FORSVARSDEPARTEMENTET
SAKNR.: 13/00552-312
24 AUG 2015
ARKBET: 251.0 - Bok
KASSERES 5 ÅR
KASSERES 30 ÅR
BEVARES

Nasjonal sikkerhetsmyndighet

Vår saksbehandler
Avdeling for Plan og strategi

Vår dato
2015-08-19

Vår referanse
A03 - S:15/02101-7

Deres dato

Deres referanse

Antall vedlegg

Side
1 av 6

Til
Forsvarsdepartementet
Postboks 8126 Dep
0032 Oslo

Endringer i sikkerhetsloven - høringssvar NSM

Nasjonal sikkerhetsmyndighet (NSM) viser til Forsvarsdepartementets (FD) høring av forslag til endringer i lov 20. mars 1998 nr. 10 om forebyggende sikkerhet (sikkerhetsloven).

NSM har siden evalueringen av sikkerhetsloven i 2012 deltatt i arbeidet som har hatt som intensjon å ta frem en ny, mer tilpasset og dynamisk lovgivning for forbyggende sikkerhet som er i tråd med den teknologiske utviklingen generelt, og innen forebyggende sikkerhet spesielt.

I forbindelse med denne prosessen som har vært ledet av FD, har NSM i flere anledninger levert til dels omfattende innspill og forslag i arbeidet. NSM er tilfreds med at departementets forslag til lovendringer er i tråd med flere av NSMs innspill til prosessen. NSM forutsetter at andre innspill og leveranser i denne forbindelse følges opp som ledd i det mer omfattende utredningsarbeid som skal lede frem mot et nytt lovgrunnlag for forebyggende nasjonal sikkerhet.

NSM har gjennomgått departementets forslag og ønsker å komme med følgende bemerkninger til de foreslåtte endringene.

1 Merknader til de enkelte forslag

1.1 Til § 2 - Lovens generelle virkeområde

1.1.1 Lovfesting av praksisen om at regjeringsmedlemmer er unntatt plikt til autorisering og sikkerhetsklarering

NSM har ingen innvendinger til departementets forslag om endring i § 2 sjette ledd om at sikkerhetslovens kapittel 6 ikke gjelder for regjeringens medlemmer. Det er allerede sedvane for at regjeringsmedlemmene i utgangspunktet ikke må ha sikkerhetsklarering. Unntaket er der utenlandske myndigheter krever slik klarering, eksempelvis i forbindelse med større anskaffelser av våpen, våpensystemer eller annet omfattende forsvars- og sikkerhetssamarbeid. NSM er enig med departementet at slike unntak kan håndteres særskilt ved behov.

Postadresse
Postboks 814
1306 SANDVIKA

Sivil telefon/telefaks
+47 67 86 40 00/+47 67 86 40 09
E-postadresse
post@nsm.stat.no

Militær telefon/telefaks
515 40 00/515 40 09
Internetadresse (URL)
www.nsm.stat.no

NSM vil imidlertid understreke at det er viktig å sikre at personell som gis tilgang til sikkerhetsgradert informasjon uten å være autorisert/klarert gis opplæring om hvordan de skal forholde seg til sikkerhetsgradert informasjon (oppbevaring, journalføring, forsendelse mv.). Uten sikkerhetsklarering og uten autorisasjonssamtale er det ikke selvsagt at man kjenner til dette.

1.1.2 Sikkerhetslovens anvendelse dersom virksomheten har kritisk infrastruktur som er omfattet av forslag til ny § 29 a

Etter NSMs erfaring benyttes enkeltvedtaksmekanismen i dagens § 2 tredje ledd i meget begrenset utstrekning.

Det er etter hvert svært mange private foretak som forvalter kritisk infrastruktur, som er omfattet av sivilt beredskapssystem eller kan ha behov for tilgang til sikkerhetsgradert informasjon av andre grunner. Bare et fåtall av disse er det fattet vedtak om at sikkerhetsloven skal gjelde for. Det er viktig å presisere at dette vil kunne få store konsekvenser for den nasjonale krisehåndteringsevnen. I dagens samfunn ivaretas en rekke samfunnskritiske funksjoner av private rettssubjekter. En privat virksomhet kan derfor ha en viktig rolle/funksjon i en beredskapsmessig sammenheng, uavhengig av om den eier et kritisk objekt eller ikke. Utøvelsen av denne funksjonen vil kunne bli vanskeliggjort/umulig dersom virksomheten ikke kan få tilgang til sikkerhetsgradert trussel- og sårbarhetsinformasjon.

Etter vår oppfatning må det være behovet for nasjonal sikkerhet som er styrende for hvem som omfattes av sikkerhetsloven, ikke om virksomheten er offentlig eller privat. Det medfører store sårbarheter at organisasjonsform er avgjørende for om en virksomhet er underlagt sikkerhetslovens krav.

