd.Gronvold@kmd.dep.no
**Sendt:** 17.01.2017 12:31:24
**Til:** Postmottak FD
**Kopi:**

**Emne:** 16/4892-7 NOU 2016:19 Samhandling for sikkerhet - høringssvar
**Vedlegg:**

Forsvarsdepartementet
Postboks 8126 Dep
0032 OSLO

**NOU**
**2016:19**

| Deres ref | Vår ref | Dato |
|---|---|---|
| 2015/3139-7/FD V 3/MAY | 16/4892-7 | 17.01.2017 |

**Samhandling for sikkerhet - høringssvar -**

Vi viser til brev 17.10.2016 med vedlagt NOU.

***Innledning***

Utvalgets mandat har vært å vurdere hva som bør reguleres i lov for å sikre nasjonal sikkerhet. Formålet med nytt lovgrunnlag skal være å beskytte kritisk infrastruktur, kritiske samfunnsfunksjoner og sensitiv informasjon mot tilsiktede, uønskede hendelser. Utvalget skal sikre et helhetlig forebyggende lovgrunnlag innen både den militære og sivile sektoren, som er relevant og robust med hensyn til dagens og fremtidens risiko- og trusselbilde. Forslaget skal sikre en kostnadseffektiv regulering, som sikrer balanse mellom akseptabel restrisiko og kostnaden for sikkerhetsnivået. Samfunnsøkonomisk lønnsomhet skal være en grunnleggende forutsetning, det vil si at aktuelle sikringstiltak må ha en samfunnsøkonomisk nytte som samlet overstiger kostnadene.

Med bakgrunn i utvalgets mandat, og utvalgets vurderinger i denne sammenheng, mener KMD at enkelte punkter i rapporten burde vært mer presisert. Dette gjelder spesielt lovens virkeområde – og hvilke virksomheter som skal omfattes av denne. Vi har også noen synspunkter på den tematiske gjennomgangen av informasjonssikkerhet (Kap. 8), og utvalgets vurderinger i denne sammenheng.

***Lovens formål og virkeområde***

- ***6.7.1. Ulike alternativer for lovens formål og virkeområde***

I mandatet fremgår det at formålet med nytt lovgrunnlag skal være å beskytte kritisk infrastruktur, kritiske samfunnsfunksjoner og sensitiv informasjon mot tilsiktede, uønskede hendelser. Etter KMDs vurdering burde også loven komme til anvendelse ved behov for sikring av kritisk samfunnsinfrastruktur mot utilsiktede hendelser som kan føre til langvarig utfall. Konsekvensen vil – uansett årsak – være utfall av viktig funksjon.

- *Side 113, 2. kolonne, 2. avsnitt:*

Utvalget mener at lovens virkeområde bør innrettes slik at enhver virksomhet, offentlig eller privat, *som har råderett over informasjon, informasjonssystemer, objekter eller infrastruktur, eller som driver aktivitet, som er av kritisk betydning for grunnleggende nasjonale funksjoner*, omfattes av loven.

Utvalget erkjenner at deres forslag til innretning av lovens formål og virkeområde sannsynligvis vil medføre at flere virksomheter vil bli underlagt den nye loven. Videre at det også er vanskelig å vurdere konkret hvor mange virksomheter som vil bli underlagt loven.

KMD mener at utvalgets forslag til presisering av lovens virkeområde er for vid og upresis med tanke på å skape en forutsigbarhet for hvilke sektorer, virksomheter, eller funksjoner som skal omfattes av sikkerhetsloven. Dette er spesielt viktig mht. departementenes arbeid med å identifisere hva som faller inn under begrepet *grunnleggende nasjonale funksjoner* innenfor eget myndighetsområde, samt hvilke virksomheter som skal ha en kritisk rolle i understøttelsen av slike funksjoner.

En nærmere presisering av lovens virkeområde vil også bidra til at det blir et mindre behov for å avklare uenigheter mellom sikkerhetsmyndighetene og relevante sektormyndigheter (ref. forslaget om opprettelsen av et tvisteorgan).

