DET KONGELIGE
FORSVARSDEPARTEMENT

Prop. 97 L

(2015–2016)

Proposisjon til Stortinget (forslag til lovvedtak)

Endringer i sikkerhetsloven (reduksjon av antall klareringsmyndigheter mv.)

Innhold

DET KONGELIGE
FORSVARSDEPARTEMENT

Prop. 97 L

(2015–2016)

Proposisjon til Stortinget (forslag til lovvedtak)

Endringer i sikkerhetsloven (reduksjon av antall klareringsmyndigheter mv.)

Tilråding fra Forsvarsdepartementet 15. april 2016, godkjent i statsråd samme dag.
(Regjeringen Solberg)

1 Proposisjonens hovedinnhold

Forsvarsdepartementet legger i proposisjonen her fram forslag til enkelte endringer i lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven).

De mest sentrale forslagene er en reduksjon av antall klareringsmyndigheter, med én sentral klareringsmyndighet i sivil sektor og én tilsvarende i forsvarssektoren (§ 23), nye bestemmelser om varsling og myndighet til å fatte vedtak ved risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført (§ 5 a) og ved anskaffelser til kritisk infrastruktur, dersom en slik anskaffelse kan innebære en risiko som nevnt foran (§ 29 a). Videre foreslås det en endring fra oppdragsbaserte til tidsbaserte leverandørklareringer i forbindelse med sikkerhetsgraderte anskaffelser (§ 28). I forslaget til endringer i loven inngår også lovfesting av gjeldende praksis på enkelte områder. Dette gjelder særlig den nasjonale responsfunksjonen for alvorlige dataangrep mot kritisk infrastruktur (NorCERT) og varslingssystemet for digital infrastruktur (VDI) (§ 9 e), rammer for behandling av personopplysninger i den forbindelse (§ 10 a) og sikkerhetsmessig overvåking av godkjente informasjonssystemer (§ 13 a).

Forslagene vil samlet sett dekke et behov som gjeldende regelverk ikke ivaretar, og dessuten bidra til effektivisering og legitimering av gjeldende praksis.

Ved kongelig resolusjon 27. mars 2015 ble det oppnevnt et eksternt utvalg med mandat til å foreslå et nytt lovgrunnlag for forebyggende nasjonal sikkerhet (Sikkerhetsutvalget). Utvalget skal etter mandatet avgi rapport i form av en NOU høsten 2016. Rapporten vil deretter bli sendt på alminnelig høring. Det er imidlertid behov for å fremme de foreliggende forslag til lovendring, uten å påvente Sikkerhetsutvalgets rapport og etterfølgende behandling.

2 Lovforslaget og høringen

2.1 Bakgrunnen for lovforslaget

Sikkerhetsloven har i liten utstrekning vært gjenstand for endringer siden loven trådte i kraft 1. juli 2001. Hovedsakelig har dette dreid seg om justeringer i kapittel 6 om personellsikkerhet (endringslov 17. juni 2005 nr. 81) og i bestemmelsene i kapittel 5 om objektsikkerhet, der det ble gitt nærmere bestemmelser om utvelgelse og klassifisering av skjermingsverdige objekter (endringslov 11. april 2011 nr. 9).

Med bakgrunn i de samfunnsmessige utviklingstrekkene innenfor sikkerhetsområdet de senere årene, har Forsvarsdepartementet sett behov for en mer gjennomgående vurdering av i hvilken utstrekning gjeldende lov møter dagens og morgendagens utfordringer innenfor forebyggende sikkerhet.

I november 2012 ble det utarbeidet en evalueringsrapport av en bredt sammensatt departementsgruppe, ledet av Forsvarsdepartementet. Gruppen konkluderte med at dagens utvikling innen teknologi og andre utviklingstrender, representerer nye sikkerhetsutfordringer som tilsier en revisjon av sikkerhetsloven. Som eksempel på andre utviklingstrender ble det vist til økt globalisering, internasjonalisering og tverrsektorielle avhengigheter.

I februar 2013 ble det derfor etablert en arbeidsgruppe bestående av Forsvarsdepartementet, Justis- og beredskapsdepartementet og Nasjonal sikkerhetsmyndighet. Arbeidsgruppen fikk i oppdrag å foreta en helhetlig revisjon av sikkerhetsloven. Samtidig ble det etablert en referansegruppe av øvrige berørte departementer.

Revisjonsarbeidet avdekket grunnleggende utfordringer om hva sikkerhetsloven bør regulere, deriblant forholdet mellom sikkerhetsloven og annet sikkerhetsrelatert sektorregelverk. Det er ulike oppfatninger om hva lovens formål og virkeområde bør være i framtiden. Innenfor objektsikkerhetsområdet er det også avdekket uenighet mellom ulike sektorer om hva reglene skal ta sikte på å beskytte mot, og på hvilken måte.

På denne bakgrunn besluttet regjeringen å dele opp arbeidet med revisjon av loven i to faser. Dette for å kunne gjennomføre enkelte av endringsforslagene uten å måtte vente på de grundige analysene som er nødvendig for å løse de forannevnte temaene.

I den første fasen vil departementet foreslå endringer i gjeldende sikkerhetslov som det er behov for å få på plass raskt. Denne proposisjonen er en oppfølging av første fase.

Sikkerhetsutvalget, nevnt i punkt 1, representerer fase to.

2.2 Høringen

Den 19. mai 2015 sendte departementet ut et høringsnotat med forslag til endringer i sikkerhetsloven med høringsfrist 20. august 2015. Notatet ble sendt til følgende instanser:

Departementene

Barne- ungdoms- og familiedirektoratet
Barneombudet
Datatilsynet
Det kriminalitetsforebyggende råd (KRÅD)
Departementenes sikkerhets- og service-organisasjon (DSS)
Direktoratet for forvaltning og IKT (Difi)
Direktoratet for naturforvaltning
Direktoratet for samfunnssikkerhet og beredskap
Finanstilsynet
Forbrukerombudet
Forbrukerrådet
Forsvarets forskningsinstitutt
Forsvarsbygg
Forsvarsstaben
Fylkesmannsembetene
Helsedirektoratet
Jernbaneverket
Klagenemnda for offentlige anskaffelser (KOFA)
Konkurransetilsynet
Kontrollutvalget for kommunikasjonskontroll
Kriminalpolitisentralen (Kripos)
Kriminalomsorgsdirektoratet

Kulturrådet
Kystdirektoratet
Landbruksdirektoratet
Likestillings- og diskrimineringsombudet
Lotteri- og stiftelsestilsynet
Luftfartstilsynet
Medietilsynet
Miljødirektoratet
Nasjonalbiblioteket
Nasjonalt folkehelseinstitutt
Nasjonal kommunikasjonsmyndighet (Nkom)
Nasjonal sikkerhetsmyndighet (NSM)
Norges vassdrags- og energidirektorat (NVE)
Oljedirektoratet
Patentstyret
Petroleumstilsynet
Politidirektoratet
Politiets sikkerhetstjeneste (PST)
Norges forskningsråd
Norsk romsenter
Norsk Utenrikspolitisk Institutt (NUPI)
Regjeringsadvokaten
Riksadvokaten
Riksantikvaren
Riksarkivet
Sekretariatet for konfliktrådene
Sjøfartsdirektoratet
Skattedirektoratet
Statens helsetilsyn
Statens jernbanetilsyn
Statens sivilrettsforvaltning
Statens strålevern
Statens vegvesen
Statistisk sentralbyrå (SSB)
Statsbygg
Sysselmannen på Svalbard
Toll- og avgiftsdirektoratet
Utdanningsdirektoratet
Utlendingsdirektoratet
Økokrim

Etterretningstjenesten
Forsvarets logistikkorganisasjon
Forsvarets sikkerhetsavdeling (FSA)

Høyesterett
Agder lagmannsrett
Borgarting lagmannsrett
Domstolsadministrasjonen
Eidsivating lagmannsrett
Frostating lagmannsrett
Generaladvokaten
Gulating lagmannsrett
Hålogaland lagmannsrett

Høgskolen i Gjøvik
Høgskolen i Narvik
Høgskolen Stord/Haugesund
Høgskolen i Ålesund
Norges teknisk- og naturvitenskapelige universitet (NTNU)
Norsk senter for menneskerettigheter (UiO)
Politihøgskolen
Senter for rettsinformatikk (UiO)
Universitetet i Bergen
Universitetet i Oslo
Universitetet i Stavanger
Universitetet i Tromsø

Det Kongelige Hoff
Ombudsmannen for Forsvaret
Riksrevisjonen
Sametinget
Stortingets kontrollutvalg for etterretnings-, overvåkings- og trygghetstjenester (EOS-utvalget)
Stortingets ombudsmann for forvaltningen

Bergen kommune
Fylkeskommunene
Kontoret for fri rettshjelp
Longyearbyen lokalstyre
Oslo kommune
Stavanger kommune
Tromsø kommune
Trondheim kommune
Ullensaker kommune

Avinor
Den norske kirke
Flytoget
Innovasjon Norge
Kirkens Bymisjon
Kirkens Familievern
Kirkens Nødhjelp
Kirkerådet
Likestillingssenteret
Norsk rikskringkasting (NRK)
Norges Bank
NSB
Posten AS
Statkraft
Statnett
Statoil
Telenor
Aerospace Industrial Maintenance Norway (AIM Norway SF)
Akademikerne
Amnesty International Norge

Antirasistisk senter
Arbeidsgiverforeningen Spekter
Bedriftsforbundet
Befalets fellesorganisasjon
CargoNet AS
Caritas Norge
Cepia Technology
Christian Michelsens Institutt
Den katolske kirke i Norge
Den Norske Advokatforening
Den norske Atlanterhavskomité
Den Norske Bank (DNB)
Den norske Dataforening
Den norske Dommerforening
Den norske Forfatterforening
Den norske Forleggerforening
Den norske Helsingforskomité
Den norske lægeforening
Den norske tannlegeforening
Det norske Menneskerettighetshuset
Det Norske Nobelinstitutt
Det norske Veritas
EDB Fellesdata
Energi Norge AS
Ericsson AS
Fafo
Fagforbundet
Fagpressen
Fellesforbundet
Finans Norge
Finansnæringens hovedorganisasjon
Finansieringsselskapenes Forening
Folk og Forsvar
Forskerforbundet
Forsvars- og sikkerhetsindustriens forening (FSi)
Frelsesarmeen
Fremtiden i våre hender
Funksjonshemmedes Fellesorganisasjon
Gatejuristen
Greenpeace Norge
Hafslund AS
Hovedorganisasjonen Virke
Human-Etisk Forbund
IKT-Norge
Industri Energi
Innvandrernes Landsorganisasjon
Institutt for fredsforskning (PRIO)
Institutt for journalistikk
Islamsk Kvinnegruppe Norge
Islamsk Råd Norge
Jottacloud
Kommunenes Sentralforbund (KS)
Kompetanseutvalget for dommere
Kongsberg Gruppen ASA
Kontaktutvalget for Pinsebevegelsen i Norge
Kopinor
Krigsskoleutdannede offiserers forening (KOL)
KUN Senter for kunnskap og likestilling
Landsforbundet for utviklingshemmede og pårørende
Landsforeningen for lesbiske, homofile, bifile og transpersoner
Landsorganisasjonen i Norge (LO)
Landsrådet for norske barne- og ungdomsorganisasjoner
Leger uten grenser
Lyse AS
Mediebedriftenes Landsforening
Menneskeverd
Miljøstiftelsen Bellona
Mnemonic AS
NAMMO AS
Nasjonal støttegruppe etter 22. juli-hendelsene
Nasjonalforeningen for folkehelsen
Naturvernforbundet
Nei til atomvåpen
NGO-forum for menneskerettigheter
Nordea
Norges Fredsråd
Norges Idrettsforbund
Norges Juristforbund
Norges kvinne- og familieforbund
Norges ingeniør- og teknologiorganisasjon (NITO)
Norges markedsføringsforbund
Norges Miljøvernforbund
Norges Offiserforbund (NOF)
Norges Rederiforbund
Norges Røde Kors
Norsk Folkehjelp
Norsk forbund for Utviklingshemmede
Norsk Forening for Etterforskning og Sikkerhet
Norsk forening for kriminalreform (KROM)
Norsk Hydro ASA
Norsk Journalistlag
Norsk Kvinnesaksforening
Norsk Militærjuridisk Forening
Norsk olje og gass
Norsk organisasjon for asylsøkere (NOAS)
Norsk Presseforbund
Norsk Redaktørforening
Norsk Sykepleierforbund
Norsk Tjenestemannslag (NTL)
Norske kvinnelige juristers forening
Norske Kvinners Sanitetsforening
Næringslivets hovedorganisasjon (NHO)
Næringslivets sikkerhetsorganisasjon (NSO)
Næringslivets sikkerhetsråd (NSR)
Organisasjonen mot Offentlig Diskriminering
Organisasjonen mot politisk overvåking

Phonero
Politiets Fellesforbund
Pragma sikkerhet
PRO-Sentret
Rafto-stiftelsen
Redd Barna
Rettighetsalliansen
Rettspolitisk forening
Rådet for psykisk helse
SAFE
Samfunnsviterne
Selvhjelp for Innvandrere og Flyktninger
Senter for informasjonssikring (NorSIS)
SINTEF – IKT
Sparebankforeningen i Norge
Statsadvokatenes forening
Statstjenestemannsforbundet
Stiftelsen bedre føre var
Stiftelsen Fritt Ord
Stiftelsen Rettferd for taperne
Stine Sofies Stiftelse
TeliaSonera Norge
Thales Norge AS
TONO
TV 2
TVNorge
UNICEF Norge
Unio
Utdanningsforbundet
Utdanningsgruppenes Hovedorganisasjon
Vinghøg AS
Watchcom Security Group
Yrkesorganisasjonenes Sentralforbund (YS)

Departementet har mottatt 50 realitetsuttalelser. Følgende instanser har gitt uttalelse:

Arbeids- og sosialdepartementet

Datatilsynet
Departementenes sikkerhets- og service-organisasjon
Direktoratet for forvaltning og IKT
Direktoratet for samfunnssikkerhet og beredskap
Finanstilsynet
Forsvarets forskningsinstitutt
Forsvarsbygg
Forsvarsstaben
Fylkesmannen i Oslo og Akershus
Fylkesmannen i Rogaland
Fylkesmannen i Vest-Agder
Høyesterett
Jernbaneverket
Kystverket
Luftfartstilsynet
Nasjonal kommunikasjonsmyndighet
Nasjonal sikkerhetsmyndighet (NSM)
Norges vassdrag- og energidirektorat
Norsk romsenter
Petroleumstilsynet
Politidirektoratet
Politiets sikkerhetstjeneste
Toll- og avgiftsdirektoratet
Utlendingsdirektoratet

Cyberforsvaret
Etterretningstjenesten
Forsvarets logistikkorganisasjon Investering
Forsvarets logistikkorganisasjon Vedlikehold
Forsvarets sikkerhetsavdeling

EOS-utvalget

Oslo kommune

Norges Bank
Norges Banks representantskap
NRK
Statnett
Telenor

Abelia
Advokatforeningen
Den Norske Bank
EnergiNorge
Finans Norge
Forsvars- og sikkerhetsindustriens forening
KraftCERT AS
Mnemonic AS
Norsk olje & gass
Norsk senter for informasjonssikring (NorSIS)
Privatpersonen Anders Bakke
Space Norway AS
Watchcom Security Group

Følgende høringsinstanser støtter forslaget eller har ingen merknader til høringen:

Helse- og omsorgsdepartementet
Kunnskapsdepartementet
Landbruks- og matdepartementet
Samferdselsdepartementet
Utenriksdepartementet

Arkivverket
Fylkesmannen i Sør-Trøndelag
Generaladvokaten
Kriminalomsorgsdirektoratet
Landbruksdirektoratet

Oljedirektoratet
Riksantikvaren
Statens jernbanetilsyn
Statens strålevern
Statistisk sentralbyrå

Kirkerådet

Stine Sofies Stiftelse

Høringsinstansenes merknader til de enkelte forslagene i høringsbrevet omhandles tematisk under de påfølgende kapitlene.

3 Lovens generelle virkeområde

3.1 Gjeldende rett

Lovens virkeområde er regulert i sikkerhetsloven § 2. Hovedregelen er at loven gjelder for forvaltningsorganer og for leverandører av sikkerhetsgraderte anskaffelser. I tillegg har Kongen myndighet til å fatte enkeltvedtak om at andre rettssubjekter skal være helt eller delvis underlagt loven. Denne myndigheten er videredelegert til Forsvarsdepartementet. Loven gjelder dessuten med visse begrensninger også for domstolene.

Etter sikkerhetsloven § 19 skal en person som skal gis tilgang til skjermingsverdig informasjon, autoriseres og sikkerhetsklareres på forhånd. Det følger av § 2 femte ledd at loven ikke gjelder for Stortinget, Riksrevisjonen, Stortingets ombudsmann for forvaltningen og andre organer for Stortinget. Stortingsrepresentanter autoriseres og sikkerhetsklareres derfor normalt ikke.

Loven er gjort gjeldende for Svalbard og Jan Mayen ved forskrift 31. mai 2013 nr. 558 om sikkerhetslovens anvendelsesområde på Svalbard og Jan Mayen.

3.2 Høringsforslaget

I høringsnotatet foreslo departementet å lovfeste praksisen om at regjeringsmedlemmer er unntatt plikt til autorisering og sikkerhetsklarering. Etter fast og langvarig praksis fulgt av ulike regjeringer, foretas det ingen autorisasjon og sikkerhetsklarering av regjeringsmedlemmer. Det er imidlertid ikke lovregulert at regjeringsmedlemmer er unntatt fra reglene om sikkerhetsklarering og autorisasjon. Departementet foreslo derfor at det gjøres unntak for regjeringsmedlemmer fra bestemmelsene i og i medhold av kapittel 6 om personellsikkerhet. Det het i høringsnotatet side 5:

> «Departementet legger til grunn at den enkeltes bakgrunn vil være godt opplyst før vedkommende utnevnes til statsråd, og at det derfor vil være et redusert behov for ytterligere personkontroll. En rutine- og pliktmessig sikkerhetsklarering av regjeringsmedlemmer har dessuten også prinsipielle betenkeligheter. Statsrådene står ansvarlige overfor Stortinget og er underlagt Stortingets kontroll. Når Kongen har valgt sitt råd, bør en sikkerhetsklarering gjennomført av embetsverket ikke kunne stå i veien for en utnevnelse eller føre til at en statsråd må gå.
>
> Så langt departementet er kjent med, er det heller ikke vanlig å sikkerhetsklarere regjeringsmedlemmer i land som det er naturlig for Norge å sammenligne seg med. I NATO er det overlatt til det enkelte lands interne regler å regulere tilgang til sikkerhetsgradert informasjon for sine senior myndighetsrepresentanter, som for eksempel regjeringsmedlemmer og medlemmer av parlamentet. Særskilte omstendigheter, som for eksempel krav fra andre stater, kan føre til at en statsråd må sikkerhetsklareres i enkelttilfeller, men dette vil kunne håndteres ved behov.»

Videre foreslo departementet i høringsnotatet et nytt fjerde ledd i sikkerhetsloven § 2. Forslaget var knyttet til ny regulering av anskaffelser til kritisk infrastruktur, jf. forslaget til ny § 29 a (se punkt 11). Forslaget hadde følgende ordlyd:

> «Kongen kan bestemme at § 29 a skal gjelde for rettssubjekter som eier eller rår over kritisk infrastruktur.»

Om forslaget til nytt fjerde ledd ble det uttalt følgende på side 31 i høringsnotatet:

> «For å fange opp kritisk infrastruktur som eies eller rådes over av rettssubjekter som per i dag ikke er underlagt sikkerhetsloven, vil departementene få i oppgave å identifisere kritisk infrastruktur i sine sektorer. Rettssubjekter som har kritisk infrastruktur, men som ikke er underlagt loven fra før, vil det bli aktuelt å fatte et avgrenset vedtak for, jf. ny § 2 fjerde ledd. Rettssubjektene vil da kunne bli underlagt varslingsplikten i § 29 a, men ikke loven for øvrig.»

3.3 Høringsinstansenes syn

Direktoratet for forvaltning og IKT (Difi) er enig i at det på generelt grunnlag er hensiktsmessig å lovfeste en fast og langvarig praksis om unntak fra plikten til autorisering og sikkerhetsklarering når det gjelder medlemmer av regjeringen. Difi ønsker imidlertid at den prinsipielle betydningen og eventuelle negative konsekvenser av lovendringen synliggjøres i noe større grad. *Forsvarets sikkerhetsavdeling (FSA)* «kan ikke se at det er vist til tungtveiende grunner for at regjeringsmedlemmer, som potensielt kan få tilgang til sikkerhetsgradert informasjon, ikke skal autoriseres eller sikkerhetsklareres». Det samme har to andre avdelinger i Forsvaret gitt uttrykk for. *Nasjonal sikkerhetsmyndighet (NSM)* på sin side, har ingen innvendinger til forslaget. NSM peker på at det allerede er sedvane for at regjeringsmedlemmer 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 i at slike unntak kan håndteres særskilt ved behov.»

Høyesterett foreslår at det tilsvarende unntaket som gjelder for dommerne i Høyesterett, også tas uttrykkelig inn i sikkerhetsloven etter mønster fra det unntaket som er foreslått for medlemmer av regjeringen. Dette er nærmere begrunnet slik:

> «Det følger av forskrift om personellsikkerhet § 7-2 første ledd at høyesterettsjustitiarius anses som sikkerhetsklarert og autorisert for høyeste sikkerhetsgrad ved utnevnelsen. At det ikke stilles noe krav om sikkerhetsklarering og autorisasjon for dommerne i Høyesterett følger videre av domstolloven § 5 – som i motsetning til de tilsvarende bestemmelsene for lagmannsrettene og tingrettene i domstolloven §§ 12 og 21 – ikke inneholder noen bestemmelse om sikkerhetsklarering og autorisasjon. Dette er også uttrykkelig forutsatt i forarbeidene til sikkerhetsloven, Ot.prp. nr. 49 (1996–97) om lov om forebyggende sikkerhetstjeneste. Det vises til side 30 hvor det uttales: 'Det foretas i dag ikke sikkerhetsklarering av Høyesteretts dommere. Lovforslaget tar ikke sikte på å endre på dette'.
>
> Det er svært viktig at unntaket for plikten til sikkerhetsklarering og autorisasjon for høyesterettsdommere videreføres. De hensyn som departementet har vist til hva gjelder regjeringsmedlemmene, […] gjelder langt på vei også for dommerne i Høyesterett. Det vises videre til drøftelsen om domstolens uavhengighet i Ot.prp. nr. 49 (1996–97) side 29 og 30. I tillegg kommer at Høyesterett er et forfatningsorgan, hvor sakene skal fordeles mellom dommerne etter et tilfeldighetsprinsipp. […] Det kan da ikke være slik at en dommer skal kunne utelukkes fra å delta ved behandlingen av en sak, eller en spesiell sakstype, fordi dommeren ikke har den nødvendige sikkerhetsklarering og er autorisert for den aktuelle beskyttelsesgrad. Dette innebærer at hensynet til Norges og våre alliertes sikkerhet mv. må ivaretas i forbindelse med utnevnelsen av nye høyesterettsdommere.»

Norges Banks representantskap opplyser i sin høringsuttalelse at representantskapet til banken er oppnevnt av Stortinget. I forbindelse med lovarbeidet vil det etter representantskapets syn være en fordel å få en avklaring på om begrepet «andre organer for Stortinget» i henhold til sikkerhetsloven § 2 omfatter representantskapet.

3.4 Departementets vurderinger

De fleste høringsuttalelser støtter forslaget om å lovfeste unntak for regjeringens medlemmer fra plikten til sikkerhetsklarering og autorisering, eller har ingen synspunkter på det.

Forslaget går ut på et unntak for svært få personer som gjennomgår en særlig «utsjekk» på høyeste politiske nivå og som ikke kan sammenlignes med det store antallet av «ordinære» klareringer. Det er dessuten tale om en lovfesting av en fast, årelang praksis som det til nå ikke har vært stilt spørsmål ved. Dersom et særskilt behov oppstår vil dessuten en sikkerhetsklarering la seg løse. Departementet ser derfor ikke at et unntak som dette har prinsipielle betenkeligheter av betydning, og fremmer derfor forslaget om at sikkerhetsloven kapittel 6 om personellsikkerhet ikke skal gjelde for regjeringens medlemmer.

Departementet har merket seg Høyesteretts uttalelse, og er enig i at dommere i Høyesterett eksplisitt bør unntas fra plikten til sikkerhetsklarering og autorisasjon etter § 19. Dette ble også forutsatt i forarbeidene til sikkerhetsloven, hvor det i Ot.prp. nr. 49 (1996–97) om lov om forebyg-

gende sikkerhetstjeneste bl.a. ble uttalt: «Det foretas i dag ikke sikkerhetsklarering av Høyesteretts dommere. Lovforslaget tar ikke sikte på å endre dette». Som også Høyesterett påpeker, inneholder ikke domstolloven § 5, som omhandler Høyesterett, noen bestemmelser om sikkerhetsklarering og autorisasjon, i motsetning til tilsvarende bestemmelser i §§ 12 og 21 om lagmannsrett og tingrett. Departementet er også enig i at hensynet til domstolenes uavhengighet tilsier at dommere i Høyesterett bør særskilt unntas fra plikten til sikkerhetsklarering og autorisasjon. Departementet fremmer derfor forslag om at også dommere i Høyesterett unntas fra kapittel 6 om personellsikkerhet.

Hva gjelder merknaden fra Norges Banks representantskap, gir forarbeidene til sikkerhetsloven, jf. Ot.prp. nr. 49 (1996–97) ingen nærmere veiledning om hvorvidt representantskapet er omfattet av begrepet «andre organer for Stortinget». Dersom representantskapet anser seg som et organ for Stortinget, heter det i forarbeidene at dette ikke er til hinder for at «disse organer etter egen beslutning finner det hensiktsmessig å anvende reglene så langt de passer». Departementet tar sikte på en egen dialog med Norges Banks representantskap på dette punkt.

Når det gjelder forslaget til nytt fjerde ledd i § 2, går departementet inn for å endre forslaget som ble sendt på høring. I høringsforslaget ble det foreslått å gi Kongen myndighet til å fatte enkeltvedtak om hvilke rettssubjekter § 29 a skal gjelde for. I henhold til høringsforslaget skulle § 29 a således gjelde for rettssubjekter som fra før var underlagt sikkerhetsloven, eller som ble omfattet av bestemmelsen gjennom enkeltvedtak. Vilkåret for å kunne fatte slikt enkeltvedtak var at rettssubjektet eier eller rår over kritisk infrastruktur.

Departementet har etter en ny vurdering konkludert med at alle virksomheter som eier eller rår over kritisk infrastruktur, bør være direkte underlagt § 29 a. Departementet mener en infrastruktur som er nødvendig for å opprettholde samfunnets grunnleggende behov og funksjoner (jf. forslaget til definisjon i § 3 nr. 21), per definisjon er så viktig at den alltid bør omfattes av § 29 a. En slik ordning vil også kreve mindre byråkrati. Departementet fremmer derfor forslag om et nytt fjerde ledd i § 2 i tråd med dette.

Departementet vil påpeke at det ikke alltid vil være åpenbart om en infrastruktur skal anses som kritisk eller ikke, noe som innebærer at det også kan være uklart hvilke virksomheter som er omfattet av § 29 a. Hensynet til forutsigbarhet for de som eier eller rår over denne type infrastruktur, tilsier derfor at myndighetene har gode rutiner for å gi informasjon som klargjør dette. Departementet fremmer som følge av dette forslag om at Kongen gis myndighet til å gi forskrift om hvordan kritisk infrastruktur skal identifiseres, og om hvordan rettssubjekter som eier eller rår over kritisk infrastruktur skal informeres. Om forslaget til ny § 29 a vises det til omtalen i punkt 11.

4 Varslingsplikt for virksomheter

4.1 Bakgrunn og gjeldende rett

Ny teknologi gjør det mulig for utenlandsk etterretning å utføre spionasje og sabotasje mot norske interesser på nye måter. Blant annet er norsk rom- og satellittvirksomhet et attraktivt mål for nye typer høyteknologisk spionasje og sabotasje.

Slik aktivitet kan potensielt utføres uten noen klar tilknytning til skjermingsverdige objekter. Aktiviteten kan for eksempel bestå i at en utenlandsk aktør får mulighet til å installere en elektronisk plattform som kan skjules i utstyr som tilsynelatende er ment for sivilt bruk. Slik teknologi kan både kartlegge og sabotere militære eller sivile kapasiteter tilhørende Norge eller Norges allierte. Teknologien kan også potensielt benyttes av ikke-statlige grupperinger eller enkeltindivider til å utføre terrorhandlinger.

Sikkerhetslovens formål er å legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Loven gir i § 3 anvisning på hvilke typer aktivitet som skal forebygges for å oppnå lovens formål. Som et samlebegrep benytter loven «sikkerhetstruende virksomhet», som i § 3 nr. 2 er definert som «forberedelse til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandlinger». Spionasje er definert i § 3 nr. 3, mens sabotasje og terrorhandlinger er definert i henholdsvis § 3 nr. 4 og 5.

Loven har videre anvisning på en rekke tiltak for å oppnå dette formålet, der den forebyggende sikkerhetstjenesten skal søke å fjerne eller redusere risiko som følge av sikkerhetstruende virksomhet.

De relevante bestemmelsene i og i medhold av sikkerhetsloven er i all hovedsak knyttet til sikring av informasjon (kapittel 4) og skjermingsverdige objekter (kapittel 5). Det finnes imidlertid ikke en klar hjemmel i loven for å kunne forebygge mer frittstående høyteknologisk virksomhet som kan innebære en fare for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Etter departementets syn gir heller ikke andre lover tilstrekkelig hjemmel til å forebygge slik aktivitet.

4.2 Høringsforslaget

4.2.1 Innledning

I høringsnotat 19. mai 2015 foreslo departementet å innta som ny § 5 a i sikkerhetsloven en bestemmelse som gir Kongen i statsråd myndighet til å fatte vedtak for å hindre planlagte eller pågående aktiviteter som innebærer en fare for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Det ble videre foreslått at virksomheter som er underlagt loven, og som får kunnskap om slike aktiviteter, skulle varsle overordnet departement om dette.

Forslaget var basert på en vurdering om at sikkerhetsloven er egnet som lovmessig forankring for en slik ny bestemmelse. Loven er sektorovergripende, og den har nettopp som formål å motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, jf. § 1 bokstav a.

Forslaget som ble sendt på høring hadde følgende ordlyd:

> «§ 5 a Varslingsplikt mv. ved risiko for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser
>
> Dersom en virksomhet får kunnskap om en planlagt eller pågående aktivitet som kan innebære en ikke ubetydelig risiko for rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser, skal virksomheten varsle overordnet departement om dette. Et departement som mottar varsel etter første punktum, bør innhente rådgivende uttalelse fra relevante organer med kompetanse innenfor det aktuelle fagområdet.
>
> Kongen i statsråd kan fatte nødvendige vedtak for å hindre en planlagt eller pågående aktivitet som nevnt i første ledd første punktum. Et slikt vedtak kan fattes uten hensyn til begrensningene i forvaltningsloven § 35.
>
> Kongen i statsråd kan gi forskrift om varslingsplikten i første ledd og om hvilke vedtak som kan treffes etter andre ledd.»

Forslaget til ny bestemmelse tok sikte på å gi norske myndigheter et lovgrunnlag for å kunne avverge eller stanse aktivitet som *legger til rette for eller kan lede fram til* at vitale nasjonale sikkerhetsinteresser blir truet, og at det skal varsles dersom virksomheter som er underlagt loven, får kunnskap om slik aktivitet.

Bestemmelsen skulle dekke et behov som gjeldende regelverk ikke ivaretar, og den vil komme i tillegg til de eksisterende bestemmelsene om forebyggende sikkerhetstjeneste.

4.2.2 Myndighet for Kongen i statsråd til å fatte nødvendige vedtak

Av høringsnotatet framgår det på side 35:

> «Bestemmelsen tar primært sikte på å gi hjemmel til å forhindre etablering av teknologiske innretninger som kan benyttes som plattform for fremmed etterretning. Behovet for en slik sikkerhetsventil har blitt større med de utfordringene ny teknologi gir. Det understrekes imidlertid at bestemmelsen er formulert slik at den også kan favne annen type aktivitet enn det som knytter seg til høyteknologiske innretninger.»

Den nye bestemmelsen skulle gi Kongen i statsråd kompetanse til å fatte de vedtak som vurderes som nødvendige, og vedtakene skulle kunne fattes mot enhver som planlegger eller utfører aktivitet som omfattes av ordlyden i høringsforslaget § 5 a. Det å nekte å gi byggetillatelse eller frekvenstillatelse, eller hindre et oppkjøp som kunne gi en aktør direkte eller indirekte adgang til å utføre sikkerhetstruende virksomhet, ble nevnt som eksempler på mulige vedtak.

At vedtakene skulle være «nødvendige» innebærer i henhold til høringsnotatet side 36 at:

> «Kongen i statsråd [ikke] skal fatte mer byrdefulle vedtak enn det som er påkrevd og vurderes som rimelig i den konkrete saken. Bestemmelsen vil være en sikkerhetsventil og forutsettes benyttet kun i helt sjeldne tilfeller. Kompetansen til å hindre en planlagt eller pågående aktivitet foreslås lagt til Kongen i statsråd. Departementet finner det naturlig at kompetansen legges til Kongen i statsråd av flere grunner. Det antas at det er snakk om et lite antall saker og at disse etter sin art vil være alvorlige og spesielle, jf. også formålet med sikkerhetsloven. At kompetansen legges til Kongen i statsråd vil derfor sikre at eventuelle tiltak som iverksettes er resultat av en vurdering på høyt nivå og står i rimelig forhold til den foreliggende risikoen.»

For å sikre at vedtak som fattes av Kongen i statsråd, også skal kunne omgjøre tidligere forvaltningsvedtak, ble det i forslaget til bestemmelsen foreslått at vedtak kunne fattes uten hensyn til begrensningene i forvaltningsloven § 35.

Det ble i høringsnotatet side 36 også foreslått at Kongen i statsråd skal kunne fatte vedtak som innebærer omgjøring av en forvaltningsavgjørelse ut over rammene som følger av forvaltningsloven § 35. Dette ble gjort for å ta høyde for tilfeller der forvaltningen allerede hadde fattet et vedtak, og det av sikkerhetshensyn anses nødvendig å omgjøre vedtaket.

4.2.3 Varslingsplikt for virksomheter som er underlagt loven

For at sentrale myndigheter skal få kunnskap om potensielt uønskede pågående eller planlagte aktiviteter, ble det foreslått at virksomheter som er underlagt sikkerhetsloven skal pålegges en varslingsplikt til overordnet departement. I høringsnotatet side 36 står det blant annet følgende om dette:

> «Dersom virksomheten får kunnskap om en planlagt eller pågående aktivitet som kan innebære fare for rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser, skal overordnet departement varsles om dette. Dette kan typisk være der virksomheten mottar en søknad eller en henvendelse fra en part, eller på annen måte blir gjort kjent med aktiviteten. Det vil her være tale om aktiviteter som planlegges eller utøves av andre aktører enn virksomheter som er underlagt loven. Virksomhetene skal varsle sitt overordnede departement. Med overordnet departement menes det departement som vedkommende virksomhet er underlagt. For kommunenes del vil overordnet departement i denne sammenheng være Kommunal- og moderniseringsdepartementet. Varslingsplikten vil kun påhvile virksomheter som loven gjelder for, dvs. forvaltningsorganer eller andre rettssubjekter som ved enkeltvedtak er omfattet av loven, jf. § 2.»

Varslingsplikten skulle etter forslaget gjelde «planlagte eller pågående aktiviteter som kan innebære en ikke ubetydelig risiko for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhets-

interesser». Passusen «ikke ubetydelig risiko» gir anvisning på den skjønnsmessige vurderingen av risikoen som må foretas i det enkelte tilfellet. Det framgår videre i høringsnotatet side 36:

> «Det er den enkelte virksomhet som må foreta vurderingen. Departementet legger til grunn at det vil være nødvendig å utforme en veileder eller instruks som forklarer hva varslingsplikten vil innebære, herunder om den skjønnsmessige vurderingen av risikoen, slik at virksomhetene gjøres kjent med, eventuelt selv utarbeider og implementerer, varslingsrutiner og -bevissthet i sin virksomhet.
>
> Dersom et departement får en slik melding bør det be om en rådgivende uttalelse fra relevante organer med kompetanse på det aktuelle fagfeltet. Den klare hovedregelen er at slik uttalelse *skal* innhentes. Departementet foreslår likevel å benytte ordet «bør», slik at dette kan unnlates i tilfeller der det vil være uhensiktsmessig eller praktisk svært vanskelig å innhente en uttalelse. Det kan for eksempel tenkes tilfeller av tidsnød, eller at departementet har fått saken tilstrekkelig opplyst på andre måter. Relevante offentlige organer er forpliktet til å gi en uttalelse når de mottar en anmodning om dette.»

I lys av formålet med den foreslåtte bestemmelsen ville det typisk være aktuelt å innhente rådgivende uttalelser fra Nasjonal sikkerhetsmyndighet, Politiets sikkerhetstjeneste og Etterretningstjenesten. Videre ble det uttalt:

> «De rådgivende uttalelsene som utarbeides skal i den grad det lar seg gjøre være av en slik karakter at departementet som har fått meldingen får en reell mulighet til å vurdere risikoen. Dersom departementet mener at den rådgivende uttalelsen ikke gir et tilstrekkelig beslutningsgrunnlag, kan det bes om bistand fra relevant departement for den enkelte sak, som for eksempel Forsvarsdepartementet, Justis- og beredskapsdepartementet eller Utenriksdepartementet. Dersom departementet som har mottatt varselet ut fra en totalvurdering anser risikoen som for høy, skal saken forelegges Kongen i statsråd, med en anbefaling om vedtak.»

4.3 Høringsinstansenes syn

4.3.1 Generelle merknader

Det har innkommet i alt 18 høringssvar som berører forslaget til ny § 5 a. Mange av høringsinstansene er generelt positive eller uttrykker konkret støtte til forslaget. Dette gjelder både med hensyn til den foreslåtte varslingsplikten og hjemmelen for Kongen i statsråd til å fatte vedtak for å hindre en planlagt eller pågående aktivitet som kan innebære en ikke ubetydelig risiko for rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser. Disse instansene er *Advokatforeningen, Cyberforsvaret, Etterretningstjenesten, Kystverket, Luftfartstilsynet, Nasjonal kommunikasjonsmyndighet, Nasjonal sikkerhetsmyndighet (NSM), Norges vassdrags- og energidirektorat, Politidirektoratet* (som også viser til uttalelser fra bl.a. Kripos, Romerike politidistrikt og Vestoppland politidistrikt), *Politiets sikkerhetstjeneste (PST), Space Norway AS* og *Utlendingsdirektoratet*.

Kripos mener at bestemmelsen vil være med å gi bedre oversikt over truende aktiviteter og kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. *Space Norway AS* støtter den retningen arbeidet har og uttaler bl.a. at det er vesentlig å sikre at det i arbeidet med ny lovgivning tas hensyn til den kompleksiteten som den globaliserte teknologiske utviklingen innebærer. *Utlendingsdirektoratet* støtter forslaget og mener at varslingsplikten vil bidra til å heve sikkerhetsnivået i UDI i positiv retning ved at den gir økt og skjerpet oppmerksomhet i alle ledd. UDI utaler også at varslingsordningen vil bidra til mindre risiko for at eventuelle utro tjenere hos leverandører av utstyr vil kunne lykkes med sitt forsett. De anser det videre som riktig og viktig at overordnet departement skal orienteres dersom det oppdages trusler som innebærer fare for rikets selvstendighet og sikkerhet, men påpeker at varslingsplikten vil kunne føre til nye administrative rutiner i virksomheten.

