FD
FORSVARSDEPARTEMENTET

Høringsnotat

Forslag til endringer i lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven)

19. mai 2015

Innhold

1 Innledning

Forsvarsdepartementet sender med dette på høring forslag om endringer i lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven).

I henhold til kronprinsregentens resolusjon 4. juli 2003 har justisministeren det overordnede ansvar for forebyggende sikkerhetstjeneste i sivil sektor, tilsvarende forsvarsministerens ansvar innen militær sektor. Justis- og beredskapsdepartementet har derfor i stor grad bidratt i utarbeidelsen av høringsnotatet for de bestemmelser som har betydning for sivil sektor.

Kort om bakgrunnen for høringen

I 2012 ble det konkludert i en evalueringsrapport utarbeidet av en flerdepartemental gruppe, ledet av Forsvarsdepartementet, med at dagens utvikling innen teknologi og andre utviklingstrender, som økt globalisering, internasjonalisering og tverrsektorielle avhengigheter, representerer nye sikkerhetsutfordringer som tilsa en revisjon av sikkerhetsloven. I 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.

Revisjonsarbeidet har avdekket grunnleggende utfordringer når det gjelder oppfatninger om hva sikkerhetsloven bør regulere, herunder hvordan forholdet mellom sikkerhetsloven og annet sikkerhetsrelatert sektorregelverk bør være. Det er ulike oppfatninger om hva lovens formål og virkeområde bør være i fremtiden. Innenfor området objektsikkerhet 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 har regjeringen besluttet å dele opp arbeidet med revisjon av loven i to faser. Dette for å kunne gjennomføre enkelte av endringene raskt, uten å måtte vente på de grundige analysene som er nødvendig for å løse de ovennevnte temaene.

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

I den andre fasen har et eksternt utvalg som ble oppnevnt ved kgl. res. den 27. mars 2015, fått i mandat å forslå et nytt lovgrunnlag for forebyggende nasjonal sikkerhet. Utvalget skal avgi rapport i form av en NOU i løpet av høsten 2016.

2 Forslag til endringer i sikkerhetsloven

Følgende bestemmelser i sikkerhetsloven foreslås endret:
- § 2 Lovens generelle virkeområde
- § 9 Nærmere om oppgavene
- § 23 Klareringsmyndighet og autorisasjonsansvarlig
- § 28 Leverandørklarering

Videre foreslår departementet fem nye bestemmelser:
- Ny § 5 a Varsling mv. ved risiko for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser
- Ny § 6 a Gebyr
- Ny § 10 a Behandling av personopplysninger
- Ny § 13 a Sikkerhetsmessig overvåking av godkjente informasjonssystemer
- Ny § 29 a Anskaffelser til kritisk infrastruktur.

2.1 § 2 Lovens generelle virkeområde

2.1.1 Gjeldende rett

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

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

2.1.2 Vurdering og forslag til endringer i § 2

Departementet foreslår to endringer i § 2 Lovens generelle virkeområde:

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

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 og dets organer. Stortingsrepresentanter autoriseres og sikkerhetsklareres derfor normalt ikke. Etter fast og langvarig praksis fulgt av ulike regjeringer, foretas det heller ingen autorisasjon og sikkerhetsklarering av regjeringsmedlemmer. Det er imidlertid ikke lovregulert at regjeringsmedlemmer er unntatt fra reglene om sikkerhetsklarering og autorisasjon. Departementet foreslår å lovfeste den gjeldende praksisen om at regjeringsmedlemmer i utgangspunktet ikke sikkerhetsklareres eller autoriseres.

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.

Departementet foreslår derfor at det gjøres unntak for regjeringsmedlemmer fra bestemmelsene i og i medhold av kapittel 6 om personellsikkerhet.

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

Departementet foreslår en ny § 29 a. Forslaget 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 ivaretar. Bestemmelsen vil kunne komme til anvendelse på kritisk infrastruktur som ikke tilfredsstiller kriteriene for å bli utpekt som skjermingsverdig objekt. Slike rettssubjekter vil ikke omfattes av § 2 tredje ledd bokstav a eller b. For rettssubjekter med slik kritisk infrastruktur er det derfor behov for et rettslig grunnlag til å fatte vedtak om delvis underleggelse av sikkerhetsloven, og departementet foreslår at dette kommer til uttrykk i et nytt fjerde ledd i § 2. Se nærmere om forslaget til ny § 29 a i punkt 2.7.

Som følge av forslaget om et nytt fjerde ledd i § 2, vil gjeldende § 2 fjerde til sjette ledd bli forskjøvet, slik at gjeldende fjerde ledd etter endringen blir nytt femte ledd, gjeldende femte ledd blir nytt sjette ledd, og gjeldende sjette ledd blir nytt sjuende ledd.

Departementet foreslår at § 2 skal lyde:

§ 2. Lovens generelle virkeområde

Loven gjelder for forvaltningsorganer. Som forvaltningsorgan regnes i loven ethvert organ for stat eller kommune. Kongen kan i tvilstilfelle bestemme om et organ er å regne som forvaltningsorgan. Kongen kan også bestemme at et forvaltningsorgan helt eller delvis skal være unntatt fra loven når det foreligger særlige grunner for det, og kan da i stedet fastsette særlige regler.

Loven gjelder også for ethvert rettssubjekt som ikke er forvaltningsorgan og som er leverandør av varer eller tjenester til et forvaltningsorgan i forbindelse med en sikkerhetsgradert anskaffelse.

Kongen kan bestemme at loven helt eller delvis også skal gjelde for ethvert annet rettssubjekt, herunder enkeltpersoner, foreninger, stiftelser, selskaper og privat og offentlig næringsvirksomhet,

a. som eier eller på annen måte har kontroll over eller fører tilsyn med skjermingsverdig objekt, eller

b. som av et forvaltningsorgan gis tilgang til sikkerhetsgradert informasjon.

Kongen kan bestemme at § 29 a skal gjelde for 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.

Loven gjelder ikke for Stortinget, Riksrevisjonen, Stortingets ombudsmann for forvaltningen og andre organer for Stortinget. *Bestemmelsene gitt i og i medhold av lovens kapittel 6 om personellsikkerhet gjelder ikke for regjeringens medlemmer.*

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

2.2 Virksomhetenes egne sikkerhetsmessige overvåking av informasjonssystemer som er godkjent i henhold til sikkerhetsloven § 13

2.2.1 Gjeldende rett

Samfunnsutviklingen har medført stadig større og mer komplekse informasjonssystemer som håndterer store mengder informasjon. Dette gjelder også systemer som er godkjent for å behandle, lagre eller transportere sikkerhetsgradert informasjon, såkalte godkjente informasjonssystemer.[1] Ondsinnet programvare blir mer avansert, og utgjør i økende grad en trussel også mot de godkjente informasjonssystemene. Globaliseringen av næringslivet medfører også at leverandører av varer og tjenester til godkjente informasjonssystemer kan ha opprinnelse i mange land. Dette åpner for nye sårbarheter, som medfører et behov for å oppdage, verifisere og håndtere eventuelle angrep eller andre uregelmessigheter som kan true systemets eller informasjonens sikkerhet.

Utviklingen medfører et økende behov for at virksomhetene sikkerhetsmessig overvåker sine godkjente informasjonssystemer. Slik overvåking er et viktig verktøy for å avdekke sikkerhetstruende hendelser. 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

[1] Jf. sikkerhetsloven § 13 om sikkerhetsmessig godkjenning av informasjonssystemer.

informasjonssystemer innebærer både automatiserte alarmer, så vel som manuell sammenstilling og analyse av data relatert til sikkerhetstruende hendelser.

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

For å kunne avdekke og spore sikkerhetstruende hendelser, 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 bestemmelse i sikkerhetsloven som klargjør rammene for den sikkerhetsmessige overvåkingen av godkjente informasjonssystemer som virksomhetene skal foreta.

2.2.2 Utenlandsk rett

I *Sverige* er det gitt bestemmelser om sikkerhetsmessig overvåking av informasjonssystemer i Forsvarsmaktens forskrifter. 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 forskrift.

Det *britiske* Security Policy Framework stiller som et obligatorisk krav (krav 9) 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 administrering 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.