Vi registrerer at det nå foreslås en ny § 29 a om anskaffelser til kritisk infrastruktur basert på samme ordning med enkeltvedtak. Ovennevnte betenkeligheter gjelder i det alt vesentlige også her. Vi frykter at tilbakeholdenheten med å fatte slike enkeltvedtak vil gjøre at effekten av § 29 a dermed vil bli liten.

1.2 Til ny § 13a – virksomhetenes egne sikkerhetsmessige overvåkning av godkjente informasjonssystemer

NSM støtter departementets forslag. For sikkerhetsgraderte systemer er det riktig å innføre den foreslåtte sikkerhetsovervåkningen. Det er viktig å understreke at godkjente informasjonssystemer behandler informasjon med et høyt beskyttelsesbehov og kun er ment for tjenstlig bruk, og at arbeidsgiver derfor må kunne benytte denne type virkemidler. Flere hendelser, og tilsyn NSM har vært på, har vist at slik sporbarhet er høyst nødvendig for å opprettholde en sikker tilstand på systemene og for å sikre at sikkerhetsgradert informasjon ikke blir kompromittert.

1.2.1 Til ny § 13a første ledd

Av bestemmelsens første ledd fremgår det *«Sikkerhetsrelevante hendelser skal registreres»*. NSM vil kunne operasjonalisere begrepet «sikkerhetsrelevant hendelse» i veilednings form, løpende tilpasset risikobildet.

NSM ser at bestemmelsen slik den er utformet i høringsnotatet kan tolkes ganske vidt. Bestemmelsen må etter vår oppfatning forstås slik at sikkerhetsmessig overvåkning

utelukkende har til formål å overvåke sikkerhetstruende hendelser som utgjør en fare for systemet eller informasjonen i systemet. Dette bør presiseres i bestemmelsen.

NSM foreslår derfor følgende endring i forslag til ny § 13a første ledd:

Den enkelte virksomhet skal kontinuerlig overvåke godkjente informasjonssystem for sikkerhetstruende hendelser ***mot informasjonssystemet eller informasjon i systemet****, fortrinnsvis ved bruk av automatisert systemovervåking. Sikkerhetsrelevante hendelser skal registreres.*

1.3 Til §§ 9 og 10a – Varslingssystem for digital infrastruktur og nasjonal responsfunksjon for alvorlige IKT-baserte hendelser

1.3.1 Til endringer i § 9 – nytt første ledd bokstav e.

NSM støtter departementets forslag om å lovfeste nasjonal responsfunksjon for alvorlige dataangrep mot samfunnskritisk infrastruktur (NorCERT) og nasjonalt varslingssystem for digital infrastruktur (VDI).

Funksjonene VDI og NorCERT har allerede i mange år vært en omfattende del av NSMs oppgaver, og er en viktig brikke i leveranser fra NSM. Oppgavene i denne forbindelse har en nær sammenheng med mange av de øvrige oppgaver som er tillagt den sektorovergripende NSM-funksjonen. Etter nåværende sikkerhetslov § 8 skal NSM koordinere de forebyggende sikkerhetstiltak. I lovens § 9 bokstav a) og e) er dette blant annet utdypet til å omfatte innhenting og vurdering av informasjon av betydning for gjennomføringen av den forebyggende sikkerhetstjeneste og å gi informasjon, råd og veiledning. Det er en stor grad av sammenfall, og mulighet for deling og gjenbruk av både kompetanse, teknologi og informasjon, mellom disse oppgavene og de tverrsektorielle oppgaver som i dag ivaretas gjennom VDI og NorCERT. Som en del av EOS-tjenestene, har NSM også et nasjonalt og internasjonalt samarbeidsnettverk som vesentlig styrker evnen til nasjonal deteksjon og hendelseshåndtering.

NSM mener også at lovfesting vil ytterligere forenkle demokratisk kontroll med virksomheten, ved at rammene for virksomheten blir tydeliggjort i lov. Gjennom lov og forskriftsregulering, vil man få økt åpenhet om de oppgaver som er tillagt NSM og således bidra til økt rettssikkerhet.

1.3.2 Til ny § 10 a

NSM slutter seg til departementets forslag om et styrket hjemmelsgrunnlag for VDI og NorCERT-funksjonens behandling av personopplysninger.

NSM registrerer gjennom VDI systemet store mengder data, i det vesentligste i form av trafikkflytdata og IP-adresser. NSM innhenter ikke bare informasjon gjennom VDI-systemet, men mottar også data fra nasjonale og internasjonale samarbeidspartnere. NSM mottar også informasjon i forbindelse med bistand til virksomheter knyttet til analyse av hendelser. All informasjon danner grunnlag for analyse, og er avgjørende for håndteringen av hendelser og koordineringen i forhold til nasjonale og internasjonale samarbeidspartnere.