NSM er også positive til forslaget om å innføre en varslingsplikt. NSM uttaler i tillegg at det er svært viktig at norske myndigheter, i et stadig mer globalisert og nettverksbasert samfunn, har en mulighet til å stanse eller endre pågående eller planlagt aktivitet som kan skade rikets selvstendighet og sikkerhet.

I noen av høringsinnspillene gis det uttrykk for skepsis eller motforestillinger til forslaget. *Telenor Norge* mener at forslaget virker unødvendig og ikke godt nok gjennomtenkt, og privatpersonen *Anders Bakke* reiser spørsmål om bestemmelsen griper inn i politiets ansvars- og virkeområde.

Norges Bank, Norsk olje og gass og *Telenor Norge* gir uttrykk for at rekkevidden og innholdet i bestemmelsen må klargjøres, og at det derfor er

viktig at det blir utarbeidet en veileder til bestemmelsen. Norges Bank forutsetter også at det gis nærmere bestemmelser om hvordan lovbestemt taushetsplikt, for eksempel etter sentralbankloven § 12, skal ivaretas der varsling må foretas til eksterne.

4.3.2 Varslingsplikt

Etterretningstjenesten og *Politidirektoratet* mener at varslingsplikten bør utvides til å omfatte virksomheter som eier eller rår over kritisk infrastruktur. *Etterretningstjenesten* uttaler blant annet:

> «De samme hensyn som taler for varslingsplikt etter § 29 a for anskaffelser, gjelder overfor andre forhold disse virksomhetene blir klar over og som ikke har sammenheng med en konkret anskaffelse, men som gjelder aktivitet som kan innebære en ikke ubetydelig risiko for rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser. Vi foreslår derfor at § 2 fjerde ledd justeres slik:
>
> *Kongen kan bestemme at §§ 5 a og 29 a skal gjelde for rettssubjekter som eier eller rår over kritisk infrastruktur.»*

Etterretningstjenesten foreslår også at tjenesten bør varsles parallelt med varsling til departementet. Etterretningstjenesten viser til tjenestens nasjonale og sektoroverskridende mandat og uttaler:

> «Det tilligger Etterretningstjenesten å kartlegge og motvirke ytre trusler mot rikets selvstendighet og sikkerhet og andre viktige nasjonale interesser, jf. lov om Etterretningstjenesten §§ 1 og 3. Tidligst mulig varsel til Etterretningstjenesten er av avgjørende betydning for at tjenesten skal kunne iverksette rettidige innhentingstiltak mv, samt gi en best mulig rådgivende uttalelse.»

Norges Bank mener at det bør vurderes om Nasjonal sikkerhetsmyndighet (NSM) skal varsles parallelt med departementet.

Politidirektoratet ser det som viktig at også olje- og energisektoren omfattes av bestemmelsen, og viser til at denne sektoren har definert seg utenfor sikkerhetsloven – til tross for at andre skjermingsverdige objekter er kritisk avhengig av strøm for å opprettholde sine funksjoner, og at sektoren er utsatt for etterretningsaktivitet.

De instansene som har hatt kritiske innspill til forslaget tar opp ulike aspekter, og flere av disse tar opp det de oppfatter som uklarheter i høringsforslaget. Også spørsmål om hvem det skal varsles til og om selve utformingen av paragrafen, kommenteres.

Forsvarets logistikkorganisasjon (FLO/INVSTAB/Industrisikkerhet) anbefaler at:

> «[R]apportering bør skje 'i linjen' til nærmeste 'foresatte', for forvaltningsorgan til ansvarlig sektor/Nasjonal sikkerhetsmyndighet, for leverandører til det forvaltningsorgan/sektor som har sikkerhetsmessig ansvar for leverandøren. Dette vil ifølge FLO sikre et bedre beslutningsgrunnlag, ved at rapportering ledsages av faglige vurderinger i linjen før det eventuelt skal sendes til departementet.»

Norges vassdrags- og energidirektorat anbefaler at det i den pågående revisjonen av de øvrige delene av sikkerhetsloven vurderes en presisering av NSMs plikt til også å informere sektormyndighetene om forhold som kan håndteres gjennom sektorens egen regulering på en hensiktsmessig måte, og at dette må sees i sammenheng med innføring av varslingsplikt.

Nasjonal kommunikasjonsmyndighet (Nkom) støtter forslaget om å lovfeste at Kongen i statsråd skal kunne fatte vedtak for å hindre aktiviteter som kan innebære risiko for rikets selvstendighet og sikkerhet. Nkom uttaler videre:

> «Forslaget til lovtekst er lagt på et så generelt nivå at det er vanskelig konstruktivt å kommentere på mulige konsekvenser av bestemmelsen eller vedtak fattet i medhold av den. Særlig vil Nkom peke på at aktuelle tiltak ikke er nærmere definert, og er foreslått forskriftsregulert. Nkom antar at en slik reguleringsmåte vil kunne begrense arten av de tiltak som lovlig kan fattes etter bestemmelsen, også etter forskrift gitt med hjemmel i den, jf. både det internrettslige og ulike konvensjonsbaserte legalitetsprinsipp».

Nkom bemerker også at selve varslingsplikten har fått en framtredende plass i bestemmelsens ordlyd, mens den nye vedtakshjemmelen er knapt utformet og plassert i andre ledd. Nkom anbefaler derfor at vedtakskompetansen løftes noe fram i bestemmelsens ordlyd, overskrift og utforming.

Videre peker Nkom på at enkelte private og offentlige rettssubjekter som er underlagt loven, ikke vil ha noe «overordnet departement» å varsle til. Av den grunn mener Nkom at det vurderes å utpeke et organ med særlig ansvar for å motta og

behandle slike meldinger. Nkom anbefaler til slutt å vurdere om det er behov for å lovfeste sanksjons- eller tvangsmidler for gjennomføring av vedtak etter bestemmelsen.

Mnemonic stiller seg positiv til at varslingsplikten lovfestes. Det settes likevel spørsmålstegn ved gjennomføringen, og Mnemonic anfører at det ikke kommer tydelig fram hva virksomhetene plikter å varsle om, og heller ikke hvem som skal ha det overordnede nasjonale ansvaret. Mnemonic mener det heller ikke er tydelig definert hvem som skal kontaktes dersom det varslede departementets kompetanse og situasjonsforståelse ikke strekker til. Mnemonic gir, i likhet med Nkom, også uttrykk for at varslinger med betydning for rikets sikkerhet bør samles hos ett organ, og uttaler videre om dette:

> «Dersom slike varslinger ikke sammenfattes risikerer styresmaktene å miste både situasjonsforståelse og handlingsrom. Vi vil også påpeke viktigheten av at det er tydelig for den enkelte virksomhet hvilket departement de skal varsle til. Ikke alle virksomheter underlagt sikkerhetsloven har en klar sektor- eller departementstilhørighet. Vi forventer at det kommer en forskrift som tydeliggjør disse punktene.
>
> Når det kommer til implementering av varslingsplikten, er vi også opptatt av at myndighetenes reaksjoner på varslingene er forutsigbare. Dette er nødvendig for å ivareta varslerne og stimulere til at loven virker etter hensikten.»

Telenor uttaler blant annet at det må klargjøres hva varslingsplikten skal omhandle, hvordan virksomheter skal bli satt i stand til å forstå at det foreligger en ikke ubetydelig risiko for rikets sikkerhet mv., og hva myndighetene eventuelt skal kunne pålegge for å hindre at det utvikles teknologiske innretninger som kan benyttes som plattform for fremmed etterretning. Telenor gir også uttrykk for at bestemmelsen virker unødvendig og ikke godt nok gjennomtenkt med henblikk på hva dette i praksis måtte innebære for både virksomhetene og myndighetene. Dersom forslaget blir opprettholdt, mener Telenor det blant annet må klargjøres hva myndighetene skal kunne pålegge for å forhindre at det utvikles teknologiske innretninger som kan benyttes som plattform for fremmed etterretning. Telenor uttaler i forbindelse med dette:

> «Telenor er eier av kritisk IKT-infrastruktur i Norge. Denne består av komplekse nett og systemer og det kreves dyp kompetanse for å kunne vurdere de tekniske innretningene. Vi stiller spørsmål til om denne kompetansen finnes hos myndighetene. Feilaktige beslutninger eller inngripen fra myndighetene i Telenors IKT-infrastruktur vil kunne få flere negative konsekvenser. For Telenor vil konsekvensene kunne bli blant annet økonomiske, kommersielle og juridiske. I tillegg kommer negative konsekvenser for Telenorkonsernet som helhet (kommersielt, stordrift, industriell utvikling, og innovasjon). Det er derfor viktig at myndighetene søker å unngå dette og at Telenor selv kan foreslå hvordan vi skal imøtekomme et eventuelt krav.
>
> Telenor har liten erfaring med hva varslingsplikt kan gi av økonomisk belastning. Vi antar imidlertid at myndighetene med innføring av varslingsplikten vil kompensere for de faktiske utgifter innføring medfører.»

Telenor gir dessuten, sammen med *Norsk olje og gass*, uttrykk for at det er viktig at virksomheter som blir underlagt bestemmelsen gis en forståelse for hva varslingsplikten vil innebære, og at de settes i stand til å vurdere hvilke aktiviteter som kan innebære fare for rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser. Norsk olje og gass mener dette er viktig for å kunne identifisere og avdekke mer frittstående høyteknologisk aktivitet. De ser det derfor som helt nødvendig at det utarbeides en veileder eller instruks.

Petroleumstilsynet mener det ikke framgår av høringsnotatet at eventuelle vedtak som blir fattet med hjemmel i ny § 5 a andre ledd, vil kunne rette seg mot «enhver» som planlegger eller utfører aktivitet som omfattes av ordlyden i bestemmelsen. Tilsynet antar at vedtak også vil kunne rette seg mot rettssubjekter som ikke er omfattet av sikkerhetsloven, og mener at dette i så fall bør klargjøres.

Forsvarets sikkerhetsavdeling stiller spørsmål om bestemmelsen er ment å omfatte personkontrollopplysninger, og uttaler:

> «Det fremgår av gjeldende § 20, sjette ledd at:
>
> 'Opplysninger som er gitt klareringsmyndigheten i forbindelse med personkontroll, skal ikke benyttes til andre formål enn vurdering av sikkerhetsklarering.'
>
> Bestemmelsen praktiseres strengt.
>
> Det må etter vårt syn presiseres hvorvidt det er tenkt å påligge klareringsmyndigheten en varslingsplikt dersom vi får kunnskap om forhold nevnt i forslag til ny § 5 i forbindelse med gjennomføring av personkontroll.»

Anders Bakke uttaler at uttrykket «risiko» i seg selv ikke er en uønsket tilstand og ifølge NS 5814:2008 kun er et uttrykk for *sannsynlighet*. Bakke stiller også spørsmål om «det å fatte vedtak om- og å inngripe mot aktiviteter griper inn i politiets ansvars- og virkeområde, og om ikke denne regelen heller burde vært ført inn i lov som regulerer politiets virksomhet».

4.4 Departementets vurderinger

4.4.1 Generelt

Høringsuttalelsene har i det vesentlige bekreftet behovet for hjemmel til Kongen i statsråd om å fatte vedtak for å hindre planlagt eller pågående aktivitet som kan innebære en fare for at rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser vil bli truet. Det er også i stor grad uttrykt støtte til forslaget om varslingsplikt for å bidra til at informasjon om slike aktiviteter bringes til relevante myndigheter.

Etter departementets vurdering er det et klart behov for en hjemmel for sentrale myndigheter til å gripe inn og stanse aktivitet, også før den sikkerhetstruende virksomheten materialiserer seg. Dette vil være et viktig supplement til gjeldende regler. Det vil her være tale om å stanse aktiviteter som har et potensiale til å kunne utvikles eller tilpasses til ulovlig etterretningsvirksomhet, sabotasje eller terrorhandlinger – i særlig grad fra aktører som representerer fremmede makter. Det vil således være aktuelt å forhindre en i utgangspunktet lovlig aktivitet, for eksempel et forskningsprosjekt, dersom dette potensielt kan bli brukt til sikkerhetstruende virksomhet. I vurderingen av om en aktivitet kan utgjøre en potensiell risiko for trussel mot vitale nasjonale sikkerhetsinteresser, vil kunnskap om og graden av tillit til virksomheten som står bak aktiviteten, måtte tillegges vekt, og råd vil måtte innhentes fra relevante faginstanser.

Departementet understreker at bestemmelsen har karakter av en sikkerhetsventil. Hjemmelen til å fatte vedtak forutsettes benyttet i sjeldne og alvorlige tilfeller. Bestemmelsen vil typisk kunne benyttes hvor det ikke foreligger andre rettslige grunnlag for å stanse en aktivitet som innebærer en risiko for at vitale nasjonale sikkerhetsinteresser blir truet. At hjemmelen til å fatte vedtak også kan benyttes for å hindre en i utgangspunktet lovlig aktivitet, tilsier etter departementets vurdering at kompetansen til å fatte vedtak bør tillegges det øverste nivået i forvaltningen – Kongen i statsråd. Ved behov, for eksempel i perioder hvor statsråd normalt ikke er samlet, må det eventuelt innkalles til ekstraordinært møte i statsråd hvor minimum halvdelen av statsrådets medlemmer møter, jf. Grunnloven § 27.

Departementet følger derfor opp forslaget fra høringsnotatet om å innføre en hjemmel til å fatte vedtak for å hindre slik planlagt eller pågående aktivitet. Høringen har imidlertid vist at det forelå enkelte uklare punkter knyttet til ordlyden i høringsnotatet, og departementet finner også at det er behov for å knytte ordlyden nærmere til begrepene som allerede er brukt i sikkerhetsloven. På bakgrunn av dette fremmer departementet derfor et forslag til ny § 5 a i sikkerhetsloven som er noe justert i forhold til ordlyden i høringsforslaget.

Selv om høringen har bekreftet at det er behov for å innføre en varslingsplikt og en myndighet for Kongen i statsråd til å fatte nødvendig vedtak, har den også gjort det klart at det er behov for veiledning om de vurderingstemaene som ligger til grunn for at varslingsplikten inntrer. Departementet tar, som også omtalt i høringsnotatet, sikte på at det utarbeides en slik veileder.

4.4.2 Varslingsplikt

4.4.2.1 Hvem som plikter å varsle

I høringsforslaget ble det lagt opp til at varslingsplikten skal gjelde for forvaltningsorganer og for andre rettssubjekter som er underlagt sikkerhetsloven, jf. § 2.

Departementet har vurdert forslagene fra høringen om å utvide varslingsplikten til også å omfatte virksomheter som eier eller rår over kritisk infrastruktur, slik forslaget til ny § 29 a om anskaffelser til kritisk infrastruktur var utformet i høringsforslaget. Etter departementets vurdering er dette ikke hensiktsmessig. Varslingsplikten etter forslaget til ny § 29 a gjelder virksomheter som eier eller rår over kritisk infrastruktur, og utløses dersom en anskaffelse til slik infrastruktur kan medføre en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført. Plikten er således saklig avgrenset, og gjelder kun forhold knyttet til selve anskaffelsen. Det vil imidlertid ikke være hensiktsmessig å gi virksomheter som eier eller rår over kritisk infrastruktur en tilsvarende generell varslingsplikt som nå foreslås i ny § 5 a. Departementet har av den grunn ikke funnet det naturlig å utvide varslingsplikten etter § 5 a.

4.4.2.2 Hvem det skal varsles til

Departementet er enig med de høringsinstansene som har påpekt at ikke alle virksomheter som er underlagt loven, vil være underlagt noe «overordnet departement». Departementet finner det også helt sentralt å klargjøre hvem det skal varsles til. Først og fremst vil dette gjelde private rettssubjekter som er underlagt sikkerhetsloven, men spørsmålet om riktig varslingsinstans kan også gjelde enkelte offentlige virksomheter som har tilhørighet til ett eller flere departementer. For å klargjøre hvem det skal varsles til, fremmer derfor departementet forslag om at virksomheter som ikke er underlagt noe departement, skal varsle Forsvarsdepartementet. Forsvarsdepartementet vil på sin side videreformidle eventuelle mottatte varslinger som naturlig hører under et annet fagdepartement. Slik videreformidling vil etter departementets oppfatning ikke være å regne som behandling av varselet.

Når det gjelder offentlige virksomheter med tilhørighet til flere departementer, ser ikke departementet grunn til å lovfeste en tilsvarende særregel. Slike virksomheter må varsle det aktuelle departementet som den aktuelle virksomheten anser som mest relevant i den konkrete saken. Dersom dette skulle vise seg å være feil, vil vedkommende departement som mottar varselet videreformidle dette til rette departement.

Det er ellers påpekt i høringen at det i henhold til forskrift om sikkerhetsadministrasjon kapittel 5 allerede foreligger en varslingsplikt om sikkerhetstruende hendelser. Til dette bemerker departementet at varslingsplikten etter § 5 a skal supplere varslingsplikten i gjeldende regelverk, og at varslingsplikten og muligheten for Kongen i statsråd til å fatte vedtak etter § 5 a, gjelder uavhengig av om det foreligger en sikkerhetstruende hendelse rettet mot den varslingspliktige virksomheten eller ikke. Virksomheter underlagt sikkerhetsloven plikter følgelig på generelt grunnlag å varsle *«ved kunnskap om en planlagt eller pågående aktivitet»* som faller inn under bestemmelsen, uavhengig av om «aktiviteten» berører eller er rettet mot den varslingspliktige virksomheten selv.

Til høringsinnspillet fra Forsvarets logistikkorganisasjon om at varsling bør skje «i linjen» til nærmeste «foresatte», bemerker departementet at de fleste rettssubjekter som er underlagt sikkerhetsloven, vil ha et overordnet departement som sin nærmeste «foresatte», og at varslingsplikten for øvrig ikke er til hinder for at varsling etter omstendighetene vurderes i linjen før oversendelse til departementet. Dersom forholdet kan være tidskritisk, bør imidlertid hensynet til tidlig varsling veie tungt.

Departementet har også vurdert forslagene i høringen om at andre etater skal varsles parallelt med varsling til departementet. Både Etterretningstjenesten, Politiets sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet er aktuelle etater til å motta slike varsler. Departementet er enig i at en parallell varsling til flere etater kan bidra til at det varslede forholdet blir raskere vurdert og håndtert. Vi mener likevel at en parallell varsling kan bli unødig belastende for varslingspliktige virksomheter. De hensynene som taler for en parallell varsling, vil dessuten kunne ivaretas ved å etablere gode rutiner for effektiv håndtering av varslingene i det enkelte departement – herunder rutiner for å innhente rådgivende og faglige uttalelser fra relevante organer. I tillegg bør det enkelte departementet selv vurdere om og eventuelt til hvilken etat eller virksomhet en konkret varsling bør videreformidles til. Departementet fremmer derfor ikke forslag om parallell varsling nå.

4.4.2.3 Innholdet i varslingsplikten og forholdet til lovbestemt taushetsplikt

Enkelte av høringsuttalelsene viser at det er behov for å klargjøre innholdet i varslingsplikten og forholdet til lovbestemt taushetsplikt nærmere. Departementet er enig i at formuleringen i høringsnotatets forslag var noe uklar og med fordel bør harmonere mer med sikkerhetsloven og gjeldende terminologi. Videre er departementet enig med de høringsinstansene som har uttalt at det er viktig å bidra til at varslingspliktige virksomheter settes i stand til å vurdere om en aktivitet faktisk kan rammes av bestemmelsen. Dette er etter departementets oppfatning viktig, både av hensyn til virksomhetene selv, og av hensyn til at varslingspliktens formål skal kunne oppfylles. Departementet har i lovforslaget derfor valgt å erstatte uttrykket «*[…] risiko for rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser*» med *«[…] risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført»*.

Dette innebærer at vurderingstemaet for både varslingsplikten og eventuelle vedtak fattet av Kongen i statsråd, er risikoen for at en aktivitet kan lede fram til eller legge til rette for å etablere eller gjennomføre sikkerhetstruende virksomhet. Når det gjelder de ulike formene for sikkerhetstruende virksomhet, vil uttrykket «etablert» omfatte både forberedelseshandlinger til spionasje, sabotasjeaksjoner og terrorangrep, og utplas-

sering av utstyr eller personer som skal inngå i spionasje. At slik virksomhet blir «gjennomført» vil i denne sammenhengen omfatte både forsøk og faktisk gjennomføring av spionasje, sabotasje eller terrorhandlinger. Departementet opprettholder forslaget fra høringsnotatet om at varslingsplikt og mulighet for Kongen i statsråd til å fatte vedtak som hindrer en aktivitet, bare skal foreligge når risikoen for at sikkerhetstruende virksomhet blir etablert eller gjennomført, ikke er «ubetydelig». Dette innebærer at det ikke utløser varslingsplikt eller grunnlag for vedtak fra Kongen i statsråd at det foreligger en helt fjerntliggende, usannsynlig eller kun teoretisk mulighet for at aktiviteten kan medføre slik virksomhet. Det stilles derimot ikke krav om sannsynlighetsovervekt. I tilfeller hvor sannsynligheten vurderes som lav, samtidig som konsekvensene av en sikkerhetstruende virksomhet vurderes som meget skadelig eller katastrofal, vil bestemmelsen kunne utløse varslingsplikt og gi hjemmel for Kongen i statsråd til å fatte nødvendig vedtak.

Av hensyn til de grunnleggende verdiene bestemmelsen skal kunne verne om, ser departementet det som avgjørende at lovbestemt taushetsplikt ikke er til hinder for varsling om aktivitet som kan medføre sikkerhetstruende virksomhet. Departementet foreslår derfor å ta inn i et tredje punktum i forslaget til § 5 a første ledd, at varslingsplikten gjelder uten hinder av lovbestemt taushetsplikt.

Departementet legger samtidig opp til at det utarbeides en veileder med nærmere informasjon om varslingsplikten og de vurderingstemaene som skal ligge til grunn for varslinger og vedtak i medhold av bestemmelsen.

4.4.3 Myndighet for Kongen i statsråd til å fatte nødvendige vedtak

Enkelte høringsinstanser har uttrykt behov for forutsigbarhet med hensyn til hvilke vedtak som kan fattes av Kongen i statsråd for å forhindre en planlagt eller pågående aktivitet.

Vedtak etter § 5 a vil kunne omfatte mange ulike forhold, og det kan være aktuelt med helt ulike typer vedtak. Som også nevnt i høringsnotatet, kan dette for eksempel dreie seg om å nekte eller omgjøre et vedtak om byggetillatelse eller frekvenstillatelse, hindre et oppkjøp som gir en aktør direkte eller indirekte mulighet for å utføre sikkerhetstruende virksomhet, eller noe helt annet. Et slikt vedtak kan således få konsekvenser for rettssubjekter og virksomheter som ikke selv er underlagt sikkerhetsloven.

Hvilke vedtak som kan bli aktuelt å fatte, vil også kunne endre seg over tid. Begrepet «vitale nasjonale sikkerhetsinteresser», må, slik det også framgår av Ot.prp. nr. 49 (1996–97), «til enhver tid vurderes og defineres av overordnede politiske myndigheter». Av den nevnte proposisjonen framgår det videre at begrepet «kan endres i pakt med samfunnsutviklingen og de sikkerhetsmessige utfordringer som Norge til enhver tid står overfor». Departementet finner det således ikke praktisk mulig å gi en utfyllende oppregning av hvilke typer av vedtak som kan bli fattet av Kongen i statsråd i medhold av den foreslåtte bestemmelsen. Det er imidlertid åpenbart at hensynene som ligger til grunn for slike vedtak må ligge innenfor formålet med sikkerhetsloven.

Vedtak etter den nye bestemmelsen vil gjelde aktiviteter som i utgangspunktet er lovlige, og det kan også være snakk om aktiviteter som spesifikt er tillatt etter annen lov eller annet vedtak. Departementet går derfor inn for å presisere klart at vedtak etter § 5 a kan fattes uavhengig av hva som i utgangspunktet følger av annen lovgivning om den aktuelle aktiviteten. Departementet går derfor inn for å tilføye ordene «*og uavhengig av om vedtaket er tillat etter annen lov eller annet vedtak*» i § 5 a andre ledd andre punktum, sammenlignet med høringsforslaget. For å sikre at vedtak som fattes av Kongen i statsråd kan tvangsfullbyrdes uten domstolsbehandling, fremmes det forslag om at slike vedtak er særskilt tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Departementet har vurdert hvordan forslaget om at Kongen i statsråd skal kunne treffe slike vedtak stiller seg med hensyn til Grunnloven §§ 97 og 105 og EMKs tilleggsprotokoll 1 art. 1. Vurderingen er at forslaget er i overensstemmelse med de krav legalitetsprinsippet og EMKs prinsipp om «rule of law» stiller, og at det heller ikke foreligger noe brudd på forbudet mot tilbakevirkende lover. Selv om selve lovforslaget vurderes å være i overensstemmelse med Grunnloven, menneskerettighetsloven og Norges internasjonale forpliktelser, vil dette måtte vurderes konkret også på det tidspunktet et eventuelt vedtak fattes med hjemmel i bestemmelsen.

5 Gebyr på tjenester

5.1 Gjeldende rett

Sikkerhetsloven har i dag ingen klar hjemmel for at en virksomhet som utfører tjenester etter loven for en annen virksomhet, kan kreve brukerbetaling (gebyr) for sitt arbeid. I det alt vesentlige kreves det ikke gebyr for slike tjenester. Forskrift om informasjonssikkerhet § 5-24 andre ledd fastsetter imidlertid at eier av et informasjonssystem skal budsjettere med og dekke alle kostnader knyttet til sikkerhetsgodkjenningen av informasjonssystemet.

5.2 Høringsforslaget

I høringsnotatet foreslo departementet å gi en klar hjemmel for å kreve gebyr, der en virksomhet utfører tjenester for en annen. Departementet mente at en gebyrordning på den ene siden kunne bidra til at virksomheter som ber om en tjeneste i større grad foretok en reell vurdering av det aktuelle behovet for tjenesten, som for eksempel sikkerhetsklarering. På den annen side mente departementet at det var viktig at en ordning med gebyr ikke medførte en svekkelse av sikkerhetstilstanden. Etter departementets syn var det derfor sentralt at eventuelle fordeler ved å ha gebyr ble veid opp mot kostnadene som virksomheter ble påført. I høringsnotatet heter det på side 28:

> «Dagens bestemmelse i forskrift om informasjonssikkerhet § 5-24 andre ledd (gebyr ved godkjenning av informasjonssystemer) bør gis en sterkere forankring i lov. Departementet har på nåværende tidspunkt ikke tatt standpunkt til hvilke eventuelle øvrige tjenester (ut over dagens adgang ved godkjenning av informasjonssystemer) det kan være aktuelt å kreve gebyr for. Eksempler på slike tjenester kan være sikkerhetsklarering av personell etter reglene i lovens kapittel 6 og sikkerhetsklarering av leverandører etter reglene i lovens kapittel 7. Videre kan det også være aktuelt med gebyr for visse tjenester som følger av reglene om informasjonssikkerhet; godkjenning av krypto-systemer, monitoring og inntrengningstesting av informasjonssystemer, samt tekniske sikkerhetsundersøkelser. Departementet antar at det i hovedsak vil være Nasjonal sikkerhetsmyndighet som er den tjenesteytende virksomhet. Det kan imidlertid tenkes at det vil være andre virksomheter som også vil yte slik bistand. Blant annet gjelder det klareringsmyndigheter.»

Videre i høringsnotatet framgår det at forslaget ikke har noen direkte rettsvirkninger i seg selv. Eventuelle nye områder som skal ilegges gebyr, må konsekvensutredes og foreslås i et eventuelt senere forskriftsarbeid, der det foretas en nærmere vurdering av kostnadsbildet, hvilke områder som kan være egnet for gebyrfinansiering, og sikkerhetsmessige konsekvenser av å gebyrlegge en tjeneste. Departementet mente på side 29 i høringsnotatet at følgende momenter burde vurderes ved innføring av eventuelle bestemmelser om gebyr:

> «– For det første er det et grunnleggende prinsipp ved offentlige gebyrer at inntektene ikke skal overstige de nødvendige utgiftene den tjenesteytende virksomheten har. Dette prinsippet må være styrende ved fastsettelsen av gebyrets størrelse.
> – Videre må det vurderes konkret om gebyr anses som et hensiktsmessig virkemiddel for å sikre en bedre og mer effektiv tjenesteyting. Det kan føre til mindre restanser, uten at det går ut over kvaliteten. Dette vil dermed også komme de betalende virksomhetene til gode som ledd i deres arbeid med forebyggende sikkerhet.
> – For det tredje bør det vurderes å standardisere størrelsen på gebyret for den enkelte tjenesten. Standardiserte priser bidrar til forutsigbarhet, både på inntekts- og kostnadssiden. På den annen side kan det være til dels store variasjoner i arbeidsomfang og tidsbruk fra sak til sak. Bruk av standardiserte satser må derfor vurderes konkret i forbindelse med hver enkelt tjeneste.
> – Det bør også vurderes differensiering av gebyret. En mulig løsning er å differensiere

gebyret avhengig av om det er offentlig virksomhet, som er direkte underlagt sikkerhetsloven, eller en privat, som underlegges som følge av vedtak. En annen form for differensiering av gebyr, er å knytte det opp mot arbeidsomfang og tidsbruk som går med hos den tjenesteytende virksomhet. Også dette må imidlertid vurderes konkret i det enkelte forskriftsarbeid.»

5.3 Høringsinstansenes syn

Flertallet av høringsinstansene som har kommet med innspill er imot forslaget om å innføre en gebyrordning der en virksomhet utfører tjenester etter loven for en annen virksomhet. *Etterretningstjenesten* mener overordnet at forslaget er for dårlig utredet, og at det ikke tilfredsstiller utredningsinstruksens krav om redegjørelse for økonomiske, administrative og sikkerhetsmessige konsekvenser. *Norsk romsenter* er av samme oppfatning og uttaler at det må gjøres «en mer grundig utredning før det kan tas stilling om hjemmel for innføring av gebyr er hensiktsmessig».

Høringsinstansene mener videre at forslaget vil kunne medføre en betydelig svekkelse av sikkerhetstilstanden. Flere frykter en situasjon der økonomiske betraktninger blir styrende for om man tar i bruk sikkerhetstjenestene. *Etterretningstjenesten* uttaler blant annet:

> «Det ligger i dagen at dersom det blir vesentlig mer kostbart for virksomhetene å samhandle med NSM, vil virksomhetene unnlate å melde forhold til NSM og unnlate å gjøre bruk av NSMs kompetanse, i hvert fall i tvilstilfeller hvor unnlatelse ikke representerer et klart lovbrudd.»

Nasjonal sikkerhetsmyndighet (NSM) viser også til at det finnes eksempler på at tilsvarende finansieringsmodell tidligere har ført til at betalingsviljen, og evnen, er styrende i risikovurderingen:

> «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.»

Flere av høringsinstansene har også prinsipielle innvendinger mot at ordningen innføres, og påpeker at det offentlige ikke burde kunne ta betalt for en lovpålagt tjeneste, hvor NSM er i en monopolsituasjon. Etterretningstjenesten viser til at:

> «det ikke kan innføres brukerbetaling for arbeid som egentlig ikke er 'tjenester', men lovpålagte krav om tiltak hvor NSM er i en nasjonal monopolsituasjon, f. eks når det gjelder kryptogodkjenning, tekniske sikkerhetsundersøkelser (TSU) og monitoring. Prinsipielt ser vi forslaget som en alternativ finansieringsmåte av NSM, som reiser en rekke prinsipielle problemstillinger og motforestillinger som ikke er berørt. Herunder kan det på prinsipielt grunnlag reises spørsmål om et tilsynsdirektorat som både utøver nasjonale kontroll- og veiledningsfunksjoner, forestår risikovurderinger og gjennomfører enkelte operative utøvende funksjoner, bør brukerfinansieres.»

NSM viser til at tjenestene NSM leverer primært kommer samfunnet og samfunnssikkerheten til gode, og at det da er betenkelig å ta betalt for de tjenestene som blir levert:

> «statssikkerhet, herunder NSMs ansvar for forbyggende sikkerhet, [bør] fullt ut 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.»

Forsvarets logistikkorganisasjon/Investering, Forsvarets sikkerhetsavdeling (FSA) og *Kystverket* viser i tillegg til at det er unaturlig å ta betalt for slike tjenester innad i staten, mens *Telenor* hevder at myndighetene ikke må påføre private rettssubjekter unødige kostnader for at disse skal forholde seg til loven, og skriver:

> «Det er i myndighetenes interesser at vi forholder oss til lovverket, og at vi bruker myndighetene som rådgivere for å ta best mulige beslutninger. Telenor mener at myndighetene selv må dimensjonere sin organisasjon etter lovens nedslagsfelt, og ikke påføre private rettssubjekter unødige kostnader for at disse skal forholde seg til loven.»

Nasjonal kommunikasjonsmyndighet, *Norsk senter for informasjonssikring* og privatpersonen *Anders Bakke* støtter i utgangspunktet forslaget om å innføre en gebyrordning, men har noen av de samme

prinsipielle innvendingene mot forslaget som de øvrige høringsinstansene. *Anders Bakke* viser i all hovedsak til at risikoen for en svekket sikkerhetstilstand må veie tyngre enn de eventuelle fordelene et gebyr vil ha på dette området.

Dersom ordningen likevel blir innført mener flere av høringsinstansene at det bør settes strengere krav til sikkerhetsklareringsmyndighetene når det gjelder servicenivå, saksbehandlingstid og kvalitet på tjenestene. *NSM* mener at det må gjennomføres grundige analyser for hvilke områder gebyrordningen er egnet for, der mulige negative konsekvenser for samfunnssikkerheten må gis en framtredende plass og tillegges stor vekt.

5.4 Departementets vurderinger

Innføring av en klar hjemmel for å kunne kreve gebyr, der en virksomhet utfører tjenester etter loven for en annen, vil etter departementets oppfatning, etter en nærmere utredning, kunne ha fordeler som oppveier de eventuelle ulemper en slik adgang vil kunne ha. Departementet viser særlig til at en gebyrordning vil kunne bidra til en bedre og mer effektiv tjenesteyting, samt at virksomheter som ber om en tjeneste i større grad foretar en reell vurdering av det aktuelle behovet for tjenesten. Forslaget vil dessuten gi § 5-24 andre ledd i forskrift om informasjonssikkerhet en sterkere forankring i lov.

Departementet har imidlertid merket seg de innspillene som har kommet inn, og de argumentene som taler mot forslaget. Departementet er på denne bakgrunn kommet til at det bør foretas ytterligere utredning før det eventuelt fremmes nytt forslag om egen hjemmel for å kunne kreve gebyr for sikkerhetstjenester. Ett område for slik utredning kan eksempelvis være innføring av gebyr for sikkerhetsklareringer på høyeste nivå (STRENGT HEMMELIG/ Cosmic Top Secret). Dette er et klareringsnivå som ikke bør foretas med mindre det foreligger et særskilt behov, og der innføring av gebyr derfor kan være et hensiktsmessig virkemiddel. Nederland er eksempel på et land der det tas gebyr for Cosmic Top Secret-klareringer. Departementet vil derfor vurdere å komme tilbake til spørsmålet om hjemmel for å kunne legge gebyr på visse sikkerhetstjenester på et senere tidspunkt.

6 Nasjonal responsfunksjon og varslingssystem

6.1 NorCERT og VDI

6.1.1 Innledning

Nasjonal sikkerhetsmyndighet driver i dag en nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur (NorCERT) og et varslingssystem for digital infrastruktur (VDI). Hensikten med NorCERT og 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 også til bedre analyse og håndtering på nasjonalt nivå.

6.1.2 Nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur (NorCERT)

Norwegian Computer Emergency Response Team (NorCERT) er Norges nasjonale senter som koordinerer håndteringen av alvorlige IKT-hendelser mot kritisk infrastruktur. NorCERT ble etablert som en integrert del av Nasjonal sikkerhetsmyndighet (NSM) fra 1. januar 2006, og er en oppfølging av St.meld. nr. 39 (2003–2004) *Samfunnssikkerhet og sivilt-militært samarbeid*. I St.meld. nr. 22 (2007–2008) *Samfunnssikkerhet – Samvirke og samordning* legges det til grunn at «[e]nheten legger til rette for effektiv håndtering av alvorlige IKT-sikkerhetsangrep mot viktig infrastruktur og informasjon i Norge».

Et helt sentralt element i utøvelsen av NorCERT er innhenting, verifisering, analyse og videreformidling av informasjon om sårbarheter, potensielle risikoer, angrepsmetoder og ondsinnet kode. Dette skjer dels gjennom Nasjonalt varslingssystem for digital infrastruktur (VDI), men også gjennom mottak av informasjon fra nasjonale og internasjonale samarbeidspartnere. Den totale mengde data danner grunnlag for analyse i forbindelse med håndtering av alvorlige hendelser, og er avgjørende for koordinering med, og bistand til, nasjonale og internasjonale samarbeidspartnere.

I tilknytning til håndtering av allerede inntrufne alvorlige angrep, bistår NorCERT også med analyse av infisert maskinvare. I disse tilfellene får NorCERT overlevert det aktuelle lagringsmediet eller en kopi av dette. Ved tilgang til lagringsmediet, vil NorCERT få adgang til innholdsdata som er lagret på mediet. Formålet med analysen er imidlertid utelukkende å kartlegge forhold knyttet til det aktuelle angrep mot systemet. Virksomhetens samtykke og samarbeid er en nødvendig forutsetning for tilgang til materialet.

Den nasjonale evnen til å håndtere alvorlige dataangrep mot kritisk infrastruktur og informasjon er avhengig av et særlig samspill mellom EOS-tjenestene. EOS-tjenestene omfatter Etterretningstjenesten, Politiets sikkerhetstjeneste og NSM. Til sammen har tjenestene i oppdrag å oppdage, varsle, motvirke og etterforske alvorlige IKT-hendelser. NSM samarbeider derfor nært med Etterretningstjenesten og Politiets sikkerhetstjeneste om håndteringen av de mest alvorlige dataangrepene. Samarbeidet er nærmere formalisert og regulert i egne retningslinjer av 15. mai 2013, fastsatt av sjefene for de tre tjenestene.

Videre samarbeider NSM med en rekke andre offentlige og sivile samarbeidsparter. NSM har en koordinerende funksjon mot de nasjonale, sektorvise responsmiljøene (sektor-CERT'er) og enkeltvirksomheter der det ikke er slike. CERT står for Computer Emergency Response Team, og er koordinerende enhet for informasjonssikkerhet. En sektor-CERT bidrar med god kunnskap om spesielle systemer og løsninger innenfor sine respektive sektorer. NSM er også det nasjonale kontaktpunktet for tilsvarende funksjoner i andre land og internasjonale organisasjoner. Som nasjonal fagmyndighet skal NSM koordinere, og legge til rette for, samarbeid mellom alle aktører innen fagfeltet.

6.1.3 Varslingssystem for digital infrastruktur (VDI)

På 1990-tallet ble det klart at bruk av Internett og tiltakende IKT-avhengighet kom til å utgjøre en stor sårbarhet for kritisk infrastruktur. Som en konsekvens ble varslingssystem for digital infrastruktur (VDI) etablert i 1999 som et forsøksprosjekt mellom Etterretningstjenesten, Politiets sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet (NSM). Fra 2003 ble driften av VDI lagt under NSM, og det er i dag en integrert del av NSMs organisasjon. Det nære samarbeidet med Etterretningstjenesten og Politiets sikkerhetstjeneste rundt funksjonen er imidlertid videreført.

VDI består av et nettverk av sensorer som utplasseres hos utvalgte offentlige og private virksomheter som innehar kritisk infrastruktur i tilknytning til deltakernes datanettverk. Sensorene samler inn data som skal gjøre det mulig for NSM tidlig å detektere, verifisere og varsle om koordinerte og alvorlige dataangrep.