2.2.3 Vurdering og forslag til ny § 13 a

Departementet foreslår en ny bestemmelse i sikkerhetsloven om virksomhetens egen adgang til sikkerhetsmessig overvåking av godkjente informasjonssystemer. Den foreslåtte bestemmelsen er i stor grad en videreføring av eksisterende regler i forskrift om informasjonssikkerhet og gjeldende praksis for sikkerhetsmessig overvåking av informasjonssystemer. Sammenlignet med dagens praksis innebærer i utgangspunktet ikke forslaget til ny lovbestemmelse noen vesentlig utvidelse med hensyn til omfanget av tillatt overvåking.

I forslaget er det lagt vekt på at bestemmelsen skal være fleksibel og teknologinøytral, for på den måten å kunne møte den stadige teknologiske utviklingen og endringer i trusselbildet. Videre er det, for bedre å kunne ivareta kravet til skadevurdering i forbindelse med en

sikkerhetshendelse, foreslått en utvidet plikt til registrering av innholdet i informasjon som utveksles mellom systemer og på tvers av autorisasjonsskiller.

Sikkerhetsmessig overvåking av IKT-systemer har klare grenseflater mot enkeltindividers personvern. Denne type tiltak bør derfor ha en klar hjemmel i lov. På grunn av det økende behovet for sikkerhetsmessig overvåking, foreslår departementet derfor å lovfeste dette direkte i sikkerhetsloven. Hjemmelsgrunnlaget blir med det klarere og den økte betydningen synliggjøres. Samtidig blir bestemmelsene om overvåking lettere tilgjengelige og synlige både for de virksomhetene som pålegges plikter i henhold til bestemmelsene og for de som ellers berøres av dem.

Ethvert kontrolltiltak som virker inngripende overfor den enkelte må ha rettslig grunnlag. I henhold til gjeldende rett i dag, er det rettslig grunnlag for arbeidsgivers kontrolltiltak i virksomheten. Det gjøres blant annet ved rett til innsyn i ansattes e-post og datalogger,[2] etter nærmere gitte vilkår i arbeidsmiljøloven kapittel 9 og personopplysningsloven §§ 8 og 9 jf. personopplysningsforskriften kapittel 9.

Det følger av personopplysningsforskriften § 9-2 at arbeidsgiver har rett til å gjennomsøke, åpne eller lese e-post i arbeidstakers e-postkasse når det

a) *«er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten»*.

Sikkerhetsmessig overvåking av graderte 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 medføre 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, mener departementet at den inngripen som sikkerhetsmessig overvåking kan medføre, må aksepteres.

Nærmere om forslagene

Forslag til *første ledd* 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 presiserer at slik overvåking ikke må utføres av personell. Det bør tilstrebes at overvåkingen skjer ved hjelp av automatiserte prosesser. Sikkerhetsrelevante hendelser skal

[2] Jf. Ot.prp. nr. 49 (2004-2005) s. 135 og 147.

registreres (logges). Ansvaret for slik overvåking og registrering påhviler den enkelte virksomhet som behandler skjermingsverdig informasjon.

Andre ledd 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.

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 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 bærbare 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 har særlig vurdert personvernhensyn i forbindelse med forslag til nytt andre ledd. 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 to-mannsregel 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 fremstår 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.

Forslag til *tredje ledd* 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.

Forslag til *fjerde ledd* viderefører bestemmelsen i § 5-18 i forskrift om informasjonssikkerhet. Informasjon som er registrert etter første ledd skal med det 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.

I forslag til *sjette ledd* 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 e-postkasse 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 e-postkasse 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 den nye bestemmelsen i sikkerhetsloven er ikke meldepliktig etter personopplysningsloven § 31 første ledd. Det presiseres videre at personopplysningsforskriftens bestemmelser nevnt ovenfor ikke kommer til anvendelse på sikkerhetsmessig overvåking som er regulert her.

Forslag til *syvende ledd* gir hjemmel til å gi nærmere bestemmelser i forskrift om sikkerhetsmessig overvåking av informasjonssystemer. Herunder reguleres 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.

Departementet foreslår at ny § 13 a skal lyde:

§ *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.

2.3 Varslingssystem for digital infrastruktur og nasjonal responsfunksjon for alvorlige IKT-baserte hendelser (VDI- og NorCERT-funksjonene)

2.3.1 Innledning – generelt om VDI- og NorCERT-funksjonene

Nasjonal sikkerhetsmyndighet driver i dag et varslingssystem for digital infrastruktur (VDI) og en nasjonal responsfunksjon for alvorlige IKT-baserte hendelser (NorCERT). Formålet med lovforslaget er å lovfeste disse funksjonene som en del av Nasjonal sikkerhetsmyndighets oppgaver. Videre skal forslaget klargjøre det rettslige grunnlaget for behandling av personopplysninger, som er en nødvendig konsekvens av utførelsen av funksjonene.

Om nasjonalt 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 samfunnskritiske funksjoner. Som en oppfølging ble VDI etablert i 1999 som et forsøksprosjekt mellom Etterretningstjenesten, Politiets sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet. Fra 2003 ble operasjon og drift av VDI varig lagt under Nasjonal sikkerhetsmyndighet, og er i dag en integrert del av Nasjonal sikkerhetsmyndighet.

VDI er et nettverk av sensorer som utplasseres i deltagernes datanettverk i samarbeid med deltageren. Data fra sensorene blir innsamlet og bearbeidet, og på bakgrunn av de innsamlede dataene kan Nasjonal sikkerhetsmyndighet blant annet identifisere og varsle om dataangrep

mot samfunnskritisk informasjon, infrastruktur og funksjoner. Formålet med VDI er å oppdage og varsle om målrettede og koordinerte angrep mot samfunnskritisk IKT-infrastruktur. VDI er også et viktig verktøy for å kvalitetssikre varsler, rapporter og innmeldte trender fra andre miljøer.

Tilknytning til VDI-systemet er i dag basert på frivillighet. Offentlige og private eiere av samfunnskritisk IKT-infrastruktur kan etter avtale med Nasjonal sikkerhetsmyndighet bli tilknyttet systemet. Partenes rettigheter og plikter i samarbeidet er nærmere regulert i avtalen. Blant annet har virksomheten full innsynsrett i data som er innsamlet fra egne sensorer. Videre er virksomheten ansvarlig for å informere egne ansatte om deltakelsen i VDI, formålet med dette, hva sensorene logger og hvordan informasjonen benyttes. Deltakende private virksomheter er forpliktet til å bidra til finansieringen av VDI og NorCERT-funksjonene gjennom et årlig vederlag.

VDI-systemet og tilknytning til dette er ikke ment å erstatte virksomhetens egne sikkerhetstiltak, men å være et komplementerende sikkerhetstiltak. Virksomhetene har derfor både en rett og plikt til å ivareta sikkerheten i egne systemer, uavhengig av tilknytning til VDI-systemet.

Om nasjonal responsfunksjon for alvorlige dataangrep mot samfunnskritisk infrastruktur

Norwegian Computer Emergency Response Team (NorCERT) er vårt nasjonale IKT-responsmiljø og skal koordinere håndteringen av alvorlige IKT-hendelser mot samfunnskritisk infrastruktur og informasjon. NorCERT-funksjonen ble etablert som en integrert del av Nasjonal sikkerhetsmyndighet fra 1. januar 2006 og er en oppfølging av St.meld. nr. 39 (2003-2004). I St. meld. nr. 22 (2007-2008) er det uttalt at «NorCERT er Norges nasjonale senter for å håndtere alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon.» Det legges i meldingen 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-funksjonen er innhenting og videreformidling av informasjon om sårbarheter, potensielle risikoer, angrepsmetoder og ondsinnet kode. Dette oppnås dels gjennom innhenting av informasjon fra VDI-systemet, og dels gjennom informasjonsdelingen som skjer som en del av nasjonalt og internasjonalt samarbeid.

Nasjonal sikkerhetsmyndighet skal gjennom NorCERT-funksjonen utvikle et system for koordinert respons og gjenoppretting, først og fremst innen virksomheter med samfunnskritiske funksjoner. Gjennom NorCERT-funksjonen skal det også produseres et oppdatert nasjonalt IKT-risikobilde. En helhetlig beskrivelse av dette bildet sikres gjennom en koordineringsgruppe med representanter også fra Etterretningstjenesten og Politiets sikkerhetstjeneste. Den nasjonale evnen til å håndtere alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon, er avhengig av et særlig samspill mellom EOS-tjenestene. Til sammen har tjenestene i oppdrag å oppdage, varsle og motvirke alvorlige IKT-hendelser. Samarbeidet er nærmere formalisert og regulert i egne retningslinjer av 15. mai 2013, fastsatt av sjefene for de tre tjenestene.