***Ansvars- og myndighetsfordelingen***

- *Side 139, 2. kolonne, 2. avsnitt.*

En av hovedoppgavene for Sikkerhetsmyndigheten skal i henhold til utvalgets forslag, være å gi informasjon, råd og veiledning til virksomheter underlagt loven. Utvalget mener her at konkret rådgivning overfor de enkelte virksomhetene bør være en helt sentral oppgave for Sikkerhetsmyndigheten innenfor alle de fagområder loven spenner over. En slik løsning vil forutsette at Sikkerhetsmyndighetens kapasitet til å gi råd til virksomheter, dimensjoneres slik at virksomheter kan få rettidige og gode råd i sitt arbeid med forebyggende sikkerhet etter loven.

Dersom Sikkerhetsmyndigheten skal tildeles en mer aktiv rolle mht. å gi informasjon, råd og veiledning til virksomheter underlagt loven, mener KMD at det er viktig at også ressurstilfanget til Sikkerhetsmyndigheten økes tilsvarende. Videre er det viktig at Sikkerhetsmyndigheten har tilstrekkelig faglig kompetanse til å kunne gi <u>*helhetlige*</u> råd og veiledninger til virksomhetene om f.eks. konsekvensene ved å implementere sikkerhetstiltak eller -løsninger som styrker konfidensialiteten i virksomheten. I en digital sammenheng blir det viktig at Sikkerhetsmyndigheten også opplyser virksomheten om evt. konsekvenser av iverksetting av tiltaket, herunder muligheten for redusert tilgjengelighet (eller brukervennlighet) som følge av implementering av tiltaket. Sikkerhetsmyndigheten bør også kunne gi råd og veiledning om avveining av ulike hensyn (konfidensialitet, integritet, tilgjengelighet) ved anbefalinger og ev. pålegg om å iverksette konkrete IKT-sikkerhetstiltak.

- *7.7.7 Tvisteorgan*

Utvalget foreslår etablering av et tvisteorgan som kan ta stilling til klager fra virksomheter som blir underlagt loven ved enkeltvedtak, og til klager fra Sikkerhetsmyndigheten på departementenes etterlevelse av loven. Konkret forslår utvalget at Kongen gis myndighet til å peke ut et kollegialt organ med fem medlemmer. Ved oppnevningen av medlemmer foreslår utvalget at det i tillegg til sikkerhetsfaglig kompetanse, skal legges vekt på kompetanse innen personvern og selvstendige rettssubjekters rettssikkerhet.

KMD mener at sammensetningen av tvisteorganet også må kunne ivareta interessene til den eller de virksomhetene som er berørt av enkeltvedtaket på en god måte. Det antas her at tvister i stor grad vil omhandle private virksomheter. Følgelig bør disse virksomhetens interesser bli ivaretatt i tvisteorganet på en hensiktsmessig måte. Vi ser frem til nærmere drøfting av dette.

***Informasjonssikkerhet***

- *Side 168, 1. kolonne. 1. avsnitt.*

Utvalget har ikke funnet grunn til å endre kriteriene for angivelse av hvilken informasjon som skal beskyttes etter sikkerhetsloven. Utvalget mener at det fortsatt bør være behov for å sikre informasjonens konfidensialitet, som er inngangskriteriet for om informasjonen skal sikkerhetsgraderes, og dermed beskyttes etter sikkerhetsloven. Etter utvalgets syn ville det unødig komplisere identifiseringen av informasjon som skal beskyttes, dersom integritet og tilgjengelighet skulle vært ytterligere inngangskriterier. Sett i sammenheng med digitaliseringen og at viktige ugraderte informasjonssystemer skal beskyttes, legger utvalget til grunn at mye viktig ugradert informasjon fanges opp og beskyttes gjennom bestemmelsene om informasjonssystemsikkerhet.