VDI registrerer metadata (data som tjener til å definere eller beskrive andre data) i den hensikt å kunne identifisere unormale kommunikasjonsmønstre hos de deltakende virksomhetene. Gjennom den enkelte VDI-sensor registrerer NSM trafikkdata som inneholder blant annet IP-adresser og domenenavn. Dette utgjør ca. 4 % av kommunikasjonen knyttet til inn- og utgående datatrafikk hos virksomheten. I denne prosessen vil det også registreres personopplysninger. Det er imidlertid *avidentifiserte* personopplysninger som inngår i den metadataen som registreres i tilknytning til datakommunikasjon inn og ut fra tilknyttede virksomheter. De avidentifiserte opplysningene må koples med andre opplysninger, som NSM ikke har tilgang til, for å kunne knyttes til en enkeltperson. Dataene er avidentifiserte i utgangspunktet, og NSM trenger derfor ikke å avidentifisere opplysningene i etterkant.

VDI-sensornettet har et signatursett som er utviklet basert på tidligere hendelser og annen kjent aktørinformasjon. Ved unormal trafikk vil det også kunne utløses en alarm basert på predefinerte signaturer. Ved slike alarmer blir det lagret en meget begrenset mengde innholdsdata i form av såkalt «pakkedump». Dette vil kun være fragmenter av innhold, fra for eksempel e-poster. Disse dataene er nødvendige for å kunne analysere og verifisere utløste alarmer.

Tilknytning til VDI er basert på frivillighet, og tilbys etter en nærmere vurdering av virksomhetens betydning for kritisk infrastruktur. Det inngås en avtale mellom NSM og den enkelte deltaker hvor partenes rettigheter og plikter nærmere reguleres. Deltakende private virksomheter er i dag forpliktet til å bidra til finansieringen av VDI og nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur (NorCERT) gjennom et årlig vederlag.

Tilknytning til VDI erstatter ikke virksomhetens egne sikkerhetstiltak, men er et komplementerende sikkerhetstiltak. Virksomhetene har derfor både en rett og plikt til å ivareta sikkerheten i egne systemer, uavhengig av tilknytning til VDI.

6.2 Gjeldende rett

Nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur og varslingssystem for digital infrastruktur er opprettet og lagt til Nasjonal sikkerhetsmyndighet etter beslutninger fra regjeringen og Stortinget, men har i dag ingen direkte forankring i lov.

6.3 Utenlandsk rett

I *Danmark* ble Governmental Computer Emergency Response Team (GovCERT) (etablert og plassert under Ministeriet for Videnskab, Teknologi og Udvikling, og var fullt operativ ved utgangen av 2010. I juni 2011 ble «Lov om behandling af personopplysninger ved driften af den statlige varslingstjeneste for internettrusler» vedtatt. Av ny lov om Forsvarets Efterretningstjeneste, som trådte i kraft 1. januar 2014, følger det at GovCERT og Militær varslingstjeneste for internettrusler (MILCERT), nå er en del av Forsvarets Efterretningstjeneste som «Center for Cybersikkerhed». Loven etablerer også behandlingsgrunnlag for innholds- og trafikkdata hos virksomheter som anmoder om midlertidig tilslutning til «netsikkerhetstjenesten». Loven viderefører elementer fra «GovCERT-loven» om begrensninger i adgangen til analyse og lagring av innholdsdata. Prinsippet om at analyse kun skal finne sted der det foreligger en begrunnet mistanke om en sikkerhetshendelse, videreføres. Det erkjennes i forslagets høringsnotat at begrensingene i slettetidspunktene for de ulike formene for data, ikke har fungert etter hensikten med loven. Derfor skilles det ikke lenger mellom pakke- og trafikkdata vedrørende lagring og sletting, og det utvider i vesentlig grad maksimal oppbevaringstid for innsamlede data som ikke knytter seg til en sikkerhetshendelse.

I *EU* la Europa-parlamentet mot slutten av 2013 fram et forslag til et direktiv for nettverks- og informasjonssikkerhet (Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union). Bakgrunnen for forslaget til direktiv er at det i EU i dag ikke er implementert tilstrekkelige og helhetlige beskyttelsestiltak for å oppnå en høy grad av nettverks- og informasjonssikkerhet. Ettersom medlemslandene har ulik kvalitet på sine implementerte sikkerhetstiltak, er det en fragmentert tilnærming til beskyttelsestiltak innen unionen. EU ønsker med dette direktivet å oppnå et høyt fellesnivå for nettverks- og informasjonssikkerhet. Av direktivets artikkel 7 følger krav til medlemsstatenes opprettelse av en nasjonal CERT, at denne har tilstrekkelige ressurser, at denne har en sikker nasjonal kommunikasjonsmulighet og at denne styres av en nasjonal kompetent myndighet som rapporterer til EU-kommisjonen. Av vedlegg 1 til direktivet, framgår en mer detaljert oppgave- og kravsbeskrivelse. Kommisjonen forutsetter at disse blir implementert som klare nasjonale retningslinjer og/eller i lovgivning.

I *NATO* er det etablert en CERT-funksjon som er tilknyttet NATOs egne systemer (NCIRC). Gjennom NATOs cyber-policy forutsettes det nasjonale strukturer som ivaretar disse behovene i det enkelte medlemsland. Det er også inngått arrangementer mellom NATO og NATOs medlemsland om samarbeid på området.

6.4 Høringsforslaget

Departementet foreslo i høringsnotatet at virksomheten som i dag utøves av Nasjonal sikkerhetsmyndighet (NSM) gjennom nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur (NorCERT) og varslingssystem for digital infrastruktur (VDI) blir lovfestet i § 9 som en del av NSMs oppgaver. Det ble foreslått at bestemmelsen inntas som ny bokstav e i § 9 første ledd. Som følge av ny bokstav e, ble det foreslått at gjeldende bokstav e blir bokstav f og at gjeldende bokstav f blir bokstav g. Forslaget innebærer utelukkende en kodifisering av ordninger som allerede har eksistert siden henholdsvis 1999 og 2006.

Departementet ga videre uttrykk for at dagens ordning med frivillig tilknytning til VDI videreføres som hovedprinsipp, men at det i forskrifter vurderes å åpne for å gjøre unntak fra dette for skjermingsverdige objekter og graderte informasjonssystemer. Unntaket var ment også å omfatte systemer som understøtter slike og som kan være spesielt utsatt for såkalte logiske trusler. Forslaget var kun ment som en sikkerhetsventil, der tilknytning til VDI ble vurdert som påkrevd ut fra det totale risikobildet, og hvor det ikke hadde vært mulig å få til en avtale basert på frivillighet. I den forbindelse understreket departementet at et eventuelt unntak fra frivillighet kun var ment å omfatte de største og viktigste systemene innen norsk IKT-infrastruktur.

6.5 Høringsinstansenes syn

Flere høringsinstanser, støtter en lovfesting av nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur (NorCERT) og varslingssystem for digital infrastruktur (VDI). *KRIPOS* uttaler at «[d]isse to funksjonene er tett knyttet sammen og anses i økende grad nødvendig for å kunne ha et helhetlig sanntidsbilde over sårbarheter og trusler mot digitalt baserte samfunnskritiske funksjoner». *Etterretningstjenesten* og *Telenor* påpeker at det bør åpnes for at virksomheter kan pålegges tilknytning til VDI. *Nasjonal kommunikasjonsmyndighet (Nkom)* mener at en slik ordning bør ha direkte hjemmel i lov.

Enkelte høringsinstanser stiller spørsmål om NorCERT og VDI er forenlige med NSMs tilsynsoppgaver. I den forbindelse uttaler *Nasjonal senter for informasjonssikring (NorSIS)*:

> «I redegjørelsen argumenteres det for at NSMs oppgaver knyttet til koordinering av nasjonal respons ved alvorlige IKT-hendelser bør lovfestes. Ser man foreslåtte formulering av operativt ansvar i e) opp mot tilsynsoppgaven i c) så kan dette medføre at NSM utøver operativ virksomhet og tilsyn i og overfor samme virksomhet. Spesielt da lovens virkeområde foreslås utvidet, bør den inngripen dette kan medføre overfor berørte virksomheter vurderes nærmere.»

Enkelte høringsinstanser stiller spørsmål ved hensiktsmessigheten av å lovregulere virksomheten, og mener organiseringen blant annet bør skje i samsvar med de behovene som samfunnsutviklingen krever. *Telenor* anerkjenner NSMs behov for å ha et tydelig mandat, ansvar og rolleavklaring mot andre myndighetsorganer, men påpeker at lovfesting vil være lite hensiktsmessig og bør unngås. Etter Telenors syn vil dagens organisering kunne være helt uhensiktsmessig om fire-fem år.

Politidirektoratet motsetter seg ikke lovfesting av ansvaret til NorCERT, men bemerker at lovfestingen kan bidra til å forsterke de uklarheter som allerede eksisterer rundt hvilke myndigheter som har ansvar for hva knyttet til alvorlige IKT-hendelser. Forarbeidene bør etter direktoratets vurdering, derfor klargjøre at det er politiet som har ansvaret for krisehåndtering i sivil sektor.

Flere høringsinstanser påpeker også at regulering av NorCERT og VDI bør sees i sammenheng med (og avvente) anbefalingene fra Digitalt sårbarhetsutvalg.

6.6 Departementets vurderinger

Departementet foreslår en lovfesting av virksomheten som i dag utøves av Nasjonal sikkerhetsmyndighet (NSM) gjennom nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur (NorCERT) og varslingssystem for digital infrastruktur (VDI). Videre foreslås en egen hjemmel for behandling av personopplysninger som er nødvendige for utførelsen av disse funksjonene, se punkt 7. Departementet mener en lov- og etterfølgende forskriftsfesting av funksjonene, og nærmere rammer for virksomheten, vil forenkle grunnlaget for EOS-utvalgets kontroll på dette området.

Av de instanser som har uttalt seg, støtter flertallet en lovregulering av NorCERT og VDI. Imidlertid registrerer departementet at enkelte instanser har stilt spørsmål om disse funksjonene er forenlige med NSMs øvrige oppgaver, da primært knyttet til tilsyn. Departementet vil peke på at forslaget ikke legger noen nye oppgaver til NSM. Denne oppgaveporteføljen har NSM allerede hatt i en rekke år, uten at departementet har erfart at det har oppstått noen interessekonflikt. Departementet vil også peke på at det ikke er uvanlig at etater med kontroll- og tilsynsansvar også har oppgaver av veiledningsmessig eller operativ karakter. En vesentlig del av de saker som NorCERT og VDI håndterer, er alvorlige IKT-angrep mot kritisk infrastruktur hvor fremmede stater kan stå bak. Denne type saker håndteres naturlig av etterretnings- og sikkerhetstjenestene. Gjennom en organisering av NorCERT og VDI i en av disse tjenestene, sikres et godt samarbeid og en god koordinering og informasjonsdeling mellom de ansvarlige aktører. En plassering av disse funksjonene utenfor EOS-tjenestene vil vanskeliggjøre en helhetlig tilnærming og informasjonsdeling knyttet til de mest alvorlige hendelsene. Dette vil kunne svekke vår nasjonale evne til håndtering av slike hendelser. Departementet mener på denne bakgrunn at NorCERT og VDI i dag er riktig organisatorisk plassert, og at dette også bør forankres i lov. Departementet er av den oppfatning at de nærmere rammer for utøvelse av funksjonen, herunder samarbeidet med de øvrige EOS-tjenestene og de sektorvise responsmiljøene, nærmere bør reguleres i forskrift.

I høringsforslaget var forslaget til ny bokstav e i § 9 utformet:

> «drive en nasjonal responsfunksjon for alvorlige dataangrep mot samfunnskritisk infrastruktur og et nasjonalt varslingssystem for digital infrastruktur.»

Departementet har endret «samfunnskritisk infrastruktur» til «kritisk infrastruktur», slik at det er i tråd med legaldefinisjonen i § 3, se punkt 11.3.2 og 11.4.7. Endringen er imidlertid ikke ment å innebære en realitetsforskjell.

Departementet har som opplyst i høringsnotatet, vurdert om det bør etableres en hjemmel for å kunne pålegge enkelte virksomheter med kritisk infrastruktur en tilknytning til VDI. Departementet ser at det er argumenter for en slik ordning, men har registrert innvendinger mot en generell hjemmel fra flere av høringsinstansene. Departementet har kommet til at et slikt pålegg må utredes nærmere. Spørsmålet bør dessuten ses i sammenheng med en vurdering av den framtidige finansieringsmodellen for NorCERT og VDI. Departementet vil derfor komme tilbake til dette spørsmålet ved en senere anledning.

7 Behandling av personopplysninger

7.1 Gjeldende rett

Behandling av personopplysninger i forbindelse med nasjonal responsfunksjon for alvorlige dataangrep mot samfunnskritisk infrastruktur (NorCERT) og varslingssystem for digital infrastruktur (VDI) hjemles i dag i personopplysningsloven § 8 første ledd bokstav f. Formålet med behandlingen er deteksjon og håndtering av alvorlige dataangrep mot kritisk infrastruktur. Det er derfor lagt til grunn at det foreligger en berettiget interesse som overstiger personvernulempen ved behandlingen.

Sjef for Nasjonal sikkerhetsmyndighet (NSM) har fastsatt en etatsintern instruks for utøvelsen av NorCERT og VDI. Instruksen skal bidra til forsvarlige rammer for gjennomføringen, deriblant ivareta personvernet. Av instruksen følger det at NSM som hovedregel kun skal behandle personopplysninger i avidentifisert form. NSM skal således ikke kople metadata med andre opplysninger, slik at de kan knyttes til identifiserbare enkeltpersoner.

NSMs behandling av opplysninger skjer videre i full åpenhet mot de virksomheter hvor VDI-sensorer er utplassert. Av avtalen som inngås med virksomhetene, følger det at virksomheten har rett til fullt innsyn i sensorenes konfigurering og de dataene som innsamles. I avtalen fastsettes en strengt formålsstyrt bruk av den informasjon som registreres. Formålet med avtalen er å styrke den nasjonale evnen til å forebygge og håndtere alvorlige IKT-baserte hendelser. Deltakende virksomheter er videre gjort kjent med at informasjon kan bli delt med Etterretningstjenesten og Politiets sikkerhetstjeneste innenfor dette formålet. Informasjon vil for øvrig ikke bli delt med tredjeparter uten virksomhetens forutgående samtykke. I avtalen er det inntatt som en plikt for den deltakende virksomhet å påse at avtalen implementeres på en slik måte at de ansattes rettigheter ivaretas. Det er etablert en egen rutine, ved avvik som medfører at personopplysninger blir registret i større omfang enn beskrevet ovenfor. I disse tilfellene vil NSM loggføre hendelsen, informere virksomheten om hendelsen, vurdere omkonfigurering av systemet for å unngå gjentakelser, samt slette all overskuddsinformasjon innen 24 timer etter at hendelsen er oppdaget. De loggførte avvikene vil bli lagt fram for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjenestene (EOS-utvalget) under utvalgets løpende inspeksjoner av NSM.

I de tilfeller der det har inntruffet en alvorlig hendelse, og NSM får digitale lagringsmedier til analyse, inngås det en bistandsavtale med virksomheten hvor denne samtykker til analysen, og hvor rammene for NorCERTs behandling av informasjonen nærmere reguleres.

EOS-utvalget skal påse at EOS-tjenestene utfører sine oppgaver innenfor rammene av lov og annet regelverk, at det ikke øves urett mot noen, og at det ikke nyttes mer inngripende midler enn det som er påkrevd etter forholdene. EOS-utvalget inspiserer NSM fire ganger i året. En av disse kontrollene har de siste årene vært dedikert til den del av virksomheten som utøver NorCERT og VDI. EOS-utvalget har i sin kontroll tilgang til all informasjon som behandles av NSM, og kan kreve tilgang til alle relevante systemer.

7.2 Høringsforslaget

I høringsnotatet foreslo departementet en ny og selvstendig hjemmel i sikkerhetsloven § 10 a om Nasjonal sikkerhetsmyndighets adgang til å behandle personopplysninger. Forslaget som ble sendt på høring hadde følgende ordlyd:

> «§ 10 a Behandling av personopplysninger
>
> Nasjonal sikkerhetsmyndighet kan behandle personopplysninger når dette er nødvendig for å utføre de oppgaver som følger av § 9 første ledd e. Opplysninger som behandles skal være korrekte, oppdaterte, tilstrekkelige og relevante for formålet med behandlingen. Opplysningene kan kun benyttes til det formål de er innhentet for. Opplysningene skal ikke lagres lenger enn det som er nødvendig for å oppfylle formålet med behandlingen.

Kongen kan gi nærmere bestemmelser om Nasjonal sikkerhetsmyndighets behandling av personopplysninger.»

Personopplysningsloven § 8 oppstiller ulike grunnlag for å behandle personopplysninger. I tillegg til ved samtykke gitt av den registrerte, kan personopplysninger behandles dersom det er fastsatt i lov og behandlingen er nødvendig for å oppfylle nærmere angitte formål. Departementet påpekte i høringsnotatet at formålet med NorCERT- og VDI-funksjonene *ikke* er å samle inn personopplysninger. Likevel er det ikke til å unngå at slike opplysninger blir behandlet som ledd i å vareta oppgavene knyttet til detektering, varsling og koordinering av håndteringen av alvorlige IKT-angrep. Departementet mente at det særlig gjelder personopplysninger som er en del av trafikkdata, men også i noen utstrekning innholdsdata. Av høringsnotatet framgår det på side 17:

«I forslag til ny § 10 a første ledd etableres det et klart hjemmelsgrunnlag for Nasjonal sikkerhetsmyndighets behandling av personopplysninger i forbindelse med drift av VDI- og NorCERT-funksjonene. Bestemmelsen tar sikte på å forsterke hjemmelsgrunnlaget for den behandlingen av personopplysninger som skjer i dag.

Departementet legger til grunn at personopplysningsloven kommer til anvendelse for behandlingen av personopplysninger, men likevel slik at unntakene i personopplysningsloven § 23 første ledd a (om unntak fra rett til innsyn og plikt til å gi informasjon av hensyn til rikets sikkerhet mv), og personopplysningsforskriften § 1-2 første ledd (om behandling av personopplysninger som er nødvendig av hensyn til rikets sikkerhet) også kommer til anvendelse. Personopplysninger vil under enhver omstendighet bli behandlet og oppbevart med minimum de sikkerhetskrav som følger av personopplysningsloven.

Departementet forutsetter at nærmere bestemmelser om behandling av personopplysninger innenfor de rammene som her er satt, fastsettes i forskrift. Det foreslås derfor et nytt andre ledd som gir hjemmel til å lage utfyllende regler i forskrift.»

7.3 Høringsinstansenes syn

Høringsinstansene støtter gjennomgående NSMs adgang til å behandle personopplysninger i forbindelse med drift av NorCERT og VDI. *Etterretningstjenesten* uttaler:

«Etterretningstjenesten kan ikke understreke sterkt nok at cybertrusselen mot Norge og norske interesser har økt betydelig og vil øke ytterligere, jf. tjenestens vurderinger i FOKUS 2015 s. 83 flg., og at landets samlede evne til å avdekke, motvirke og håndtere de mest alvorlige cyberhendelser krever sanntids og kontinuerlig informasjonsutveksling og samarbeid mellom EOS-tjenestene, både gjennom cyberkoordineringsgruppen (CKG) og øvrige mekanismer mellom tjenestene. Dersom det kan reises tvil om tjenestene kan utveksle relevant informasjon seg imellom for dette formål, både i form av rådata og i form av bearbeidede data og uavhengig av hvorledes tjenestene har kommet i besittelse av slike data, vil dette svekke myndighetenes deteksjons- og håndteringsevne.

Etterretningstjenesten mener derfor at prinsippet om at NSMs responsfunksjon skal basere seg på koordinert innsats og informasjonsdeling med de øvrige EOS-tjenestene må lovfestes sammen med lovfestingen av selve responsfunksjonen.»

Difi synes det er positivt at NSMs grunnlag for behandling av personopplysninger klargjøres og at det gis utfyllende regler i forskrift:

«Ut fra høringsnotatet er det noe uklart om det blir noen endring i behandling av innholdsdata. Det kan med fordel komme klarere frem om dette bare er en lovfesting av dagens praksis eller om det innebærer en utvidelse. Dersom opplysninger skal kunne deles med andre EOS tjenester bør det komme klart fram, enten direkte i § 10a eller i forskriften.»

KRIPOS mener en klar rettslig regulering av NSMs behandling av personopplysninger vil skape en langt bedre forutberegnelighet for den enkelte, og samtidig klargjøre adgangen til behandling av informasjon i langt større grad enn at det må foretas en skjønnsmessig vurdering etter personopplysningsloven § 8 f.

Flere høringsinstanser etterlyser imidlertid en nærmere konkretisering av hjemmelsgrunnlaget, og nærmere redegjørelse for hvilke behandlingsformer som er aktuelle.

Datatilsynet støtter i utgangspunktet en lovfesting av NSMs adgang til å behandle slike data, men mener at lovhjemmelens utforming har enkelte svakheter:

> «Hjemmelen er lite konkret, den mangler nærmere angivelser av hvilke behandlingsformer og hvilke personopplysningskategorier som er tenkt omfattet. Dermed fremstår den i realiteten som en in blanco-fullmakt for innsamling, registrering, lagring, analyse, sammenstilling og utlevering (samt alle andre tenkelige behandlingsformer, jf. personopplysningsloven § 2 nr. 2) av et uinnskrenket antall datakategorier. På bakgrunn av høringsnotatet er det dessuten vanskelig å forutse omfanget av enkeltindivider som vil bli berørt.
>
> […]
>
> Høringsnotatet burde ha gitt en fyldigere analyse av sakens faktiske sider, og de konsekvenser som kan tenkes å følge etter en eventuell lovendring. Ettersom lovforslaget ifølge departementet innebærer en kodifisering av eksisterende praksis, burde det ha vært mulig å dele av de erfaringene som er høstet så langt. (…) Departementet gjentar flere steder at formålet med datainnsamlingen ikke er å behandle personopplysninger. Likevel er det klart at både metadata og innholdsdata vil bli lagret og analysert. Begge kategoriene kan etter omstendighetene være å regne som personopplysninger i personopplysningslovens forstand. En vurdering av tiltakenes nødvendighet og proporsjonalitet er derfor på sin plass også her. Som nevnt over, forutsetter dette en klar fremstilling både av fakta og av følger.»

Nkom uttaler at et sentralt spørsmål ved sikkerhetsmessig overvåking av denne type er eventuelle begrensninger i bruk av overskuddsinformasjon:

> «Hva som aktivt kan søkes etter og analyseres følger av lovens formålsbegrensning og det konkrete forslaget til ny § 9 første ledd bokstav e. Det er imidlertid sannsynlig at man i dette arbeidet vil komme over informasjon om for eksempel straffbare forhold som ikke utgjør en fare for samfunnskritisk infrastruktur som sådan. Det vil slik Nkom ser det vesentlig svekke legitimiteten til VDI dersom slik informasjon overføres fra NorCERT til andre myndigheter.»

For *NRK* er det avgjørende spørsmålet om dagens begrensning i tilgang til innholdsdata i praksis blir videreført eller ikke, m.a.o. om lovendringen innebærer en oppmykning av NSMs adgang til å innhente personopplysninger/innholdsdata:

> «NRK mener likevel det er grunn til å reise spørsmål om §§ 9 første ledd bokstav e og 10 a kan åpne opp for en mer generell adgang til å innhente innholdsdata.»

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

> «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)».

7.4 Departementets vurderinger

Forslaget til ny § 10 a er utelukkende en kodifisering av gjeldende praksis, og en forsterkning av hjemmelsgrunnlaget for behandling av personopplysninger som Nasjonal sikkerhetsmyndighet (NSM) har hatt adgang til siden varslingssystem for digital infrastruktur (VDI) ble etablert i 1999. I tråd med gjeldende praksis er behandling av personopplysninger i forbindelse med Nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur (NorCERT) og VDI, tydelig avgrenset til det som er nødvendig for å detektere, verifisere, analysere og håndtere alvorlige IKT-angrep mot kritisk infrastruktur.

En rekke høringsinstanser stiller likevel spørsmål om forslaget innebærer en utvidet adgang til å behandle innholdsdata. Departementet presiserer at det *ikke* tas sikte på å innføre hjemmel for behandling av personopplysninger ut over hva som allerede behandles i dag. Departementet er imidlertid enig med høringsinstansene i at rammene for behandlingen bør tydeliggjøres.

Respekten for privatlivets fred er nedfelt i Grunnloven § 102 og Den europeiske menneskerettighetskonvensjon (EMK) artikkel 8. EMK

artikkel 8 nr. 1 beskytter retten til privatliv, familieliv, hjem og korrespondanse, og legger skranker på offentlige myndigheters inngripen i disse rettigheter. EMK artikkel 8 nr. 2 åpner imidlertid for at offentlige myndigheter kan gjøre inngripen i rettighetene dersom inngrepet har hjemmel i lov, ivaretar nærmere angitte formål, og er «nødvendig i et demokratisk samfunn» for å oppfylle ett eller flere av de legitime formålene, som for eksempel nasjonal sikkerhet.

Hensikten med NorCERT og VDI er å innhente, analysere og dele informasjon om angrep mot kritisk infrastruktur. Formålet med behandlingen er å identifisere angrep, og å kunne analysere slike når de har inntruffet. For å ivareta sine oppgaver har NSM ikke behov for identifiserbare personopplysninger. NorCERT og VDI behandler i det alt vesentlige bare avidentifiserte «metadata». Det er derfor uten interesse for NSM å sammenstille metadata med andre data slik at disse kan knyttes til identifiserbare enkeltindivider. I forlengelsen av dette bemerker departementet at formålet med ordningen på ingen måte innebærer et inngrep i pressens kildevern.

Gjennomføringen av NorCERT og VDI kan imidlertid i ytterste konsekvens innebære behandling av identifiserbare personopplysninger. Behandling av identifiserbare personopplysninger kan skje når det registreres begrenset mengde innholdsdata (pakkedump) i forbindelse med utløste alarmer i VDI, eller når NSM får utlevert lagringsmedier og logger for analyse. NSMs formål med behandlingen vil imidlertid utelukkende være å analysere det inntrufne angrepet, og begrense konsekvensene av dette. I de tilfeller hvor NSM bistår virksomheter i analyse av logger eller infiserte maskiner, skjer dette etter samtykke fra, og i samarbeid med, den berørte virksomhet. Av 17 662 utløste alarmer i 2014, inneholdt 5 alarmer fragmenter av lesbart innhold, og som utgjorde identifiserbare personopplysninger. Disse ble håndtert i henhold til gjeldende rutiner, og protokollført. Departementet vil også understreke at det er full åpenhet mellom virksomheten og NSM knyttet til konfigurering av sensorene og den informasjon disse skal registrere, samt at EOS-utvalget fører løpende kontroll med NSMs virksomhet.

Oppgavene som ivaretas av NorCERT og VDI er en forutsetning for vår nasjonale evne til å ivareta sikkerheten knyttet til våre mest kritiske systemer og funksjoner. Ivaretakelse av den nasjonale sikkerheten er et legitimt formål etter EMK art. 8 nr. 2. Oppgavene kan ikke ivaretas uten behandling av opplysninger, herunder også personopplysninger. Behandling av personopplysninger framstår derfor som nødvendig.

I proporsjonalitetsvurderingen må det tas hensyn til at sterke samfunnsmessige interesser tilsier en høy grad av nasjonal deteksjonsevne knyttet til digitale angrep. NSM har erfart at nettverksoperasjoner stadig blir mer målrettede og avanserte. Manglende deteksjons- og håndteringsevne vil kunne lette fremmede staters etterretningsaktivitet, og svekke vår nasjonale evne til å beskytte vår mest kritiske informasjon, IKT- infrastruktur og andre samfunnsviktige funksjoner.

Informasjonsdeling er en grunnleggende forutsetning for Norges nasjonale evne til å håndtere alvorlige IKT-angrep. Begrepet behandling av personopplysninger omfatter også utlevering, jf. personopplysningsloven § 2 første ledd nr. 2. NorCERT er avhengig av å motta informasjon for å kunne forebygge, avdekke og håndtere hendelser. Informasjonen må kunne deles med et bredt spekter aktører for at formålet med responsfunksjonen skal kunne ivaretas. For å håndtere de mest alvorlige angrep, hvor fremmede stater kan stå bak, er det nødvendig å etablere informasjonsflyt mellom EOS-tjenestene. For å sette sektorene og virksomhetene i stand til å håndtere enkelthendelser og beskytte sine systemer, må informasjon også kunne deles med sektorvise responsmiljøer, virksomheter og andre berørte aktører. Det vil ikke bli utlevert informasjon til andre aktører der dette ikke er i samsvar med NorCERT og VDIs formål. Forutsetningen for utlevering av informasjon er at denne benyttes innenfor rammene av formålet med NorCERT og VDI. Opplysningene kan kun benyttes til det formål de er innhentet for, jf. personopplysningsloven § 11.

Opplysninger som fremkommer i forbindelse med NorCERT og VDI kan bare benyttes til forebygging, deteksjon og håndtering av alvorlige dataangrep mot kritisk infrastruktur. Dette innebærer at overskuddsinformasjon om andre forhold i en virksomhet verken blir oppbevart eller utlevert. Det vil være naturlig at de nærmere detaljer, blant annet for utlevering og sletting av personopplysninger, fastsettes i forskrift.

Ut fra informasjonen som registreres, og formålet med behandlingen, representerer dette etter departementets oppfatning ikke en trussel mot de verdier som EMK artikkel 8 og Grunnloven § 102 skal verne. Departementet har etter en konkret avveining kommet til at en eventuell behandling av identifiserbare personopplysninger er nødvendig for å ivareta Norges nasjonale evne til å håndtere alvorlige IKT-angrep.

Departementet har gjort lovhjemmelen i forslag til ny § 10 a mer tilgjengelig, klar og presis enn den var i høringsrunden. I første ledd bokstav a til d presiserer departementet hvilke kategorier personopplysninger som kan behandles:

> «Når det er nødvendig for å utføre oppgavene etter § 9 første ledd bokstav e, kan Nasjonal sikkerhetsmyndighet behandle personopplysninger i form av
>
> a. metadata om IKT-trafikk til og fra virksomheter som er knyttet til det nasjonale varslingssystemet for digital infrastruktur
> b. informasjon som er nødvendig for å analysere utløste alarmer i varslingssystemet
> c. IP-adresser mottatt fra nasjonale og internasjonale samarbeidspartnere
> d. logger og infisert maskinvare, etter samtykke fra en virksomhet der dette er nødvendig i forbindelse med bistand til håndtering av alvorlige dataangrep.»

I andre ledd angir departementet i hvilket andre tilfeller personopplysninger kan behandles og stiller krav til behandlingen:

> «I andre tilfeller enn nevnt i første ledd, kan personopplysninger også behandles når dette er strengt nødvendig for å ivareta oppgavene etter § 9 første ledd bokstav e, og behandlingen etter en konkret vurdering framstår som både nødvendig og proporsjonal i forhold til det inngrepet den representerer i personvernet.»

Grunnkravene i personopplysningsloven § 11 gjelder ved behandling av personopplysninger etter forslag til ny § 10 a. Departementet er derfor enig med Datatilsynet i at det blir overflødig å gjengi innholdet i personopplysningsloven § 11 i forslaget til ny § 10 a første ledd andre til fjerde punktum. Departementet mener at en slik dobbeltregulering vil være uheldig, og kan skape usikkerhet om tolkningen av bestemmelsen. På bakgrunn av dette viderefører departementet ikke § 10 a første ledd andre til fjerde punktum fra høringsforslaget. Forslaget lød:

> «Opplysninger som behandles skal være korrekte, oppdaterte, tilstrekkelige og relevante for formålet med behandlingen. Opplysningene kan kun benyttes til det formål de er innhentet for. Opplysningene skal ikke lagres lenger enn det som er nødvendig for å oppfylle formålet med behandlingen.»

Departementet har imidlertid vurdert om det i stedet bør henvises til personopplysningsloven § 11 i forslaget til ny § 10 a, og kommet til at det vil være overflødig.

For øvrig presiseres det at forslaget til ny § 10 a ikke er ment å representere en innskrenkning i NSMs adgang til å behandle personopplysninger i andre tilfeller enn de som er nevnt i § 9 første ledd bokstav e.

8 Sikkerhetsmessig overvåking av godkjente informasjonssystemer

8.1 Gjeldende rett

Ondsinnet programvare blir mer avansert, og utgjør i økende grad en trussel også mot de godkjente informasjonssystemene. Godkjente informasjonssystemer er systemer som er godkjent for behandling av sikkerhetsgradert informasjon.

Utviklingen medfører et økende behov for at virksomhetene sikkerhetsmessig overvåker sine godkjente informasjonssystemer. Slik overvåking er et viktig verktøy for å avdekke sikkerhetstruende hendelser mot systemet. Med sikkerhetstruende hendelser menes sikkerhetstruende virksomhet, kompromittering av skjermingsverdig informasjon og grove sikkerhetsbrudd, jf. forskrift om sikkerhetsadministrasjon § 1-2 nr. 2. Sikkerhetsmessig overvåking av godkjente informasjonssystemer innebærer både logging, automatiserte alarmer, så vel som manuell sammenstilling og analyse av data relatert til sikkerhetstruende hendelser.

Reguleringen av sikkerhetsmessig overvåking av godkjente informasjonssystemer framgår ikke direkte av sikkerhetsloven i dag, men følger av informasjonssikkerhetsforskriften § 5-2. Her går det fram at sikker drift og vedlikehold er et av hovedmålene for sikkerheten i godkjente informasjonssystemer. Informasjonssystemet skal da kontinuerlig overvåkes for sikkerhetstruende hendelser, jf. første ledd nr. 2 c i bestemmelsen.

8.2 Utenlandsk rett

I Sverige er det gitt bestemmelser om sikkerhetsmessig overvåking av informasjonssystemer i «Försvarsmaktens föreskrifter om säkerhetsskydd». Etter kapittel 7 § 11 skal systemer som håndterer sikkerhetsgradert informasjon være gjenstand for sikkerhetslogging. Etter § 14 skal det etableres mekanismer som beskytter mot inntrengning i systemet og som muliggjør detektering av dette. I § 15 kreves det etablert sikkerhetsfunksjonalitet som beskytter mot ondsinnet kode. Tilsvarende bestemmelser er gitt i kapittel 4 i «Rikspolisstyrelsens föreskrifter och allmänna råd om säkerhetsskydd».

Det britiske «Security Policy Framework» stiller som et obligatorisk krav at det skal implementeres tekniske kontrollmekanismer i alle informasjonssystemer. Disse skal være proporsjonale med verdien, viktigheten og sensitiviteten av informasjonen som behandles i systemet. Blant de tiltak som skal vurderes implementert, er policy for innholdskontroll og forebyggende systemovervåking. Videre skal det etableres systemer for administrasjon av brukerkontoer for å sikre individuell ansvarlighet for handlinger i systemet. I NATO behandles sikkerhetsmessig overvåking i dokumentet «AC/35-D/2004 Primary Directive on CIS Security». Det stilles krav om at systemeierne skal implementere prosedyrer og systemer som kan detektere og reagere på sikkerhetstruende hendelser i IKT-systemene.

8.3 Høringsforslaget

8.3.1 Innledning

Departementet foreslo i høringsnotatet en ny bestemmelse i sikkerhetsloven om virksomhetens egen adgang til sikkerhetsmessig overvåking av godkjente informasjonssystemer. Siden sikkerhetsmessig overvåking av IKT-systemer har klare grenseflater mot enkeltindividets personvern, mente departementet at det burde ha en klar hjemmel i lov. Hjemmelsgrunnlaget blir med det klarere, og den økte betydningen synliggjøres. Departementet påpekte at forslaget i stor grad er en videreføring av eksisterende regler i forskrift om informasjonssikkerhet og gjeldende praksis for sikkerhetsmessig overvåking av informasjonssystemer. Forslaget innebærer i utgangspunktet ikke noen vesentlig utvidelse av omfanget av tillatt overvåking. Departementet skriver på side 9 i høringsnotatet:

> «Sikkerhetsmessig overvåking av godkjente informasjonssystemer gjøres for å ivareta høy grad av sikkerhet i systemene og for å hindre

eller begrense omfanget av en kompromittering i systemene. En vesentlig del av forslag til ny § 13 a er derfor ment som en klargjøring og presisering av virksomhetens egen rett og plikt til å utøve kontroll med godkjente informasjonssystemer. Det etableres derfor en klar hjemmel for sikkerhetsmessig overvåking hvor behandling av personopplysninger også kan inngå. Departementet understreker at behandling av personopplysninger som følge av sikkerhetsmessig overvåking av inn- og utgående kommunikasjon, fortsatt vil måtte skje i tråd med grunnleggende prinsipper i arbeidsmiljøloven og personopplysningsloven.»

Systemer som er godkjent i henhold til sikkerhetsloven § 13, behandler informasjon som kan ha skadefølger for rikets sikkerhet eller andre vitale nasjonale sikkerhetsinteresser, dersom den blir kjent for uvedkommende. Slik informasjon må ha en høy grad av beskyttelse. Gitt de potensielt store skadefølgene, la departementet til grunn at den inngripen som sikkerhetsmessig overvåking kan medføre, må anses å ligge innenfor personopplysningslovens ramme.

Forslaget som ble sendt på høring hadde følgende ordlyd:

«§ 13 a Sikkerhetsmessig overvåking av godkjente informasjonssystemer

Den enkelte virksomhet skal kontinuerlig overvåke godkjente informasjonssystem for sikkerhetstruende hendelser, fortrinnsvis ved bruk av automatisert systemovervåking. Sikkerhetsrelevante hendelser skal registreres.

Når informasjon utveksles mellom systemer, på tvers av autorisasjonsskiller, eller til bærbare lagringsmedier, skal informasjonen som utveksles registreres og lagres.

Der flere virksomheter er tilknyttet samme informasjonssystem, kan en virksomhet etter avtale med de andre virksomhetene forestå overvåking og registrering i henhold til første og andre ledd på vegne av den ansvarlige virksomhet.

Med mindre annet er bestemt, skal informasjon registrert etter første ledd lagres i fem år.

Informasjon som nevnt i første og andre ledd skal kun benyttes til formål om å håndtere sikkerhetstruende hendelser.

Den enkelte virksomhet skal påse at autoriserte brukere av informasjonssystemer som overvåkes i henhold til denne bestemmelse får informasjon om formålet med behandlingen, om de tiltak som er iverksatt, om informasjonen vil bli utlevert, og eventuelt hvem som er mottaker.

Kongen kan gi nærmere bestemmelser om sikkerhetsmessig overvåking av informasjonssystemer, herunder om hvilke typer data som kan eller skal registreres og lagres, lagringstid for registrerte data, hvem som skal kunne gis tilgang til de lagrede data og hvordan tilgang skal gis.»

8.3.2 Overvåking

Forslag til første ledd i ny § 13 a er en videreføring av §§ 5-2 c og 5-3 e i forskrift om informasjonssikkerhet. Her oppstilles hovedregelen om at informasjonssystemer som er godkjent i henhold til § 13, kontinuerlig skal overvåkes for sikkerhetstruende hendelser. Departementet presiserte i høringsnotatet at slik overvåking ikke trenger å måtte utføres av personell. Det bør tvert om tilstrebes at overvåkingen skjer ved hjelp av automatiserte prosesser. Sikkerhetsrelevante hendelser skal den virksomhet som behandler skjermingsverdig informasjon registrere og følge opp.

8.3.3 Registrering og lagring

Forslag til andre ledd i ny § 13 a gir hjemmel for å overvåke og registrere utveksling (import og eksport) av data mellom interne systemer, mellom interne og eksterne systemer, på tvers av autorisasjonsskiller, eller til bærbare lagringsmedier. Med autorisasjonsskiller menes her utveksling av informasjon mellom systempartisjoner som behandler ulike autorisasjonsområder, for eksempel HEMMELIG og NATO SECRET, samt ulike graderingsnivåer, for eksempel BEGRENSET og ugradert, jf. forskrift om informasjonssikkerhet § 5-7 første ledd nr. 3 og 4. I høringsnotatet skriver departementet på side 10:

«Registrering og analyse av trafikk- og innholdsdata vil ofte være nødvendig for å oppdage kompromittering av et informasjonssystem. Det er videre trolig eneste mulighet for å kunne fastslå skadeomfang, og å oppdage den eller de ansvarlige med hensyn til slik kompromittering. Et eksempel på viktige trusler som adresseres er såkalt Advanced Persistent Threat (APT), hvor avanserte angripere gjennomfører langvarige angrep. Angriperne stjeler data fra kompromitterte brukerkonti og sender disse dataene i skjul over nettverket til maskiner på utsiden av systemet. Et annet eksempel er at minnepinner eller andre bær-

bare lagringsmedier misbrukes til å stjele store volum med graderte data, enten som en bevisst handling fra en utro bruker, eller gjennom ondsinnet programvare.