Etterretningstjenesten er den nasjonale utenlandsetterretningstjenesten og har et nasjonalt, lovbestemt sektoroverskridende ansvar for å innhente informasjon om og vurdere trusselen fra fremmede stater, organisasjoner og individer. Som ledd i dette har tjenesten ansvar for å identifisere og utarbeide trusselvurderinger om ytre cybertrusler. Etterretningstjenesten har fagmyndighet og ansvar for utøvelse av offensive cyberoperasjoner. Tjenesten koordinerer samspillet i forsvarssektoren mellom offensive og defensive virkemidler når dette er nødvendig.

Politiets sikkerhetstjeneste er den nasjonale innenlandske etterretnings- og sikkerhetstjenesten, og har til oppgave å forebygge og etterforske nettverksangrep og nettverksoperasjoner som faller inn under områdene etterretningsvirksomhet, terrorisme, politisk ekstremisme, ikke-spredning og trusler mot myndighetspersoner. Videre har tjenesten ansvaret for å utarbeide trusselvurderinger på disse ansvarsområdene (herunder om indre cybertrusler) og å drive sikkerhetsrådgivning etter behov. Politiets sikkerhetstjeneste har ansvaret for å gjennomføre nettverksinnsamlingsoperasjoner innenlands, og har også det innenlandske ansvaret for nettoperative mottiltak innenfor disse ansvarsområdene.

Videre har Nasjonal sikkerhetsmyndighet et nært samarbeid med *andre offentlige og sivile samarbeidsparter*. Nasjonal sikkerhetsmyndighet har en koordinerende funksjon mot de nasjonale, sektorvise responsmiljøene (sektor-CERT'er) og enkeltvirksomheter der det ikke er slike. Sektor-CERT'er bidrar med god kunnskap om spesielle systemer og løsninger innenfor sine respektive sektorer. Nasjonal sikkerhetsmyndighet er også det nasjonale kontaktpunktet for enheter med tilsvarende funksjoner i andre land og internasjonale organisasjoner. Som nasjonal fagmyndighet skal Nasjonal sikkerhetsmyndighet koordinere med, og legge til rette for samarbeid mellom, alle aktører innen fagfeltet.

2.3.2 Gjeldende rett

VDI- og NorCERT-funksjonene er opprettet og lagt til Nasjonal sikkerhetsmyndighet etter beslutninger fra regjeringen og Stortinget. Aktivitetene som utføres innenfor rammen av de to funksjonene er ikke eksplisitt forankret i lov.

Gjennom *VDI-funksjonen* registrerer Nasjonal sikkerhetsmyndighet store mengder data, i det vesentligste i form av trafikkdata som inneholder blant annet IP-adresser. Nasjonal sikkerhetsmyndighet innhenter ikke bare informasjon gjennom VDI-systemet, men mottar også data fra nasjonale og internasjonale samarbeidspartnere. Dataene danner grunnlag for analyse i forbindelse med håndtering av hendelser, og er avgjørende for koordinering med og bistand til nasjonale og internasjonale samarbeidspartnere. Behandling av data er derfor helt avgjørende for at Nasjonal sikkerhetsmyndighet skal ha mulighet for å ivareta ansvaret og oppgavene direktoratet er pålagt. Basert på dagens hjemmelsgrunnlag er den informasjon som registreres i VDI-systemet og/eller analyseres av *NorCERT funksjonen* i Nasjonal sikkerhetsmyndighet, som en altoverveiende hovedregel trafikkdata og ikke innholdsdata. I de tilfeller innholdsdata behandles vil dette typisk være ved en konkret mistanke om en alvorlig hendelse. NorCERT-funksjonen behandler trafikkdata i forbindelse med avdekking og håndtering av alvorlige dataangrep mot samfunnskritisk infrastruktur, og det kan i enkelte tilfeller også være behov for å analysere innholdsdata.

Lov om behandling av personopplysninger (personopplysningsloven) definerer i § 2 1) «personopplysning» som opplysninger og vurderinger som kan knyttes til enkeltperson. Gjennom VDI- og NorCERT-funksjonene vil Nasjonal sikkerhetsmyndighet få tilgang til personopplysninger. Vilkår for behandling av personopplysninger følger av personopplysningsloven § 8. I utgangspunktet kan det enten gjøres etter samtykke, der det er fastsatt i lov, eller der det er nødvendig på grunn av nærmere angitte formål. Rettslig grunnlag for behandling av personopplysninger gjennom VDI- og NorCERT-funksjonene er i dag forankret i § 8 f. Det må da foretas en nødvendighetsvurdering av behandlingen. Behandling av personopplysninger må for det første ivareta en berettiget interesse, og videre må hensynet til den registrertes personvern ikke overstige denne interessen. I den grad sensitive personopplysninger, jf. personopplysningsloven § 2 nr. 8, blir behandlet, er rettslig grunnlag personopplysningsloven § 9 første ledd f.

Behandling av personopplysninger er en forutsetning for at Nasjonal sikkerhetsmyndighet gjennom VDI- og NorCERT-funksjonene skal kunne detektere, varsle og koordinere håndteringen av alvorlige IKT-hendelser. For Nasjonal sikkerhetsmyndighet vil formålet med registrering og analysering av data aldri være å behandle personopplysninger, men utelukkende å oppdage ondsinnet kode, unormale forhold eller aktiviteter som kan skjule seg i kommunikasjonen og i innholdet i kommunikasjonen. Som det fremgår nedenfor, foreslår departementet at adgangen fastsettes i lov – sikkerhetsloven. En slik løsning gir etter departementets oppfatning et mer forutsigbart og klarere rettslig grunnlag for behandlingen enn den skjønnsmessige vurderingen som i dag må foretas etter personopplysningsloven § 8 f.

2.3.1 Utenlandsk rett

I *Danmark* ble GovCERT (Governmental Computer Emergency Response Team) 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 MILCERT (Militær varslingstjeneste for internettrusler) nå er en del av Forsvarets Efterretningstjeneste som «Center for Cybersikkerhed». Senterets virksomhet er fra 1. juli 2014 lovregulert i ny «Lov om Center for Cybersikkerhet». Loven etablerer et behandlingsgrunnlag for innholdsdata og trafikkdata både for virksomheter og myndigheter tilsluttet «Center for Cybersikkerhets netsikkerhetstjeneste» og myndigheter på Forsvarsministeriets område. 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 utvides i vesentlig grad maksimal oppbevaringstid for innsamlede data som ikke knytter seg til en sikkerhetshendelse.

I *EU* la Europaparlamentet mot slutten av 2013 frem 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 direktivets vedlegg 1, fremgår en mer detaljert oppgave- og kravsbeskrivelse. Disse forutsettes av Kommisjonen å bli 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.

2.3.2 Vurdering og forslag til endringer i § 9 og ny § 10 a

Nærmere om forslag til ny § 9 første ledd e.

Departementet foreslår at virksomheten som i dag utøves av Nasjonal sikkerhetsmyndighet gjennom VDI- og NorCERT-funksjonene lovfestes i § 9 som en del av Nasjonal sikkerhetsmyndighets oppgaver. Bestemmelsen foreslås inntatt som ny *e.* i § 9 første ledd. Som følge av ny e., forskyves dagens e. og f. Disse vil få bokstavene *f.* og *g*.

Departementet mener at dagens ordning med frivillig tilknytning til VDI skal videreføres som hovedprinsipp, men at det i forskrifter bør vurderes åpnet for å gjøre unntak fra dette for skjermingsverdige objekter og graderte informasjonssystemer, eller systemer som understøtter slike og som kan være spesielt utsatt for såkalte logiske trusler. Dette vil kun være som en «sikkerhetsventil» der tilknytning til VDI-systemet vurderes som påkrevd ut fra en vurdering av det totale risikobildet, og hvor det ikke har vært mulig å få til en avtale basert på frivillighet. Departementet vil understreke at unntak fra frivillighet kun er ment å omfatte de største og viktigste systemene innen norsk IKT-infrastruktur.

Gjennom VDI-funksjonen og samarbeidet med private virksomheter tilknyttet dette, får Nasjonal sikkerhetsmyndighet også tilgang til informasjon som kan være av konkurransemessig betydning for de berørte virksomheter. Denne informasjonen håndteres etter bestemmelsene i forvaltningsloven § 13. Departementet mener at denne ordningen er hensiktsmessig og foreslår ingen endringer her.