Behandling av data er således helt avgjørende for at NSM skal ha mulighet for å ivareta det ansvaret og de oppgavene man er pålagt. Disse dataene kan inneholde personopplysninger av varierende sensitivitet, samt bedriftssensitive opplysninger. NSMs fokus er imidlertid ikke

å innhente eller behandle personopplysninger, men å identifisere ondsinnet kode mv. som måtte være integrert i informasjonen.

For å videreutvikle VDI funksjonen kan det i fremtiden, som en følge av teknologisk utvikling, være behov for å registrere innholdsdata i større utstrekning enn i dag. NSM legger til grunn at lovforslaget vil åpne for dette, og at nærmere reguleringer av rammene for virksomheten i så fall vil bli fastsatt i forskrift.

NSM mener imidlertid at § 10 a bør gis en annen utforming. Bestemmelsen slik den er formulert i høringsnotatet kan oppfattes slik at NSM kun kan behandle personopplysninger i de tilfeller det skjer etter § 9 første ledd e, og underforstått; ikke i andre tilfeller. Det er åpenbart at en slik tolkning ikke skal legges til grunn. Det er en rekke oppgaver i loven for øvrig som forutsetter at det behandles personopplysninger også i andre tilfeller (f.eks. bestemmelsene om personellsikkerhet, monitoring og til dels inntrengingstesting). I tillegg viser departementets begrunnelse i høringsnotatet at paragrafen ikke er ment å begrense andre tilfeller der det behandles personopplysninger, men å gi et tydelig og forutsigbart hjemmelsgrunnlag til å behandle personopplysninger for akkurat oppgavene etter § 9 første ledd e. Dette burde imidlertid i større grad vært gjenspeilet i forslaget til ordlyd i § 10 a. Slik forslaget er nå, fører paragrafen paradoksalt nok til at etableringen av et tydelig hjemmelsgrunnlag for én type oppgave, utilsiktet skaper utydelighet om hjemmelsgrunnlaget for alle andre oppgaver der det er nødvendig å behandle personopplysninger.

NSM foreslår derfor at et av to alternativer benyttes:

Primært anbefaler NSM at bestemmelsen omskrives til å gjelde all behandling av personopplysninger ved at bestemmelsen gis en generell henvisning til § 9, og åpner for at NSM kan behandle personopplysninger der det er nødvendig for å utføre de oppgaver som følger av sikkerhetsloven. Vi kan ikke se at en slik endring vil representere annet enn en kodifisering av gjeldende praksis. Endringen vil imidlertid tydeliggjøre hjemmelsgrunnlaget.

Subsidiært anbefaler NSM at teksten i overskriften og andre ledd i § 10 a gis et snevrere omfang ved å tilføye *«... for oppgaver som følger av § 9»*, eller ved å tilføye et nytt tredje ledd, *«Bestemmelsene i denne paragrafen begrenser ikke behandlingen av personopplysninger der det er nødvendig for å oppfylle andre bestemmelser i loven».*

1.4 Til § 23 – Reduksjon av antall klareringsmyndigheter

NSM støtter departementets forslag om at det opprettes to klareringsmyndigheter, én for forsvarssektoren og én for sivile sektorer, de begrunnelsene som er anført for forslaget, og måten § 23 er utformet for å oppnå dette. Vi støtter også unntaket om at EOS-tjenestene fortsatt skal klarere sitt eget personell. NSM ser at spesielle hensyn gjør seg gjeldende knyttet til klareringer av personell innen disse tjenestene.

NSM støtter departementets forslag om at lovteksten om autorisasjon flyttes til første setning i bestemmelsen. Det vil bidra til å fremheve autorisasjonsinstituttet, herunder at det er autorisasjonsbehovet som normalt er grunnlaget for klareringsbehovet, at det skal gjennomføres autorisasjonssamtaler og at det skal skje på alle graderingsnivåer.

NSM støtter departementets uttalelse i høringsnotatet under punkt 2.4.3 side 22,om at det ideelt sett bør være bare én klareringsmyndighet for Stortinget og organer under Stortinget, og at det samme bør gjelde for domstolene. Forutsetningen for god kvalitet i saksbehandlingen, er at klareringsmyndighetene har et relativt stort tilfang av saker. Små miljø med få saker bør så langt som mulig unngås.

NSM mener at Stortinget kan vurdere om de kan dra nytte av at det nå etableres to klareringsmyndigheter, for eksempel ved at de av eget tiltak lar den sivile klareringsmyndighet forestå førsteinstansbehandling av sine klareringssaker, men selv er klageinstans. En slik ordning bør ivareta de konstitusjonelle hensyn. NSM mener at tilsvarende ordning kan vurderes ved domstolene.