Analyse av utvekslede trafikk- og innholdsdata kan avsløre angriperens kommandoer som sendes inn i nettverket, skjulte datastrømmer som sendes ut av nettverket og uvanlig bruk av minnepinner. Omfanget av loggingen og analysemetoder vil være avhengig av blant annet trusselen mot systemet, det operative miljøet og informasjonens graderingsnivå. Omfanget og analysemetodene vil også kunne forandre seg over tid, avhengig av den tekniske utviklingen og utviklingen med hensyn til trusselbildet og angrepsmetoder. Departementet mener det er viktig at bestemmelsen åpner for slik fleksibilitet, slik at tiltaket ikke raskt blir utdatert og med det mister sin relevans.»

Departementet vurderte særlig personvernhensyn i forbindelse med forslag til nytt andre ledd, og av høringsnotatet framgår det videre:

«For å ivareta personvernhensyn knyttet til registrering, overvåking og analyse av brukerdata må virksomheten, eventuelt systemeier på vegne av virksomheten, implementere forsvarlige rutiner for behandling av opplysningene. Hvilke tiltak som vil være forsvarlige, avhenger av hva slags informasjon som behandles. Et mulig tiltak er overføring av sensitive loggdata til egne lagringsservere som er øremerket for dette formålet. Videre kan det innføres tomannsregel for interaktiv tilgang til slike loggdata, f.eks. ved at personene som utfører virksomhetens kontroll deler en brukerkonto for dette arbeidet og har hver sin del av passordet. Det kan også innføres nærmere angitte forutsetninger for interaktiv tilgang til slike loggdata, f.eks. ved at det skal foreligge en godkjenning fra særskilte personer for hver runde med interaktive søk som igangsettes. Når personvernhensynene vurderes, må det også legges vekt på at brukerne som får tilgang til opplysninger er særlig trente i å håndtere sensitiv informasjon og er godt informert om hvordan sikring av slik informasjon skal skje. Departementet viser også til forholdsmessighetsprinsippet i sikkerhetsloven § 6 første ledd om at det ikke skal brukes mer inngripende midler og metoder enn det som framstår som nødvendig. Behovet for omfanget av registrering og lagring av data kan være mindre på lavgraderte systemer enn på de høyere graderte systemer. Departementet legger til grunn at utfyllende bestemmelser vil bli gitt i forskrift eller veiledning, slik at loggeomfanget her nærmere kan tilpasses de ulike systemers sikkerhetsbehov.»

8.3.4 Overvåking på vegne av andre

Forslag til tredje ledd i ny § 13 a regulerer de tilfeller der flere virksomheter er tilknyttet samme informasjonssystem. I slike tilfeller kan systemeier etter avtale med den enkelte virksomhet forestå overvåking og registrering på vegne av den ansvarlige virksomhet. Systemeier bør alltid påse at den enkelte virksomhet som bruker informasjonssystemet er kjent med kravene til informasjonssystemets sikkerhet, herunder kravene til sikkerhetsovervåking og registrering av sikkerhetsrelevante hendelser, og at relevante tiltak er iverksatt.

8.3.5 Lagringstid og formålet med behandlingen

Forslag til fjerde ledd i ny § 13 a viderefører bestemmelsen i § 5-18 i forskrift om informasjonssikkerhet. Det innebærer at informasjon som er registrert etter første ledd skal lagres i minst fem år.

Forslag til femte ledd angir hvilke formål den registrerte informasjonen kan benyttes til. Informasjonen kan bare benyttes til håndtering av sikkerhetstruende hendelser. For disse formål kan det være behov for å utlevere hele eller deler av informasjonen også til Nasjonal sikkerhetsmyndighet, politiet og andre relevante virksomheter. Nærmere bestemmelser er gitt i forskrift om sikkerhetsadministrasjon.

8.3.6 Informasjon til brukerne

I forslag til sjette ledd i ny § 13 a pålegges virksomheten informasjonsplikt på tilsvarende måte som personopplysningsloven § 19. Etter departementets oppfatning kan det være hensiktsmessig å gi slik informasjon i autorisasjonssamtalen. Autorisasjonssamtale gjennomføres med alle som skal ha tilgang til graderte informasjonssystemer. Det legges til grunn at innsyn i opplysninger registrert i medhold av denne bestemmelsen ikke vil være av en slik art at reglene om innsyn i epostkasse mv. i personopplysningsforskriften kapittel 9 kommer til anvendelse. I den grad det er behov for å foreta tiltak som følge av aktivitet etter bestemmelsen ved å foreta innsyn i ansattes epostkasse med videre, skal imidlertid slikt innsyn

skje i overensstemmelse med reglene i personopplysningsforskriften kapittel 9. Overvåking av informasjonssystemer er også regulert i personopplysningsforskriften § 9-2 siste ledd. Behandling av personopplysninger i forbindelse med registrering av aktiviteter i informasjonssystemer er regulert i personopplysningsforskriften § 7-11. Behandling av opplysninger registrert i medhold av forslaget til den nye bestemmelsen i sikkerhetsloven, er ikke meldepliktig etter personopplysningsloven § 31 første ledd. Det presiseres videre at personopplysningsforskriftens bestemmelser nevnt foran, ikke kommer til anvendelse på sikkerhetsmessig overvåking som er regulert her.

8.3.7 Forskriftshjemmel

Forslag til sjuende ledd i ny § 13 a gir hjemmel til å gi nærmere bestemmelser i forskrift om sikkerhetsmessig overvåking av informasjonssystemer. Forskriften regulerer hvilke typer data som kan eller skal registreres, lagringstid for registrerte data, hvordan lagring skal skje, hvem som skal kunne gis tilgang til de lagrede data og hvordan tilgang skal gis. Oppregningen av hvilke forhold det kan gis nærmere bestemmelser om, er ikke uttømmende.

8.4 Høringsinstansenes syn

De fleste av høringsinstansene som har uttalt seg om bestemmelsen, støtter forslaget.

Advokatforeningen uttaler at foreningen har forståelse for de foreslåtte endringene i sikkerhetsloven:

> «Selv om forslaget innebærer økt omfang av overvåkning i tilknytning til godkjente informasjonssystemer, synes departementet å ha vurdert behovet grundig».

Nasjonal sikkerhetsmyndighet (NSM) uttaler:

> «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.»

Etter NSMs syn er det imidlertid behov for å tydeliggjøre at den sikkerhetsmessige overvåkningen bestemmelsen hjemler, utelukkende skal ha til formål å overvåke hendelser som kan utgjøre en fare for systemet eller informasjonen i systemet.

Datatilsynet er enig i at det bør etableres en klar hjemmel i lov for sikkerhetsmessig overvåking.

Enkelte høringsinstanser etterlyser imidlertid en grundigere og mer konkret analyse av problemstillingen, herunder en vurdering av tiltakets nødvendighet og proporsjonalitet. I den forbindelse uttaler Datatilsynet:

> «Vi tillater oss også å legge til at lovfesting er påkrevet fordi det sikrer legitimitet og forankring i folkestyret, og at vedtak i formell lovs form blir desto viktigere ved innføring av metoder som griper inn i borgernes grunnleggende menneskerettigheter. Slik legitimitet forutsetter en grundig drøfting og avveining av de interessene som står mot hverandre. Blant annet må lovgiver avklare forholdet til Grunnloven og de grunnleggende menneskerettighetene. Vi viser her til at den enkeltes rett til privatliv og kommunikasjon er vernet av Grunnloven § 102, jf. også Den europeiske menneskerettskonvensjonen (EMK) artikkel 8(1), som er inkorporert i norsk rett gjennom lov 21. mai nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven).
>
> [...]
>
> Tiltakenes nødvendighet og proporsjonalitet må også vurderes. Ifølge EMK artikkel 8 (2) kan offentlige myndigheter gripe inn i individets rettigheter etter artikkel 8 (1), under forutsetning av at det er 'nødvendig i et demokratisk samfunn', av hensyn til nærmere angitte tungtveiende interesser.»

Enkelte høringsinstanser peker videre på et behov for klargjøring av visse sider ved forslaget.

Etterretningstjenesten mener det bør klargjøres om lagringsplikten etter fjerde ledd også gjelder informasjon som utveksles mellom systemer og autorisasjonsskiller etter andre ledd. Behovet for å lovregulere lagringstid for innholdsdata registrert etter andre ledd, påpekes også av *Advokatforeningen. Nasjonal kommunikasjonsmyndighet (Nkom)* uttaler:

> «Hva gjelder annet ledd gir denne en plikt til å registrere og lagre informasjon som utveksles mellom systemer, mellom autorisasjonsskiller eller til bærbare lagringsmedier. Nkom har ikke kommentarer til plikten som sådan, men

er usikker på om det her menes at selve informasjonen som utveksles skal lagres.»

Cyberforsvaret og Forsvarets sikkerhetsavdeling (FSA) ser behov for å tydeliggjøre hvilke data begrepet sikkerhetsrelevante hendelser omfatter. De samme instanser påpeker også at registrering og lagring av informasjon som utveksles mellom systemer vil kunne være krevende og kostbart. De anbefaler derfor at denne plikten ikke gjøres absolutt. *Politidirektoratet* forstår bestemmelsen slik at den avskjærer muligheten til å benytte informasjonen fra overvåkningen av informasjonssystemet til en etterfølgende straffesaksbehandling. Politidirektoratet stiller derfor spørsmål ved at viktig bevismateriale fra overvåkning med sikkerhetsgraderte informasjonssystemer ikke kan benyttes til strafferettslige formål.

Cyberforsvaret stiller også spørsmål til begrensningene av informasjonsdeling, og foreslår at lovteksten utvides slik at det åpnes for deling av informasjon der hensikten er å forebygge sikkerhetstruende hendelser.

Flere av høringsinstansene advarer mot at den sikkerhetsmessige overvåkingen fortrinnsvis skal skje automatisert, og påpeker at automatiserte prosesser alene ikke er godt nok. En helautomatisk prosess kan gi en rekke feilkilder som både kan medføre at hendelser ikke oppdages, eller at det oppstår uberettiget mistanke om en hendelse.

8.5 Departementets vurderinger

For å kunne avdekke og kartlegge omfanget av sikkerhetstruende hendelser på en tilfredsstillende måte, er det blant annet en forutsetning at trafikk- og innholdsdata kan lagres. Lagring av innholdsdata er ikke klart regulert i dag. Departementet foreslår derfor en ny bestemmelse i sikkerhetsloven som klargjør rammene for den sikkerhetsmessige overvåkingen av godkjente informasjonssystemer som virksomhetene selv skal foreta.

Departementet har merket seg at Datatilsynet savner en grundigere og mer konkret analyse av interesseavveiningene, samt de foreslåtte tiltakenes nødvendighet og proporsjonalitet. Departementet vil innledningsvis presisere at forslaget er avgrenset til systemer som er godkjent for behandling av sikkerhetsgradert informasjon. Dette er systemer som er klare etterretningsmål, og som derfor må ha et høyt sikkerhetsnivå. Sikkerhetsmessig overvåking av disse systemene slik at angrep på et tidlig tidspunkt kan oppdages, og omfanget kartlegges, framstår derfor etter departementets vurdering som nødvendig.

De systemer som vil være gjenstand for overvåking etter forslagets § 13 er i mindre grad egnet til, eller beregnet for, kommunikasjon av privat karakter, eller annen type privat bruk. Dette er lukkede systemer uten direkte tilknytning til internett. Omfanget av privat kommunikasjon og privat bruk av disse systemene vil derfor være begrenset. Det vil likevel være slik at kommunikasjon av privat karakter vil kunne forekomme, da primært som e-post eller nettprat med videre, mellom brukerne i det lukkede systemet.

Forslagets grenseflater mot enkeltindividets personvern vil derfor i det alt vesentligste være knyttet til bruk av informasjonen som samles inn ved loggføring av aktivitet i systemene, samt registrering av innhold ved overføring av informasjon mellom ulike graderingsnivåer. Personvern knyttet til bruk av logger vil alltid være en sentral utfordring. Logger vil kunne si noe om hvem som har jobbet med hva, på hvilket tidspunkt. Dette er informasjon som kan ha interesse også i andre sammenhenger. Departementet mener derfor at loggene bare må inneholde informasjon som er strengt nødvendig for formålet, og at bruken av loggene bare skal nyttes til håndtering av sikkerhetstruende hendelser. Nasjonal sikkerhetsmyndighet (NSM) har i sin høringsuttalelse foreslått en presisering i lovteksten for å sikre nettopp den strenge formålsavgrensingen. Departementet støtter denne endringen, slik at bestemmelsens første ledd nå presiserer at man skal «overvåke godkjente informasjonssystemer for sikkerhetstruende hendelser mot informasjonssystemet eller informasjon i systemet». Departementet vil videre presisere at det ligger innenfor formålet at den registrerte informasjonen også kan benyttes i en etterforskningssak knyttet til en sikkerhetstruende hendelse i systemet.

I proporsjonalitetsvurderingen må det tas hensyn til at den informasjonen som behandles i systemet er av stor betydning for nasjonen Norge. Dette er informasjon som, dersom den kommer på avveie, vil kunne ha skadefølger for vår nasjonale sikkerhet.

Omfanget av systemer som blir gjenstand for sikkerhetsmessig overvåking etter § 13 a er også av et begrenset omfang. Det er kun et fåtall systemer i offentlig forvaltning som er godkjent for å behandle sikkerhetsgradert informasjon, og som således vil være underlagt kravene til sikkerhetsmessig overvåking i § 13 a. Sikkerhetsmessig overvåking vil bidra til at sikkerhetstruende hendelser kan identifiseres. Når slike forekommer,

skal loggingen gjøre virksomheten i stand til å foreta en vurdering av omfanget og karakteren av skaden som har oppstått, gjenopprette sikker tilstand, samt sikre sporbarhet og ansvarlighet for utførte handlinger i samsvar med kravene i sikkerhetsloven for øvrig. I samsvar med prinsippene i sikkerhetsloven § 6, vil omfanget av loggingen måtte bero på en konkret risikovurdering knyttet til det enkelte system, hvor det ikke benyttes mer inngripende tiltak enn nødvendig. Det vil være naturlig at omfanget av logging er større på høyt graderte systemer enn på de lavgraderte systemene.

Systemer som blir gjenstand for sikkerhetsmessig overvåking etter § 13 a blir videre administrert av sikkerhetsklarert personell som både forstår behovet for og betydningen av sikkerhetstiltak overfor denne type informasjon. Administratorer i disse systemene er også underlagt lovpålagte forpliktelser til å beskytte informasjonen som håndteres. I tillegg følger det av lovforslaget at alle brukere av disse informasjonssystemene skal informeres om den sikkerhetsmessige overvåking systemet er gjenstand for.

Departementet vil gi nærmere forskrifter om rammene for sikkerhetsmessig overvåking, og om tiltak for å sikre en forsvarlig behandling av de personopplysninger som registreres etter § 13 a.

Enkelte høringsinstanser har stilt spørsmål om innholdsdata vil bli lagret etter forslagets andre ledd. Formålet med dette leddet tilsier at også innhold må lagres. Dette er nødvendig for å kunne kartlegge skadeomfang ved en sikkerhetstruende hendelse. Registrering av metadata framstår ikke som tilstrekkelig, da det vil kunne åpne for manipulasjon.

Departementet legger til grunn at en lagringstid på 5 år også er påkrevd for informasjon som registreres etter andre ledd. De samme hensyn som tilsier lagring av loggdata i 5 år gjør seg gjeldende også her. Departementet har klargjørt forslaget til lovtekst på dette punktet. Oppbevaring av loggdata med videre i 5 år representerer ingen endring fra gjeldende rett, men innebærer kun en lovfesting av det som i dag følger av forskrift om informasjonssikkerhet § 5-18.

Loggingsplikten knytter seg til sikkerhetsrelevante hendelser. Som påpekt av blant annet Forsvarets sikkerhetsavdeling, er det ikke gitt noen legaldefinisjon av dette begrepet. Sikkerhetsrelevante hendelser vil omfatte den aktivitet i systemet som vil gjøre det mulig å identifisere en sikkerhetstruende hendelse og kartlegge omstendighetene rundt hendelsen når den inntreffer. Departementet finner det ikke hensiktsmessig å gi noen legaldefinisjon som uttømmende beskriver dette begrepet. For å sikre tilstrekkelig dynamikk i forhold til den teknologiske utviklingen, bør innholdet i dette begrepet nærmere operasjonaliseres i veiledninger fra NSM.

Departementet har vurdert forholdet til Den europeiske menneskerettighetskonvensjon (EMK) artikkel 8. Som redegjort for foran er de systemer som vil være gjenstand for sikkerhetsmessig overvåking etter § 13 a, i liten grad egnet for privat bruk. Den sikkerhetsmessige overvåking som iverksettes har på den andre siden en sterk forankring i nasjonale sikkerhetsbehov. Departementet mener således at tiltaket er forenlig med EMK artikkel 8.

Enkelte høringsinstanser stiller spørsmål ved hensiktsmessigheten av at systemovervåkingen etter lovforslaget primært skal være automatisert. Departementet vil påpeke at det i praksis ikke vil være mulig å gjennomføre sikkerhetsmessig overvåking fullt ut manuelt. Systemovervåking må primært skje ved bruk av automatiserte verktøy konfigurert spesielt for dette formålet. Der hendelser detekteres, vil disse være gjenstand for en manuell analyse. Etter departementets oppfatning bidrar automatiserte prosesser til at personvernulempen reduseres.

På bakgrunn av dette har departementet slått sammen forslagets § 13 a fjerde og femte ledd, samtidig som hjemmelen til å gi forskrift er presisert nærmere i nåværende sjette ledd.

9 Reduksjon av antall klareringsmyndigheter

9.1 Gjeldende rett

I henhold til sikkerhetsloven § 19 skal personkontroll og sikkerhetsklarering gjennomføres før en person gis tilgang til skjermingsverdig informasjon gradert KONFIDENSIELT eller høyere. For tilgang til informasjon gradert BEGRENSET kreves ikke sikkerhetsklarering, men vedkommende må være autorisert. Etter sikkerhetsloven § 23 er hvert enkelt departement klareringsmyndighet for personell innen sitt myndighetsområde. Myndigheten kan delegeres, og dette er i stor utstrekning gjort. Etter flere reduksjonsprosesser, sist i 2006, er det i dag totalt 42 klareringsmyndigheter. Av disse er 5 innenfor forsvarssektoren (deriblant Etterretningstjenesten og Nasjonal sikkerhetsmyndighet), 7 innenfor den dømmende makt (Høyesterett og lagmannsrettene), samt 3 innenfor Stortingets organer (Stortingets presidentskap, Stortingets administrasjon og Riksrevisjonen). I tillegg er Politiets sikkerhetstjeneste, som en av EOS-tjenestene (sammen med Etterretningstjenesten og Nasjonal sikkerhetsmyndighet), egen klareringsmyndighet. For øvrig er det 26 ulike sivile klareringsmyndigheter, som utgjøres av de enkelte departementene og enheter disse har delegert klareringsmyndighet videre til.

Klareringsmyndighetsstrukturen ble vurdert ved revisjonen av sikkerhetsloven i 2006, jf. Ot.prp. nr. 59 (2004–2005). Arbeidsgruppen som den gang ble nedsatt for å se på regelverket la fram tre forslag til klareringsmyndighetsstruktur:

1. En desentralisert modell med utgangspunkt i dagjeldende sikkerhetslov § 23,
2. To klareringsmyndigheter; en for sivil sektor og en for militær sektor,
3. En felles klareringsmyndighet.

Departementet konkluderte den gang med å beholde eksisterende struktur. Det ble likevel gitt klare føringer for at delegasjonspraksisen skulle strammes inn, jf. Ot.prp. nr. 59 (2004–2005) s. 30:

> «Departementet vil følgje med på den vidare utviklinga på dette feltet, og det vil bli ei sentral tilsynsoppgåve for Nasjonal sikkerhetsmyndighet å følgje opp etterlevinga av regelen i § 23. Det er naudsynt at departementa i tida framover strammar inn delegeringspraksisen. Dersom dette ikkje skjer, vil departementet eventuelt måtte sjå på andre strukturløysingar, også dei modellane om ei eller to klareringsstyringsmakter som er nemnde ovanfor.»

Departementets oppfordring om å stramme inn delegasjonspraksisen har imidlertid hatt en begrenset virkning, og antallet klareringsmyndigheter har ikke blitt vesentlig redusert etter denne lovrevisjonen.

9.2 Utenlandsk rett

I *Sverige og Danmark* tilligger det den enkelte virksomhet selv å sikkerhetsklarere eget personell. Ved sikkerhetsklarering i Sverige innhenter virksomheten informasjon fra de relevante registre, for deretter selv å fatte avgjørelse om personen skal sikkerhetsklareres. I Danmark er det styrelseschefen (etatssjefen) som fatter avgjørelse om sikkerhetsklarering. Etatssjefen klarerer også ansatte hos private leverandører som leverer til etaten. Klareringsavgjørelsen gjelder kun for arbeid i, og leveranser til, egen virksomhet.

I *Storbritannia* fattes avgjørelser i henhold til «Baseline Personnel Security Standard» (BPS) av den enkelte virksomhet. Avgjørelser om sikkerhetsklarering er imidlertid sentralisert. De fattes, med unntak for etterretnings- og sikkerhetstjenestene, av «Defence Business Services National Security Vetting» (DBS NSV).

9.3 Høringsforslaget

9.3.1 Hovedpunktene i forslaget

Departementet foreslo i høringsnotatet at det opprettes to klareringsmyndigheter; én for forsvarssektoren og én for sivil sektor, hvor henholdsvis Forsvarsdepartementet og Justis- og beredskapsdepartementet har det overordnede ansvaret. Forslaget medfører en betydelig reduksjon av antall klareringsmyndigheter, hvor den vesentligste end-

ringen er en sentralisering av klareringsmyndighetene innen sivil sektor. I forslaget ble det forutsatt at de tre EOS-tjenestene fortsetter å klarere eget personell, grunnet de særlige forhold som gjør seg gjeldende for disse tjenestene. Videre ble det åpnet for at andre enn EOS-tjenestene kan gis slik myndighet dersom særlige grunner tilsier det. Av konstitusjonelle hensyn la departementet til grunn at Stortinget, domstolene og Statsministerens kontor fortsatt opprettholdes som egne klareringsmyndigheter. Ideelt sett burde det for Stortinget og organer underlagt Stortinget, kun være én klareringsmyndighet. Det samme gjelder for domstolene. Av habilitetshensyn anså departementet det som hensiktsmessig at den sivile klareringsmyndigheten klarerer personellet i klareringsmyndigheten i forsvarssektoren, og vice versa.

EOS-utvalget har også pekt på at det i dag er for mange klareringsmyndigheter, og gitt uttrykk for at utvalget anser dette som uheldig. Departementet påpekte at formålet med forslaget er å øke kvaliteten og effektivisere saksbehandlingen av klareringssaker. Status i dag er fragmenterte og lite robuste fagmiljøer, hvor Nasjonal sikkerhetsmyndighet (NSM) fungerer som et «bindeledd» i kraft av sin rolle som klagebehandler og opplæringsansvarlig. Skjev fordeling av antall saker og mange enheter med klareringsmyndighet utfordrer kvaliteten og effektiviteten i saksbehandlingen. Departementet ga i høringsnotatet uttrykk for at dagens situasjonen ikke er tilfredsstillende.

I 2012 ble det totalt behandlet ca. 35 000 klareringssaker. Ved seks av klareringsmyndighetene ble det ikke registrert saker. 11 av klareringsmyndighetene var registrert med under 20 saker, mens to tredjedeler av klareringsmyndighetene (30) hadde færre enn 100 saker. I perioden 1.1.2007 – 23.5.2014 ble det fattet 247.208 vedtak i klareringssaker. En av klareringsmyndighetene hadde ingen saker i perioden, 24 av klareringsmyndighetene hadde et lavere snitt enn 100 saker i året og de 33 minste klareringsmyndighetene hadde samlet i perioden til sammen kun 6,92 % av sakene. Saksfordelingen i hele perioden var som følger:

Forsvarssektoren:	208 905 vedtak (84,51 % av den totale mengden)
Sivil sektor:	36 338 vedtak (14,70 % av den totale mengden)
Lovgivende makt:	1 707 vedtak (0,69 % av den totale mengden)
Dømmende makt:	162 vedtak (0,07 % av den totale mengden).

NSM har opplyst at det er gjennomført en rekke tilsyn med klareringsmyndighetene i 2013 og 2014. Tilsynene avdekket flere avvik knyttet til behandlingen av saker om sikkerhetsklarering. Avvikene skyldes primært mangel på kompetanse og erfaring innen fagfeltet. NSM har oppgitt at de fire vanligste og mest alvorlige feilene er følgende:

– Klareringsbehovet er ikke tilstrekkelig begrunnet og dokumentert,
– sakene er ikke tilstrekkelig opplyst,
– sikkerhetssamtale er ikke gjennomført, selv om dette var nødvendig, og
– det er utvist sviktende skjønn i vurderingene.

I høringsnotatet skriver departementet at kompleksiteten i sakene generelt øker, og at det stilles stadig større krav til kompetanse hos klareringsmyndighetene:

> «Eksempelvis er det langt flere personer med utenlandsk opprinnelse eller dobbelt statsborgerskap som skal klareres i dag enn tidligere. Dette vil igjen medføre behov for flere sikkerhetssamtaler. Videre vil det medføre behov for en generell styrking av kompetansen til saksbehandlerne. Kompetanse utvikles best gjennom konkret behandling av saker i et visst volum og i et større fagmiljø hvor man kan diskutere ulike problemstillinger og utveksle erfaringer. Gjennom et visst volum av saker vil man oppnå regelmessig befatning med ulike problemstillinger og vurderinger som skal gjøres. Videre er det viktig at den enkelte saksbehandler får tilstrekkelig erfaring fra arbeid med sikkerhetssamtaler for å vedlikeholde samtalekompetansen. Med bakgrunn i den begrensede mengden klareringssaker som sivil sektor har totalt sett, og den skjeve fordelingen av saker mellom et stort antall virksomheter, er det avgjørende for kvalitetshevingen at oppgavene og kompetansen samles og organiseres i én enhet.»

Etter å ha vurdert ulike alternativer, kom departementet i høringsnotatet til at hensynet til enhetlig saksbehandling, robuste fagmiljøer, individets rettssikkerhet og sikkerheten i forsvarssektoren og i sivil sektor, i størst grad blir ivaretatt ved etablering av to klareringsmyndigheter:

> «Ett alternativ er at det innføres et delegasjonsforbud fra departementene, noe som innebærer at hvert enkelt departement klarerer personell innenfor egen sektor. Et annet alternativ er at hvert enkelt departement delegerer

klareringsmyndigheten til én underlagt virksomhet med ansvar for sikkerhetsklareringer innenfor den sektoren som er departementets ansvarsområde. Svakheten med de to nevnte alternativene er at enkelte departement har så få klareringssaker at en sentralisering innenfor sektoren ikke vil gi det nødvendige sakstilfang for å opprettholde tilstrekkelig kompetanse. Et tredje alternativ, og som anbefales, er at det utpekes to klareringsmyndigheter, én for sivil sektor og én for forsvarssektoren. I tillegg opprettholdes dagens løsning med at EOS-tjenestene klarerer eget personell, samt de særregler og unntak som framkommer i sikkerhetsloven § 2 fjerde og femte ledd. En slik sentralisering, med dertil økende sakstilfang for klareringsmyndighetene, vil danne grunnlag for å bygge store og robuste kompetansemiljøer. Denne løsningen vil bidra til å sikre likebehandling og være en rettssikkerhetsmessig styrking sammenlignet med dagens situasjon.»

9.3.2 Særlig om organiseringen av den sivile klareringsmyndigheten

Personell med klareringsbehov i sivil sektor er i hovedsak ansatte i departementene og i direktorater, tilsyn og tjenester som jobber med sikkerhetsrelaterte spørsmål. Innenfor de sivile klareringsmyndighetene er det betydelig variasjon i antallet saker som behandles. Enkelte myndigheter behandler opp mot 1 000 saker per år, og man har dedikerte fagmiljøer som jobber med sikkerhetsklareringer. I den andre enden av skalaen finnes klareringsmyndigheter som knapt behandler saker i det hele tatt, og hvor saksbehandlingen utføres av ressurser som har andre oppgaver som sine primære gjøremål. Den foreslåtte omorganiseringen medfører at Justis- og beredskapsdepartementet får ansvaret for etablering av én sentral sivil klareringsmyndighet direkte underlagt departementet, som ivaretar klareringssakene innen den sivile sektoren. Saker som i dag behandles av 26 sivile klareringsmyndigheter blir dermed behandlet av én sivil klareringsmyndighet underlagt Justis- og beredskapsdepartementet etter endringen. Med unntak av to, er alle klareringsmyndighetene lokalisert i Oslo. Videre heter det i høringsnotatet side 23:

> «Departement og virksomheter opprettholder sitt ansvar som autorisasjonsmyndighet, herunder innhenting av personopplysningsblanketter, vurdering av anmodning og gjennomføring av autorisasjonssamtaler. Gjennom autorisasjonsprosessen tar arbeidsgiver stilling til hvorvidt han/hun har den nødvendige grad av tillit til at den autoriserte håndterer sikkerhetsgradert informasjon korrekt. Autorisasjonssamtaler skal gjennomføres før autorisasjon finner sted, men også i etterkant dersom autorisasjonsansvarlig blir kjent med eksempelvis straffbare forhold, sikkerhetsbrudd, lønnstrekk og psykiske problemer hos den autoriserte/sikkerhetsklarerte. Oppgaver som tillegges ny sivil klareringsmyndighet er vurdering av hvorvidt vedkommendes sikkerhetsmessige skikkethet tilsier en klarering i tråd med anmodningen jf. § 21, herunder innhenting av opplysninger om spionasje, straffbare handlinger, misbruk av alkohol eller andre rusmidler, økonomiske forhold osv. Videre gjennomfører klareringsmyndigheten sikkerhetssamtaler og utsteder klareringsbevis.»

9.3.3 Særlig om organiseringen av klareringsmyndigheten i forsvarssektoren

I forsvarssektoren er det i dag fem klareringsmyndigheter. Etter forslaget vil Forsvarets sikkerhetsavdeling overta sikkerhetsklareringene til Forsvarsdepartementet og Forsvarsbygg (deriblant Forsvarets forskningsinstitutt (FFI) og Aerospace Industrial Maintenance Norway (AIM)). Nasjonal sikkerhetsmyndighet (NSM) og Etterretningstjenesten vil fortsatt være egne klareringsmyndigheter. Etter omorganiseringen vil klareringsmyndighetene behandle STRENGT HEMMELIG/Cosmic Top Secret (CTS)-klareringer og sikkerhetsklarere utenlandske statsborgere. NSM vil være klageinstans for klareringsmyndighetene i forsvarssektoren. Forsvarsdepartementet vil imidlertid fortsatt være klageinstans for saker som gjelder NSMs klarering av eget personell. Departementet ga uttrykk for at det ville være uheldig om Forsvarets sikkerhetsavdeling, som et sideordnet organ, skulle ivareta denne klagesaksbehandlingen. Forsvarsdepartementet som overordnet organ for Nasjonal sikkerhetsmyndighet og regelverksforvalter av sikkerhetsloven anses derfor best egnet.

Forsvarets sikkerhetsavdeling behandler i dag ca. 18 000 saker årlig. Forsvarsdepartementet behandlet 242 saker på nasjonalt nivå og 105 NATO-avgjørelser i 2014. Forsvarsbygg opplyser at en der behandler ca. 3000 saker årlig. I 2015 forventes en økning til ca. 4000 på grunn av økt aktivitet i Kampflybaseprosjektet, samtidig som FFI og AIM har en økning i forbindelse med sin femårs-syklus. Når det gjelder antall klareringer for

STRENGT HEMMELIG/CTS, som etter forslaget blir overført fra NSM til de andre klareringsmyndighetene, viser tall fra de siste årene at dette vil være mellom ca. 500–1000 saker pr. år. Den vesentligste del av disse sakene faller inn under forsvarssektoren. Tallene viser at det kan være variasjoner fra år til år. Flyttingen av sakene til Forsvarets sikkerhetsavdeling vil følgelig føre til en økning i Forsvarets sikkerhetsavdelings portefølje.

9.3.4 Nærmere om lovforslaget

Dagens § 23 første til fjerde ledd omhandler den nærmere organisering av klareringsmyndigheter under dagens regime med at hvert departement er klareringsmyndighet for personell innenfor sitt område. Som følge av forslaget vil første til fjerde ledd falle bort og erstattes av forslag til nytt andre og tredje ledd. Departementet foreslo ikke materielle endringer i femte ledd som omhandler autorisasjon. Ved en inkurie står ordet «sikkerhetssamtale» i tredje punktum i dag. Riktig ord er autorisasjonssamtale. Departementet foreslo at denne feilen rettes opp. Av regeltekniske hensyn foreslo departementet videre at femte ledd flyttes til nytt første ledd. Autorisasjon skal gjøres for samtlige graderingsnivå, mens sikkerhetsklarering stilles det kun krav om ved tilgang til KONFIDENSIELT eller høyere. Departementet viste til at det er mer pedagogisk at regulering av autorisasjon kommer først i bestemmelsen. Som en konsekvens av endring i rekkefølge i bestemmelsen, er også tittelen i § 23 foreslått endret slik at autorisasjon nevnes først.

9.4 Høringsinstansenes syn

De fleste høringsinstanser som har uttalt seg til spørsmålet, støtter i hovedsak departementets høringsforslag om reduksjon av antall klareringsmyndigheter. *Mnemonic* opplever at dagens klareringsordning ikke fungerer optimalt, fordi det kan ta svært lang tid å gjennomføre en klareringsprosess, og videre kan det gi leverandører med allerede klarert personell et fortrinn. Flertallet av høringsinstansene mener at en reduksjon av antall klareringsmyndigheter vil gi en enhetlig, godt faglig forankret, effektiv og tilfredsstillende saksbehandling. I den forbindelse uttaler *EOS-utvalget*:

> «Dette vil etter utvalgets syn kunne gi et bedre grunnlag for likebehandling av saker, en mer effektiv saksbehandling og høyere grad av profesjonalitet, forutsatt at det tilføres tilstrekkelig med ressurser og kompetanse til klareringsmyndighetene. Reduksjonen kan legge til rette for bedre fagmiljøer som kan bidra til å øke både rettsikkerheten for den enkelte og allmennhetens tillit til forsvarlig saksbehandling i en delvis lukket forvaltningsprosess.»

Forsvars- og sikkerhetsindustrienes forening antar at endringen vil ha positive sikkerhetsmessige effekter. *Direktoratet for forvaltning og IKT* (*Difi)* skriver at forslaget også kan forbedre informasjonssikkerheten, og gjøre det enklere å føre tilsyn med «tilganger samtidig som færre personer samlet sett antakelig vil ha behov for tilgang». *Fylkesmannen i Oslo og Akershus* mener at en sivil klareringsmyndighet med et større volum saker og spisskompetanse er den beste måte å bøte på kompleksiteten i klareringssaker. *Norsk olje og gass* skriver at industrien ser det som svært positivt at myndighetene får en tydelig klareringsstruktur. *Norges vassdrags- og energidirektorat (NVE)* mener imidlertid at en omlegging av ordningen vil bidra til økt byråkratisering, ved at flere myndigheter på ulike måter skal inn i hver klareringssak. Etter direktoratets syn vil endringen gi mindre effektiv saksbehandling og øke behovet for flere ansatte med sikkerhetsklarering. For øvrig påpeker direktoratet behovet for å få høy prioritet på særlig viktige klareringssaker:

> «Som selvstendig klareringsmyndighet har NVE til nå kunnet prioritere viktige saker frem i køen. Dette er gjerne knyttet til konstitueringer/ansettelser i viktige lederstillinger. Dette er viktig å sikre også dersom man velger å gå over til en felles sivil klareringsmyndighet.»

Flertallet av høringsinstansene understreker viktigheten av at klareringsmyndighetene får tilstrekkelig ressurser til å drive effektiv og kvalitetssikker saksbehandling, slik at behandlingstiden for klareringssaker reduseres. *Difi* oppfatter Oslo Economics AS sine vurderinger av de økonomiske besparelsene som noe usikre, «siden det tydelig fremkommer i høringsnotatet at det likevel ikke blir full samlokalisering». *Forsvarsbygg* mener det tempokravet som er satt for gjennomføringen av de ulike prosjektene, vil kunne gi store utslag i forsinkelser for gjennomføringen. *Kystverket* nærer en viss bekymring for at saksbehandlingstiden kan bli uforholdsmessig lang ved at kun to klareringsmyndigheter skal håndtere en saksmengde på opp mot 35.000 sikkerhetsklareringer per år:

> «Dette kan bli en utfordring for virksomheter med et stort klareringsbehov. Vi mener derfor at det er fornuftig at man åpner for at det kan utpekes andre klareringsmyndigheter når særlige grunner taler for det.»

Nasjonal kommunikasjonsmyndighet (Nkom) mener det er stor sannsynlighet for at flere av de forutsetninger som er lagt til grunn i høringsnotatet ikke vil vise seg holdbare. Gitt dagens bemanning, anser Nkom en overgangsperiode på ett til halvannet år som mer realistisk enn fire måneder. Nkom anbefaler at dagens klareringsmyndigheter ferdigbehandler allerede innkomne klareringssaker, mens den nye myndigheten får alle nye saker etter en viss dato. I tillegg mener Nkom at økt respons- og oppetid på IKT-systemet er avgjørende for å nå målsettingen om økt effektivitet. Etter Nkoms syn er det derfor behov for økte ressurser i sentral drifts- og støtteorganisasjon. *Norges Bank* forutsetter at en klareringsmyndighet for sivil sektor først iverksettes når de nødvendige ressurser og opplæring er på plass, slik at overgangen til ny ordning ikke medfører unødig opphold i klareringene. For øvrig skriver *Fylkesmannen i Oslo og Akershus* og *Fylkesmannen i Vest-Agder* at det må åpnes for tett og god dialog mellom anmodende myndighet og klareringsmyndigheten.

Politidirektoratet er av den oppfatning at de største sivile klareringsmyndigheter på størrelse med Norsk kommunikasjonsmyndighet og Politidirektoratet bør opprettholdes for at det sivile klareringsinstituttet ikke skal bli for sårbart, og har for øvrig merknad til bruken av ordet «sikkerhetssamtale» i sikkerhetsloven:

> «Det følger av sikkerhetsloven § 21 tredje ledd 3. punktum at «Sikkerhetssamtale skal gjennomføres der dette ikke anses som åpenbart unødvendig.» Direktoratet forstår begrunnelsen til lovforslaget § 23 slik at det er nødvendigheten av sikkerhetssamtale som krever en selvstendig begrunnelse, mens lovteksten synes å kreve at det er det åpenbart unødvendige som krever begrunnelse. Lovteksten forstått slik vil med andre ord alltid kreve sikkerhetssamtale dersom unnlatelse av dette ikke kan begrunnes tilstrekkelig som åpenbart unødvendig. Dersom aktuell bestemmelse skal forstås slik at det alltid må gjennomføres sikkerhetssamtale med mindre det kan begrunnes som åpenbart unødvendig, vil dette underbygge sannsynligheten for økt saksbehandlingstid ved en reduksjon til kun to klareringsmyndigheter.