Nærmere om forslag til ny § 10 a

Departementet foreslår også en ny *§ 10 a* som klargjør Nasjonal sikkerhetsmyndighets adgang til å behandle personopplysninger.

Selv om formålet med VDI- og NorCERT-funksjonene ikke er å samle inn personopplysninger, er det ikke til å unngå at slike opplysninger behandles som ledd i å ivareta oppgavene knyttet til detektering, varsling og koordinering av håndteringen av alvorlige IKT-angrep. Det gjelder særlig personopplysninger som en del av trafikkdata, men også i noen utstrekning innholdsdata. Personopplysningsloven § 8 oppstiller ulike grunnlag for å behandle personopplysninger. I tillegg til ved samtykke gitt av den registrerte, kan det gjøres dersom det er fastsatt i lov eller at behandlingen er nødvendig for å oppfylle nærmere angitte formål. Departementet mener adgangen bør reguleres gjennom en selvstendig hjemmel i sikkerhetsloven, istedenfor å benytte det generelle og mer skjønnsmessige grunnlaget i personopplysningsloven § 8 f, slik som i dag.

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 har vurdert konsekvenser for personvernet som følge av forslaget. Behandling av trafikkdata innebærer ikke et utvidet inngrep sammenlignet med gjeldende ordninger. IP-adresser vil måtte koples med andre opplysninger for å kunne knyttes til en fysisk person. Dette er informasjon Nasjonal sikkerhetsmyndighet ikke er i besittelse av og heller ikke har behov for i ivaretakelsen av sine oppgaver. Nasjonal sikkerhetsmyndighet vil således bare behandle disse opplysningene i en avidentifisert form.

I den utstrekning personopplysninger behandles i identifiserbar form (innholdsdata) vil formålet være analyse av ondsinnet kode eller håndtering av et mulig eller identifisert IKT-angrep rettet mot samfunnskritisk IKT-infrastruktur eller samfunnskritiske funksjoner. Sterke samfunnsmessige interesser nødvendiggjør en effektiv avdekking og håndtering av alvorlige IKT-angrep. Formålet med aktiviteten er ikke innsamling eller annen form for behandling av personopplysninger. Som ledd i utøvelsen av funksjonene er det flere situasjoner hvor det vil være behov for å behandle innholdsdata: For å oppdage angrep blir det gjennom VDI-systemet plassert sensorer i nettverket slik at de kan registrere unormal trafikk i tilknyttede virksomheters inn- og utgående datastrømmer. Det er videre behov for sensorer som er konfigurert slik at det utløses en alarm ved et angrep. For å kunne verifisere et angrep må det lagres en begrenset datamengde knyttet til angrepet, som også kan omfatte innholdsdata, for å muliggjøre analyse av den utløste alarmen. Ondsinnet kode kan også være inkorporert i e-poster eller vedlegg til slike. Behandling av innholdsdata kan også være nødvendig for å analysere denne type angrep. Der en virksomhet har vært utsatt for et IKT-angrep kan det også være behov for at Nasjonal sikkerhetsmyndighet, gjennom NorCERT-funksjonen, bistår ved å analysere harddisker eller servere. Dette er nødvendig for å kunne kartlegge angrepets omfang, hvilken informasjon som er kompromittert og for å kunne gi anbefalinger om skadereduserende tiltak. Ingen av de tilfellene hvor innholdsdata behandles, vil altså formålet med aktiviteten være å behandle personopplysninger. Slike opplysninger vil imidlertid måtte behandles som et nødvendig ledd i utførelsen av oppgaven. På denne bakgrunn er det etter departementets vurdering nødvendig å gi adgang til å behandle både trafikkdata og innholdsdata.

Tilknytning til VDI-systemet er frivillig og vil være samtykkebasert. Unntaksvis kan det bli tale om å gi pålegg om tilknytning til systemet, jf. ovenfor om vurdering av dette i forskrift. Ordningen innebærer at sensorene i VDI-systemet drives i nært samarbeid mellom Nasjonal sikkerhetsmyndighet og de tilknyttede virksomhetene. Som ledd i tilknytningen til VDI inngås en avtale mellom Nasjonal sikkerhetsmyndighet og virksomheten hvor rettigheter og plikter i tilknytning til utplassering av sensorer reguleres nærmere. I avtalen reguleres rammene for Nasjonal sikkerhetsmyndighets bruk av innsamlet informasjon, og virksomhetens rett til innsyn i konfigurasjon av sensor og i de data som samles inn. Registrerer VDI-sensoren alvorlig uønsket datatrafikk, vil virksomheten bli varslet om dette. Ved inngåelse av avtale om tilknytning til VDI forutsettes det at virksomhetene implementerer avtalen på en slik måte at de ansattes rettigheter etter personopplysningsloven og arbeidsmiljøloven ivaretas. Nasjonal sikkerhetsmyndighets behandling av innsamlede data i tilknytning til VDI- og NorCERT-funksjonene er også underlagt EOS-utvalgets kontroll.

Departementet legger til grunn at personopplysningsloven kommer til anvendelse for behandlingen av personopplysninger, dog 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.

Departementet foreslår at § 9 skal lyde:

§ 9. Nærmere om oppgavene

Nasjonal sikkerhetsmyndighet skal

a. innhente og vurdere informasjon av betydning for gjennomføringen av forebyggende sikkerhetstjeneste,

b. søke internasjonalt samarbeid, herunder med andre lands og organisasjoners tilsvarende tjenester, når dette tjener norske interesser,

c. føre tilsyn med sikkerhetstilstanden i virksomheter, herunder kontrollere at den enkeltes plikter i eller i medhold av loven her overholdes, og eventuelt gi pålegg om forbedringer,

d. bidra til at sikkerhetstiltak utvikles, herunder iverksette forskning og utvikling på områder av betydning for forebyggende sikkerhetstjeneste,

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

f. gi informasjon, råd og veiledning til virksomheter, og

g. for øvrig utføre de oppgaver som fremgår av bestemmelsene i og i medhold av loven her.

Kongen kan gi nærmere bestemmelser om Nasjonal sikkerhetsmyndighets utøvelse av oppgavene.

Departementet foreslår at ny § 10 a skal lyde:

§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.

2.4 Reduksjon av antall klareringsmyndigheter

2.4.1 Gjeldende rett

I henhold til sikkerhetsloven § 19 skal personkontroll og sikkerhetsklarering gjennomføres på forhånd når en person vil kunne få tilgang til skjermingsverdig informasjon gradert KONFIDENSIELT eller høyere. For tilgang til informasjon gradert BEGRENSET kreves ikke sikkerhetsklarering, men vedkommende må være autorisert. Etter dagens regelverk er hvert enkelt departement klareringsmyndighet for personell innen sitt myndighetsområde, jf. sikkerhetsloven § 23. 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 (herunder 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. Gjenstående er det 26 ulike sivile klareringsmyndigheter, som utgjøres av de enkelte departementene og enheter disse har delegert klareringsmyndighet videre til.

Ved revisjonen av sikkerhetsloven i 2006 ble klareringsmyndighetsstrukturen vurdert, jf. Ot.prp.nr. 59 (2004-2005). Arbeidsgruppen som den gang ble nedsatt for å se på regelverket la frem 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 frametter 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 at departementene strammer inn delegasjonspraksisen har imidlertid hatt en begrenset virkning, og antallet klareringsmyndigheter har ikke blitt vesentlig redusert i etterkant av denne lovrevisjonen.

2.4.2 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 (etatssjef) 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).

2.4.3 Vurdering og forslag til endringer i § 23

Skjev fordeling av antall saker og mange enheter med klareringsmyndighet gir utfordringer med hensyn til kvaliteten og effektiviteten i saksbehandlingen. Departementet er fortsatt bekymret for at flere av de mindre klareringsinstansene ikke makter å vedlikeholde tilstrekkelig kompetanse til å sikre nødvendig kvalitet i sin saksbehandling. De endringene som ble gjort i klareringsmyndighetsstrukturen ved forrige lovrevisjon i 2006, har ikke ført til at situasjonen anses tilfredsstillende. Status i dag er fragmenterte og lite robuste fagmiljøer, hvor Nasjonal sikkerhetsmyndighet fungerer som et «bindeledd» i kraft av sin rolle som klagebehandler og kursarrangør for opplæring av medarbeidere som skal behandle klareringssaker. Formålet med dette forslaget er å øke kvaliteten og effektivisere saksbehandlingen av klareringssaker.

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)

Nasjonal sikkerhetsmyndighet 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. Nasjonal sikkerhetsmyndighet 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.