Med bakgrunn i den raske teknologiske utviklingen i samfunnet, mener KMD at utvalget burde hatt en mer balansert tilnærming til hvordan informasjonen skal beskyttes etter sikkerhetsloven. Vi er enig i at det er viktig å beskytte

informasjonens konfidensialitet, men i et samfunn der tilnærmelsesvis alt blir digitalisert, vil også betydningen av å beskytte informasjonens tilgjengelighet og integritet øke tilsvarende. Balansen mellom de tre sikkerhetsaspektene (konfidensialitet, tilgjengelighet og integritet) må ivaretas på en slik måte at beskyttelsen av de *funksjonene* som behandler informasjonen er så god som mulig. Dette er helt avgjørende for å ivareta de verdiene som sikkerhetsloven skal hegne om.

- *Kap 8.6.3 og 8.6.4 vedr. beskyttelse av informasjonssystemer og infrastruktur.*

Utvalget foreslår en videreføring av de fleste av dagens lovbestemmelser om sikkerhetstiltak. Sikkerhetsmessig godkjenning, monitorering, inntrengningstesting, sikkerhetsmessig overvåkning og tekniske sikkerhetsundersøkelser foreslås videreført. Kryptosikkerhet foreslås derimot ikke videreført i loven. Utvalget skriver at de oppfatter det slik at kryptosikkerhet omfatter spesifikke sikkerhetstiltak som ikke må reguleres i lov, og at de derfor foreslår at hele reguleringen flyttes til forskrift.

En videreføring av de ovennevnte sikkerhetstiltak forutsetter – i et fremtidig gjennomdigitalisert samfunn – at Sikkerhetsmyndigheten blir tilført ressurser for å kunne tilby den nødvendige veiledning, og for å utvikle og vedlikeholde de tekniske tjenestene. KMD mener at utvalget i denne sammenheng i større grad burde vurdert økt bruk av sikkerhetsgodkjente aktører i markedet for å avlaste Sikkerhetsmyndigheten på dette viktige, men svært ressurskrevende, sikkerhetsområdet.

KMD er enig med utvalgets vurdering at reguleringen av kryptosikkerheten kan flyttes til forskrift.

***Personvern***

I lovutkastet kapittel 4 finnes generelle krav til forebyggende sikkerhet. I § 4-7 omtales behandling av personopplysninger. Det heter i bestemmelsen at behandling av personopplysninger skal følge prinsippene i EUs personvernforordning, EU 2016/679 vedtatt 27. april 2016 artikkel 5 jf. artikkel 23. For ordens skyld gjør vi oppmerksom på at forordningen skal gjennomføres i norsk rett.

Virksomheter underlagt sikkerhetsloven er i dag også underlagt personopplysningsloven. Det er gjort unntak fra deler av personopplysningsloven av hensyn til rikets sikkerhet. Som utvalget selv peker på i utredningen pkt. 7.7.9, er det foreløpig ikke noe som tyder på at et nytt norsk personvernregelverk basert på forordningen ikke vil få generell anvendelse. Dette i motsetning til forordningen, som blant annet ikke får anvendelse på behandling av personopplysninger for ivaretakelse av nasjonal sikkerhet og forsvar.

Dersom forordningen gjennomføres slik at den gjelder helt generelt for behandling av personopplysninger i Norge, vil det ev. måtte vurderes unntak for behandling av personopplysninger i samsvar med sikkerhetsloven. Etter vår vurdering vil en bestemmelse som den foreslått i utkastet til ny sikkerhetslov § 4-7, som viser til at behandling av personopplysninger skal følge *prinsippene* i EUs personvernforordning, således kunne bli forvirrende og i verst fall direkte misvisende. Dette bør det tas hensyn til i det videre arbeidet med ny sikkerhetslov. Det må blant annet få konsekvenser for behandling av personopplysninger som ledd i personkontroll, jf. for eksempel § 8-7, 7. ledd.

Med hilsen

Hanne Finstad (e.f.)
avdelingsdirektør

Odd Grønvold
fagdirektør

*Dette dokumentet er elektronisk godkjent og sendes uten signatur.*