Nasjonal sikkerhetsmyndighet (NSM) registrerer at det foreslås en adgang til også å etablere andre klareringsmyndigheter, og forutsetter at denne bestemmelsen gis en meget snever anvendelse, fordi omfattende bruk av bestemmelsen «vil uthule de gevinster man søker å oppnå gjennom hovedregelen». NSM mener små klareringsmyndigheter bare bør etableres der det foreligger meget tungtveiende grunner for dette.

Anders Bakke savner en bedre redegjørelse og begrunnelse for hvorfor departementet ønsker å opprettholde klareringsmyndighetene ved EOS-tjenestene, domstolene, Stortinget og Statsministerens kontor, dersom «formålet med lovendringen er å unngå fragmenterte og lite robuste fagmiljøer som ikke makter å vedlikeholde tilstrekkelig kompetanse til å sikre nødvendig kvalitet i sin saksbehandling». *Norges Bank* henstiller til at det i lovproposisjon til Stortinget gjøres en vurdering av klareringspraksis i de forskjellige samfunnssektorene. Banken mener det vil være av interesse å få belyst hvorvidt sektorene har samme praksis for vurdering av klareringsbehov.

Departementenes sikkerhets- og serviceorganisasjons (DSS) mener at autorisasjonsansvaret best kan ivaretas av ledere som kan utøve dette som en integrert del av den daglige sikkerhetsmessige ledelse. DSS har derfor siden 2012, med hjemmel i personellsikkerhetsforskriften § 5-1, gjennomført en delegasjon av autorisasjonsansvaret til linjeledelsen. En slik intern delegasjon av autorisasjonsansvaret er også med fordel gjennomført i andre virksomheter. På denne bakgrunn vil DSS foreslå at setningen «Autorisasjon gis normalt av virksomhetens leder» i sikkerhetslovens § 23, 5. ledd vurderes fjernet for at regelverket i større grad skal gjenspeile dagens praksis, og antar at siste setning i § 23, 5 ledd uansett vil være dekkende. Som et alternativ til å etablere en helt ny klareringsmyndighet, mener DSS at det i stedet bør vurderes om DSS kan ivareta denne rollen:

> «DSS har allerede et velfungerende fagmiljø som vil kunne danne kjernen i oppbyggingen av en klareringsavdeling for departementene. Det antas at en slik løsning vil kunne være kostnadseffektiv og samtidig være i tråd med DSS sin tjenesteytende rolle for departementene.»

Norges Banks representantskap ser positivt på at endringer knyttet til klareringsmyndighet og autorisasjonsansvarlig (§ 23) vil ivareta representantskapets eventuelle behov for klarering. De senere årene er representantskapets uavhengige stilling og relasjon til Stortinget blitt styrket. Dette er

blant annet tydeliggjort i sentralbankloven og ved direkte rapportering til Stortinget. På denne bakgrunn mener representantskapet det vil være mest naturlig om Stortinget blir klareringsmyndighet for representantskapets medlemmer og ansatte i tilsynssekretariatet.

NSM mener at Stortinget kan vurdere om det kan dra nytte av at det nå etableres to klareringsmyndigheter, for eksempel ved at Stortinget 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.

Innenfor sektorer med behov for et høyt antall klareringer bør det etter *Telenors* syn være egne organer med forståelse og kompetanse innenfor sin sektor. *Telenor* anbefaler derfor at klareringsmyndigheten for ekomsektoren fortsatt tillegges Nkoms ansvarsområde: «Ekom er et slikt område hvor kompetanse om kompleksiteten i infrastrukturen, ny sårbar teknologi, leverandøravhengighet og et mer sammensatt trusselbilde er sentralt å forstå også for klareringsmyndigheten».

Norges Bank viser til viktigheten av at det etableres tilfredsstillende elektroniske samhandlingsplattformer, slik at myndighetene som fremmer klareringsanmodninger kan samhandle elektronisk med den nye klareringsmyndigheten. *NRK* mener elektronisk søknadsprosess og saksbehandling for enkle klareringer bør innføres i forbindelse med gjennomføringen av den foreslåtte lovendringen.

9.5 Departementets vurderinger

9.5.1 Innledning

Departementet mener etableringen av to klareringsmyndigheter, én for forsvarssektoren og én for sivil sektor, vil gi en mer enhetlig og effektiv behandling av saker. Videre vil det bidra til å øke rettssikkerheten til den enkelte og allmennhetens tillitt til forsvarlig saksbehandling. En reduksjon av antall klareringsmyndigheter vil også ivareta tett og god dialog med anmodende myndighet og klareringsmyndigheten.

9.5.2 Organiseringen av klareringsmyndighetene

Justis- og beredskapsdepartementet vil få ansvaret for etableringen av en sentral klareringsmyndighet, som ivaretar klareringssakene innen den sivile sektoren. Den sivile klareringsmyndigheten vil være direkte underlagt Justis- og beredskapsdepartementet. Justis- og beredskapsdepartementet vil komme tilbake til hvem som skal være den sivile klareringsmyndigheten, da spørsmålet vil bli gjenstand for en egen utredning.

Som det framgår av departementets høringsnotat er det innenfor de sivile klareringsmyndigheter en betydelig variasjon i antallet saker som behandles. Reduksjon av antall sivile klareringsmyndigheter fra 26 til 1 vil gi et bedre grunnlag for likebehandling av saker, øke rettssikkerheten til den enkelte og allmennhetens tillitt til forsvarlig saksbehandling.

Departementet har i sikkerhetsloven § 23 åpnet opp for at også andre enn EOS-tjenestene kan gis klareringsmyndighet når særlige grunner taler for det. Nasjonal sikkerhetsmyndighet mener bestemmelsen bør gis en meget snever anvendelse. Departementet mener dette hensynet er ivaretatt ved at andre klareringsmyndigheter kun kan utpekes når «særlige grunner» taler for det. Bestemmelsen må sees i sammenheng med departementets forslag om å redusere antallet klareringsmyndigheter, og hovedregelen om at det skal være én klareringsmyndighet for forsvarssektoren og én for den sivile sektoren.

Av sikkerhetsloven § 2 fjerde ledd første punktum framgår det at loven gjelder for domstolene med de særregler som følger av bestemmelsene om sikkerhetsklarering og autorisasjon i og i medhold av domstolloven og straffeprosessloven. Videre følger det av sikkerhetsloven § 2 femte ledd at loven ikke gjelder for Stortinget, Riksrevisjonen, Stortingets ombudsmann for forvaltningen og andre organer for Stortinget. I departementets høringsforslag er kun sikkerhetsloven § 23 foreslått endret. Departementet har ikke funnet grunn til å endre virkeområdet for sikkerhetsloven i § 2 fjerde og femte ledd. En eventuell endring av virkeområdet for sikkerhetsloven krever en nærmere utredning av de konstitusjonelle hensynene og forholdet til andre lover. Departementet har foreslått at EOS-tjenestene klarerer sitt eget personell, på grunn av disse tjenestenes særskilte oppgaver.

I høringsnotatet skriver departementet at det ideelt sett for Stortinget og organer underlagt Stortinget, bør være kun én klareringsmyndighet. Departementet viser til punkt 3.4, der det legges opp til en egen dialog med Norges Banks representantskap på dette punktet.

Departementet noterer seg enkelte høringsinstansers ønske om å innføre elektronisk saksbehandling i forbindelse med gjennomføringen av

den foreslåtte lovendringen, men finner det ikke naturlig å gå nærmere inn på spørsmålet her. *Norges Bank* ber om at det i lovproposisjonen gjøres en vurdering av klareringspraksis i de forskjellige samfunnssektorene. Departementet viser til vurderingene som er gjort i høringsforslaget, se punkt 9.3.

Flertallet av høringsinstansene understreker viktigheten av at klareringsmyndighetene får tilstrekkelig ressurser til å drive effektiv og kvalitetssikker saksbehandling, slik at behandlingstiden for klareringssaker reduseres. Enkelte mener at de økonomiske konsekvensene underkommuniseres og at det er stor sannsynlighet for at flere av de forutsetninger som er lagt til grunn ikke vil vise seg holdbare. Departementet omtaler problemstillingene i punkt 12 om økonomiske og administrative konsekvenser.

9.5.3 Autorisasjonssamtale

Av sikkerhetsloven § 23 femte ledd fjerde punktum framgår det at Nasjonal sikkerhetsmyndighet gir nærmere regler om autorisasjon og om hvem som er autorisasjonsansvarlig. Etter departementets syn er sikkerhetsloven § 23 femte ledd andre punktum *ikke* en overflødig bestemmelse, da den angir hvem som normalt skal gi autorisasjon. Av informasjonssikkerhetsforskriften § 5-1 framgår det også at virksomhetens leder er ansvarlig for å autorisere personell for tilgang til sikkerhetsgradert informasjon. Dersom virksomheten har et stort autorisasjonsbehov, kan virksomhetens leder delegere myndigheten til å gi autorisasjon.

Som det framgår av departementets høringsnotat, skyldes bruken av ordet «sikkerhetssamtale» i sikkerhetsloven § 23 en inkurie. Det er bakgrunnen for at departementet har foreslått at «sikkerhetssamtale» endres til det korrekte ordet «autorisasjonssamtale». En sikkerhetssamtale er en formell samtale som klareringsmyndigheten kan gjennomføre med den som anmodes sikkerhetsklarert, for eventuelt å fjerne usikkerhet i spørsmålet om sikkerhetsklarering bør gis. En autorisasjonssamtale avholdes av autorisasjonsansvarlig for å avklare tillitsforholdet mellom autorisasjonsansvarlig og en person i forbindelse med dennes autorisasjon. Det er naturligvis ulike forutsetninger som legges til grunn for gjennomføring av sikkerhetssamtale etter sikkerhetsloven § 21 og en autorisasjonssamtale etter sikkerhetsloven § 23.

9.5.4 Forslag til ordlyd i bestemmelsen

I høringsnotatet foreslo departementet at reduksjon av antall klareringsmyndigheter lovfestes i sikkerhetsloven § 23 andre ledd og tredje ledd med følgende ordlyd:

> «Kongen utpeker to klareringsmyndigheter, en for forsvarssektoren og en for sivil sektor. Etterretnings- og sikkerhetstjenestene klarerer eget personell.
>
> Kongen kan utpeke andre klareringsmyndigheter når særlige grunner taler for det.»

Departementet har i høringsforslaget forutsatt at de tre EOS-tjenestene fortsetter å klarere sitt eget personell. Denne videreføringen av gjeldende rett er presisert i sikkerhetsloven § 23 andre ledd andre punktum. Bestemmelsen om klareringsmyndigheter innleder med at Kongen utpeker to klareringsmyndigheter, og avslutter med at Kongen utpeker andre klareringsmyndigheter når særlige grunner taler for det. Det kan dermed reises tvil om det er Kongen som også bestemmer at Etterretnings- og sikkerhetstjenesten skal klarere eget personell. Det er ikke tilsiktet. Departementet mener derfor at det kan være mer pedagogisk om forskriftshjemmelen i § 23 andre ledd første punktum og forskriftshjemmelen i § 23 tredje ledd står etter hverandre i samme ledd. Videre bør bestemmelsen om EOS-tjenestene plasseres til slutt. Departementet foreslår også at andre ledd første setning forenkles språklig. Ordlyden i § 23 andre ledd blir etter dette:

> «Kongen utpeker en klareringsmyndighet for forsvarssektoren og en for den sivile sektoren. Kongen kan utpeke andre klareringsmyndigheter når særlige grunner taler for det. Etterretnings- og sikkerhetstjenestene klarerer eget personell.»

10 Sikkerhetsgraderte anskaffelser – varighet av leverandørklarering

10.1 Gjeldende rett

En sikkerhetsgradert anskaffelse er en anskaffelse som medfører at leverandøren får tilgang til eller må tilvirke skjermingsverdig informasjon, eller kan få tilgang til et skjermingsverdig objekt, eller som innebærer at anskaffelsen må sikkerhetsgraderes av andre årsaker, jf. sikkerhetsloven § 3 nr. 17. I slike anskaffelser stiller sikkerhetsloven krav om at det, som en del av anskaffelsen, skal implementeres særskilte sikkerhetstiltak.

Ved sikkerhetsgraderte anskaffelser, på alle graderingsnivåer, skal det inngås sikkerhetsavtale mellom anskaffelsesmyndigheten og leverandøren. Før en leverandør kan få tilgang til skjermingsverdig informasjon som er sikkerhetsgradert KONFIDENSIELT eller høyere, eller dersom det av andre grunner anses nødvendig, skal leverandøren i tillegg ha gyldig leverandørklarering for angitt sikkerhetsgrad, jf. sikkerhetsloven § 28 første ledd.

En leverandørklarering innebærer at det foretas en vurdering av leverandørens sikkerhetsmessige skikkethet og evne til forsvarlig håndtering av skjermingsverdig informasjon. En leverandørklarering gjelder for *det enkelte oppdrag.* Dette betyr at det må søkes om klarering for hvert enkelt oppdrag, og klareringen faller automatisk bort når oppdraget er fullført. Det er i forarbeidene (Ot.prp. nr. 49 (1996–97) s. 61 flg.) ikke begrunnet nærmere hvorfor denne begrensningen er valgt, men det framgår at bestemmelsen er en videreføring fra tidligere direktiver. Virksomheten som gjennomfører en sikkerhetsgradert anskaffelse, må søke om leverandørklaring for den enkelte sikkerhetsgraderte anskaffelsen. Nasjonal sikkerhetsmyndighet (NSM) er klaringsmyndighet, jf. § 28 første ledd siste punktum. En leverandør som innehar en leverandørklarering, skal uten ugrunnet opphold orientere NSM om endringer i styre eller ledelse, forandringer i eierstrukturen, flytting av lokaliteter og utstyr, åpning av gjeldsforhandlinger eller begjæring om konkurs, og om andre forhold som kan ha betydning for leverandørens sikkerhetsmessige skikkethet. Hvis forholdene anses å representere en sikkerhetsrisiko som ikke kan elimineres gjennom forebyggende sikkerhetstiltak, kan NSM inndra leverandørklareringen, jf. § 28 fjerde ledd, jf. forskrift om forsvars- og sikkerhetsanskaffelser § 3-3. Saksbehandlingsreglene i sikkerhetsloven kapittel 6 om personellsikkerhet, herunder bestemmelsen om begrunnelse og klage, gjelder så langt det passer for leverandørklaringer, jf. § 28 femte ledd.

10.2 Utenlandsk rett og NATO

I *Sverige* er det statlige myndigheter, kommuner og landsting som kan foreta anskaffelser som innebærer tilgang til informasjon om rikets sikkerhet. Disse skal i så fall inngå en sikkerhetsavtale med leverandøren på det aktuelle sikkerhetsnivået. Kravet om inngåelse av sikkerhetsavtale gjelder ikke for alle leverandører, og gjelder for eksempel ikke for rettssubjekter som offentlige organer utøver rettslig myndighet over. Dette gjelder selv om virksomhetene utøver virksomhet som har betydning for rikets sikkerhet eller har til oppgave å beskytte mot terrorisme.

Dansk industrisikkerhet bygger på bestemmelsene i Statsministerens sikkerhedscirkulære, NATOs industrisikkerhetsbestemmelser og de standarder som er etablert i MISWIG-samarbeidet (Multinational Industrial Security Working Group), en arbeidsgruppe som også Norge er medlem av. Sikkerhedscirkulæret gir ikke konkrete bestemmelser om sikkerhetsgraderte anskaffelser. Med hjemmel i sirkulæret er det for Forsvaret fastsatt egne «Bestemmelser for den militære sikkerhedstjeneste». Her gis det også bestemmelser om sikkerhetsgraderte anskaffelser foretatt av Forsvaret, samt internasjonale sikkerhetsgraderte anskaffelser. Forsvarets Efterretningstjeneste forestår sikkerhetsmessig godkjenning og oppfølging av leverandører i forbindelse med sikkerhetsgraderte anskaffelser. Forsvarets Efterretningstjeneste fastsetter leverandørklareringens varighet i forbindelse med godkjennelsen av den enkelte søknad.

I *Storbritannia* må alle leverandører til statlige myndigheter som kan få tilgang til informasjon eller verdier sikkerhetsgradert SECRET eller høyere, ha en leverandørklarering. Leverandørklarerte virksomheter føres inn i den såkalte «List X», og omtales som «List X Contractors». Ordningen er tidsbasert: så lenge en leverandør står på «List X» kan den benyttes til sikkerhetsgraderte kontrakter. «List X Contractors»-regimet forvaltes av det britiske forsvarsdepartementet, og det er utarbeidet særskilte sikkerhetskrav som leverandørene må tilfredsstille i «Security Requirement for List X Contractors».

Sikkerhetsgraderte anskaffelser til *NATO* reguleres i «NATO Security Policy». Regelverket oppstiller de sikkerhetskrav som kommer til anvendelse ved NATO- sikkerhetsgraderte kontrakter, jf. dokument «C-M(2002)49 Enclosure G» og «AC/35-D/2003»». Regelverket er inkorporert i norsk regelverk. For alle kontrakter gradert NATO CONFIDENTIAL eller høyere, skal det foreligge en «Facility Security Clearance» (FSC) før leverandøren gis tilgang til sikkerhetsgradert informasjon. Dette gjelder også hvis gradert informasjon må frigis i anbuds- eller forhandlingsfasen. Leverandørklarering gis av myndighetene i det landet leverandøren er hjemmehørende. Varigheten av en leverandørklarering vil følge av de enkelte nasjoners regelverk på området. De krav som stilles til leverandører kommer tilsvarende til anvendelse for underleverandører. Regelverket har særskilte reguleringer for tildeling av NATO-graderte kontrakter til industri fra land som ikke er medlem av alliansen.

For offentlige oppdragsgivere må regelverket om sikkerhetsgraderte anskaffelser sees i sammenheng med regelverket for offentlige anskaffelser. En sikkerhetsgradert anskaffelse er i utgangspunktet omfattet av lov 16. juli 1999 nr. 69 om offentlige anskaffelser og forskrift 4. oktober 2013 nr. 1185 om forsvars- og sikkerhetsanskaffelser. Nevnte lov og forskrift gjelder imidlertid ikke der en anskaffelse kan unntas med hjemmel i *EØS-avtalen* artikkel 123. Dette er også reflektert i forskrift om sikkerhetsgraderte anskaffelser § 2-3. Endringene som foreslås er etter departementets vurdering ikke i strid med EØS-avtalen.

10.3 Høringsforslaget

I høringsnotatet foreslo departementet endring av sikkerhetsloven § 28 første ledd andre punktum, slik at leverandørklarering gis etter anmodning fra en anskaffelsesmyndighet, men med en tidsavgrenset varighet. Systemet med klarering for hvert enkelt oppdrag er i dag for tungvint og genererer et unødvendig høyt antall søknader om leverandørklarering. Tilnærmingen synes også å være i utakt med praksis i en del andre land så vel som med internasjonalt regelverk. Forslaget forutsetter endring i forskrift om sikkerhetsgraderte anskaffelser. Formålet med forslaget var å effektivisere arbeidet med sikkerhetsgraderte anskaffelser. I høringsnotatet side 26 skriver departementet:

> «Med et slikt forslag vil det ikke være nødvendig for industrien å søke klarering for det enkelte oppdrag. Der leverandøren fortsatt innehar en leverandørklarering, vil en bekreftelse fra Nasjonal sikkerhetsmyndighet om at gyldig leverandørklarering foreligger, være tilstrekkelig. Industrien har også uttalt seg positivt til en slik endring fra oppdragsbasert til tidsbasert leverandørklarering. Det blir blant annet pekt på at dagens ordning er en byråkratiserende prosedyre og at den gjør det vanskeligere for utenlandske kunder, som ikke er innforstått med det norske systemet.
>
> Departementet foreslår at det fastsettes i forskrift hvor lenge en leverandørklaring skal gjelde. Sett hen til hva som gjelder for personellklareringer, mener departementet at en leverandørklaring for eksempel kan gis for en periode på fem år. Det må i så fall innføres et regime for tildeling og oppfølging. Dette må reguleres nærmere i forskrift. Bestemmelsene må sikre tildeling av leverandørklaringer på like vilkår og en forsvarlig oppfølging av leverandører i klareringsperioden.»

Departementet har i høringsnotatet vurdert hvorvidt det skal settes begrensninger for hvem som kan søke om en leverandørklarering eller ikke, og har særlig vurdert to alternativer:

> «Ett alternativ er at bedrifter kan bli leverandørklarert etter søknad, uten at det er krav om å dokumentere noe reelt behov. På den måten kan alle potensielle leverandører stille likt i framtidige konkurranser om oppdrag. Ulempen ved en slik ordning er at det kan bli oppfattet og framstilt som en offentlig sikkerhetsmessig godkjenning, og et kvalitetsstempel, som virksomheter kan ønske å ha for å styrke sin generelle markedsmessige posisjon. Dette kan føre til at det blir behandlet og gitt flere leverandørklaringer enn det reelt sett er behov for. Departementet antar at en slik utvikling i en viss utstrekning vil kunne motvirkes ved for

eksempel å ha et søknadsgebyr av en viss størrelsesorden. En annen side ved en slik ordning er at personell i leverandørens styre og ledelse skal sikkerhetsklareres som ledd i en leverandørklarering. Sikkerhetsklarering er regnet som et inngripende virkemiddel som ikke bør benyttes uten i de tilfeller hvor det foreligger et reelt behov. Leverandørklarering etter søknad vil derfor kunne utfordre prinsippet om en restriktiv personellklareringspraksis.

Det andre alternativet er at leverandørklaring gis etter dokumentert behov, med en tilhørende anmodning om leverandørklarering fra en anskaffelsesmyndighet. Dette vil være i samsvar med den ordning som i dag er etablert for sikkerhetsklarering av personer. Departementet mener denne løsningen vil sikre at saker ikke blir behandlet med mindre det foreligger et reelt behov.»

10.4 Høringsinstansenes syn

Omtrent alle høringsinstansene støtter departementets forslag om å gå fra oppdragsbasert til tidsbasert leverandørklarering. I høringsnotatet har departementet antydet fem år som naturlig varighet av leverandørklareringer. Flertallet av høringsinstansene stiller seg positive til det og legger vekt på at det vil effektivisere arbeidet med sikkerhetsgraderte anskaffelser. *Utlendingsdirektoratet* mener tidsbasert leverandørklarering forutsetter at godkjenningen ikke gis for et så langt tidsrom at det skapes usikkerhet om klareringen kvalitetsmessig er holdt vedlike mot slutten av klareringsperioden. *Mnemonic* mener en slik klarering må gis under forutsetning av at leverandøren forplikter seg til å varsle klareringsmyndighet om eventuelle større endringer i løpet av 5 årsperioden: «Alternativt må klareringsperioden reduseres med de konsekvensene det har for tidsbruk». Mnemonic anbefaler også å vurdere om det finnes eksisterende sertifiseringsordninger det kan være hensiktsmessig å knytte en slik leverandørklarering opp mot, hvor man eventuelt kan stille ytterligere krav. *Fylkesmannen i Vest-Agder* uttaler:

«Imidlertid er det en kjensgjerning at mye kan skje på eiersiden i leverandørbedriftene i løpet av forholdsvis kort tid. En ting er at de driftsforholdene som kunden kommer i kontakt med kan være forholdsvis stabile. En annen ting er eierforholdene rundt leverandøren. Disse kan forandre raskt og for den del flyttes til land som Norge har spesielt fokus på sikkerhetsmessig. Denne utviklingen må kunne fanges opp og evt. medføre en revurdering av leverandørklareringen også før den løper ut.»

Nasjonal sikkerhetsmyndighet (NSM) mener bestemmelsen, brukt riktig og aktivt, kan gi økt sikkerhet, og mener at hjemmelsgrunnlaget for informasjonsinnhenting bør tydeliggjøres i bestemmelsen og/eller i forarbeidene:

«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.»

Forsvarets logistikkorganisasjon/Investering (FLO/I) mener loven bør åpne for at NSM kan delegere klareringsmyndighet – leverandørklarering til en sektor.

«Hovedtyngden av de leverandører som i dag omfattes av sikkerhetsloven er leverandører til forsvarssektoren. FLO erfarer at disse i betydelig grad finner det vanskelig å forstå og etterleve loven og at de ønsker én aktør å forholde seg til både hva gjelder, rådgivning, godkjenninger og tilsyn.

Når leverandørklarereringer for en periode av 5 år gis til en leverandør må det samtidig utpekes én som skal være sikkerhetsmessig ansvarlig (sektor/forvaltningsorgan) for leverandøren i perioden.

En slik mulighet vil redusere NSMs kontrollspenn og gjøre det enklere for leverandører å forholde seg til loven. Samtidig vil det åpne for muligheten til at en innen en sektor gir én aktør hovedansvaret for å koordinere innen sektoren. Den nye materielletaten bør kunne være en slik aktør innen forsvarssektoren f.eks. på området sikkerhetsgraderte anskaffelser.»

For å unngå store effektiviserings- og kostnadstap i anskaffelsesprosessene, er det etter *Forsvarsbyggs* syn avgjørende at det avsettes nødvendige ressurser hos klarerende myndigheter til å gjennomføre leverandørklareringer. *Forsvars- og sikkerhetsindustrien (FSi)* understreker at det er viktig å få behandlet søknad om klarering også i tilfeller hvor det ikke foreligger noen opplagt anskaffelse eller anskaffelsesmyndighet, men saklige

behov for klarering, eksempelvis deltakelse på militære øvelser, forsvarsstudier, NATO-studier og møter hos utenlandske forsvarsbedrifter.

Norges Bank anbefaler at NSM etablerer en forenklet norsk leverandørklarering på basis av leverandørklarering i definerte samarbeidsland (f.eks. basert på britiske «List X»). Norges Bank mener at en tydeligere definert og gjennomført ordning for leverandørklareringer, samt ordninger med noen grad av overførbare leverandørklareringer fra andre land, vil være med på å motvirke fare for at utenlandske leverandører ser det som regulatorisk og politisk risikabelt å gå inn i prosjekter i Norge. Videre påpeker *Norges Bank* at leverandørklarering også er aktuelt for konsulenter som yter tjenester i forbindelse med sikring av skjermingsverdige objekter eller drifter systemer knyttet til skjermingsverdige objekter.

Norsk Romsenter savner en vurdering knyttet til sikkerhetsgraderte anskaffelser for EU og European Space Agency (ESA) tilsvarende det som er gjort for NATO, men mener det er fornuftig å endre systemet slik det er foreslått.

10.5 Departementets vurderinger

Departementets forslag innebærer en endring fra oppdragsbasert til tidsbasert leverandørklarering. I sikkerhetsloven § 28 første ledd andre punktum står det at leverandørklareringen gjelder for det enkelte oppdrag. Departementet har i høringsnotatet foreslått å endre denne bestemmelsen til en forskriftshjemmel, som gir Kongen myndighet til å bestemme den generelle gyldighetstid for leverandørklareringer. I høringsnotatet antyder departementet en varighet på fem år, tilsvarende den varighet som gjelder for personellklareringer. Departementet foreslår imidlertid ikke å lovfeste hvor lenge en leverandørklarering skal gjelde.

Forslaget om tidsbasert leverandørklarering forutsetter en endring av forskrift om sikkerhetsgraderte anskaffelser. De nærmere regler om tildeling og oppfølging av en tidsbestemt leverandørklarering vil framgå av forskrift. Forslag til endringer i forskriften vil bli sendt på alminnelig høring. Lovforslaget vil ikke tre i kraft før nødvendige endringer i forskrift har vært på høring. Det vil også være naturlig at endringer i lov og forskrift trer i kraft fra samme dato. Samtidig er det en nødvendig forutsetning for lovforslaget at det avsettes nødvendige ressurser til gjennomføringen av tidsbasert leverandørklarering, se punkt 12.3.

Flere av høringsinstansene foreslår endringer i sikkerhetsloven som krever nærmere utredning og eventuelt høring. Dette gjelder blant annet adgangen til å delegere klareringsmyndighet etter sikkerhetsloven § 28 første ledd tredje punktum, foreta leverandørklarering av konsulenter som yter tjenester i forbindelse med sikring av skjermingsverdige objekter og personer som deltar på militære øvelser, forsvarsstudier, møter hos utenlandske forsvarsbedrifter mv. Departementet vil ikke gå nærmere inn på disse spørsmålene i denne omgang. Departementet anser det videre heller ikke som naturlig å drøfte spørsmålet om NSM bør etablere en forenklet norsk leverandørklarering på basis av leverandørklarering i definerte samarbeidsland, da dette ikke er et spørsmål som krever lovregulering.

11 Anskaffelser til kritisk infrastruktur

11.1 Bakgrunn

11.1.1 Kritisk infrastruktur og økt risiko for spionasje, sabotasje og terror

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. Samfunnets økte avhengighet av kritisk infrastruktur gjør at denne problemstillingen trolig vil få stadig større relevans framover.

Begrepet kritisk infrastruktur er ikke helt entydig, og det finnes en rekke ulike definisjoner av begrepet. En definisjon av kritisk infrastruktur som departementet mener fremdeles har aktualitet, er definisjonen som ble lagt til grunn av Infrastrukturutvalget i NOU 2006: 6 *Når sikkerheten er viktigst.* Begrepet ble der definert slik:

> «Kritisk infrastruktur er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse.»

Denne definisjonen består av følgende tre hovedbegreper[1]:

1. *Kritisk infrastruktur* – som er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner.
2. *Samfunnets kritiske funksjoner* – som er de funksjonene som dekker samfunnets grunnleggende behov.
3. *Samfunnets grunnleggende behov* – som er et noe uklart begrep, som utdypes nærmere nedenfor.

Selv om begrepet «samfunnets grunnleggende behov» nevnes til sist i definisjonen, tar definisjonen utgangspunkt i dette begrepet, og utleder innholdet i de to andre begrepene ut fra det. Definisjonen utløser tre spørsmål som må besvares i nedennevnte rekkefølge for å kunne identifisere kritisk infrastruktur:

1. Hva er samfunnets *grunnleggende behov*?
2. Hvilke *samfunnsfunksjoner* er kritiske for å dekke disse behovene?
3. Hva slags *systemer og anlegg* er helt nødvendige for å opprettholde disse funksjonene?

Først etter å ha besvart det tredje spørsmålet har vi identifisert de systemene og anleggene som utgjør kritisk infrastruktur.

Det første spørsmålet vi må ta stilling til, er imidlertid hva som er samfunnets grunnleggende behov. Dette kan også formuleres som et spørsmål om hva som er samfunnets viktigste verdier.

NOU 2006: 6 legger til grunn at en mulig måte å identifisere samfunnets grunnleggende behov på, er å ta utgangspunkt i psykologen Abraham Maslows behovspyramide. Muligens kan de to nederste nivåene i pyramiden omtales som grunnleggende behov (på individnivå). De to nederste nivåene er menneskets «fysiske behov» og «behov for trygghet». Som følge av dette kan en muligens si at samfunnets grunnleggende behov kollektivt sett, er å kunne ivareta innbyggernes fysiske behov og behov for trygghet.

Hva som utgjør samfunnets grunnleggende behov i sikkerhetslovens forstand, må vurderes i lys av sikkerhetslovens formål. Dette er blant annet «å motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser». Trolig vil både befolkningens fysiske behov og behovet for trygghet måtte anses som grunnleggende behov også i sikkerhetslovens forstand.

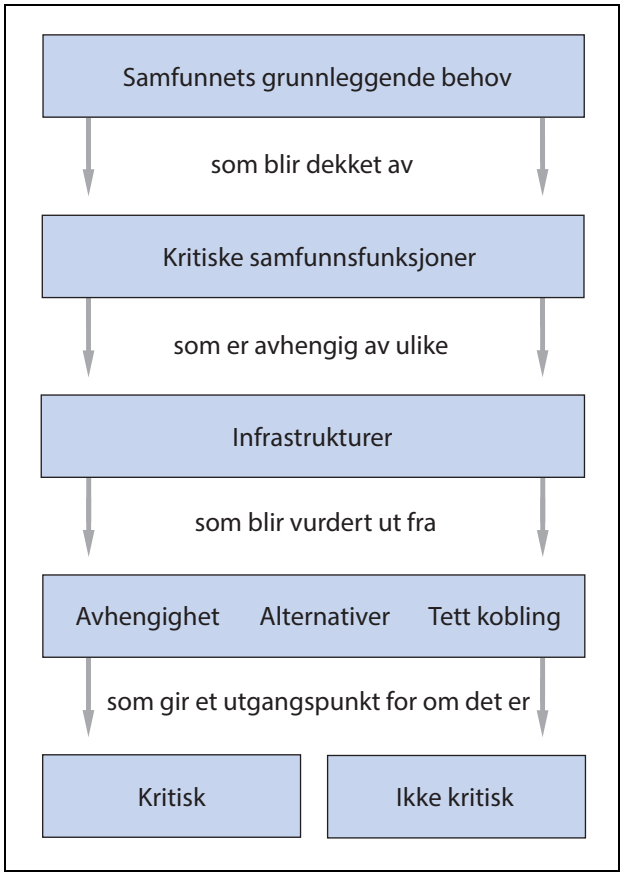
Etter å ha identifisert de grunnleggende behovene, er neste steg å identifisere hvilke kritiske

[1] I tillegg bruker definisjonen begrepet «befolkningens trygghetsfølelse». Dette begrepet er brukt for å tydeliggjøre at det har en selvstendig verdi at befolkningen føler seg trygge, uavhengig av om befolkningen faktisk (objektivt sett) er trygge. Departementet vil ikke utdype dette begrepet i redegjørelsen.

samfunnsfunksjoner som trengs for å dekke disse behovene. Altså å finne ut hva som trengs av funksjoner i samfunnet for at de grunnleggende behovene skal bli ivaretatt. Det være seg myndighetsfunksjoner eller funksjoner drevet av andre.

Et eksempel på en opplisting av kritiske samfunnsfunksjoner finner vi i rapporten «Samfunnets kritiske funksjoner», utgitt av Direktoratet for samfunnssikkerhet og beredskap (DSB) i 2015[2]. DSB har tatt utgangspunkt i at en funksjon er kritisk dersom samfunnet i løpet av syv dager etter at funksjonen har sviktet ikke lenger klarer å tilfredsstille ett eller flere grunnleggende behov. DSB har sortert funksjonene i fire behovskategorier.

- nasjonal styringsevne og suverenitet
  - (1) nasjonal styring, (2) forsvar
- befolkningens sikkerhet
  - (3) lov og orden, (4) helse og omsorg, (5) redningstjenester, (6) sikkerhet mot eksponering av farlige stoffer, (7) informasjonssikkerhet, (8) overvåking av naturfarer
- befolkningens velferd
  - (9) matforsyning, (10) vann og avløp, (11) sosiale ytelser og tjenester, (12) finansielle tjenester, (13) energiforsyning, (14) elektronisk kommunikasjon, (15) transport, (16) satellittbaserte tjenester
- kultur og natur
  - (17) vern av kulturelle verdier, (18) vern mot forurensning.



Figur 11.1 Retningslinjer for identifisering av kritisk infrastruktur utfra samfunnets grunnleggende behov.

Kilde: NOU 2006: 6 *Når sikkerheten er viktigst*

Departementet mener denne opplistingen kan tjene som et eksempel på hvordan man kan knytte ulike kritiske samfunnsfunksjoner opp mot de grunnleggende behovene, avhengig av hvordan man velger å angi grunnleggende behov eller verdier. Departementet understreker imidlertid at listen kun må ses på som et eksempel.

Etter å ha identifisert de kritiske samfunnsfunksjonene, må man identifisere hvilke systemer og anlegg som er helt nødvendige for å opprettholde de ulike kritiske samfunnsfunksjonene. Ved å besvare dette spørsmålet finner vi ut hva som er kritisk infrastruktur.

Infrastrukturutvalget oppstilte i NOU 2006:6 en modell for identifisering av kritisk infrastruktur, se figur 11.1.

Figur 11.1 opererer med tre stikkord til hjelp for å identifisere kritisk infrastruktur: (1) avhengighet, (2) alternativer og (3) tett kobling.

Avhengighet – første trinn innebærer å finne ut hvem eller hva som er avhengig av den aktuelle infrastrukturen. Dersom et stort antall av kritiske samfunnsfunksjoner er avhengig av infrastrukturen, tilsier det at infrastrukturen er kritisk. Dette kriteriet veier tyngst når kritisk infrastruktur skal identifiseres. Eksempelvis er praktisk talt alle kritiske samfunnsfunksjoner avhengig av strøm gjennom kraftinfrastrukturen og elektronisk kommunikasjon gjennom ekominfrastrukturen.

Alternativer – andre trinn innebærer å vurdere alternativer. Hvis det ikke finnes alternativer til den aktuelle infrastrukturen, tilsier det at den er kritisk. Og motsatt kan det tilsi at infrastrukturen ikke er kritisk dersom det finnes alternativer. Eksempelvis har Norge et stort antall kraftverk spredt ut over hele landet. Dette medfører at bortfall av ett kraftproduserende anlegg ikke får store konsekvenser for kraftleveransen sett under ett. Dette kan dermed tilsi at et kraftverk ikke er kritisk infrastruktur.

Tett kobling – tredje trinn innebærer å vurdere i hvilken grad infrastrukturen er tett koblet. Et tett koblet system innebærer at forstyrrelser ett sted i systemet får umiddelbare konsekvenser for

[2] Ikke ferdigstilt. Utkast ble sendt på høring 30. september 2015.

Tabell 11.1 Oversikt over kritiske samfunnsfunksjoner.

Matforsyning:	produksjonsanlegg, distribunaler, logistikksystemer
Vann og avløp:	vannverk, renseanlegg, pumper, høydebasseng
Sosiale ytelser og tjenester:	NAVs it-systemer
Finansielle tjenester:	finansiell infrastruktur
Energiforsyning:	(1) kraftverk, transformatorer, kraftnett osv.
	(2) fjernvarmeanlegg, pumpestasjoner, ledningsnett
	(3) raffinerier, havneanlegg, tankanlegg
Elektronisk kommunikasjon:	kjernenett, transportnett, svitsjer
Transport:	veinett, jernbanelinjer, terminaler, trafikkstyringssystemer
Satellittbaserte tjenester:	satellitter, bakkestasjoner.

Kilde: Direktoratet for samfunnssikkerhet og beredskap. *Samfunnets kritiske funksjoner. Hvilken funksjon må samfunnet opprettholde til enhver tid?* (Høringsutgave – september 2015)

systemet som helhet. Høy grad av tett kobling tilsier at infrastrukturen er kritisk. Eksempler kan hentes fra offentlig transport. Jernbane og lufttrafikk i Norge er avhengig av sentralisert styring i sanntid for effektiv og sikker drift. Busstrafikk kan derimot operere uten en sentralisert styring, eller i hvert fall med langt lavere grad av sentralisert kontroll og styring i sanntid. Bortfall av knutepunkter i tett koblede systemer vil få store konsekvenser for funksjonsdyktigheten til infrastrukturen. El-nettet, særlig sentralnettet, er et ytterligere eksempel.

DSB har i sin rapport identifisert infrastruktur under 8 av de 18 kritiske samfunnsfunksjonene, se tabell 11.1.[3] Bakgrunnen for at DSB kun har knyttet infrastruktur til 8 av de 18 kritiske samfunnsfunksjonene, er ikke at de resterende 10 samfunnsfunksjonene ikke er avhengige av infrastruktur. Alle kritiske samfunnsfunksjoner er avhengige av kritisk infrastruktur. Forklaringen er at enkelte kritiske samfunnsfunksjoner er mer direkte avhengige av kritisk infrastruktur enn andre, og at det derfor er mer naturlig å sortere infrastrukturen inn under disse. Eksempelvis er alle de kritiske samfunnsfunksjonene avhengige av kraftnettets infrastruktur. Imidlertid er det mest naturlig å omtale denne infrastrukturen under samfunnsfunksjonen «energiforsyning». Tilsvarende er det også på andre områder.

Tabellen viser hva som kan anses som kritisk infrastruktur, knyttet til den enkelte kritiske samfunnsfunksjonen. Tabellen er verken bestemmende eller uttømmende, men tjener som et eksempel. Opplistingen ovenfor er uansett kun på typenivå, slik at den konkrete identifiseringen av systemer og anlegg vil måtte gjennomføres i den enkelte sektor. Eksemplifiseringen er inntatt for å gjøre anskaffelser til kritisk infrastruktur mer håndgripelig, og for å synliggjøre hva slags infrastruktur som potensielt kan være utsatt for spionasje og sabotasje.