Nasjonal sikkerhetsmyndighets oppfatning er at saksbehandlingsfeil ved de små klareringsmyndighetene i større grad skyldes manglende kompetanse, sammenlignet med saksbehandlingsfeil hos de større klareringsmyndighetene, som ofte skyldes at myndighetene ressursmessig er underdimensjonert. Tilsynsfunn som er gjort indikerer også at de klareringsmyndighetene som har stor grad av nærhet til personellet de klarerer, har problemer med å fatte negative avgjørelser. Avhengig av graderingsnivået foretar klareringsmyndigheten en objektiv personkontroll basert på blant annet opplysninger i personopplysningsblanketten og opplysninger fra en rekke registre. For å sikre kvaliteten og objektiviteten i vurderingsgrunnlaget for sikkerhetsklareringer kreves det en viss avstand mellom klareringsmyndigheten og den personen som skal klareres. Nasjonal sikkerhetsmyndighet har videre opplyst at man gjennom behandlingen av klagesaker erfarer det samme som i tilsynsrollen. Behandlingen av klagesaker avdekker ofte saksbehandlingsfeil og/eller at saken er mangelfullt opplyst. Ofte er heller ikke relevante momenter i vurderingsgrunnlaget for sikkerhetsklarering etter sikkerhetsloven § 21 vurdert. Nasjonal sikkerhetsmyndighet mener også at skjønnet som skal utøves i klareringssaker er krevende for flere av klareringsmyndighetene, hvilket trolig er grunnen til at ellers like saker blir behandlet ulikt. Videre har Nasjonal sikkerhetsmyndighet også sett flere eksempler på at personer med tilknytning til andre land er gitt sikkerhetsklarering uten at Nasjonal sikkerhetsmyndighets landvurderinger er benyttet i vurderingen, jf. personellsikkerhetsforskriften § 3-3 tredje ledd.

Utviklingstrender tilsier at slike utfordringer som Nasjonal sikkerhetsmyndighet beskriver vil forsterkes i fremtiden. Departementets inntrykk er at kompleksiteten i sakene generelt øker, og at det stilles stadig større krav til kompetanse hos klareringsmyndighetene for å kunne håndtere sakene på en god måte. 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.

Departementet mener at antallet klareringsmyndigheter bør reduseres betydelig. 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 har vurdert ulike alternativer. 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. 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.

Hensynet til enhetlig tilnærming til behandling av klareringssaker, etablering av robuste fagmiljøer, ivaretakelse av individets rettssikkerhet og styrking av sikkerheten i forsvarssektoren og i sivil sektor, vil i størst grad bli ivaretatt ved det tredje alternativet. I tillegg er dette alternativet en økonomisk og administrativt bedre løsning enn dagens situasjon (se nedenfor i punkt 3 om økonomiske og administrative konsekvenser).

Departementet foreslår på denne bakgrunn 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 endringen er en sentralisering av klareringsmyndighetene innen sivil sektor. I forslaget er det forutsatt at de tre EOS-tjenestene fortsetter å klarere eget personell grunnet de særlige forhold som gjør seg gjeldende for disse tjenestene. Departementet er også av den oppfatning at det gis åpning for at også andre (enn EOS-tjenestene) kan gis slik myndighet dersom særlige grunner tilsier det. Av konstitusjonelle hensyn bør Stortinget, domstolene og Statsministerens kontor fortsatt opprettholdes som egne klareringsmyndigheter. Ideelt sett bør det for Stortinget og organer underlagt Stortinget, kun være én klareringsmyndighet. Det samme gjelder for domstolene. Av habilitetshensyn anser departementet det hensiktsmessig at den sivile klareringsmyndigheten klarerer personellet i klareringsmyndigheten i forsvarssektoren, og vice versa.

Særlig om organisering 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 ressurser 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.

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.

Særlig om organiseringen av klareringsmyndigheten i forsvarssektoren
I forsvarssektoren er det i dag fem klareringsmyndigheter. Etter forslaget vil Forsvarets sikkerhetsavdeling overta Forsvarsdepartementets og Forsvarsbyggs sikkerhetsklareringer (herunder Forsvarsbyggs klareringer for Forsvarets forskningsinstitutt (FFI) og Aerospace Industrial Maintenance Norway (AIM)). Nasjonal sikkerhetsmyndighet og Etterretningstjenesten vil fortsatt være egne klareringsmyndigheter. Etter omorganiseringen vil klareringsmyndighetene behandle Cosmic Top Secret (CTS)-klareringer, som etter dagens ordning behandles av Nasjonal sikkerhetsmyndighet i første instans. Det vil også ligge til de enkelte klareringsmyndighetene å sikkerhetsklarere utenlandske statsborgere. Nasjonal sikkerhetsmyndighet vil være klagemyndighet for klareringsmyndighetene i forsvarssektoren. Forsvarsdepartementet vil imidlertid fortsatt være klageinstans for saker som gjelder Nasjonal sikkerhetsmyndighets klarering av eget personell. Departementet mener 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. Etter det opplyste behandlet Forsvarsdepartementet 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 CTS-klareringer som etter forslaget blir overført fra Nasjonal sikkerhetsmyndighet 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.

2.4.4 Nærmere om lovforslaget

Dagens § 23 første, annet, tredje og 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, andre, tredje og fjerde ledd falle bort og erstattes av forslag til nytt andre og tredje ledd.

Dagens femte ledd omhandler autorisasjon. Det foreslås ingen materielle endringer i dette leddet. Ved en inkurie er det brukt ordet «sikkerhetssamtale» i tredje punktum. Riktig ord er autorisasjonssamtale. Det foreslås at denne feilen rettes opp. Av regeltekniske hensyn foreslår 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 mener derfor det er mer pedagogisk at regulering av autorisasjon kommer først i bestemmelsen. Som en konsekvens av endring i rekkefølge i bestemmelsen, foreslås også tittelen i § 23 endret slik at autorisasjon nevnes først.

Departementet foreslår at § 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 *autorisasjonssamtale* er avholdt. Nasjonal sikkerhetsmyndighet gir nærmere regler om autorisasjon og om hvem som er autorisasjonsansvarlig.

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.

2.5 Sikkerhetsgraderte anskaffelser – varighet av leverandørklarering

2.5.1 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.

I sikkerhetsgraderte anskaffelser på alle graderingsnivåer skal det inngås sikkerhetsavtale mellom anskaffelsesmyndigheten og leverandøren. I tillegg, før en leverandør kan få tilgang til skjermingsverdig informasjon sikkerhetsgradert KONFIDENSIELT eller høyere, eller dersom det av andre grunner anses nødvendig, skal leverandøren 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) side 61 flg.) ikke begrunnet nærmere hvorfor denne begrensningen er valgt, men det fremgår at bestemmelsen er en videreføring fra tidligere direktiver. Virksomheten som gjennomfører en sikkerhetsgradert anskaffelse må søke om leverandørklaring for den enkelte sikkerhetsgraderte anskaffelse. Nasjonal sikkerhetsmyndighet er klaringsmyndighet, jf. § 28 første ledd siste punktum. En leverandør som innehar en leverandørklarering skal uten ugrunnet opphold orientere Nasjonal sikkerhetsmyndighet 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 Nasjonal sikkerhetsmyndighet inndra leverandørklareringen, jf. § 28 fjerde ledd, jf. forskriften § 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.

2.5.2 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). 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».[3] Regelverket oppstiller de sikkerhetskrav som kommer til anvendelse ved NATO- sikkerhetsgraderte kontrakter. 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.

2.5.3 Forholdet til EØS-avtalen

For offentlige oppdragsgivere må regelverket om sikkerhetsgraderte anskaffelser ses 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.

2.5.4 Vurdering og forslag til endringer i § 28

Departementet mener systemet med klarering for hvert enkelt oppdrag er 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. Departementet foreslår derfor at leverandørklarering skal gis for en nærmere definert tidsperiode. Formålet med forslaget er å effektivisere arbeidet med sikkerhetsgraderte anskaffelser. Forslaget vil være en forenkling for så vel industrien som for myndighetene.

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

[3] Dokument C-M(2002)49 Enclosure G og AC/35-D/2003

Nasjonal sikkerhetsmyndighet om at gyldig leverandørklarering foreligger være tilstrekkelig. Industrien har også uttalt seg positivt til en 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 innføres et regime for tildeling og oppfølging når klaringer gis for en bestemt periode. 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 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. Ulempen ved en slik ordning er at det kan bli oppfattet og fremstilt som en offentlig sikkerhetsmessig godkjenning, og et kvalitetsstempel som virksomheter kan ønske å ha for å styrke sin generelle markedsmessige posisjon. Dette kan medføre 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.