NSM registrerer at det foreslås en adgang til også å etablere andre klareringsmyndigheter. NSM forutsetter at denne bestemmelsen gis en meget snever anvendelse. Omfattende bruk av bestemmelsen vil uthule de gevinster man søker å oppnå gjennom hovedregelen. Små klareringsmyndigheter bør bare etableres der det foreligger meget tungtveiende grunner for dette.

1.5 Til § 28 – varighet av leverandørklarering

NSM støtter departementets forslag om at leverandørklarering bare gis etter anmodning fra en anskaffelsesmyndighet, slik som i dag, og begrunnelsene i høringsnotatet som er anført for dette.

NSM støtter departementets forslag om at Kongen fastsetter en generell gyldighetstid for leverandørklareringer, og de begrunnelser som er anført for dette. At klarering gis for en definert tidsperiode er også i tråd med hva vi oppfatter som en internasjonalt etablert praksis.

1.6 Til ny § 6a – Gebyr

Departementet foreslår at det etableres en lovhjemmel for å kunne kreve gebyr der en virksomhet utfører tjenester for en annen virksomhet i medhold av sikkerhetsloven.

NSMs prinsipielle standpunkt er at statssikkerhet, herunder NSMs ansvar for forbyggende sikkerhet, fullt ut bør være bevilgningsfinansiert. NSM er av den oppfatning at de tjenestene direktoratet utfører, leveres i egenskap av å være Norges nasjonale sikkerhetsmyndighet, og at disse tjenestene primært kommer samfunnet og samfunnssikkerheten til gode.

Gebyr kan få negative sikkerhetsmessige konsekvenser. Ved innføring av gebyr kan det medføre en fare for at innsats og fokus ikke blir på de områder og mot de virksomheter hvor behovet ut fra risiko og en bredere sikkerhetsmessig vurdering er størst, men at betalingsevne og -vilje blir styrende. Finansieringsmodellen for VDI/NorCERT er et eksempel på en slik utvikling.

For det tilfellet at gebyr likevel innføres må det gjennomføres en grundig analyse av hvilke områder som er egnet for dette. Mulige negative konsekvenser for samfunnssikkerheten må gis en fremtredende plass i en slik analyse, og tillegges stor vekt.

1.7 Til ny § 29 a – Anskaffelser til kritisk infrastruktur

NSM støtter departementets forslag om ny lovbestemmelse for anskaffelser til kritisk infrastruktur. Vi mener bestemmelsen, brukt riktig og aktivt, kan gi økt sikkerhet.

En effektiv bestemmelse forutsetter imidlertid at myndighetene som skal avgi rådgivende uttalelse kan innhente nødvendig informasjon for å gjøre de vurderinger som er påkrevd.

Det må sikres at de offentlige organer som skal gi rådgivende uttalelse etter anmodning fra et departement, har de tilstrekkelige hjemler til å innhente all informasjon av betydning for anskaffelsen, herunder informasjon om leverandøren, fra alle relevante kilder og registre i inn

og utland. Hjemmelsgrunnlaget for informasjonsinnhenting bør således tydeliggjøres i bestemmelsen og/eller dens forarbeider.

1.8 Til ny § 5a – Varslingsplikt mv. ved risiko for rikets selvstendighet og andre nasjonale sikkerhetsinteresser

NSM støtter departementets forslag og er enige i departementets vurderinger. I et stadig mer globalisert og nettverksbasert samfunn anser NSM det som svært viktig at norske myndigheter har en mulighet til å stanse, eller endre pågående eller planlagt aktivitet som kan skade rikets sikkerhet og selvstendighet. NSM mener bestemmelsen er hensiktsmessig utformet ved å plassere det overordnede ansvaret hos det enkelte fagdepartementet.

I høringsnotatet punkt 2.8.2 side 36, er det anført at «Departementet legger til grunn at det vil være nødvendig å utforme en veileder eller instruks som forklarer hva varslingsplikten vil innebære...». Det fremgår imidlertid ikke av teksten hvem som skal utforme veilederen, i motsetning til i forslaget til ny § 29a, hvor det eksplisitt er anført at ansvaret er lagt til NSM. Dette bør klargjøres.

2 Økonomiske og administrative konsekvenser

NSM kan ikke se at dokumentets kapittel 3 om økonomiske og administrative konsekvenser berører eventuelle ressurskonsekvenser i NSM som utfører sikkerhetslovens funksjoner på vegne av myndighetene. NSM forutsetter at dette blir fulgt opp i styringsdialogen med departementet.

3 Øvrige kommentarer

Ved gjennomgang av høringsnotatet har NSM identifisert enkelte unøyaktigheter i fremstillingen. NSM vil kunne være behjelpelig med korrigering av disse ved utarbeidelse av proposisjonstekst.

Med hilsen

for Kjetil Nilsen
Direktør