11.1.2 Gjeldende rett

Reglene i sikkerhetsloven kapittel 7 om sikkerhetsgraderte anskaffelser gir myndighetene adgang til å stille sikkerhetsmessige krav ved visse leveranser til norsk kritisk infrastruktur. Forutsetningen er at leveransen faller inn under lovens definisjon av «sikkerhetsgradert anskaffelse». Dette er i § 3 nr. 17 definert som anskaffelse der leverandøren «vil kunne få tilgang til skjermingsverdig informasjon eller objekt, eller som innebærer at anskaffelsen må sikkerhetsgraderes av andre årsaker». Det vil si at en anskaffelse til kritisk infrastruktur først beskyttes av reglene om sikkerhetsgraderte anskaffelser dersom den aktuelle infrastrukturen er utpekt som et skjermingsverdig objekt i medhold av sikkerhetsloven § 17, eller anskaffelsen innebærer at leverandøren vil få tilgang til skjermingsverdig informasjon.

[3] Noe redigert fra departementets side, ved at infrastrukturen «butikker» og «bensinstasjoner» er fjernet fra henholdsvis funksjonene matforsyning og energiforsyning.

Dersom en anskaffelse er sikkerhetsgradert, skal anskaffelsesmyndigheten og leverandøren etter sikkerhetsloven § 27 inngå en sikkerhetsavtale. Sikkerhetsavtalen skal blant annet omhandle praktisk gjennomføring av undersøkelser hos leverandøren og annen kontroll med leverandøren for å vurdere sikkerhetstilstanden, og for å kontrollere at leverandøren forholder seg i samsvar med kravene i sikkerhetsloven. En sikkerhetsavtale kan bare inngås med utenlandske leverandører dersom det godkjennes av Nasjonal sikkerhetsmyndighet (NSM).

Sikkerhetsloven § 28 gjelder for sikkerhetsgraderte anskaffelser der leverandøren vil kunne få tilgang til informasjon gradert KONFIDENSIELT eller høyere, og bestemmelsen oppstiller et krav om leverandørklarering. En leverandørklarering utføres av NSM, og den har som formål å undersøke om leverandøren er sikkerhetsmessig skikket til å foreta leveransen. Dersom undersøkelsene konkluderer med at det foreligger tvil om leverandøren er sikkerhetsmessig skikket, vil det ikke bli gitt klarering. I forbindelse med denne vurderingen ser NSM på leverandørens evne og vilje til å etterleve sikkerhetskravene som følger av sikkerhetsloven, og det foretas også personkontroll av personer i leverandørens styre og ledelse.

Sikkerhetslovens regler om sikkerhetsgraderte anskaffelser gir således myndighetene mulighet til å kontrollere selskaper som leverer til kritisk infrastruktur, forutsatt at anskaffelsen gir leverandøren tilgang til gradert informasjon eller til et utpekt skjermingsverdig objekt. Imidlertid vil ikke alle anskaffelser til kritisk infrastruktur bli fanget opp av reglene om sikkerhetsgraderte anskaffelser. På langt nær all kritisk infrastruktur er utpekt som skjermingsverdige objekter.

Ved en leveranse til kritisk infrastruktur som ikke er et skjermingsverdig objekt, vil leverandøren etter omstendighetene kunne utnytte tilgangen til den kritiske infrastrukturen til å utføre sabotasje, eller til å spionere via infrastrukturen som det leveres til, selv om leveransen i seg selv ikke gir leverandøren tilgang til skjermingsverdig informasjon eller til et skjermingsverdig objekt. Slik tilgang for leverandører kan for eksempel utnyttes ved leveranser av både fysiske komponenter, vedlikeholdstjenester og programvare. Problemstillingen kan aktualisere seg innenfor flere ulike typer infrastruktur. Departementet har registrert tilfeller der myndighetene ikke har hatt hjemmel til å nekte leveranser til norsk kritisk infrastruktur, selv om saken har vært vurdert slik at det forelå en potensiell fare for spionasje eller sabotasje mot Norge.

11.2 Høringsforslaget

11.2.1 Hovedpunktene i høringsforslaget

På bakgrunn av ovennevnte, så departementet et behov for et rettslig grunnlag for myndighetene til å stille sikkerhetsmessige krav ved anskaffelser også til kritisk infrastruktur som ikke var utpekt som skjermingsverdige objekter. Departementet sendte følgende forslag til bestemmelse på høring:

> «§ 29 a Anskaffelser til kritisk infrastruktur
>
> En virksomhet skal varsle ansvarlig fagdepartement dersom en anskaffelse til kritisk infrastruktur som virksomheten eier eller rår over kan innebære en ikke ubetydelig risiko for rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser. Departementet som mottar varselet bør innhente en rådgivende uttalelse om leveransens risikopotensiale og leverandørens sikkerhetsmessige pålitelighet fra relevante organer.
>
> Dersom det foreligger risiko som nevnt i første ledd første punktum kan anskaffelsen nektes gjennomført, eller det kan settes vilkår. Dette gjelder også dersom det allerede er inngått avtale om anskaffelsen. Vedtak om å nekte anskaffelsen eller sette vilkår fattes av Kongen i statsråd. Dersom vilkårene for å nekte anskaffelsen eller sette vilkår ikke er oppfylt, gir departementet virksomheten tilbakemelding om dette.
>
> Kongen i statsråd kan gi forskrift om anskaffelser til kritisk infrastruktur.»

I høringen ble det også foreslått et nytt fjerde ledd i sikkerhetsloven § 2, for å kunne fange opp eiere av kritisk infrastruktur som ikke var underlagt sikkerhetsloven fra før, se nærmere omtale i punkt 3.2.

Forslaget til ny § 29 a ble i høringsnotatet oppsummert slik:

> «Departementet foreslår en ny bestemmelse som gir Kongen i statsråd kompetanse til å nekte en anskaffelse til norsk kritisk infrastruktur gjennomført, dersom det foreligger en ikke ubetydelig risiko for rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser. Det gis også hjemmel til å sette vilkår ved enkelte anskaffelser. Forslaget til ny bestemmelse vil supplere dagens regler om sikkerhetsgraderte anskaffelser, og tar sikte på å dekke behov som gjeldende regelverk ikke iva-

retar. Bestemmelsen er ment å være en sikkerhetsventil, og forutsettes benyttet kun i sjeldne tilfeller. Bestemmelsen vil kunne komme til anvendelse på kritisk infrastruktur som ikke tilfredsstiller kriteriene for å bli utpekt som skjermingsverdig objekt. Bestemmelsen pålegger også virksomhetene en varslingsplikt.»

Om forslaget til varslingsplikt sto det i høringsnotatet blant annet:

«Varslingsplikten vil kun påhvile virksomheter som loven gjelder for, dvs. forvaltningsorganer eller andre rettssubjekter som ved enkeltvedtak er omfattet av loven, jf. sikkerhetsloven § 2. […] Rettssubjekter som har kritisk infrastruktur, men som ikke er underlagt loven fra før, vil det bli aktuelt å fatte et avgrenset vedtak for, jf. ny § 2 fjerde ledd. Rettssubjektene vil da kunne bli underlagt varslingsplikten i § 29 a, men ikke loven for øvrig.

Det er den enkelte virksomhet som, basert på en samlet vurdering, må avgjøre hvorvidt det foreligger en anskaffelse som utløser varslingsplikt. […] I vurderingen vil det være sentralt hva som skal leveres, og til hvilke deler av infrastrukturen. Virksomheten skal ta stilling til om leveransen *kan* misbrukes til sikkerhetstruende virksomhet, *forutsatt* at leverandøren har ondsinnede intensjoner. Videre vil det være av sentral betydning hvilke leverandører som faktisk er aktuelle, og om leverandørene kommer fra land som Norge har et sikkerhetsmessig samarbeid med […]».

Når det gjaldt myndighetenes behandling av et eventuelt varsel stod det i høringsnotatet blant annet:

«Departementet antar at det i mange tilfeller som omfattes av § 29 a vil være naturlig å innhente uttalelse fra både Nasjonal sikkerhetsmyndighet, Politiets sikkerhetstjeneste og Etterretningstjenesten. Departementet vil også fremheve Nasjonal kommunikasjonsmyndighet (tidligere Post- og teletilsynet) som et mulig relevant organ. Offentlige organer plikter å bistå når de blir forespurt i medhold av § 29 a.

[…] Uttalelsene bør så langt det er mulig gi anbefalinger knyttet til valg av leverandør, og om eventuelle risikoreduserende tiltak.

Fagdepartementet skal, basert på de rådgivende uttalelsene, ta stilling til om den aktuelle anskaffelsen innebærer en akseptabel eller for høy risiko. […] Dersom risikoen anses som akseptabel og håndterbar, skal fagdepartementet meddele dette til virksomheten, og anskaffelsen kan gjennomføres. Dersom risikoen anses som for høy, og saken ikke kan løses tilfredsstillende ved bruk av tiltak i eget sektorregelverk, skal saken forelegges Kongen i statsråd med anbefalinger om tiltak.»

Departementet uttalte i notatet om selve hjemmelen til å fatte vedtak blant annet:

«Kongen i statsråd kan tillate anskaffelsen, tillate anskaffelsen på visse vilkår, eller nekte anskaffelsen gjennomført. Avgjørelsen vil måtte baseres på en helhetsvurdering der sikkerhetshensyn står sentralt, men der det også tas hensyn til blant annet økonomiske forhold og ønsket om hensiktsmessig utvikling av infrastruktur og næringsvirksomhet.»

11.2.2 Andre særlige momenter omtalt i høringsforslaget

Om forholdet til internasjonale forpliktelser uttalte departementet i høringsnotatet side 33 følgende:

«Departementet har vurdert forholdet til Norges internasjonale forpliktelser – herunder forholdet til WTO-avtaleverk (GATT, GATS, GPA og TRIPS), EØS-avtalen, Norges bilaterale frihandelsavtaler og Norges bilaterale investeringsbeskyttelsesavtaler. […] Departementet har konkludert med at selve innføringen av bestemmelsen ikke vil være i strid med internasjonale forpliktelser, men at vedtak som Kongen i statsråd eventuelt fatter i medhold av bestemmelsen, vil måtte vurderes individuelt. Denne vurderingen må foretas ut fra det konkrete vedtaket som Kongen i statsråd fatter i saken, og omfanget av dette sett opp mot den eller de internasjonale forpliktelsene som gjør seg gjeldende i den aktuelle saken. Generelt kan det sies at de fleste internasjonale avtalene som Norge er part i, inneholder unntak for såkalte 'essensielle sikkerhetsinteresser', eller lignende. Unntakene er jevnt over snevre, men de innebærer at Norge vil kunne påberope seg at vedtak fattet i medhold av § 29 a må godtas under henvisning til at vedtaket ivaretar Norges essensielle sikkerhetsinteresser. Sikkerhetsklausulene er ulikt formulert i de ulike rettsaktene, og det må derfor legges til grunn at adgangen for unntak er ulik, avhengig av

> hvilket regime det dreier seg om. […] Det finnes også supplerende folkerettslige prinsipper som kan benyttes til å begrunne vedtak ut fra de samme betraktningene, herunder det folkerettslige prinsippet om 'necessity'.»

Forholdet til Grunnloven ble i høringsnotatet side 33 beskrevet slik:

> «Departementet har vurdert forholdet til Grunnloven, og har herunder særlig vurdert forholdet til §§ 97 og 105 om henholdsvis tilbakevirkende kraft og ekspropriasjon. Som omtalt ovenfor, vil bestemmelsen ikke kunne anvendes på avtaler som blir inngått før loven trer i kraft, og bestemmelsen vil derfor ikke komme i konflikt med Grunnlovens § 97. Hva gjelder forholdet til § 105 (samt EMKs tilleggsprotokoll 1 art. 1), vil den klare hovedregelen være at inngripen i avtaler som omfattes av § 29 a, ikke anses som ekspropriasjon vernet av § 105. Dette kan imidlertid stille seg annerledes dersom myndighetene griper inn i en avtale lenge etter at avtalen ble inngått, og der hvor ingen av avtalepartene har skyld i at myndighetene ikke har grepet inn på et tidligere tidspunkt. Det kan i et slikt tilfelle potensielt oppstå et krav på erstatning, forutsatt at vedtaket kan sies å gripe inn i en etablert formuesposisjon.»

Forholdet til anskaffelsesregelverket ble i høringsnotatet side 34 beskrevet slik:

> «Virksomheter som er underlagt anskaffelsesregelverket og som skal foreta en anskaffelse som vil kunne utløse varslingsplikt etter § 29 a, må som utgangspunkt følge anskaffelsesregelverkets prosedyrer. Virksomheten bør imidlertid så tidlig som mulig i prosessen kommunisere utad at det kan bli foretatt en sikkerhetsmessig vurdering av både anskaffelsen og aktuelle kandidater, og at det foreligger en risiko for myndighetsinngripen etter § 29 a. Slik informasjon vil gi bedre forutsigbarhet for aktuelle tilbydere. Dersom det anses nødvendig å fravike anskaffelsesregler for å etterleve § 29 a, må det vurderes konkret om det foreligger hjemmel for dette i hvert enkelt tilfelle.»

Om sanksjoner sto følgende i høringsnotatet side 34:

> «Departementet har vurdert om det bør gis hjemmel til å ilegge administrative sanksjoner eller straff ved brudd på varslingsplikten i § 29 a. Departementet har imidlertid valgt ikke å foreslå dette. Departementet mener det er tilstrekkelig som «sanksjon» at Kongen i statsråd har mulighet til å gripe inn i inngåtte avtaler, i de tilfeller der varslingsplikten er brutt (jf. bestemmelsens andre ledd, andre punktum).»

Spørsmålet om tilbakevirkende kraft ble i høringsnotatet side 33 omtalt slik:

> «Bestemmelsen gis ikke tilbakevirkende kraft. Avtaler som allerede er inngått når bestemmelsen trer i kraft, kan det ikke gjøres inngrep i. Departementet presiserer at forslaget til andre ledd andre punktum (*'Dette gjelder også dersom det allerede er inngått avtale om anskaffelsen')* ikke sikter til avtaler som ble inngått før loven trådte i kraft, men til tilfeller der myndighetene får kunnskap om en avtale først etter at den er inngått.»

11.3 Høringsinstansenes syn

11.3.1 Sammendrag

25 høringsinstanser har gitt merknader til forslaget til § 29 a, og flere av innspillene er omfattende.

Høringsinstansene er delte i sitt syn på bestemmelsen. Noen høringsinstanser er positive og mener bestemmelsen vil gi bedret sikkerhet knyttet til anskaffelser. Blant disse er *Cyberforsvaret, Forsvars- og sikkerhetsindustriens forening, Jernbaneverket, Nasjonal sikkerhetsmyndighet, Norsk romsenter, Politidirektoratet, Politiets sikkerhetstjeneste* og *Space Norway.*

Andre høringsinstanser er negative, og de frykter særlig for negative konsekvenser med hensyn til økonomi og tidsbruk. Blant disse er *Abelia, Den Norske Bank (DNB), Energi Norge, Finans Norge, Forsvarsbygg, Kraftcert AS, Norges vassdrags- og energidirektorat (NVE), Statnett, Telenor* og privatpersonen *Anders Bakke.*

Det er særlig den foreslåtte varslingsplikten flere av høringsinstansene har innvendinger mot. Flere instanser tror bestemmelsen vil bli vanskelig å praktisere, og noen av disse mener at begrepene som benyttes i bestemmelsen er uklare. Flere instanser problematiserer også sammenhengen mellom bestemmelsen og annet regelverk, særlig anskaffelsesregelverket og regelverk innen sektorene finans og kraft.

11.3.2 Begrepet «kritisk infrastruktur»

Mange av høringsinstansene etterspør en legaldefinisjon av begrepet «kritisk infrastruktur». Blant

disse er *Arbeids- og sosialdepartementet*, *Departementenes servicesenter*, *Direktoratet for samfunnssikkerhet og beredskap*, *Forsvarets logistikkorganisasjon*, *Jernbaneverket*, *Nasjonal kommunikasjonsmyndighet (Nkom)*, *Norges Bank*, *NVE*, *Petroleumstilsynet*, *Politidirektoratet* og *Telenor*.

Flere av disse instansene mener en definisjon er påkrevd for å få en felles begrepsforståelse, og for at bestemmelsen skal bli forutsigbar å praktisere.

Norges Bank uttaler at etableringen av «kritisk infrastruktur» som et begrep på siden av det allerede eksisterende «skjermingsverdige objekter», gjør regelverket komplisert. Og videre oppfatter banken at «kritisk infrastruktur» i forslaget til ny § 29 a i for liten grad gir en avgrensning nedad mot infrastruktur som ikke er ansett som kritisk. Norges Bank mener at en slik avgrensning «med fordel kan gjøres i lovens § 3, eventuelt utdypet i forskrift, da eventuelt som begrepet 'kritisk infrastruktur og kritiske samfunnsfunksjoner'».

NVE bemerker at «teknologisk utvikling tilsier at statisk identifisering/kartlegging fra departementenes side neppe vil oppfylle bestemmelsens intensjon». Videre legger NVE til grunn at sikkerhetsloven gjelder for kritisk infrastruktur som er av betydning for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. NVE skriver:

> «Med henvisning til tidligere prosesser rundt innmelding av skjermingsverdige objekter, har FD og OED/NVE hatt ulik oppfatning av hvilken infrastruktur som oppfyller dette kriteriet. Det bør ved en eventuell lovendring klargjøres nærmere operasjonelle kriterier for hva som kan karakteriseres kritisk infrastruktur som faller inn under lovens formål.»

Petroleumstilsynet uttaler:

> «Hva som menes med 'kritisk infrastruktur' i denne sammenhengen er uklart, og potensielt meget omfattende, jf. høringsnotatet punkt 2.7.1. Dette innebærer en fleksibilitet i bestemmelsens anvendelsesområde, og samtidig en betydelig grad av uforutsigbarhet for mulige pliktsubjekter, herunder private rettssubjekter i petroleumsnæringen, med tanke på om det vil bli fattet vedtak etter § 2 fjerde ledd eller ikke. De potensielt store konsekvensene av å bli omfattet av vedtak etter § 2 fjerde ledd tilsier at det tydeliggjøres bedre hva som faller inn under begrepet 'kritisk infrastruktur'.»

11.3.3 Normen «ikke ubetydelig risiko»

Flere høringsinstanser mener vurderingsnormen «ikke ubetydelig risiko for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser» kan bli vanskelig å praktisere, og at normen bør klargjøres. Blant høringsinstansene som anfører dette er *Energi Norge, Anders Bakke, Jernbaneverket, Nkom, Norsk olje og gass, Petroleumstilsynet* og *Finans Norge.*

Nkom uttaler at man «vurderer terskelen for varsling, 'ikke ubetydelig risiko', til å være relativt lav. Kombinert med at vedtakskompetansen foreslås å komme til anvendelse også 'dersom det allerede er inngått avtale om anskaffelsen', og at infrastruktureier dermed vil ha et insentiv til å varsle i tvilstilfeller, vil dette slik Nkom ser det kunne lede til et betydelig antall varslinger etter den foreslåtte § 29 a».

Anders Bakke bemerker at «[d]en foreslåtte regelen mangler beskrivelse av hva virksomheten skal vurdere risiko eller sannsynlighet for hva slags konsekvens eller uønsket hendelse eller tilstand reglen sikter til».

11.3.4 Bestemmelsens forhold til annet regelverk

Flere høringsinstanser etterspør hvordan § 29 a forholder seg til annet regelverk. *Energi Norge, DNB, Norges Bank, NVE* og *Statnett* spør særlig hvordan bestemmelsen forholder seg til reglene om offentlige anskaffelser.

DNB peker på at ansvaret for å sikre finansiell stabilitet allerede ligger under Norges Banks ansvarsområde, jf. sentralbankloven § 1. DNB refererer til finanstilsynsloven § 4 c og lov 17. desember 1999 nr. 95 om betalingssystemer m.v., og viser til at både Norges Bank og Finanstilsynet har hjemmel for å nekte etablering og sette vilkår for etablering og drift. DNB mener disse hjemlene fullt ut er tilstrekkelig for myndighetene til å kunne vurdere om etablering og drift vil være til ikke ubetydelig risiko for rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser.

Energi Norge mener «kraftforsyningen i økende grad underlegges en dobbelregulering fra to ulike regelverk og tilsynsmyndigheter: a) Energilovens krav til beredskap og sikring forvaltet av OED og NVE, b) Nye krav og regler forvaltet av Forsvarsdepartementet og NSM. Hvordan ansvars- og rollefordelingen mellom OED og Forsvarsdepartementet og mellom NVE og NSM skal håndteres, fremgår ikke så langt vi kan se av høringsforslaget.».

Finans Norge uttaler at det er behov for kunnskap om anskaffelser mv innen bank, finans og betalingsforetak som foreslås håndtert gjennom en utvidelse av sikkerhetslovens virkeområde, bør kunne håndteres gjennom koordinering mellom ulike departementer og myndighetsorganer, framfor å underlegge finansnæringen ytterligere reguleringer.

Nkom peker på at det ikke framgår av høringsnotatet hvordan hensynet til kontradiksjon overfor verken eiere av infrastruktur, eller leverandøren(e) som risikerer å bli utestengt, vil bli ivaretatt. Nkom legger til grunn at forvaltningslovens regler vil gjelde også i saker etter § 29 a, og mener at forholdet til dette regelverket med fordel kan beskrives nøyere i forarbeidene til endringene i sikkerhetsloven.

NVE mener det bør komme klarere fram hvilke typer anskaffelser varslingsplikten vil kunne komme til anvendelse på, og forutsetter at det utarbeides veiledningsmateriale som gir nærmere informasjon.

Norges Bank uttaler at det er et behov for at det gjøres klarere om paragrafen får virkning både for kritisk infrastruktur, som i dag ikke er omfattet av sikkerhetsloven, og for utpekte skjermingsverdige objekter. Banken forutsetter også at det gis nærmere bestemmelser om hvordan lovbestemt taushetsplikt utenom sikkerhetsloven (jf. for eksempel sentralbankloven § 12) skal ivaretas der varsling må foretas til eksterne.

Statnett er positiv til at det gis anledning til å vurdere en leverandørs sikkerhetsmessige skikkethet, og at det på lovmessig grunnlag gis anledning å nekte en anskaffelse til kritisk infrastruktur. Samtidig vises det til at Statnett allerede er underlagt et detaljert og omfangsrikt sikkerhets- og beredskapsregelverk i energilovens beredskapsforskrift. Selskapet ser det som uheldig å splitte opp regelverket knyttet til sikkerhet og beredskap i to ulike lover med to ulike forvaltningsmyndigheter. Statnett mener underleggelse av deler av sikkerhetsloven vil føre til en uoversiktlig og kompliserende situasjon, og at framtidige utvidelser og endringer derfor må skje innenfor energiloven.

11.3.5 Praktiseringen av bestemmelsen

Flere høringsinstanser har uttalt seg om praktiseringen av bestemmelsen, og mulige problemer knyttet til dette. Blant annet om praktiske problemstillinger som kan oppstå ved anvendelsen av bestemmelsen i ulike sektorer.

Abelia understreker at transparens i anskaffelsesregelverket er svært viktig for at leverandører på et tidlig tidspunkt skal kunne foreta avveininger av egen deltakelse. Abelia mener at enkeltleverandører som ikke skulle være aktuelle må bli gjort oppmerksom på dette på et svært tidlig tidspunkt i prosessen og med klare begrunnelser slik at det er forutsigbarhet for den enkelte leverandør. Abelia mener at vurderinger av hvilke selskaper som eventuelt ikke er aktuelle som leverandører må baseres på objektive, transparente kriterier.

Direktoratet for samfunnssikkerhet og beredskap (DSB) uttaler at departementenes identifisering av kritisk infrastruktur i egen sektor bør ta utgangspunkt i en oversikt over kritiske samfunnsfunksjoner fra Justis- og beredskapsdepartementet. DSB viser til at Justis- og beredskapsdepartementet i henhold til kgl.res. 15. juni 2012 er tillagt ansvar for å «utarbeide og vedlikeholde oversikt over hvilke funksjoner som i et tverrsektorielt perspektiv er kritisk for samfunnssikkerheten».

Forsvars- og sikkerhetsindustriens forening påpeker behovet for at en ny varslingsplikt for virksomheter ledsages av godt veiledningsmateriale og at kriterier og varslingspliktens omfang, identifisering av rett adressat, samt formkrav kommuniseres tydelig til aktuelle bedrifter slik at rettstilstanden er forutsigbar for hver enkelt bedrift.

Nkom uttaler at «vurderingen av potensialet til statlige aktører i cyberdomenet er en vesentlig og dimensjonerende faktor for design av gode sikkerhetsløsninger. Opprinnelsesland for leverandør av utstyr er således en del av totalbildet. I IKT og ekomsektoren er imidlertid de fleste leverandører globale aktører som integrerer utstyr fra en rekke ulike underleverandører fra ulike land. Å avgjøre hvilket land utstyret 'kommer fra' vil dermed i en del tilfeller kun ha verdi som en teoretisk øvelse. [..] Effektive sikkerhetstiltak må dermed ha et bredere fokus enn hva den foreslåtte bestemmelsen isolert sett kan ivareta, og det er nødvendig at sikkerhetstiltakene omfatter tekniske, administrative og organisatoriske barrierer uavhengig av opprinnelsesland på utstyret til tilbyderne».

Videre peker Nkom på at deler av det som kan defineres som kritisk infrastruktur i enkelte norske ekomnett fysisk er plassert i utlandet (blant annet komponenter i enkelte kjernenett). Nkom anbefaler departementet å vurdere hvorvidt de foreslåtte reglene skal få anvendelse i slike tilfeller, eventuelt hvordan dette skal hensyntas i risikovurderingen etter § 29 a.

Nkom uttaler videre:

> «I høringsnotatets punkt 2.7.3 drøftes det hvilke momenter virksomheten må vurdere

ved anskaffelser til kritisk infrastruktur. Inngangsvilkåret er at leveransen kan misbrukes til sikkerhetstruende virksomhet, forutsatt at leverandøren har ondsinnede intensjoner. Nkom vil påpeke at dette vil være tilfellet for de fleste IKT anskaffelser til kritisk infrastruktur (både drifts- og støttesystemer). Systemene er komplekse, og det vil være svært vanskelig – i enkelte tilfeller umulig – å avdekke om det for eksempel er programmert inn bakdører eller funksjonalitet egnet for sabotasje.»

Nkom peker til slutt på at private virksomheter og for eksempel kommuner gjerne ikke vil ha lett tilgang til informasjon om, eller kompetanse til å vurdere, forhold knyttet til «rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser». Nkom mener dette særlig vil gjøre seg gjeldende for rettssubjekter som utelukkende omfattes av sikkerhetsloven etter den foreslåtte § 2 fjerde ledd, ettersom disse som utgangspunkt ikke vil kunne behandle gradert informasjon. Nkom mener virksomheter som utpekes i medhold av § 2 fjerde ledd vil ha særlig behov for veiledning og informasjon, ettersom disse ellers vil ha få eller ingen forutsetninger for å kunne foreta risikovurderingen det legges opp til.

Norges Bank mener forslaget til § 29 a i stor grad synes formulert ut fra anskaffelser av fysisk materiell og programvare. Norges Bank henstiller til at det gis en nærmere beskrivelse av hvordan anskaffelse av kommunikasjonstjenester, samt rådgivnings- og systemdriftstjenester til kritisk infrastruktur eventuelt berøres av den nye § 29 a.

NVE legger til grunn at all infrastruktur som bestemmelsen kan tenkes å bli gjort gjeldende for, er underlagt en eller annen form for offentlig regulering. NVE mener derfor det bør presiseres at det må være det enkelte departements ansvar løpende å vurdere om ny infrastruktur eller planlagte endringer i eksisterende infrastruktur kan være av betydning for rikets selvstendighet og sikkerhet.

Norsk olje og gass uttaler at det før ikrafttredelse bør «være et strukturert system på plass, herunder kompetanse, forståelse og bevisstgjøring hos virksomhetene om hvilke type anskaffelser som kan innebære en ikke ubetydelig risiko for rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser».

Norsk romsenter uttaler at dette er en viktig endring som sikrer mulighet for bedre å ivareta sikkerhetsmessige krav til kritisk infrastruktur. Samtidig mener romsenteret at det er viktig at saksbehandling kan foretas så raskt som mulig og at Nasjonal sikkerhetsmyndighet ivaretar sin veiledningsplikt på kost- og tidseffektiv måte.

Petroleumstilsynet antar at det vil kunne være krevende, særlig for private rettssubjekter, å vurdere om det foreligger varslingsplikt. Tilsvarende mener tilsynet at det vil være krevende for myndighetene å følge opp hvorvidt varslingsplikten overholdes. Det kan ikke se at det er omtalt hvordan dette skal følges opp og hva som vil være konsekvensen for virksomheten av ikke å overholde varslingsplikten.

Statnett uttaler:

«En samlet vurdering vil etter vårt skjønn innebære å ha informasjon og kompetanse om forhold som kun EOS-myndighetene innehar. For å gjennomføre en samlet vurdering som ivaretar disse forholdene, vil det med forslaget til ny lovtekst, kun være mulig å få dette til ved å varsle om anskaffelsen da et varsel utløser en mulig vurdering fra kompetente myndigheter. Det er per i dag heller ingen formalisert kanal for å få opplysninger om leverandør eller underleverandører kommer fra et land som Norge har et sikkerhetsmessig samarbeid med.»

Statnett uttaler videre:

«I departementets høringsforslag fremgår det ikke hvor lang saksbehandlingstiden vil være etter en eventuell varsling iht. ny § 29 a. Som det fremkommer over, vil en saksbehandlingstid som trekker ut i tid, kunne føre til en ikke hensiktsmessig uforutsigbarhet når det gjelder tid, kost og kvalitet.»

11.3.6 Mulige konsekvenser av bestemmelsen

Flere høringsinstanser har uttalt seg om mulige konsekvenser av bestemmelsen, og om hvorvidt det er hensiktsmessig å innføre en slik bestemmelse. En fellesnevner for flere av innspillene er at høringsinstansene frykter negative konsekvenser, og da særlig med hensyn til tidsbruk og økte kostnader.

Abelia uttaler at det vil være svært uheldig dersom endringer i lovverk og bestemmelser skulle få utilsiktede, uheldige og fordyrende konsekvenser for norsk næringsliv.

DNB uttaler at med mindre tilsvarende bestemmelser gjelder for DNBs største konkurrenter, også utenlandske, vil dette kunne påvirke DNBs konkurransesituasjon betydelig i negativ retning. DNB mener bestemmelsen vil kunne

medføre at DNBs anskaffelser blir mer kostbare på grunn av mangelfull relevant konkurranse mellom aktuelle leverandører, og videre at begrensninger i hvilke leverandører som kan velges, kan medføre at godkjente aktuelle leverandører over tid verken holder tritt med den tekniske utvikling, kravene til kompetanse eller generell prisutvikling på området. DNB mener myndighetene allerede har anledning til å sette de vilkår som er nødvendige for nasjonal sikkerhet, og uttaler:

> «Ytterligere regulering av finansnæringen på dette området er derfor unødvendig og vil bare skape ytterligere byråkrati både for myndighetene og finansnæringen. Det vil neppe være i tråd med Regjeringens reform for avbyråkratisering og effektivisering.»

DNB uttaler at «det er unødvendig å gi en ny hjemmel for å pålegge en gjennomregulert bransje ytterligere plikter til rapportering enn de som allerede er pålagt selskapet i dag. Sikkerhetsmyndighetenes behov for oversikt og kunnskap bør dekkes gjennom intern koordinering og informasjonsflyt på myndighetssiden».

Energi Norge mener forslaget vil få særlig betydning for private virksomheter i energi- og ekomsektoren som i dag ikke er omfattet av sikkerhetsloven. For virksomheter som allerede er omfattet av sikkerhetsloven, kan forslaget etter Energi Norges syn innebære ytterligere byråkratisering og begrensninger i salg og leveranser av tjenester som både vil forsinke og fordyre dagens anskaffelsesprosesser. Energi Norge uttaler:

> «Nye reguleringer som svekker tempoet i utvikling og tilpasning av kraftsystemet kan i seg selv svekke forsyningssikkerheten. Omfanget av lovforslaget og konsekvensene for norsk kraftsektor knyttet til nytteverdi og kostnader for samfunnet er så langt vi kan se ikke utredet. Dette bør gjøres før eventuelle endringer gjennomføres.»

Energi Norge mener dessuten det er naturlig å avvente både Lysneutvalgets konklusjoner og Sikkerhetsutvalgets anbefalinger før eventuelle endringer i sikkerhetsloven foretas.

Finans Norge mener at «medarbeidere i finansbedrifter generelt neppe har tilstrekkelig kompetanse til å foreta en god vurdering av hvorvidt anskaffelsen innebærer en 'ikke ubetydelig risiko for rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser'». Etter Finans Norges syn kan en slik vurdering best foretas av myndighetene på grunnlag av koordinering mellom myndighetsorganer basert på allerede etablert pliktig anskaffelsesrapportering for virksomheter i finansiell sektor. Det er Finans Norges vurdering at forslaget ikke bidrar til økt sikkerhet for kritisk infrastruktur i finansiell sektor. Finans Norge viser til at bankvirksomhet, herunder betalingsformidling og interbankavregning og -oppgjør, er konsesjonsbelagt virksomhet og allerede underlagt en lang rekke rapporteringskrav og tilsyn fra ulike myndigheter. Finans Norge mener ytterligere krav om rapportering til flere instanser for samme anskaffelse/underleverandør vil være kostnadsdrivende både for myndighetene og for virksomhetene uten at det vil ha positive effekter.

Finans Norge savner en bredere diskusjon om alternative måter å oppnå det samme på, framfor å introdusere nye rapporterings- og inngrepstiltak. Finans Norge viser til at finansnæringen allerede nå samarbeider med myndighetene, blant annet ved samarbeidsavtale mellom FinansCERT og NorCERT. Finans Norge oppfatter at Lysneutvalgets mandat legger opp til en vurdering av denne type samarbeide, og mener det er uheldig at det nå foreslås ny spesifikk regulering innenfor en av de sektorene Lysneutvalget vurderer.

Forsvarsbygg uttaler:

> «Forslaget sier ingen ting om på hvilket tidspunkt i anskaffelsesprosessen varselet skal gis. I og med at leverandøren skal vurderes, kan Forsvarsbygg vanskelig se at den aktuelle vurderingen kan gjennomføres på et tidligere tidspunkt enn etter evalueringen av innkomne tilbud er gjennomført. Dette vil innebære at den foreslåtte endringen vil ha konsekvenser for tiden det tar å gjennomføre en anskaffelse. Den tidsmessige forsinkelsen vil tilsvare saksbehandlingstiden for å håndtere varselet. De kostnadsmessige konsekvenser ved økt tidsbruk som er vurdert på side 41 i høringsnotatet – herunder at det tilsynelatende er lagt til grunn at det ikke vil ha noen konsekvenser for leverandører som allerede er omfattet av lov om offentlige anskaffelser – fremstår dermed som uriktig.»

KraftCERT mener forslaget vil medføre en dobbeltregulering av en betydelig mengde selskaper i flere sektorer, deriblant energi- og petroleumsindustrien, samt finans- og helseforetak. KraftCERT mener at «dobbeltreguleringen vil kunne lede til uklarheter i forståelse av gjeldende regler og derfor også forsinkelser i eksisterende sikringsarbeid

og -tiltak. I tillegg vil det potensielt føre til betydelige og unødige kostnader, ikke minst i form av økt byråkrati». KraftCERT uttaler videre:

> «I dag reguleres større anskaffelser av sektorielle myndigheter, så foruten dobbeltregulering vil dette øke sannsynligheten for store anskaffelsesprosjekter med betydelige forsinkelser. I tillegg vil mer omstendelige anskaffelsesprosedyrer lede til potensielt store økte kostnader.»

Nkom er bekymret for at «det som er tenkt som en 'sikkerhetsventil' for særlige tilfeller i realiteten vil framstå som en godkjenningsordning, som kan lede fokus bort fra behovet for, og forventningene til, et helhetlig sikkerhetsregime. En slik utvikling kan igjen medføre større sikkerhetsrisiki enn hva bestemmelsen i realiteten vil kunne benyttes til å verne mot. Nkom anbefaler derfor primært at det ikke gis noen form for 'godkjennelse' av anskaffelsen på den foreslåtte måte, annet enn at virksomheten får beskjed om at et vedtak er fattet i den ene eller andre retning. Alternativt bør informasjonen til virksomheten tydelig gjøre oppmerksom på om det anses at det er vilkårene som ikke er oppfylt eller om Kongen i statsråd har lagt avgjørende vekt på andre hensyn.»

Norges Bank uttaler:

> «I høringsnotatet vises det til at de fleste anskaffelser som blir berørt av varslingskravet allerede er underlagt regelverk om offentlige anskaffelser, og at man legger til grunn at konsekvensene grunnet økt tidsbruk derfor ikke vil bli vesentlige. Norges Bank har vanskelig for å se at ikke varslingsplikt, departementets innhenting av informasjon og vurderinger fra relevante organer mv. vil kreve betydelig tid og vil kunne medføre vesentlige forsinkelser i anskaffelsesprosjektene. Dette spesielt ved innhenting av informasjon om leverandører som befinner seg utenfor Europa. På denne bakgrunn mener Norges Bank at det bør fremgå at behovet for sikkerhetsvurderinger ikke skal medføre unødvendige forsinkelser i anskaffelsesprosjektene.»

NVE peker på at en bestemmelse som pålegger virksomheter med kritisk infrastruktur, men hvor infrastrukturen ikke er skjermingsverdige objekter, i praksis må anses som en utvidelse av sikkerhetslovens virkeområde. NVE uttaler:

> «En slik endring vil i praksis signalisere at sikkerhetslovens bestemmelser om sikkerhetsgraderte anskaffelser har et videre anvendelsesområde enn til å gjelde anskaffelser som involverer skjermingsverdig informasjon eller objekter. Det kan således stilles spørsmål om ikke forslaget foregriper konklusjoner på vurderinger som er tiltenkt fase 2 av arbeidet med sikkerhetsloven.»

Petroleumstilsynet mener at systemet for varsling og videre saksbehandling etter ny § 29 a slik det foreslås lagt opp, vil kunne innebære en ikke ubetydelig tidsbruk, som antas å kunne være problematisk for blant andre petroleumsnæringen. Petroleumstilsynet peker videre på at dersom en anskaffelse nektes, eventuelt dersom det settes vilkår, kan dette få privatrettslige konsekvenser mellom den som skal anskaffe og leverandøren.

Statnett advarer mot å etablere en prosess som vil utsette kostbare, kompliserte og kritiske anskaffelser, og mener dette vil få uhensiktsmessig store økonomiske konsekvenser. Statnett mener «det vil være naturlig å varsle for å sikre seg mot en eventuell fremtidig inngripen av Kongen i statsråd etter kontraktsinngåelse. Dette igjen for å unngå store kostnader ved et eventuelt fremtidig kontraktsbrudd på en allerede inngått kontrakt. Det er da naturlig å anta at uforholdsmessig mange anskaffelser blir varslet, og dermed trekker uforholdsmessig ut i tid. En annen effekt vil kunne være at antallet leverandører som ønsker å delta i en anskaffelsesprosess blir færre. Dette med tilhørende mulige konsekvenser for kost og kvalitet.» Statnett mener at de økonomiske og administrative konsekvensene ikke er tilstrekkelig utredet og vurdert. Statnett mener at lovforslaget slik det framstår, ikke er formålstjenlig og vil kunne føre til mindre helhet i arbeidet med sikkerhet og beredskap.

Telenor uttaler:

> «Ved innføring av varslingsplikt om anskaffelse vil det innføres et forsinkende ledd for oss som virksomhet. Myndighetene må innrette seg slik at de på en meget rask og effektiv måte kan avklare om anskaffelsen trenger en særskilt risikovurdering eller ikke.»