Departementet foreslår på denne bakgrunn at leverandørklarering gis etter anmodning fra en anskaffelsesmyndighet, slik som i dag, men med en tidsavgrenset varighet.

Sikkerhetsloven § 28 første ledd andre punktum om varighet på leverandørklarering foreslås endret i tråd med forslaget som er redegjort for ovenfor.

Endringen forutsetter en endring i forskrift om sikkerhetsgraderte anskaffelser.

Departementet foreslår at § 28 skal lyde:

§ 28. Leverandørklarering

Før en leverandør kan få tilgang til skjermingsverdig informasjon sikkerhetsgradert KONFIDENSIELT eller høyere, eller dersom det av andre grunner anses nødvendig, skal leverandøren ha gyldig leverandørklarering for angitt sikkerhetsgrad. *Kongen fastsetter den*

generelle gyldighetstid for leverandørklareringer. Nasjonal sikkerhetsmyndighet er klareringsmyndighet.

Leverandørklarering skal ikke gis dersom det foreligger rimelig tvil om leverandørens sikkerhetsmessige skikkethet. Ved avgjørelse om sikkerhetsmessig skikkethet skal det bare legges vekt på forhold som er relevante for å vurdere leverandørens evne og vilje til å utøve forebyggende sikkerhetstjeneste etter bestemmelsene i eller i medhold av loven her. I vurderingen skal inngå personkontroll av personer i leverandørens styre og ledelse.

Leverandøren skal gi alle opplysninger som antas å kunne være av betydning for klareringsspørsmålet.

Leverandøren skal uten ugrunnet opphold orientere Nasjonal sikkerhetsmyndighet om endringer i styre eller ledelse, forandringer i eierstrukturen, flytting av lokaliteter og utstyr, åpning av gjeldsforhandling eller begjæring om konkurs og andre forhold som kan ha betydning for leverandørens sikkerhetsmessige skikkethet. Anses slike forhold å representere en sikkerhetsrisiko og risikoen ikke kan elimineres gjennom å utøve forebyggende sikkerhetstjeneste, kan Nasjonal sikkerhetsmyndighet inndra leverandørklareringen. Skjermingsverdig informasjon eller objekt kan ikke overføres til ny eier eller inngå i bobehandling ved gjeldsforhandling eller konkurs, med mindre Nasjonal sikkerhetsmyndighet har samtykket til dette.

For øvrig gjelder reglene i kapittel 6, herunder reglene om begrunnelse og klage, så langt de passer.

2.6 Gebyr

2.6.1 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 ved godkjenning av informasjonssystemer, skal eier av systemet budsjettere med og dekke alle kostnader knyttet til sikkerhetsgodkjenningen.

2.6.2 Vurdering og forslag til ny § 6 a

Departementet foreslår i § 6 a en klar hjemmel for å kunne kreve gebyr der en virksomhet utfører tjenester for en annen. Formålet med forslaget er å sikre hjemmel for gebyrlegging av tjenester. Forslaget innebærer at det åpnes for nærmere å regulere i forskrift at det kan kreves gebyr for visse tjenester som, i medhold av bestemmelser gitt i sikkerhetsloven med underliggende forskrifter, utføres av en virksomhet for en annen.

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 kryptosystemer, 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.

Departementet ser at det kan være flere fordeler med en gebyrordning. For det første vil den tjenesteytende virksomheten tilføres økte ressurser ved økt saksmengde. På enkelte områder antas også at en gebyrordning vil kunne bidra til at virksomheter som ber om en tjeneste i større grad foretar en reell vurdering av det aktuelle behovet for tjenesten, som for eksempel sikkerhetsklarering.

På den annen side er det viktig at en ordning med gebyr ikke medfører en svekkelse av sikkerhetstilstanden. Det er viktig å unngå en situasjon hvor gebyrordningen medfører at nødvendige sikkerhetstiltak ikke blir iverksatt på bakgrunn av rene økonomiske vurderinger. Det er derfor sentralt at eventuelle fordeler ved å ha gebyr veies opp mot de kostnader den enkelte virksomhet påføres.

Forslaget til ny § 6 a gir kun en rettslig adgang til å fastsette forskrift om gebyr. Forslaget har derfor ingen direkte rettsvirkninger i seg selv. Eventuelle nye områder som skal ilegges gebyr, må utredes og foreslås i et eventuelt senere forskriftsarbeid. Departementet har sett på hvilke momenter som bør vurderes ved 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.

I et eventuelt forskriftsarbeid forutsetter departementet at det vurderes og konsekvensutredes nærmere hvilke områder som kan være egnet for gebyrfinansiering. Dette gjelder både kostnadsbildet så vel som de sikkerhetsmessige konsekvenser av å gebyrlegge en tjeneste.

Departementet foreslår at ny § 6 a skal lyde:

§ 6 a *Gebyr*

Kongen kan fastsette nærmere forskrift om gebyr for tjenester som utføres med hjemmel i denne lov. Gebyret må være formålstjenlig, og gebyret skal ikke overstige kostnadene ved ytelsen.

2.7 Forslag til ny bestemmelse om anskaffelser til kritisk infrastruktur

2.7.1 Gjeldende rett

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.

Med kritisk infrastruktur menes her anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner og befolkningens trygghetsfølelse. Med samfunnets kritiske funksjoner menes funksjoner som er absolutt nødvendige for å ivareta befolkningens grunnleggende behov (behov for drikkevann, mat, varme, nasjonal sikkerhet, styring og kriseledelse, demokratisk rettsstat, trygghet for liv og helse, lov og orden, finansiell stabilitet, grunnleggende sikkerhet for lagret informasjon, kulturelle verdier av nasjonal betydning, samt natur og miljø). Blant annet vil følgende allmenne innsatsfaktorer være nødvendige for å kunne opprettholde disse kritiske samfunnsfunksjonene: ekom-tjenester, elforsyning, vannforsyning, avløpshåndtering, drivstofforsyning, vare- og persontransport, satellittbaserte tjenester og meteorologiske tjenester.

Utstrakt bruk av utenlandske leverandører er potensielt problematisk fordi det medfører en forhøyet risiko for spionasje, sabotasje og terror til skade for norske interesser. Samfunnets økte avhengighet av kritisk infrastruktur gjør at denne problemstillingen trolig vil få stadig større relevans fremover. Departementet har registrert tilfeller der myndighetene ikke har hatt hjemmel til å nekte leveranser til norsk kritisk infrastruktur, selv om det har blitt vurdert å foreligge en potensiell fare for spionasje eller sabotasje mot Norge.

Sikkerhetsloven inneholder bestemmelser som 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 sikkerhetsgraderte anskaffelser. Definisjonen av sikkerhetsgraderte anskaffelser er knyttet opp mot at leverandøren vil kunne få tilgang til sikkerhetsgradert informasjon eller til et skjermingsverdig objekt.

Imidlertid vil ikke alle anskaffelser til kritisk infrastruktur bli fanget opp av reglene om sikkerhetsgraderte anskaffelser. En leverandør vil etter omstendighetene kunne utnytte tilgang

til kritisk infrastruktur 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 ser behov for et rettslig grunnlag for myndighetene til å stille sikkerhetsmessige krav også i slike tilfeller.

2.7.2 Vurdering og forslag til ny § 29 a

Hovedpunktene i forslaget

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 ivaretar. 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.

Varslingsplikt for virksomhetene

For at myndighetene skal kunne få kunnskap om risikofylte anskaffelser på et så tidlig tidspunkt som mulig, foreslår departementet at virksomheter som eier eller rår over kritisk infrastruktur i visse tilfeller skal være forpliktet til å varsle om planlagte anskaffelser. Varslingsplikten vil kun påhvile virksomheter som loven gjelder for, dvs. forvaltningsorganer eller andre rettssubjekter som ved enkeltvedtak er omfattet av loven, jf. sikkerhetsloven § 2. 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.

Det er den enkelte virksomhet som, basert på en samlet vurdering, må avgjøre hvorvidt det foreligger en anskaffelse som utløser varslingsplikt. Varslingsplikten utløses dersom anskaffelsen innebærer en «ikke ubetydelig risiko for rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser». 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. I tilfeller der det foreligger en risiko, men denne er av en slik art at den kan håndteres tilfredsstillende av virksomheten selv, kan dette tilsi at varsling ikke er påkrevd.

Virksomheten skal varsle så snart det er klart for virksomheten hvilke leverandører som er aktuelle kandidater for anskaffelsen, og før det er besluttet å benytte en konkret leverandør.

Varselet skal sendes til det departementet som forvalter regelverket i den aktuelle sektoren (i lovteksten kalt «ansvarlig fagdepartement»).

Når et departement mottar et varsel

Et departement som mottar et varsel fra en virksomhet, bør innhente rådgivende uttalelser om leveransens risikopotensiale og om de aktuelle leverandørenes sikkerhetsmessige pålitelighet. Uttalelsene skal innhentes fra relevante organer med kompetanse i de aktuelle spørsmålene. Den klare hovedregelen er at departementet *skal* innhente slike uttalelser. Det foreslås likevel å benytte ordet «bør» i lovteksten, slik at innhenting 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.

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 som gis skal være så detaljerte at de gir fagdepartementet en reell mulighet til å vurdere risikoen for sikkerhetstruende virksomhet opp mot andre hensyn som gjør seg gjeldende i saken. Ettersom de rådgivende organene har ulik kompetanse og myndighet, antar departementet at uttalelsene i ulik grad vil fokusere på henholdsvis leveransens risikopotensiale og på leverandørenes sikkerhetsmessige pålitelighet. 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 fagdepartementet mener de rådgivende uttalelsene ikke gir et tilstrekkelig beslutningsgrunnlag, kan fagdepartementet kreve bistand fra Forsvarsdepartementet eller Justis- og beredskapsdepartementet. Det er likevel fagdepartementet som til sist må ta avgjørelsen basert på en helhetsvurdering av hensynene som gjør seg gjeldende i saken. 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.

Vedtaket av Kongen i statsråd

Dersom Kongen i statsråd får en anbefaling forelagt seg, tilligger det Kongen i statsråd å fatte endelig vedtak i saken. Vedtakskompetansen er lagt til Kongen i statsråd fordi sakene som det vil være aktuelt å fatte vedtak i, vil være av en slik alvorlighetsgrad at beslutningen bør tas av regjeringen som kollegium. Samtidig vil det være tale om så få saker at det ikke anses ressursmessig problematisk å legge vedtakskompetansen til Kongen i statsråd. 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.

Veiledningsplikt for Nasjonal sikkerhetsmyndighet
Departementet foreslår at Nasjonal sikkerhetsmyndighet utarbeider generelt veiledningsmateriale som gjøres tilgjengelig for aktuelle virksomheter. Dette for at varslingsplikten skal kunne bli forutsigbar og mulig å praktisere, uten at det utvikler seg en praksis med overdreven varsling.

Kompetanse til å gi forskrift – Kongen i statsråd
I medhold av tredje ledd er Kongen i statsråd gitt kompetanse til å gi forskrift om varslingsplikten etter første ledd og om hvilke vedtak som kan treffes etter andre ledd. Fordi det er Kongen i statsråd som er gitt kompetanse til å fatte vedtak etter andre ledd, må kompetansen til å gi forskrift ligge på samme nivå. Departementet antar ar det kan bli aktuelt å gi nærmere regler om anvendelsen av denne bestemmelsen.

Overgangsbestemmelser
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.

Forholdet til internasjonale forpliktelser
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. Det finnes også supplerende folkerettslige prinsipper som kan benyttes til å begrunne vedtak ut fra de samme betraktningene, herunder det folkerettslige prinsippet om «necessity». 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.

Forholdet til Grunnloven
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

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.

Sanksjoner

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).

Regeltekniske justeringer

Departementet foreslår at bestemmelsen inntas i kapittel 7. Sikkerhetsgraderte anskaffelser. På denne bakgrunn foreslås ny overskrift til kapittel 7: Sikkerhetsgraderte anskaffelser og anskaffelser til kritisk infrastruktur.

Departementet foreslår følgende overskrift i kapittel 7:

Kapittel 7. Sikkerhetsgraderte anskaffelser *og anskaffelser til kritisk infrastruktur*

Departementet foreslår at ny § 29 a skal lyde:

§ 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.

2.8 Forslag til ny bestemmelse om varsling mv. ved risiko for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser

2.8.1 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.

Etterretningsaktivitet kan potensielt utføres uten noen klar tilknytning til skjermingsverdige objekter. Aktiviteten kan for eksempel bestå i at en utenlandsk aktør får tilgang 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.

Relevante bestemmelser i sikkerhetsloven er i all hovedsak knyttet til skjermingsverdige objekter, herunder sikring av slike objekter. Det finnes 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. Departementet mener at sikkerhetsloven er egnet som lovmessig forankring for en slik ny bestemmelse. Loven er sektorovergripende, og har nettopp som formål å motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, jf. loven § 1 bokstav a.

2.8.2 Vurdering og forslag til ny § 5 a

Departementet foreslår å innta en ny bestemmelse i sikkerhetsloven kapittel 2. Bestemmelsen skal regulere to forhold. For det første gir den Kongen i statsråd fullmakt 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. For det andre oppretter bestemmelsen en varslingsplikt for virksomheter som er underlagt sikkerhetsloven i tilfeller der det foreligger en ikke ubetydelig risiko for slik aktivitet.

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.

Kompetanse til å fatte nødvendige vedtak av Kongen i statsråd

Forslaget gir Kongen i statsråd kompetanse til å fatte de vedtak som vurderes som nødvendige. Slike vedtak vil kunne fattes mot enhver som planlegger eller utfører aktivitet som omfattes av ordlyden i forslaget til § 5 a. Mulige vedtak kan for eksempel være å nekte å gi byggetillatelse eller frekvenstillatelse, alternativt å hindre et oppkjøp som gir en aktør direkte eller indirekte adgang til å utføre sikkerhetstruende virksomhet. At vedtakene skal være «nødvendige» innebærer 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.

Det presiseres i bestemmelsen at Kongen i statsråd kan fatte vedtak som innebærer omgjøring av en forvaltningsavgjørelse ut over rammene som følger av forvaltningsloven § 35. Dette for å ta høyde for tilfeller der forvaltningen allerede har fattet et vedtak og det av sikkerhetshensyn anses nødvendig å omgjøre vedtaket.

Varslingsplikt for virksomheter som er underlagt loven

For å få kunnskap om potensielt uønskede pågående eller planlagte aktiviteter på et så tidlig tidspunkt som mulig, foreslås det at virksomheter som er underlagt sikkerhetsloven skal pålegges en varslingsplikt. 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 gjelder bare planlagte eller pågående aktiviteter som kan innebære en ikke ubetydelig risiko for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Passusen «ikke ubetydelig risiko» gir anvisning på den skjønnsmessige vurderingen av risikoen som må foretas i det enkelte tilfellet. 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 bestemmelsen vil det typisk være aktuelt å innhente rådgivende uttalelser fra Nasjonal sikkerhetsmyndighet, Politiets sikkerhetstjeneste og Etterretningstjenesten. 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.

Kompetanse til å gi forskrift – Kongen i statsråd

I medhold av tredje ledd er Kongen i statsråd gitt kompetanse til å gi forskrift om varslingsplikten etter første ledd og om hvilke vedtak som kan treffes etter andre ledd. Fordi det er Kongen i statsråd som er gitt kompetanse til å fatte vedtak etter andre ledd, må kompetansen til å gi forskrift ligge på samme nivå. Departementet antar at det kan bli aktuelt å gi nærmere regler om anvendelsen av denne bestemmelsen.

Forholdet til Grunnloven og Norges internasjonale forpliktelser

Departementet har vurdert bestemmelsens forhold til Grunnloven og til Norges internasjonale forpliktelser. Departementets vurderinger og konklusjon når det gjelder forslaget til ny § 5 a er i all hovedsak tilsvarende som for ny § 29 a, og det vises derfor til redegjørelsen under punkt 2.7.2 ovenfor. Kort oppsummert mener departementet at bestemmelsen i § 5 a i seg selv ikke vil være i strid med Grunnloven eller Norges internasjonale forpliktelser, men at alle vedtak som eventuelt blir fattet med hjemmel i bestemmelsen, vil måtte vurderes konkret på vedtakstidspunktet opp mot de forpliktelsene vedtaket berører.