Telenor uttaler videre:

> «Konsulentselskapet BDO har anslått at utgifter til implementering av nye retningslinjer for anskaffelser til respektive kritiske infrastruktur er ett årsverk pr virksomhet. BDO har i sin rapport antatt at tidsbruken ikke vil bli vesentlig endret da de fleste allerede er underlagt

regelen om offentlige anskaffelser. Telenor bemerker at private virksomheter ikke er underlagt offentlige anskaffelser og selv må utrede hvilke konsekvenser dette vil ha for virksomheten. Det antas fra Telenor sin side at myndighetene vil kompensere for de faktiske utgifter innføring av dette vil medføre.»

Telenor mener bestemmelsen ikke er forankret i en forståelse av kompleksiteten, sammenhengene og avhengighetene i dagens og framtidens IKT-infrastruktur og -bruk. Telenor mener det er uklart hvem som blir omfattet og hvilken rolle sektormyndigheten skal ha. Lovendringen virker etter Telenors syn forhastet og bør avventes og ses i sammenheng med neste fase i vurderinger av endring av sikkerhetsloven. Telenor mener det kan stilles spørsmål om slike særskilte krav ved anskaffelser til kritisk infrastruktur hører hjemme i sikkerhetsloven eller i den enkelte sektorlovgivning. Telenor uttaler:

«Telenor bidrar sterkt til å utvikle det digitale Norge, og gjør ikke dette alene. Våre leverandører bidrar aktivt med sin innovasjon og kunnskap for å sørge for at vi stadig utvikler oss. Telenor vil derfor utfordre myndighetens innstilling om å nekte anskaffelser. Det bør heller stilles særskilte sikkerhetskrav og åpenhet om hvordan anskaffelsene blir implementert.»

Utlendingsdirektoratet (UDI) uttaler at en eventuell varslingsplikt og påfølgende kvalitetskontroll av NSM vil være med på å kvalitetssikre enkelte anskaffelser, og vil ha en positiv effekt for sikkerheten i UDIs løsninger. UDI bemerker samtidig at: «Dersom NSM stiller strengere krav til sikkerhet enn vi tidligere har hatt, vil forslaget imidlertid kunne være kostnadsdrivende. Det samme gjelder varslingsplikt ved anskaffelser til kritisk infrastruktur.»

11.3.7 Andre innspill

Enkelte høringsinstanser har også kommet med innspill om andre temaer.

Jernbaneverket uttaler:

«Konsekvensen av å vurdere feil kan være betydningsfull og vi stiller spørsmål til om hver enkelt offentlig anskaffer vil ha tilstrekkelig oversikt til å kunne foreta en nasjonal sikkerhetsmessig vurdering. Vi foreslår derfor at hvilke anskaffelser som kan være av sikkerhetsmessig betydning avgjøres på et mer overordnet nivå.»

KraftCERT uttaler at dersom man virkelig ønsker å nå et mål om en sikrere infrastruktur, ville en naturlig løsning muligens være å gå i dialog med de sektorielle myndighetene om de eksisterende forskrifter og revisjoner i hver sektor. KraftCERT uttaler dessuten at: «Dersom det foreligger konkrete anbefalinger om anskaffelser bør dette kanaliseres gjennom sektorielle myndigheter, både fordi større transparens på tvers av sektorene vil kunne tilrettelegge for at det tas bedre avgjørelser i sikkerhetsøyemed, men kanskje særlig fordi dette gjør selskaper i stand til å vurdere og gjøre sikkerhetsundersøkelse av løsninger som allerede er anskaffet og satt i drift.»

Nkom deler departementets vurdering av at det ikke er nødvendig med sanksjonsbestemmelser for overtredelse av varslingsplikten som sådan, men anmoder departementet om å vurdere sanksjonsbestemmelser for overtredelse av Kongen i statsråds vedtak om nektelse av, eller vilkår for, anskaffelse.

NSM mener det må sikres at de offentlige organene som skal gi en 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. NSM mener hjemmelsgrunnlaget for informasjonsinnhenting bør tydeliggjøres i bestemmelsen og/eller dens forarbeider. NSM frykter at myndighetene vil vise tilbakeholdenhet med å fatte enkeltvedtak om nye virksomheter som eier eller rår over kritisk infrastruktur med hjemmel i nytt fjerde ledd i § 2, og at dette igjen vil gjøre at effekten av § 29 a vil bli liten.

Norges Bank foreslår at kritisk infrastruktur gjøres til et fjerde nivå av systemet med skjermingsverdige objekter. Banken uttaler:

«Av hensyn til en helhetlig tilnærming til sikkerhetsstyring vil banken tilrå at det i lovens kapittel 5 etableres et hierarki for kritisk infrastruktur og kritiske samfunnsfunksjoner i fire nivåer. Her kan de eksisterende skjermingsverdige objekter utgjøre de tre øverste nivåene, mens strukturene som omfattes av forslaget til ny § 29 a får et annet navn og legges på det fjerde, laveste, nivået. […]

Norges Bank vil også anbefale at det i denne sammenheng, og gjerne i forskrift, gis en nærmere avgrensning av hvilke sektorer som omfattes av 'kritisk infrastruktur' eller 'kritisk infrastruktur og kritiske samfunnsfunksjoner'. Dette kan være en parallell til de ni sekto-

rene som er definert som 'the national infrastructure' av britiske Centre for the Protection of National Infrastructure (CPNI), de 16 sektorene som er definert som 'critical infrastructure' i den amerikanske presidentens direktiv PPD-21 Critical Infrastructure Secutity and Resilience eller de 17 sektorene som ble nevnt av Infrastrukturutvalget (NOU 2006: 6). Det bør videre fremgå hvilke departement som har ansvar for hvilke sektorer.»

NVE mener den foreslåtte ordlyden til forskriftskompetanse i bestemmelsens tredje ledd er for vid i sin utforming.

Anders Bakke mener at høringsnotatet klart gir uttrykk for at regelen skal ha anvendelse på objekter som ikke er skjermingsverdige:

«I følge sikkerhetsloven § 17 første ledd, om utvelgelse av skjermingsverdige objekter, skal utvelgelse av disse objektene skje innenfor lovens formål. Objektene som det nå foreslås tiltaksregler for, faller derfor – slik jeg forstår det – utenfor lovens formål. Dette gjør det naturlig å foreslå at disse reglene, dersom de trer i kraft, heller får sin plass i en egen lov som omhandler andre sikkerhetsmessige hensyn enn de som faller inn under sikkerhetsloven.»

11.4 Departementets vurderinger

11.4.1 Innledning

Det framgår av høringen at flere store markedsaktører og bransjeorganisasjoner mener særlig varslingsplikten i § 29 a vil kunne virke kompliserende, forsinkende og fordyrende.

Varslingsplikten ble foreslått fordi departementet ønsket at myndighetene skulle få kjennskap til risikofylte anskaffelser, og på et så tidlig tidspunkt som mulig. Departementet mener dette fremdeles er et relevant og viktig hensyn.

På bakgrunn av høringsinnspillene foreslår imidlertid departementet flere justeringer i forslaget som ble sendt på høring. Formålet med justeringene er å gjøre bestemmelsen enklere å praktisere, samt å minske muligheten for at det oppstår uheldige konsekvenser av bestemmelsen. Departementet ønsker blant annet å gjøre det tydelig at virksomhetene selv har ansvaret for å vurdere risiko ved anskaffelser, og for å iverksette risikoreduserende tiltak. Videre vil departementet understreke at virksomhetenes egen håndtering er det primære, og at det kun i noen få saker vil være aktuelt å varsle myndighetene.

Departementet foreslår følgende fire hovedendringer sammenlignet med forslaget som ble sendt på høring:

1. Lovfeste at § 29 a skal gjelde alle virksomheter som foretar anskaffelser til kritisk infrastruktur, uavhengig av om virksomheten er underlagt sikkerhetslovens øvrige bestemmelser.
2. Innføre en uttrykkelig plikt for virksomhetene til å foreta risikovurderinger ved anskaffelser til kritisk infrastruktur.
3. Presisere at virksomhetene ikke behøver å varsle myndighetene dersom virksomhetene selv iverksetter risikoreduserende tiltak.
4. Gjøre begrepsbruken i bestemmelsen enklere.

I tillegg foreslår departementet flere mindre endringer basert på innspill i høringsrunden.

11.4.2 Plikt til å foreta en risikovurdering

Departementet foreslår at virksomheter pålegges en uttrykkelig plikt til å foreta en risikovurdering ved anskaffelser til kritisk infrastruktur. Meningen er å gjøre det tydelig at virksomhetene selv har ansvaret for å vurdere risiko ved anskaffelser og for eventuelt å iverksette risikoreduserende tiltak. Virksomhetenes varsling til myndighetene skal være et sekundært virkemiddel, forbeholdt spesielle situasjoner.

Det kan her trekkes paralleller til hvitvaskingslovens regler om kundekontroll, undersøkelsesplikt og rapporteringsplikt (jf. hvitvaskingsloven §§ 6, 17 og 18). På en lignende måte vil § 29 a fungere. Virksomhetenes egenkontroll og risikohåndtering vil være det ordinære, mens involvering av myndighetene vil være et ekstraordinært virkemiddel for spesielle situasjoner.

Departementet fremmer forslag om at virksomhetene skal foreta en risikovurdering ved alle anskaffelser til kritisk infrastruktur. Det er ikke et krav at vurderingen må være skriftlig, men departementet antar at skriftlighet generelt vil være det beste og mest riktige. Omfanget av risikovurderingene må tilpasses den enkelte anskaffelsen, og virksomhetene har selv ansvaret for å tilpasse ressursbruken.

Departementet anser det ikke hensiktsmessig å lage et fast sett med vurderingskriterier i loven, siden infrastrukturen er svært ulik, og det handler om svært ulike virksomheter. Virksomhetene må selv finne gode kriterier ut fra egen virksomhet og den aktuelle infrastrukturen. Skulle det imidlertid vise seg at praktiseringen av bestemmelsen blir vanskelig, kan det bli aktuelt å gi utdypende vurderingskriterier i forskrift. Departementet tar for

øvrig sikte på at det utarbeides veiledningsmateriell til bestemmelsen.

Virksomhetenes forutsetninger for å kunne vurdere risiko vil variere. Store virksomheter vil lettere kunne ha tilgang til egne tekniske miljøer og informasjon fra myndighetene om trusler og aktører som kan utgjøre en trussel, enn mindre virksomheter.

Alle eiere av kritisk infrastruktur må kunne forventes å ha inngående kunnskap om egen infrastruktur. Dette innebærer både kunnskap om verdien av infrastrukturen, altså dens betydning for samfunnet, og om potensielle sårbarheter ved infrastrukturen. Det kan derimot ikke forventes at alle eiere av kritisk infrastruktur skal ha kunnskap om mulige trusler og aktører som kan utgjøre en trussel. Dette er informasjon som primært besittes av myndighetene, og som i varierende grad deles med andre.

Mange virksomheter vil i sine risikovurderinger derfor måtte fokusere på sårbarheter ved infrastrukturen og ikke på trusler. Virksomhetene vil både måtte undersøke om anskaffelsen teknisk eller fysisk sett åpner en mulighet for at noen kan utføre eller legge til rette for sikkerhetstruende virksomhet og vurdere mulige konsekvenser av slik virksomhet.

Begrepet «ikke ubetydelig risiko» innebærer at det er situasjoner med risiko ut over det «normale» som skal varsles. Vurderingen vil måtte omfatte både sannsynlighet, sårbarhet og mulige konsekvenser. På sannsynlighetssiden innebærer kriteriet at det normalt ikke skal varsles dersom det kun foreligger en helt fjerntliggende eller rent teoretisk mulighet for at anskaffelsen skal kunne resultere i sikkerhetstruende virksomhet. Det bør være noe konkret med den aktuelle anskaffelsen som tilsier at risikoen er noe høyere enn ved andre anskaffelser. Bestemmelsen innebærer imidlertid ikke et krav om sannsynlighetsovervekt.

Departementet vil bemerke at det i mange tilfeller kan være tilnærmet umulig å gjøre nøyaktige sannsynlighetsberegninger av risikoen for at handlinger som spionasje, sabotasje og terror skal inntreffe. Man vil ofte ikke ha nok kunnskap om truslene til å få fullgode vurderinger, og ved for eksempel IKT-anskaffelser til kritisk infrastruktur kan det rent praktisk være svært vanskelig å avdekke om det for eksempel er programmert inn bakdører eller funksjonalitet egnet for sabotasje eller spionasje. I tilfeller der det ikke lar seg gjøre å få tilstrekkelig kunnskap til å vurdere sannsynligheten, vil vurderingen måtte bli konsentrert rundt sårbarhet og mulige konsekvenser.

Dersom virksomheten konkluderer med at det totalt sett foreligger en risiko, og denne er mer enn ubetydelig, bør virksomheten iverksette risikoreduserende tiltak. Slike tiltak kan for eksempel være tekniske, administrative eller organisatoriske barrierer. Slike barrierer kan i sum bidra til at det opprinnelige risikonivået reduseres til et ubetydelig nivå. Dersom virksomheten gjennom egne risikoreduserende tiltak får risikoen ned på et ubetydelig nivå, kan virksomheten gjennomføre anskaffelsen uten å varsle myndighetene.

11.4.3 Varslingsplikt

Departementet foreslår videre å pålegge en varslingsplikt for virksomheter som ønsker å gjennomføre en anskaffelse som innebærer en ikke ubetydelig risiko for sikkerhetstruende virksomhet. I forslaget som ble sendt på høring, kom det ikke tydelig fram at virksomhetene kunne unngå plikten til å varsle ved å iverksette egne risikoreduserende tiltak. Departementet foreslår derfor en ny ordlyd som uttrykkelig fastslår at plikten til å varsle ikke inntrer dersom virksomheten gjennom egne risikoreduserende tiltak fjerner risikoen, eller gjør den ubetydelig. Varslingsplikten vil dermed først inntre dersom en virksomhet likevel ønsker å gjennomføre en anskaffelse som innebærer en ikke ubetydelig risiko. Det kan være flere årsaker til at en virksomhet ønsker å gjennomføre en anskaffelse, selv om den innebærer en slik risiko. Virksomheten kan ha problemer med på egen hånd å identifisere egnede risikoreduserende tiltak, eller situasjonen kan være at man av økonomiske eller andre årsaker ikke ønsker å implementere tiltakene. Det kan også tenkes at virksomheten mener at det ikke lar seg gjøre å iverksette fullgode risikoreduserende tiltak uten å ha nærmere kunnskap om trusler og trusselaktører. I slike tilfeller vil en dialog med myndighetene kunne gi virksomheten informasjon som gjør det enklere å ta valg om risikoreduserende tiltak.

Varselet skal gis til overordnet departement. Private aktører og andre virksomheter som ikke har et overordnet departement i forvaltningsrettslig forstand, skal varsle til det departementet som forvalter regelverket i den aktuelle sektoren. Ved uklarhet kan varselet gis til Forsvarsdepartementet. Offentlige virksomheter med tilhørighet til flere departementer må varsle det aktuelle departementet som virksomheten anser som mest relevant i den konkrete saken, jf. det som er sagt under punkt 4.4.2.2. Dersom det skulle vise seg å være feil, vil vedkommende departement som

mottar varselet, videreformidle dette til rett departement.

11.4.4 Myndighetenes behandling av et varsel

Som foreslått i høringen, går departementet inn for at et departement som mottar et varsel, bør innhente rådgivende uttalelser fra relevante organer. Her vil blant annet Politiets sikkerhetstjeneste, Etterretningstjenesten og Nasjonal sikkerhetsmyndighet kunne være aktuelle organer. De rådgivende organene vil kunne benytte alle kildene som organet har lovlig tilgang til. Uttalelsene bør redegjøre for sårbarheter og trusler, og så langt det er mulig også inneholde konkrete råd om valg av risikoreduserende tiltak og leverandører.

Etter å ha samlet nødvendig informasjon, kan saken avgjøres i departementet. Departementet kan tillate anskaffelsen slik den er tenkt, eller departementet kan gjøre sikkerhetsmessige tilpasninger i dialog med virksomheten. Eventuelt kan departementet fatte vedtak ved bruk av hjemler i sektorregelverk. Dersom departementet ikke skulle finne tilfredsstillende løsninger ved bruk av disse virkemidlene, kan departementet fremme saken for Kongen i statsråd med anbefalinger om tiltak.

Kongen i statsråd kan treffe vedtak om å nekte anskaffelsen gjennomført. Det kan også være aktuelt med mindre inngripende vedtak, som pålegg om risikoreduserende tiltak, eller å sette andre vilkår for gjennomføringen.

Grunnvilkåret for at Kongen i statsråd skal ha vedtakskompetanse, er at det foreligger en ikke ubetydelig risiko. I tillegg må vedtak fra Kongen i statsråd være innenfor lovens formål. Sistnevnte vil si at vedtaket må være innrettet for å «motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser», jf. § 1. Det er som følge av dette ikke enhver type sikkerhetstruende virksomhet Kongen i statsråd kan fatte vedtak for å stanse. For eksempel innebærer formålsbegrensningen at det ikke er hjemmel til å gripe inn ved risiko for industrispionasje som kun er egnet til å skade en enkeltbedrifts forretningsvirksomhet.

11.4.5 Forholdet til andre pågående utredningsprosesser

Noen høringsinstanser mener lovarbeidet burde stanses i påvente av arbeidet til det digitale sårbarhetsutvalget (Lysneutvalget) og Sikkerhetsutvalget (Traavikutvalget). Departementet vil til dette påpeke at noe av bakgrunnen for at arbeidet med sikkerhetsloven ble delt i to faser, var nettopp behovet for å få på plass enkelte endringer i sikkerhetsloven raskt, samtidig som andre problemstillinger skulle vurderes av et utvalg. Det er etter departementets syn fremdeles behov for å få på plass § 29 a raskt. Lysneutvalgets rapport ble avgitt i november 2015. Denne gir ikke noen grunn til å avvente en behandling av foreliggende lovforslag. Sikkerhetsutvalget skal etter mandatet avlegge rapport i form av en NOU i oktober 2016, hvoretter rapporten vil bli sendt på bred høring.

11.4.6 Begrepsbruk

Høringsforslaget hadde en annen ordlyd enn forslaget slik det nå foreligger. I henhold til høringsforslaget inntrådte varslingsplikten dersom en anskaffelse innebar «en ikke ubetydelig risiko for rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser». Denne ordlyden er endret i departementets nye forslag, og bestemmelsen bruker nå ordlyden «ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført». Begrepet «sikkerhetstruende virksomhet» er definert i lovens § 3 som en samlebetegnelse for spionasje, sabotasje og terrorhandlinger. Endringen er gjort for å forenkle ordlyden, og for å gjøre det tydeligere hva som skal vurderes. Se de særskilte merknadene under punkt 13 for nærmere informasjon.

I § 29 a andre ledd er begrepet «ansvarlig fagdepartement» byttet ut med «overordnet departement». Endringen er ikke ment å innebære en realitetsforskjell, men er foretatt på bakgrunn av høringsinnspill om at begrepsbruken bør være lik i §§ 29 a og 5 a. For virksomheter som er organisatorisk underlagt et departement, er det i de fleste tilfeller klart hva som ligger i «overordnet departement». Enkelte virksomheter kan derimot være knyttet til flere departementer. Departementet viser til de særlige merknadene til § 29 a når det gjelder hvem det i slike tilfeller skal varsles til.

11.4.7 Begrepet «kritisk infrastruktur»

Flere høringsinstanser har ønsket en legaldefinisjon av begrepet «kritisk infrastruktur». Departementet anerkjenner at det kan være hensiktsmessig med en felles forankring av begrepets betydning i sikkerhetsloven, og departementet foreslår derfor å lovfeste en definisjon av begrepet. Departementet har valgt å definere kritisk infrastruktur kortere og noe annerledes enn det som følger av definisjonen i sivilbeskyttelsesloven § 3 bokstav d og definisjonen som Infrastrukturutvalget brukte i NOU 2006: 6 *Når sikkerheten er viktigst*. Den

foreslåtte formuleringen er ment å dekke de samme forholdene og lyder:

> «Kritisk infrastruktur; anlegg og systemer som er nødvendige for å opprettholde samfunnets grunnleggende behov og funksjoner.»

Departementet viser til punkt 11.1.1, hvor det er redegjort for definisjonen som ble brukt av Infrastrukturutvalget i NOU 2006: 6, og for mulig metodebruk for identifisering av kritisk infrastruktur i lys av den. Forslaget til ny definisjon er innholdsmessig lik definisjonen i NOU 2006: 6, og metodebruken for identifisering av kritisk infrastruktur vil også være lik.

11.4.8 Forholdet til annet regelverk

Flere høringsinstanser har stilt spørsmål om hvordan § 29 a forholder seg til annet regelverk. Det er særlig fire typer regelverk høringsinstansene nevner; reglene om offentlige anskaffelser, regler om taushetsplikt, regelverk innen energi og kraft og regler om varslingsordninger innen bank og finans.

Departementet foreslår å lovfeste i § 29 a at varslingsplikten gjelder uten hinder av lovbestemt taushetsplikt.

Når det gjelder regler om varslingsplikt og konsesjonsordninger innen bank og finans, vil § 29 a komme som et supplement til disse. Departementet mener at finanstilsynsloven § 4 c om godkjenning av utkontraktering av virksomhet og betalingssystemloven §§ 2-3 og 3-2 om konsesjon og meldeplikt, ikke fullt ut ivaretar de samme hensynene som forslaget til sikkerhetsloven § 29 a. Selv om hensynet til finansiell stabilitet er relevant når det gjelder beskyttelse av kritisk infrastruktur, er ikke regelverket for bank og finans innrettet mot risikoen for spionasje og sabotasje på samme måte som § 29 a. Departementet mener at Finanstilsynet og Norges Bank ikke bør pålegges å vurdere alle meldinger de mottar etter de nevnte reglene opp mot risikobegrepet i § 29 a. Derfor mener departementet at også aktører innen bank og finans skal varsle i medhold av § 29 a. Departementet kan ikke se at dette innebærer en uforholdsmessig stor byrde på disse aktørene, særlig med tanke på at antallet varsler i medhold av § 29 a trolig vil bli lavt.

Enkelte andre høringsinstanser har stilt spørsmål om forholdet mellom § 29 a og sikkerhetslovens regler om skjermingsverdige objekter. Bakgrunnen er at deler av norsk kritisk infrastruktur er utpekt som skjermingsverdige objekter. Loven pålegger eierne av infrastruktur som er utpekt som et skjermingsverdig objekt å beskytte infrastrukturen med beskyttelsestiltak, jf. § 17 b. I tillegg skal eventuelle anskaffelser til denne infrastrukturen gjennomføres som graderte anskaffelser. Departementet mener reglene om sikkerhetsgraderte anskaffelser i all hovedsak ivaretar de samme hensynene som § 29 a bygger på, og at det dermed vil være tilstrekkelig at en anskaffelse gjennomføres som en sikkerhetsgradert anskaffelse. Det vil som et resultat av dette ikke være nødvendig å varsle i henhold til § 29 a ved en sikkerhetsgradert anskaffelse.

Enkelte høringsinstanser viser til at selskaper innen kraft og energi til daglig er underlagt krav i energiloven og dens beredskapsforskrift, og at innføringen av § 29 a kan medføre en uoversiktlig situasjon og uklarhet omkring roller. Departementet kan ikke se at det vil være spesielt problematisk for selskapene innen kraft og industri å forholde seg til § 29 a. Det bør heller ikke oppstå uklarhet omkring roller, ettersom selskaper innen kraft og energi vil ha Olje- og energidepartementet som overordnet eller tilknyttet departement, og de kan derfor forholde seg til samme myndighet ved henvendelser om § 29 a som ved henvendelser relatert til energiloven og beredskapsforskriften.

Flere høringsinstanser har stilt spørsmål om forholdet mellom § 29 a og regelverket om offentlige anskaffelser. Ved anskaffelser til kritisk infrastruktur bør virksomhetene allerede i konkurransegrunnlaget innarbeide krav som bidrar til å redusere risikoen for at sikkerhetstruende virksomhet kan bli etablert eller gjennomført. Det kan være aktuelt med krav både til leverandørens kvalifikasjoner og til leveransen eller ytelsen. En forutgående risikovurdering av anskaffelsen kan være bestemmende for hvilke krav som er aktuelle å stille til leverandøren og anskaffelsen. Det bør også i konkurransegrunnlaget informeres om § 29 a, og at myndighetene vil kunne stille vilkår eller nekte anskaffelsen gjennomført dersom risikoen for etablering eller gjennomføring av sikkerhetstruende virksomhet ikke er ubetydelig.

I saker der det foreligger en ikke ubetydelig risiko, men virksomheten ikke kan eller ikke ønsker å innføre tilfredsstillende risikoreduserende tiltak, må det varsles. Det vil da være mest hensiktsmessig om virksomheten ikke utlyser konkurransegrunnlaget før varselet har blitt behandlet. Om mulig vil virksomheten, i dialog med departementet, kunne fastsette krav i konkurransegrunnlaget som på tilfredsstillende måte reduserer risikoen for sikkerhetstruende virksomhet. Dette vil kunne redusere usikkerheten

om mulige inngrep fra myndighetene på et senere tidspunkt. Det vil også kunne bidra til større forutsigbarhet for leverandørene, og sikre at kun leverandører som har en reell mulighet for å nå opp i konkurransen, bruker tid og ressurser på et tilbud. For å sikre at en slik prosess ikke unødig forsinker anskaffelser til kritisk infrastruktur, har departementet vurdert å foreslå saksbehandlingsfrister. Omfanget og kompleksiteten vil imidlertid kunne variere så vidt mye i slike saker, at det vanskelig kan fastsettes en konkret frist. Det er likevel en klar forventning om at myndighetene behandler slike saker raskt.

Departementet antar at mulige konflikter mellom anskaffelsesregelverket og § 29 a primært vil kunne oppstå dersom Kongen i statsråd vedtar å stanse eller stille vilkår til en anskaffelse. Et slikt vedtak vil potensielt kunne medføre erstatningskrav basert på anskaffelsesregelverket eller alminnelig erstatningsrett. Vedtakelsen av bestemmelsen vil i seg selv derimot ikke kunne medføre noe slikt krav.

11.4.9 Andre forhold som tas opp av høringsinstansene

Noen høringsinstanser spør hvilke saksbehandlingsregler og rettssikkerhetsgarantier som skal gjelde for bestemmelsen. Departementet vil bemerke at forvaltningslovens regler om enkeltvedtak vil gjelde også for vedtak som fattes av Kongen i statsråd. Vedtak fra Kongen i statsråd er ikke unntatt fra krav om begrunnelse eller reglene om innsyn. Et vedtak fra Kongen i statsråd kan ikke påklages eller klages inn for Sivilombudsmannen, men må eventuelt bringes inn for domstolene.

Det er også stilt spørsmål om bestemmelsens anvendelse for infrastruktur som er kritisk for Norge, men er fysisk plassert i utlandet. Departementet vil bemerke at regelen i utgangspunktet også gjelder for infrastruktur som befinner seg i utlandet, forutsatt at norske myndigheter har anledning å la norsk lov få anvendelse for infrastrukturen. Typisk vil det måtte være at et selskap med sitt hovedsete i Norge eier eller rår over den aktuelle infrastrukturen.

Alle typer anskaffelser vil i prinsippet kunne være aktuelle knyttet til bestemmelsen, også kommunikasjonstjenester og rådgivnings- og systemdrifttjenester, som det uttrykkelig er blitt spurt om.

Enkelte peker på at et eventuelt vedtak kan få privatrettslige konsekvenser mellom leverandør og oppdragsgiver. Departementet er innforstått med dette, og mener alle eiere av kritisk infrastruktur bør regulere i sine kontrakter hvilke konsekvenser en eventuell myndighetsinngripen etter § 29 a skal ha i forholdet mellom partene.

Departementet har blitt anmodet om å vurdere sanksjonsbestemmelser for overtredelse av Kongen i statsråds vedtak om å nekte eller sette vilkår for en anskaffelse. Departementet har valgt å regulere dette ved å ta inn følgende ordlyd i bestemmelsen:

> «Vedtak etter første punktum er særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.».

Etter nærmere overveielser fremmer departementet forslag om at ny § 2 fjerde ledd om virkeområde til ny § 29 a, skal ha en annen ordlyd enn den som ble foreslått i høringsrunden, se departementets vurdering i punkt 3.4.

Den nye ordlyden innebærer en forenkling, siden loven selv fastsetter at § 29 a gjelder for alle anskaffelser til kritisk infrastruktur, uavhengig av om virksomheten er underlagt sikkerhetslovens øvrige bestemmelser. Hensynet til forutsigbarhet for rettssubjektene skal ivaretas ved at departementene løpende informerer rettssubjektene etter hvert som kritisk infrastruktur identifiseres. Det foreslås å gi hjemmel i fjerde ledd andre punktum til å fastsette forskrift om hvordan kritisk infrastruktur skal identifiseres, og om hvordan rettssubjekter som eier eller rår over infrastrukturen skal informeres.

12 Økonomiske og administrative konsekvenser

12.1 Generelt

Departementet har vurdert de økonomiske og administrative konsekvensene av lovforslagene. Det er særlig forslagene som gjelder redusert klareringsmyndighetsstruktur, endringer i varighet av leverandørklarering, varslingsplikt og kompetanse for Kongen i statsråd til å fatte vedtak ved risiko for sikkerhetstruende virksomhet, og tilsvarende bestemmelse om anskaffelser til kritisk infrastruktur dersom samme type risiko foreligger, som det er sett nærmere på. Flere av forslagene har administrativ effektivisering som formål. Dette gjelder særlig forslagene om reduksjon av antall klareringsmyndigheter og endring av varighet på leverandørklareringer.

12.2 Reduksjon i antall klareringsmyndigheter

12.2.1 Særlig om klareringsmyndigheten i sivil sektor

Reduksjon av antall klareringsmyndigheter i sivil sektor forventes å ha en positiv samfunnsøkonomisk effekt. Den samfunnsøkonomiske besparelsen er beregnet til i overkant av 80 mill. kroner over 15 år. Besparelsen er knyttet til økt effektivitet ved at flere saker kan behandles med færre årsverk, og kostnadsbesparelser ved samlokalisering på ett sted i stedet for 26 ulike steder. Omorganiseringen er vurdert å gi bedre kvalitet i saksbehandlingen og kortere og mer forutsigbar ventetid for myndighetene som anmoder om sikkerhetsklarering.

Forslaget vil medføre overføring av bevilgninger til Justis- og beredskapsdepartementet fra departementer som i dag bevilger midler til sivile klareringsmyndigheter. De øvrige departementene (alle unntatt Forsvarsdepartementet) vil gjennom tiltaket redusere ressursbruk og utgifter på området, mens Justis- og beredskapsdepartementet overtar oppgaver (og utgifter). Det er beregnet at 26 virksomheter anvender ca. 24 årsverk på klareringsoppgavene i 2014. Det er knyttet en viss usikkerhet til beregningen av den besparelsen som her kan oppnås, idet departementer og virksomheter fortsatt vil opprettholde sitt ansvar som autorisasjonsmyndighet med blant annet innhenting av personopplysningsblanketter og gjennomføring av autorisasjonssamtaler. Imidlertid er hovedbegrunnelsen for omorganiseringen å få en bedre kvalitet i saksbehandlingen som kan sikre nødvendig kompetanse på behandling av klareringsanmodninger og gjennomføring av sikkerhetssamtaler mv. Omorganiseringen forventes også å gi en kortere og mer forutsigbar ventetid for myndighetene som anmoder om sikkerhetsklarering. Ekstrakostnader ved etablering av én sivil klareringsmyndighet vil dekkes innenfor berørte departementers gjeldende budsjettrammer gjennom inndekning av en forholdsmessig andel av kostnadene.

12.2.2 Særlig om klareringsmyndigheten i forsvarssektoren

Forslaget om en reduksjon av antallet klareringsmyndigheter vil ikke ha økonomiske eller administrative konsekvenser av betydning i forsvarssektoren. Forsvarets sikkerhetsavdeling (FSA) har allerede i dag hovedtyngden av klareringssaker i denne sektoren. Konkret innebærer forslaget at Forsvarsbygg og Forsvarets forskningsinstitutt (FFI) som klareringsmyndigheter opphører, ved at disse etatenes klareringssaker i framtiden skal behandles i FSA. Også Forsvarsdepartementets klareringssaker i første instans overføres til FSA. Etterretningstjenesten og Nasjonal sikkerhetsmyndighet beholder oppgaven som klareringsmyndighet for eget personell.

I en overgangsfase vil det være en risiko for noe økte restanser. Ved eventuelle ansettelser av personell til å foreta sikkerhetsklareringer skal disse sertifiseres og læres opp. Det vil derfor kunne ta noen tid før FSA oppnår full effektivitet på saksbehandlingen. Departementet foreslår derfor at det i en overgangsperiode tas høyde for å beholde noe av dagens portefølje i Forsvarsdepartementet og Forsvarsbygg. Forsvarsbygg foretar i dag også klareringssakene til FFI i henhold til egen avtale. Departementet mener det

kan være grunn til å ha en overgangsperiode på cirka ett år.

Departementet er kjent med at ressurssituasjonen i FSA er krevende, og det foregår parallelle prosesser, som forbedret saksbehandlingsverktøy og tilføring av økt saksbehandlingskapasitet, for å tilpasse ressursene til saksmengden. En samordning av klareringsmyndigheten i forsvarssektoren som foreslått, vil ikke medføre behov for nye lokaler eller større ressursoverføringer. Forslaget antas på den bakgrunn ikke å ha økonomiske eller administrative konsekvenser av betydning. Det tas sikte på en intern overføring av ressurser fra Forsvarsdepartementet og Forsvarsbygg til FSA i en grad som er tilpasset den økte saksbehandlingsmengden. Finansieringen av den foreslåtte endringen vil kunne foretas innen gjeldende budsjettrammer.

12.3 Varigheten av leverandørklareringer

Konsulentselskapet BDO har vurdert økonomiske og/eller administrative besparelser og konkurransevridende konsekvenser av å endre fra oppdragsbasert til tidsbasert leverandørklarering med varighet på opptil 5 år.

BDO konkluderer med at det ikke foreligger vesentlige økonomiske eller administrative konsekvenser forbundet med den foreslåtte endringen. Endringen antas først og fremst å bidra til at sikkerhetsgraderte anskaffelser kan gjennomføres hurtigere. BDO konkluderer videre med at den foreslåtte endringen kan ha en konkurransevridende effekt, i den forstand at endringen muligens kan føre til et komparativt konkurransefortrinn for leverandører med gyldig leverandørklarering på konkurransetidspunktet.

Departementet anser det som positivt at saksbehandlingstiden vil bli redusert med den foreslåtte endringen. Det vil gi mulighet til å gjennomføre sikkerhetsgraderte anskaffelser hurtigere og mere effektivt. Imidlertid registrerer departementet at endringen etter BDOs vurdering potensielt kan bidra til at noen aktører i markedet oppnår et konkurransefortrinn over tid. BDO skriver at dette potensielt kan gi en eller flere rådende aktører fordeler på lang sikt fordi det vil kunne være økonomisk fordelaktig for kjøperen (Forsvaret) å beholde eksisterende leverandører. BDO uttaler videre at det er viktig å ha et bevisst forhold til at slik problematikk kan oppstå, og eventuelt legge inn mekanismer for å redusere risiko for at dette inntreffer.

Departementet er enig i at det er viktig å ha et bevisst forhold til eventuelle konkurransevridende effekter. Eventuelle «mekanismer for å redusere risiko» er imidlertid allerede ivaretatt i gjeldende regelverk. Lov om offentlige anskaffelser stiller krav om at leverandører skal likebehandles og ikke diskrimineres. Etter departementets syn vil endringen fra oppdragsbasert til tidsbestemt leverandørklarering vanskelig kunne ha en konkurransevridende effekt uten at konkurransen samtidig er lagt opp på en måte som bryter med prinsippene i lov om offentlige anskaffelser. Videre mener departementet at tidsbestemte leverandørklareringer ikke vil være konkurransevridende dersom klareringsenheten evner å ta av store topper. Da vil en ny leverandør kunne bli klarert i tide og således reelt sett være med i konkurransen. I alle tilfeller er det svært viktig at gjeldende regelverk på området blir fulgt, således at ingen leverandører blir favorisert.

12.4 Anskaffelser til kritisk infrastruktur

Loven får i utgangspunktet ingen umiddelbare økonomiske konsekvenser for offentlig sektor. Et eventuelt varsel vil kreve oppfølging og ressursbruk hos departementet som mottar varselet, og hos myndigheter som blir anmodet om å avgi rådgivende uttalelser om leveransens risikopotensiale og leverandørens sikkerhetsmessige pålitelighet. Eventuelle merutgifter tas innenfor eksisterende rammer.

Iverksetting av loven vil få noen konsekvenser for virksomheter som eier eller rår over kritisk infrastruktur. Noen av disse virksomhetene vil måtte implementere nye retningslinjer og/eller rutiner for anskaffelser til kritisk infrastruktur. Den enkelte private virksomhet vil anslagsvis kunne påføres kostnader tilsvarende ett årsverk til implementering av nye rutiner/retningslinjer. Bestemmelsen vil også kunne medføre økt tidsbruk ved den enkelte anskaffelse, grunnet kravet om å vurdere risikoen ved anskaffelsen.

For anskaffelser som innebærer en ikke ubetydelig risiko for sikkerhetstruende virksomhet, vil de økonomiske konsekvensene kunne bli moderate for eiere av kritisk infrastruktur, både offentlige og private. Her vil det kunne påløpe kostnader til implementering av risikoreduserende tiltak, og det vil kunne bli ytterligere økt tidsbruk. Eventuelle merutgifter for det offentlige vil tas innenfor ordinære budsjettprosesser.

Dersom Kongen i statsråd vedtar å gripe inn i en anskaffelse, kan dette potensielt få store øko-

nomiske konsekvenser både for offentlig og privat sektor. De største konsekvensene antas å kunne komme ved vedtak om å utestenge én eller flere leverandører fra et marked. Spesielt innenfor ekomsektoren vil det kunne være aktuelt at varslingsplikten utløses på kort sikt. Forutsatt at et varsel medfører utestengelse av én eller flere leverandører fra ekommarkedet, er et anslag fra konsulentselskapet BDO at endringen kan medføre en kostnadsdrivende effekt på investeringer innenfor sektoren mellom 1 og 10 pst., dvs. 80 til 800 millioner kroner årlig. I tillegg kommer eventuelle effekter for driftskostnadene innenfor sektoren. Departementet vil påpeke at et vedtak om å utestenge leverandører i ytterste konsekvens vil kunne medføre kostnader på flere milliarder kroner for enkelttilbydere, forutsatt at Kongen i statsråd pålegger tilbydere å bytte leverandør i sin helhet. En konsekvens av slik utestengelse vil også kunne være reduserte investeringer, redusert innovasjon og redusert vekst i ekombransjen.

12.5 Varslingsplikt for virksomheter

Selve varslingsplikten antas ikke å ha større økonomiske eller administrative konsekvenser for berørte etater. Departementene vil kunne få noe økt veiledningsansvar ved innføring av varslingsplikt og påføres noe merarbeid ved oppfølging av varslinger. Utgiftene knyttet til dette vil tas innenfor gjeldende rammer.

Adgangen for Kongen i statsråd til å fatte nødvendige vedtak antas kun å bli brukt i svært sjeldne tilfeller. Eventuelle vedtak som blir gjort for å hindre en planlagt eller pågående aktivitet, vil etter omstendighetene kunne få økonomiske konsekvenser for berørte næringsdrivende.

Det er videre foretatt en vurdering av om regelendringen vil kunne gjøre Norge til et mindre attraktivt marked å investere i for globale aktører. Globale investorer vurderer vanligvis regulatorisk og politisk risiko ved investeringer i det globale markedet. Den foreslåtte bestemmelsen kan tolkes til å bidra til uforutsigbarhet i enkelte prosesser. Samtidig kan investorer i land som Norge har et sikkerhetsmessig samarbeid med, med høy grad av sannsynlighet kunne forutsette at bestemmelsen ikke vil gjøres gjeldende overfor potensielle investeringer. Videre blir utenlandske investeringer i Norge i praksis trygget av arbeidet som norske sikkerhetsmyndigheter gjør for å sikre landets selvstendighet og trygghet. I lys av dette kan utenlandske investorer se på den nye bestemmelsen som positiv, og at den kan bidra til å gjøre det norske markedet mer attraktivt å investere i.

13 Merknader til lovforslagene

Til § 2

Sikkerhetsloven § 2 angir lovens generelle virkeområde. Loven gjelder for forvaltningsorganer, definert som ethvert organ for stat eller kommune (§ 2 første ledd). Loven gjelder også for leverandører av varer eller tjenester til et forvaltningsorgan i forbindelse med en sikkerhetsgradert anskaffelse (§ 2 annet ledd). I tillegg kan loven, etter vedtak av Kongen, gjøres gjeldende for ethvert annet rettssubjekt som har ansvar for skjermingsverdig objekt eller gis tilgang til sikkerhetsgradert informasjon (§ 2 tredje ledd). I forskrift 27. juni 2003 nr. 802 om delegering av myndighet til Forsvarsdepartementet etter sikkerhetsloven § 3 tredje ledd, er Kongens myndighet delegert til Forsvarsdepartementet.

Nytt fjerde ledd angir virkeområdet til § 29 a om anskaffelser til kritisk infrastruktur. *Første punktum* slår fast at § 29 a gjelder ved alle anskaffelser til kritisk infrastruktur. Bestemmelsen innebærer at alle rettssubjekter som eier eller rår over kritisk infrastruktur, må forholde seg til § 29 a. Dette inkluderer også rettssubjekter som ikke ellers er omfattet av sikkerhetsloven. Rettssubjekter som eier eller rår over kritisk infrastruktur, vil således være underlagt pliktene i § 29 a, men ikke lovens øvrige plikter (med mindre dette følger av § 2 første til tredje ledd). *Andre punktum* gir Kongen myndighet til å gi forskrift om hvordan kritisk infrastruktur skal identifiseres, og om hvordan rettssubjekter som eier eller rår over kritisk infrastruktur skal informeres. Det vil ikke alltid være åpenbart om en infrastruktur skal anses som kritisk eller ikke. Hensynet til forutsigbarhet for de som eier eller rår over denne infrastrukturen, tilsier at myndighetene har gode rutiner for å gi informasjon som klargjør dette.

Hvilke plikter som følger av § 29 a er omtalt under punkt 11.1 og under de særskilte merknadene til § 29 a.

Gjeldende fjerde ledd blir nytt *femte ledd*.

I nytt *sjette ledd* gjøres det unntak for regjeringens medlemmer og dommere i Høyesterett fra bestemmelser gitt i og i medhold av lovens kapittel 6 om personellsikkerhet. Dette innebærer at det ikke stilles krav om sikkerhetsklarering og autorisasjon for regjeringens medlemmer og dommere i Høyesterett. Unntaket er en lovfesting av en langvarig og fast praksis. Det vises til departementets vurderinger i punkt 3.2 og 3.4.

Femte og sjette ledd blir nytt *sjuende* og *åttende ledd*.

Til § 3 første ledd nytt nummer 21

I bestemmelsen er det inntatt en definisjon av *kritisk infrastruktur*. Definisjonen er ny og formuleringen er kortere og noe annerledes enn definisjonen i sivilbeskyttelsesloven § 3 bokstav d og definisjonen som Infrastrukturutvalget benyttet i NOU 2006: 6 *Når sikkerheten er viktigst*, men den dekker i hovedsak de samme forholdene. Det vises til nærmere omtale i punkt 11.1.2 og 11.4.7.

Til ny § 5 a

Paragrafen er ny og pålegger virksomheter underlagt sikkerhetsloven en varslingsplikt til departementet ved kunnskap om risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført. Bestemmelsen gir også Kongen i statsråd kompetanse til å fatte vedtak for å hindre at slik virksomhet blir etablert eller gjennomført – uten hensyn til begrensningene i forvaltningsloven § 35 – og uavhengig av om aktiviteten er tillatt etter annen lov eller annet vedtak. «Sikkerhetstruende virksomhet» er definert i sikkerhetsloven § 3 nr. 2 som «forberedelse til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandlinger, samt medvirkning til slik virksomhet». Departementets generelle merknader framgår av punkt 4.4.

Første ledd første punktum regulerer selve varslingsplikten. Plikten til å varsle inntrer når en virksomhet underlagt sikkerhetsloven får kunnskap om en planlagt eller pågående aktivitet som kan medføre en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført. Uttrykket «får kunnskap om» stiller ikke krav om visshet eller strenge krav til graden av kunnskap om at slik virksomhet faktisk vil bli eta-

blert eller gjennomført. Ordet «kunnskap» omfatter her både «kjennskap til», og «indikasjoner» på at slik virksomhet kan bli etablert.

Ordet «aktivitet» favner vidt. Både iøynefallende aktiviteter som f.eks. oppføring av bygninger eller utplassering av antenner, og mindre synlige aktiviteter, som f.eks. planer om utbygging, ferdsel i et område eller oppkjøp av virksomheter, omfattes av begrepet. Varslingsplikten omfatter aktiviteter som er «planlagt eller pågående», noe som innebærer at den også gjelder aktiviteter som ennå ikke har materialisert seg, men hvor det f.eks. er mottatt en søknad. Dette er viktig for å sikre at potensiell sikkerhetstruende virksomhet kan bli stanset før virksomheten faktisk blir etablert eller gjennomført.

Bestemmelsen stiller ikke krav om at det må foreligge en viss bestemt sannsynlighet for at en sikkerhetstruende virksomhet kan etableres eller gjennomføres. At aktiviteten skal kunne medføre en «ikke ubetydelig risiko» for etablering eller gjennomføring av sikkerhetstruende virksomhet, innebærer derimot at varslingsplikten ikke inntrer hvis dette framstår som usannsynlig, eller det kun er en teoretisk mulighet for det. Terskelen for varslingsplikten må ellers ses i sammenheng med de mulige konsekvensene av en sikkerhetstruende virksomhet. Dersom konsekvensen kan bli katastrofal, vil også terskelen for når det foreligger varslingsplikt bli lav. Motsatt vil terskelen kunne heves dersom konsekvensen av en mulig sikkerhetstruende virksomhet regnes som liten.

Uttrykket «etablert» omfatter både forberedelseshandlinger til spionasje, sabotasjeaksjoner og terrorangrep, og utplassering av utstyr eller personer som skal inngå i spionasje. At sikkerhetstruende virksomhet blir «gjennomført», omfatter både forsøk og faktisk gjennomføring av spionasje, sabotasje eller terrorhandlinger.

Bestemmelsen i første punktum fastsetter videre at varselet skal rettes til det departementet som er «overordnet departement» for den aktuelle virksomheten. Dette vil være det departementet som er direkte overordnet virksomheten, eller som virksomheten er administrativt underlagt. Bestemmelsen innebærer samtidig en plikt for departementene til å motta og behandle slike varsel, og det er ikke adgang til å delegere denne oppgaven til et direktorat eller andre underordnede organer.

For de fleste offentlige virksomheter vil det være klart hvilket departement som er overordnet virksomheten. Enkelte offentlige virksomheter har derimot tilhørighet til flere departementer, slik at det kan oppstå usikkerhet om hvem som skal motta et varsel. I slike tilfeller må varsling skje til det tilknyttede departementet som framstår mest relevant for saken. Skulle dette være feil, plikter det aktuelle departementet å sende varslet videre til det departement som har fagansvaret i den konkrete saken.

Spørsmålet om «overordnet» departement vil imidlertid stille seg annerledes for private virksomheter som er underlagt loven, jf. § 2 annet ledd om at loven gjelder leverandører til sikkerhetsgraderte anskaffelser, og rettssubjekter det er truffet vedtak om etter tredje ledd at loven skal gjelde for. Slike virksomheter vil ikke ha noe overordnet departement i vanlig forstand, og det vil variere om de kan sies å være administrativt underlagt noe departement. Det er derfor fastsatt i *første ledd andre punktum* at varsling skal skje til Forsvarsdepartementet dersom virksomheten ikke er underlagt noe «overordnet departement». Dersom saken gjelder et fagfelt som ikke hører under Forsvarsdepartementet, vil Forsvarsdepartementet videreformidle varslet til det rette departementet for behandling. Etter første ledd *tredje punktum* gjelder varslingsplikten etter første og andre punktum uten hinder av lovbestemt taushetsplikt. Dette innebærer at varslingsplikten skal etterleves, selv om dette innebærer videreformidling av opplysninger som i utgangspunktet er omfattet av lovbestemt taushetsplikt. Bestemmelsen skal sikre at lovbestemt taushetsplikt ikke er til hinder for de grunnleggende og viktige nasjonale sikkerhetsinteressene som paragrafen skal ivareta.

Etter *første ledd fjerde punktum* er det fastslått at departementet ved behandling av varsel etter første og andre punktum bør innhente rådgivende uttalelser fra relevante organer med kompetanse innenfor det aktuelle fagområdet. Departementet som vurderer et varsel og avgjør hvordan det skal håndteres, har ansvaret for å innhente rådgivende uttalelser. I tilfeller hvor varsling har skjedd til Forsvarsdepartementet, jf. første ledd andre punktum, men varselet videresendes for behandling til rett departement, er det vedkommende departement som vurderer om en rådgivende uttalelse skal innhentes. Dette gjelder for øvrig også når et varsel er sendt til et antatt overordnet departement, men blir videresendt for behandling til et annet departement. Både Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet og Etterretningstjenesten kan være aktuelle organer å konsultere i slike situasjoner. Etter omstendighetene kan det også være aktuelt å innhente rådgivende uttalelser fra andre virksomheter med særlig kompetanse innen det aktuelle fagområdet.

Det klare utgangspunktet skal her være at slike uttalelser skal innhentes. Departementet foreslår likevel ingen lovfestet plikt til dette. Å innhente en uttalelse vil i enkelte tilfeller være åpenbart unødvendig, og må derfor kunne unnlates. Dette kan for eksempel være aktuelt dersom saken vurderes å være tilfredsstillende opplyst gjennom varslingen, eller at varselet vurderes å være åpenbart grunnløst.

Andre ledd første punktum gir en hjemmel for Kongen i statsråd til å fatte nødvendige vedtak for å hindre en planlagt eller pågående aktivitet som nevnt i første ledd første punktum. At vedtaket skal være «nødvendig» innebærer at Kongen i statsråd ikke skal fatte mer byrdefulle vedtak enn det som er påkrevd, og som vurderes som rimelig i den konkrete saken. Bestemmelsen vil være en sikkerhetsventil, og den forutsettes benyttet kun i helt spesielle tilfeller. Kompetansen til å fatte vedtak er lagt til Kongen i statsråd, og den kan ikke delegeres. Departementet legger til grunn at det vil være tale om et lite antall saker, og at disse sakene etter sin art vil være alvorlige og spesielle, jf. også formålet med sikkerhetsloven. At kompetansen legges til Kongen i statsråd sikrer at eventuelle tiltak som iverksettes, er resultat av en vurdering på høyt nivå, og at de står i et rimelig forhold til den foreliggende risikoen.

I henhold til *andre ledd andre punktum* kan vedtak etter første punktum for det første fattes uten hensyn til begrensningene i forvaltningsloven § 35. Bestemmelsen tar høyde for tilfeller der forvaltningen allerede har fattet et vedtak, og det av hensyn til risiko for sikkerhetstruende virksomhet anses nødvendig å omgjøre vedtaket. Videre slås det i bestemmelsen fast at vedtak etter første punktum også kan fattes uten hensyn til om aktiviteten er tillatt etter annen lov eller annet vedtak. Et vedtak av Kongen i statsråd kan derfor i praksis sette til side en rekke ulike former for vedtak og aktiviteter som i utgangspunktet er tillatt, f.eks. nekte gjennomføring eller stille ytterligere vilkår for en byggetillatelse, frekvenstillatelse, ferdselsrett, jaktrett, en våpentillatelse eller et privat oppkjøp av en virksomhet.

I andre ledd *tredje punktum* er det fastsatt at vedtak etter første punktum er tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13. Dette innebærer at vedtak som fattes av Kongen i statsråd, kan tvangsfullbyrdes av namsmyndighetene, uten at man først må få dom for dette. Slik tvangsfullbyrdelse kan f.eks. gå ut på fravikelse av fast eiendom, ved at personer eller løsøre fjernes fra eiendommen, etter tvangsfullbyrdelsesloven § 13-11, rett for staten til å gjennomføre riving eller fjerning av installasjoner etter tvangsfullbyrdelsesloven § 13-14 første ledd eller pålegg om å stille sikkerhet etter tvangsfullbyrdelsesloven § 13-16 første ledd.

Etter *tredje ledd* kan Kongen i statsråd gi forskrift om varslingsplikten etter første ledd og om hvilke vedtak som kan fattes etter andre ledd. Forskriftskompetansen er således lagt på samme nivå som kompetansen til å fatte vedtak, og heller ikke denne kompetansen kan delegeres til andre. Det kan typisk bli aktuelt å utarbeide forskrifter som gir nærmere regler om hvordan varslingsplikten skal gjennomføres, og som nærmere fastsetter hvilke vedtak Kongen i statsråd kan fatte.

Til § 9

Ny første ledd bokstav e kodifiserer den nasjonale responsfunksjonen for alvorlige dataangrep mot kritisk infrastruktur (NorCERT) og varslingssystemet for digital infrastruktur (VDI) som en del av Nasjonal sikkerhetsmyndighet (NSM). Bestemmelsen representerer utelukkende en formalisering av en allerede vedtatt og etablert ordning. NorCERT-funksjonen i NSM utøver i dag disse oppgavene. Det vurderes imidlertid som lite hensiktsmessig å introdusere begrepet «NorCERT» i lovgivningen, da betegnelsen på denne funksjonen kan endres over tid. Det er derfor søkt å finne betegnelser som er dekkende for de oppgaver som funksjonen er tillagt. En nærmere konkretisering av oppgavene som ligger til VDI og NorCERT bør skje i en utfyllende forskrift.

Bestemmelsen inntas som ny § 9 første ledd bokstav e. Dette medfører at dagens bokstav e, blir ny *bokstav f*. Dagens bokstav f sier bare at loven skal følges. Bestemmelsen er overflødig og videreføres derfor ikke.

Til ny § 10 a

Paragrafen er ny og tydeliggjør når Nasjonal sikkerhetsmyndighet (NSM) kan behandle personopplysninger for å ivareta oppgaver som er tillagt nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur (NorCERT) og varslingssystem for digital infrastruktur (VDI), og hvilke kategorier informasjon som kan behandles.

Første ledd oppstiller et nødvendighetskriterium. I dette ligger at det bare kan behandles informasjon som er relevant for ivaretagelsen av de oppgaver som er tillagt NorCERT og VDI. Behandlingen må være nødvendig for å ivareta VDI- og NorCERT-funksjonens oppgaver. *I bokstav a til d* presiseres hvilke kategorier person-

opplysninger som kan behandles. Opplysninger nevnt i bokstav a og c er avidentifiserte. Opplysninger som registreres etter bokstav b er pakkedump som også kan inneholde fragmenter av identifiserbare personopplysninger. Der NSM behandler personopplysninger etter bokstav d vil man kunne få lagringsmedier til analyse, og identifiserbare personopplysninger vil inngå. Formålet med behandlingen vil imidlertid utelukkende være å analysere lagringsmedia eller logg for å avdekke ondsinnet kode. Forutsetningen for behandlingen er samtykke fra virksomheten.

Bestemmelsens *andre ledd* tar sikte på å etablere et nødvendig handlingsrom i de mest alvorlige tilfeller for andre kategorier behandlinger enn de som skjer i en normalsituasjon. Denne bestemmelsen vil for eksempel kunne anvendes ved håndtering av tilfeller hvor det har inntruffet et alvorlig angrep mot kritisk IKT-infrastruktur eller funksjoner som det er grunn til å tro at en fremmed stat kan stå bak. Behandling vil her skje etter en konkret nødvendighets- og proporsjonalitetsvurdering.

Behandlingen av personopplysninger skal være i samsvar med grunnkravene i personopplysningloven § 11.

I *tredje ledd* gis hjemmel for å kunne gi utfyllende bestemmelser i forskrifter. Det vises for øvrig til departementets vurderinger i punkt 7.4.

Til ny § 13 a

Bestemmelsen er ny og viderefører i stor grad eksisterende regler i forskrift om informasjonssikkerhet og gjeldende praksis vedrørende overvåking av informasjonssystemer. Bestemmelsen etablerer et klarere hjemmelsgrunnlag, og synliggjør den økte betydningen av sikkerhetsmessig overvåking av godkjente informasjonssystemer. Samtidig er bestemmelsen lettere tilgjengelige for virksomheter som pålegges plikter, og for de som ellers berøres.

Første ledd oppstiller hovedregelen om at informasjonssystemer som er gjenstand for godkjenning etter sikkerhetsloven § 13 kontinuerlig skal overvåkes for sikkerhetstruende hendelser. Forslaget er en videreføring av forskrift om informasjonssikkerhet §§ 5-2 første ledd bokstav c, og 5-3 bokstav e. Ansvaret påhviler den enkelte virksomhet.

I *andre ledd* gis hjemmel for å registrere utveksling av data som skjer mellom systemer eller autorisasjonsskiller. Dette omfatter også innholdet av informasjonen som utveksles. Denne bestemmelsen er ny i loven. I samsvar med prinsippene i sikkerhetsloven § 6 vil omfanget av loggingen bero på en konkret risikovurdering.

Tredje ledd skal regulere de tilfeller der flere virksomheter er knyttet til samme informasjonssystem. I slike tilfeller kan systemeier etter avtale med hver enkelt virksomhet, forestå overvåkningen og registreringen på vegne av den ansvarlige.

Fjerde ledd første punktum viderefører bestemmelsen i forskrift om informasjonssikkerhet § 5-18 om at informasjon registrert etter første og andre ledd skal lagres i 5 år. Fjerde ledd andre punktum oppstiller en klar avgrensing mot bruk av informasjon som logges og registreres etter første og andre ledd til alle andre formål enn håndteringen av sikkerhetstruende hendelser. For dette formål kan informasjonen utleveres til relevante virksomheter. Nærmere bestemmelser er gitt i forskrift om sikkerhetsadministrasjon.

Femte ledd pålegger virksomheten informasjonsplikt i samsvar med personopplysningsloven § 19.

I sjette ledd gis hjemmel for å kunne gi utfyllende bestemmelser i forskrift.

Det vises for øvrig til omtalen av bestemmelsen under punkt 8.3 og 8.5.

Til § 23

Dagens § 23 femte ledd omhandler autorisasjon.

Av regeltekniske hensyn foreslår departementet at dagens femte ledd blir nytt *første ledd.* Mens autorisasjon skal gjøres for samtlige graderingsnivåer, stilles det krav om sikkerhetsklarering kun ved tilgang til informasjon som er KONFIDENSIELT eller høyere. Departementet mener derfor at det er mer pedagogisk at regulering av autorisasjon omtales i *første ledd*. For å gjenspeile denne endringen foreslår departementet at tittelen i § 23 skal endres fra «Klareringsmyndighet og autorisasjonsansvarlig» til «Autorisasjonsansvarlig og klareringsmyndighet».

Av gjeldende § 23 femte ledd tredje punktum fremgår det at autorisasjon ikke skal gis før det foreligger melding om sikkerhetsklarering, med unntak for de tilfeller som er beskrevet i § 19 tredje ledd, og sikkerhetssamtale er avholdt.

Ordet «sikkerhetssamtale» er erstattet med «autorisasjonssamtale». Bakgrunnen for det er at bruken av ordet «sikkerhetssamtale» i dagens tredje punktum skyldes en inkurie, og det er derfor viktig at det erstattes med det korrekte ordet «autorisasjonssamtale». Forslaget innebærer ingen materielle endringer.

Etter dagens regelverk er hvert enkelt departement klareringsmyndighet for personell innenfor

sitt myndighetsområde. Myndigheten kan delegeres, noe som er gjort i stor utstrekning. Den nærmere organiseringen av klareringsmyndigheter framgår av gjeldende § 23 første til fjerde ledd.

Departementet reduserer antall klareringsmyndigheter. Endringen innebærer at dagens første til fjerde ledd endres og får ny utforming i *andre ledd*.

Av § 23 *andre ledd første punktum* framgår det at Kongen utpeker to klareringsmyndigheter, en for forsvarssektoren og en for sivil sektor. Den nærmere organiseringen av klareringsmyndighetene vil bli bestemt av Kongen.

Av *andre ledd andre punktum* framgår det at Kongen kan utpeke andre klareringsmyndigheter når særlige grunner taler for det. Denne bestemmelsen må sees i sammenheng med departementets forslag om å redusere antallet klareringsmyndigheter, og hovedregelen om at det skal være én klareringsmyndighet for forsvarssektoren og én for sivil sektor.

I *andre ledd tredje punktum* foreslår departementet å lovfeste at etterretnings- og sikkerhetstjenestene klarerer eget personell. Det betyr at EOS-tjenestene fortsetter å klarere sitt eget personell, på grunn av sine særskilte oppgaver.

Til § 28

Det framgår av gjeldende § 28 første ledd andre punktum at leverandørklareringen gjelder for det enkelte oppdrag. Det betyr at det må søkes om klarering for hvert enkelt oppdrag, og klareringen faller automatisk bort når oppdraget er fullført.

Departementet endrer *første ledd andre punktum* til at Kongen fastsetter gyldighetstiden for leverandørklareringer. Forslaget innebærer en materiell endring fra oppdragsbasert til tidsbasert leverandørklarering, og gir adgang til å fastsette varigheten av leverandørklareringer i forskrift. Leverandørklareringen skal imidlertid, slik som i dag, gis etter anmodning fra en anskaffelsesmyndighet. Tildeling og oppfølging av tidsbestemte klareringer må reguleres nærmere i forskrift, herunder tildeling av leverandørklareringer på like vilkår og en forsvarlig oppfølging av leverandører i klareringsperioden. Formålet med innføringen av tidsbasert leverandørklarering er å effektivisere og forenkle arbeidet med sikkerhetsgraderte anskaffelser.

Til ny § 29 a

Bestemmelsen er ny, og tar sikte på å motvirke at kritisk infrastruktur blir utsatt for, eller brukt til, spionasje og sabotasje. I lovteksten er disse handlingene omtalt under fellesbenevnelsen sikkerhetstruende virksomhet, som er definert i § 3 nr. 2. Paragraf 29 a pålegger virksomheter som eier eller rår over kritisk infrastruktur, å foreta en risikovurdering ved anskaffelser til kritisk infrastruktur, og å handle ut fra utfallet av risikovurderingen. Bestemmelsen pålegger virksomheter å varsle myndighetene dersom virksomheten ønsker å gjennomføre en anskaffelse som kan innebære en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført. Bestemmelsen gir Kongen i statsråd hjemmel til å gripe inn i anskaffelser til kritisk infrastruktur der det foreligger en slik risiko. Bestemmelsen gjelder for alle virksomheter som er underlagt loven i henhold til § 2, og som eier eller rår over kritisk infrastruktur.

Hva som til ethvert tidspunkt skal anses som kritisk infrastruktur, avgjøres av myndighetene med utgangspunkt i definisjonen inntatt i § 3 nr. 21. En redegjørelse for begrepet kritisk infrastruktur er gitt i punkt 11.1. Det er departementene som identifiserer kritisk infrastruktur i de ulike sektorene. I forslaget til § 2 fjerde ledd andre punktum er Kongen gitt myndighet til å gi forskrift om identifisering av kritisk infrastruktur og om informasjon til rettssubjekter som eier eller rår over kritisk infrastruktur.

Første ledd pålegger virksomhetene å foreta en risikovurdering ved anskaffelser til kritisk infrastruktur. *Første punktum* oppstiller selve plikten til å foreta en risikovurdering. Plikten påhviler virksomheter som eier eller rår over kritisk infrastruktur. Vurderingen kan utføres av virksomheten selv eller av en tredjepart på oppdrag fra virksomheten. Det vil normalt være naturlig å nedtegne risikovurderingen skriftlig, men det er ikke et krav. *Andre punktum* regulerer innholdet i risikovurderingen. Virksomheten skal i risikovurderingen ta stilling til om anskaffelsen kan innebære en risiko for at leverandøren eller andre utnytter anskaffelsen til å utføre spionasje eller sabotasje. Lovteksten bruker begrepene «etablere» eller «gjennomføre» (sikkerhetstruende virksomhet). Disse begrepene er ment å fange opp både det å tilrettelegge for at sikkerhetstruende virksomhet kan gjennomføres på et senere tidspunkt, og det å gjennomføre sikkerhetstruende virksomhet samtidig med anskaffelsen. Å etablere sikkerhetstruende virksomhet kan for eksempel være å programmere inn en bakdør i et datasystem som kan utnyttes i ettertid. Som omtalt under punkt 11.4.2 ovenfor, vil risikovurderingen måtte bestå av en sammensatt vurdering der mulige sårbarheter, trusler og konsekvenser

inngår. Terskelen for hvor stor risiko som er akseptabel, går der risikoen kan karakteriseres som ubetydelig eller ikke. Hva som nærmere ligger i dette kriteriet, er beskrevet i punkt 11.4.2. *Tredje punktum* fastslår at virksomheten ikke behøver å foreta en risikovurdering dersom det framstår som åpenbart at anskaffelsen ikke kan innebære noen slik risiko. For eksempel vil virksomheten ikke behøve å vurdere risikoen ved vanlige innkjøp til daglig drift eller rutinemessig utskifting av mekaniske deler.

Andre ledd oppstiller en varslingsplikt for virksomheter som ønsker å gjennomføre en anskaffelse som kan innebære en ikke ubetydelig risiko for sikkerhetstruende virksomhet. *Første punktum* oppstiller selve plikten til å varsle. Plikten inntrer dersom en risikovurdering konkluderer med at anskaffelsen kan innebære en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført. Nærmere omtale av kriteriet «ikke ubetydelig risiko» er gitt i punkt 11.4.2. Varselet skal gis til overordnet departement. For offentlige virksomheter vil det som oftest være klart hvilket departement som er deres overordnede. Når det gjelder uavhengige organer, vil det overordnede departementet i denne sammenhengen være det departementet virksomheten er administrativt underlagt. Enkelte organer er derimot knyttet til flere departementer, og det kan være usikkert hvem av dem varselet skal rettes til. Virksomheten må da velge ett av de aktuelle departementene og varsle til det. Skulle dette være feil, skal det departementet som har mottatt varselet, sende det videre til riktig mottaker. *Andre punktum* slår fast at virksomheter som ikke har et overordnet departement, skal varsle Forsvarsdepartementet. Dette vil i praksis gjelde private virksomheter. *Tredje punktum* innebærer at plikten til å varsle går foran eventuell lovbestemt taushetsplikt. *Fjerde punktum* gir virksomheter som avdekker en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført, anledning til selv å finne og iverksette risikoreduserende tiltak. Dersom dette resulterer i at risikoen senkes til et ubetydelig nivå, kan virksomheten gjennomføre anskaffelsen uten å involvere myndighetene. Risikoreduserende tiltak kan for eksempel være tekniske, administrative eller organisatoriske barrierer. Også valg av leverandører og underleverandører kan ses på som risikoreduserende tiltak.

Virksomhetene har ikke noen plikt til å gjennomføre alle risikoreduserende tiltak som kan bidra til å senke risikoen til et ubetydelig nivå. Dersom virksomheten ikke ønsker å iverksette ett eller flere risikoreduserende tiltak, for eksempel fordi de anses som for kostbare, står virksomheten fritt til å avgjøre dette. Virksomheten vil imidlertid være forpliktet til å varsle i tråd med regelen i første punktum dersom den ønsker å gjennomføre en anskaffelse som innebærer en ikke ubetydelig risiko. Når det gjelder hvordan prosedyrene i § 29 a rent praktisk kan gjennomføres som del av en anskaffelsesprosess, viser departementet til punkt 11.4.8.

Tredje ledd gjelder forvaltningens behandling av et varsel, og oppstiller en hovedregel om at departementet som mottar et slikt varsel bør innhente rådgivende uttalelser fra relevante organer. Bestemmelsen medfører likevel ikke noen rettslig plikt. Se mer om dette i punkt 11.4.4.

Fjerde ledd gir Kongen i statsråd mulighet til å fatte vedtak i enkeltsaker. *Første punktum* inneholder selve hjemmelen for Kongen i statsråd til å fatte vedtak. Forutsetningen for at Kongen i statsråd skal ha kompetanse til å gripe inn, er at risikoen for sikkerhetstruende virksomhet er mer enn ubetydelig. Det kan i prinsippet fattes alle typer vedtak. Den mest inngripende typen vedtak vil være å stanse en anskaffelse som sådan eller å forby bruk av visse leverandører. En mindre inngripende type vedtak er å stille vilkår om å innføre risikoreduserende tiltak. Se også her punkt 11.4.4. *Andre punktum* innebærer at Kongen i statsråd har kompetanse til å fatte vedtak, selv om anskaffelsesmyndigheten og leverandøren har inngått avtale om anskaffelsen. Normalt vil varslingsplikten være brutt dersom Kongen i statsråd må gripe inn i en avtale som allerede er inngått. Men det kan også tenkes tilfeller der trusselbildet brått endres, og at dette foranlediger en inngripen fra myndighetene. Andre punktum innebærer imidlertid ikke at det kan fattes vedtak om avtaler som ble inngått før loven trådte i kraft. Se også punkt 11.2.2. *Tredje punktum* pålegger det aktuelle departementet å underrette virksomheten dersom Kongen i statsråd ikke fatter vedtak i saken. Dette er presisert fordi det ikke følger uttrykkelig av forvaltningsloven at det skal varsles om denne typen beslutninger. *Fjerde punktum* innebærer at myndighetene ikke behøver å gå veien om domstolene for å kunne tvangsfullbyrde et vedtak fattet av Kongen i statsråd. Myndighetene kan for eksempel med namsmannens hjelp fysisk tvangsgjennomføre innholdet i et vedtak, jf. tvangsfullbyrdelsesloven § 13-14 første ledd. Det vil også kunne være aktuelt å ilegge løpende tvangsmulkt.

Femte ledd gir Kongen i statsråd hjemmel til å gi forskrift om anskaffelser til kritisk infrastruktur. Hjemmelen kan blant annet brukes til å

pålegge eiere av kritisk infrastruktur om å innføre visse typer sikkerhetstiltak eller rutiner ved anskaffelser til kritisk infrastruktur. Kompetansen kan ikke delegeres.

Til ikrafttredelse av loven, jf. lovforslagets del II

Det foreslås at loven trer i kraft fra den tid Kongen bestemmer. I dette tilfellet er det nødvendig med forskjellig ikrafttredelsestidspunkt for de forskjellige bestemmelsene, bl.a. av hensyn til at etablering av ny sivil klareringsmyndighet vil ta noe tid. Etter forslaget kan Kongen derfor fastsette forskjellige ikraftsettingstidspunkter for de forskjellige bestemmelsene.

Forsvarsdepartementet

t i l r å r :

At Deres Majestet godkjenner og skriver under et framlagt forslag til proposisjon til Stortinget om endringer i sikkerhetsloven (reduksjon av antall klareringsmyndigheter mv.).

Vi HARALD, Norges Konge,

s t a d f e s t e r :

Stortinget blir bedt om å gjøre vedtak til lov om endringer i sikkerhetsloven (reduksjon av antall klareringsmyndigheter mv.) i samsvar med et vedlagt forslag.

Forslag
til lov om endringer i sikkerhetsloven (reduksjon av antall klareringsmyndigheter mv.)

I

I lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste gjøres følgende endringer:

§ 2 fjerde til åttende ledd skal lyde:

§ 29 a gjelder for alle anskaffelser til kritisk infrastruktur. Kongen kan gi forskrift om identifisering av kritisk infrastruktur og om informasjon til rettssubjekter som eier eller rår over kritisk infrastruktur.

Loven gjelder for domstolene med de særregler som følger av bestemmelsene om sikkerhetsklarering og autorisasjon i og i medhold av domstolloven og straffeprosessloven Kongen kan fastsette ytterligere særregler.

Bestemmelsene gitt i og i medhold av lovens kapittel 6 om personellsikkerhet gjelder ikke for regjeringens medlemmer og dommere i Høyesterett.

Loven gjelder ikke for Stortinget, Riksrevisjonen, Stortingets ombudsmann for forvaltningen og andre organer for Stortinget.

Loven gjelder for Svalbard og Jan Mayen i den utstrekning Kongen bestemmer.

§ 3 første ledd nytt nr. 21 skal lyde:

Kritisk infrastruktur; anlegg og systemer som er nødvendige for å opprettholde samfunnets grunnleggende behov og funksjoner.

Ny § 5 a skal lyde:

§ 5 a *Varslingsplikt og myndighet til å fatte vedtak ved risiko for sikkerhetstruende virksomhet*

En virksomhet som får kunnskap om en planlagt eller pågående aktivitet som kan medføre en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført, skal varsle overordnet departement om dette. Dersom den varslingspliktige virksomheten ikke er underlagt noe departement, skal varselet gis til Forsvarsdepartementet. Varslingsplikten gjelder uten hinder av lovbestemt taushetsplikt. Ved behandling av varsel etter første og andre punktum bør det innhentes rådgivende uttalelser fra relevante organer med kompetanse innenfor det aktuelle fagområdet.

Kongen i statsråd kan fatte nødvendige vedtak for å hindre en planlagt eller pågående aktivitet som nevnt i første ledd første punktum. Et slikt vedtak kan fattes uten hensyn til begrensningene i forvaltningsloven § 35, og uavhengig av om aktiviteten er tillatt etter annen lov eller annet vedtak. Vedtak etter første punktum er særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Kongen i statsråd kan gi forskrift om varslingsplikten i første ledd og om hvilke vedtak som kan fattes etter andre ledd.

Ny § 9 første ledd bokstav e og f skal lyde

e. drive en nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur og et nasjonalt varslingssystem for digital infrastruktur,

f. gi informasjon, råd og veiledning til virksomheter.

I kapittel 3 skal ny § 10 a lyde:

§ 10 a Behandling av personopplysninger

Når det er nødvendig for å utføre oppgavene etter § 9 første ledd bokstav e, kan Nasjonal sikkerhetsmyndighet behandle personopplysninger i form av

a) metadata om IKT-trafikk til og fra virksomheter som er knyttet til det nasjonale varslingssystemet for digital infrastruktur
b) informasjon som er nødvendig for å analysere utløste alarmer i varslingssystemet
c) IP-adresser mottatt fra nasjonale og internasjonale samarbeidspartnere
d) logger og infisert maskinvare, etter samtykke fra en virksomhet der dette er nødvendig i forbindelse med bistand til håndtering av alvorlige dataangrep.

I andre tilfeller enn nevnt i første ledd, kan personopplysninger også behandles når dette er strengt nødvendig for å ivareta oppgavene etter § 9 første ledd bokstav e, og behandlingen etter en konkret vurdering framstår som både nødvendig og proporsjonal i forhold til det inngrepet den representerer i personvernet.

Kongen kan gi forskrift om Nasjonal sikkerhetsmyndighets behandling av personopplysninger.

Ny § 13 a skal lyde:

§ 13 a Sikkerhetsmessig overvåking av godkjente informasjonssystemer

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

Informasjon som utveksles mellom systemer, på tvers av autorisasjonsskiller eller til bærbare lagringsmedier, skal registreres og lagres.

Flere virksomheter som er tilknyttet samme informasjonssystem, kan avtale at en av virksomhetene skal forestå overvåking og registrering etter første og andre ledd på vegne av den ansvarlige virksomheten.

Informasjon registrert etter første og andre ledd skal lagres i fem år. Slik informasjon skal kun benyttes for å håndtere sikkerhetstruende hendelser.

Den enkelte virksomhet skal påse at autoriserte brukere av informasjonssystemer som overvåkes i henhold til denne bestemmelse får informasjon om formålet med behandlingen, om de tiltak som er iverksatt, om informasjonen vil bli utlevert og eventuelt om hvem som er mottaker.

Kongen kan gi forskrift om

a) hvilke typer data som kan eller skal registreres og lagres
b) hvem som skal ha tilgang til registrert og lagret data
c) hvordan tilgang skal gis
d) unntak fra lagringstid på fem år.

§ 23 skal lyde:

§ 23 Autorisasjonsansvarlig og klareringsmyndighet

Autorisasjon kan gis dersom autorisasjonsansvarlig ikke har opplysninger som gjør det tvilsomt om vedkommende sikkerhetsmessig er til å stole på. Autorisasjon gis normalt av virksomhetens leder. Autorisasjon skal ikke gis før det foreligger melding om sikkerhetsklarering, med unntak for de tilfeller som er beskrevet i § 19 tredje ledd, og en *autorisasjonssamtale* er avholdt. Nasjonal sikkerhetsmyndighet gir nærmere regler om autorisasjon og om hvem som er autorisasjonsansvarlig.

Kongen utpeker en klareringsmyndighet for forsvarssektoren og en for den sivile sektoren. Kongen

kan utpeke andre klareringsmyndigheter når særlige grunner taler for det. Etterretnings- og sikkerhetstjenestene klarerer eget personell.

§ 28 første ledd andre punktum skal lyde:
Kongen gir forskrift om gyldighetstiden for leverandørklareringer.

Kapittel 7 overskriften skal lyde:

Kapittel 7. Sikkerhetsgraderte anskaffelser og anskaffelser til kritisk infrastruktur

I kapittel 7 skal ny § 29 a lyde:
§ 29 a *Varslingsplikt og myndighet til å fatte vedtak ved anskaffelser til kritisk infrastruktur*

Ved anskaffelser til kritisk infrastruktur skal det foretas en risikovurdering. I vurderingen skal det tas stilling til om anskaffelsen innebærer en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført mot eller ved bruk av infrastrukturen. Plikten til å foreta en risikovurdering gjelder ikke dersom det framstår som åpenbart at anskaffelsen ikke kan innebære noen slik risiko.

En virksomhet som eier eller rår over kritisk infrastruktur, skal varsle overordnet departement dersom en risikovurdering som nevnt i første ledd konkluderer med at anskaffelsen kan innebære en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført. Virksomheter som ikke er underlagt noe departement, skal varsle Forsvarsdepartementet. Varslingsplikten gjelder uten hinder av lovbestemt taushetsplikt. Plikten gjelder ikke dersom virksomheten selv iverksetter risikoreduserende tiltak som fjerner risikoen, eller gjør den ubetydelig.

Et departement som mottar varsel etter andre ledd, bør innhente en rådgivende uttalelse fra relevante organer om leveransens risikopotensiale og leverandørers sikkerhetsmessige pålitelighet.

Dersom en anskaffelse til kritisk infrastruktur kan medføre en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført, kan Kongen i statsråd fatte vedtak om at anskaffelsen skal nektes gjennomført, eller om at det settes vilkår for gjennomføringen. Dette gjelder også dersom det allerede er inngått avtale om anskaffelsen. Dersom det ikke fattes vedtak etter første punktum, skal departementet underrette virksomheten om dette. Vedtak etter første punktum er særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Kongen i statsråd kan gi forskrift om anskaffelser til kritisk infrastruktur.

II

Loven gjelder fra den tid Kongen bestemmer. Kongen kan bestemme at de forskjellige bestemmelsene skal tre i kraft til forskjellig tid.

Bestilling av publikasjoner

Offentlige institusjoner:
Departementenes sikkerhets- og serviceorganisasjon
Internett: www.publikasjoner.dep.no
E-post: publikasjonsbestilling@dss.dep.no
Telefon: 22 24 00 00

Privat sektor:
Internett: www.fagbokforlaget.no/offpub
E-post: offpub@fagbokforlaget.no
Telefon: 55 38 66 00

Publikasjonene er også tilgjengelige på
www.regjeringen.no

Trykk: 07 Oslo AS – 04/2016