Departementet har også vurdert utformingen av bestemmelsen når det gjelder de krav legalitetsprinsippet (og EMKs prinsipp om «rule of law») stiller til at rettsregler skal være så presist angitt som mulig. Departementets konklusjon er at bestemmelsen er i samsvar med disse prinsippene.

Departementet foreslår at ny § 5 a skal lyde:

§ 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.

2.9 Ikrafttredelse

Departementet foreslår at det åpnes for at lovforslagene kan tre i kraft på ulike tidspunkt. Dette er særlig begrunnet i ulike behov for forskriftsendringer før lovendringene kan tre i kraft.

3 Økonomiske og administrative konsekvenser

3.1 Innledning

Departementet har vurdert de økonomiske og administrative konsekvensene av lovforslagene. Det er særlig forslagene som gjelder redusert klareringsmyndighetsstruktur, endringer i varighet av leverandørklarering, bestemmelse om anskaffelser til kritisk infrastruktur og bestemmelse om varsling mv. ved risiko for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser 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. Forslaget om hjemmel for å fastsette gebyr gir i seg selv ingen økonomiske konsekvenser, men gir hjemmel til å gi forskrift om fastsettelse av gebyr.

3.2 Forslag om reduksjon av antall klareringsmyndigheter

Særlig om klareringsmyndigheten i sivil sektor

Forslaget om etablering av én sivil klareringsmyndighet er vurdert av Oslo Economics AS. Analysen av både prissatte og ikke-prissatte effekter viser at den foreslåtte omorganiseringen av de sivile klareringsmyndighetene forventes å ha en betydelig positiv samfunnsøkonomisk effekt. Forslaget forventes å gi en samfunnsøkonomisk besparelse på i overkant av 80 mill. kroner over 15 år fordelt på redusert ressursbruk i det offentlige (67,2 mill. kroner) og reduserte samfunnsøkonomiske skattefinansieringskostnader (13,4 mill. kroner). Besparelsen er knyttet til økt effektivitet ved at færre årsverk kan behandle flere saker og kostnadsbesparelser knyttet til samlokalisering på ett sted i stedet for 26 ulike steder. Etableringskostnad knyttet til opprettelsen av én sivil klareringsmyndighet på ca. 9 mill. kroner er særlig knyttet til dublering av lønnskostnader. Denne kostnaden vil imidlertid innen to år inndekkes gjennom reduserte driftskostnader. Omorganiseringen er vurdert å gi bedre kvalitet i saksbehandlingen og kortere og mer forutsigbar ventetid for myndighetene som anmoder om sikkerhetsklarering.

Det må presiseres at forslaget om endring av klareringsstrukturen er sektorovergripende. 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). Tiltaket vil berøre de fleste departementer og noen underlagte virksomheter – og deres kapitler. Det er beregnet at 26 virksomheter anvender ca. 24 årsverk på klareringsoppgavene i 2014. Det legges til grunn at etablering av én sivil klareringsmyndighet skal gjennomføres innenfor berørte departementers gjeldende budsjettrammer gjennom en inndekning av en forholdsmessig andel av kostnadene. En naturlig følge av dette er at ikrafttredelse av bestemmelsen og etableringen av én sivil klareringsmyndighet, vil måtte avvente den nødvendige budsjettinndekningen som endringen krever.

Særlig om klareringsmyndigheten i forsvarssektoren

I en overgangsfase er det en generell risiko for at det blir økte restanser. Ved eventuelle ansettelser av personell til å foreta sikkerhetsklareringer skal disse sertifiseres og læres opp. Det vil derfor kunne ta noe tid før Forsvarets sikkerhetsavdeling oppnår full effektivitet på saksbehandlingen. Departementet foreslår derfor at det i en overgangsperiode tas høyde for å beholde noe av dagens porteføljе i Forsvarsdepartementet og Forsvarsbygg. I likhet med hva som gjelder for sivil sektor, antas det at en overgangsperiode vil vare i ca. fire måneder. Departementet er kjent med at ressurssituasjonen i Forsvarets sikkerhetsavdeling er krevende, og det foregår parallelle prosesser for å tilpasse ressursene til saksmengden. Etter departementets oppfatning vil økningen som følge av samordning av klareringsmyndigheten i forsvarssektoren ikke medføre behov for nye lokaler eller større ressursoverføringer. Forslaget antas på den bakgrunn ikke å ha store økonomiske eller administrative konsekvenser. Finansiering av den foreslåtte endringen vil foretas innenfor Forsvarsdepartementets gjeldende budsjettrammer. Det tas sikte på en intern overføring av ressurser fra Forsvarsdepartementet og Forsvarsbygg til Forsvarets sikkerhetsavdeling i en grad som er tilpasset den økte saksbehandlingsmengden.

3.3 Forslag om endring av varighet av leverandørklareringer

På oppdrag fra Forsvarsdepartementet ble konsulentselskapet BDO bedt om å vurdere to typer konsekvenser ved å endre fra oppdragsbasert leverandørklarering til tidsbestemt godkjenning av leverandør i en periode opp til 5 år. For det første, eventuelle økonomiske og/eller administrative besparelser og for det andre, eventuelle konkurransevridende konsekvenser ved en slik endring.

Når det gjelder de generelle økonomiske og/eller administrative konsekvenser, vurderer BDO at det hovedsakelig vil dreie seg om en tidsmessig besparelse ved at klareringsmyndigheten slipper arbeidet med å foreta reklareringer i en periode og leverandøren slipper å vente på reklarering. Samlet tid fra søknad kommer inn til den er ferdigbehandlet, er i dag normalt flere uker. Når godkjenning først foreligger, vil saksbehandlingstiden falle bort ved senere oppdrag leverandøren har i godkjenningsperioden. For øvrig er endringen fra oppdragsbasert til tidsbasert vurdert til ikke å ha økonomiske eller administrative konsekvenser av betydning, verken i positiv eller negativ forstand.

På spørsmål om endringen kan ha en konkurransevridende effekt, vurderer BDO at det kan ha det. En mulig konsekvens er at en eller flere rådende aktører får fordeler på lang sikt, fordi det er økonomisk fordelaktig for den anskaffende myndighet å fortsette og bruke samme leverandører («customer switching costs»).[4] En slik innsnevring av krets av leverandører som blir benyttet kan i praksis føre til reduksjon i antall aktuelle leverandører. Videre kan det føre til at de leverandørene som blir benyttet, bedrer forhandlingsposisjonen med tanke på pris av varer og tjenester. En annen konsekvens av at Forsvaret/anskaffende myndighet benytter seg

[4] Porter, M.E. 1979. The Five Competitive Forces That Shape Strategy. Harvard Business Review.

av færre leverandører er at det kan bli, og i alle fall oppfattet som at det er, for nær kontakt over tid mellom anskaffende myndighet og enkelte tjenesteleverandører. BDO viser til internasjonale erfaringer hvor slike forhold har fremstått negativt i media. Blant annet har Lockheed Martin og andre leverandører blitt beskyldt for å ha for nære bånd til det amerikanske Forsvarsdepartementet. Det anses viktig å legge inn mekanismer for å redusere risiko for at slike situasjoner inntreffer.

3.4 Forslag om bestemmelse ved anskaffelse til kritisk infrastruktur

De økonomiske og administrative konsekvensene av forslag til ny § 29 a har blitt utredet av konsulent-selskapet BDO. I rapport av 15. juli 2014 konkluderer BDO, under visse forbehold, med følgende:

Implementeringskostnader
Det antas at enkelte virksomheter vil ha et behov for å implementere nye retningslinjer for anskaffelser til sin kritiske infrastruktur. Utgifter til dette anslås til ca. ett årsverk per virksomhet/implementeringsprosjekt.

Kostnader forbundet med økt tidsbruk i anskaffelsesprosesser
I sin rapport antar BDO at de fleste anskaffelser som blir berørt, allerede er underlagt regelverk om offentlige anskaffelser. BDO legger til grunn at konsekvensene grunnet økt tidsbruk derfor ikke vil bli vesentlige. Samtidig påpekes det at innkjøpsvolumet i de berørte sektorene er stort, slik at kostnadene ikke uten videre kan forutsettes å være neglisjerbare. Departementet vil imidlertid påpeke at det er flere private virksomheter som kan bli berørte av ny § 29 a, men som ikke er underlagt regelverket om offentlige anskaffelser. BDOs forutsetning om at de fleste som blir berørt allerede er underlagt regelverket om offentlige anskaffelser, kan dermed være noe upresis. Flere av de virksomhetene som er aktuelle for § 29 a vil måtte forholde seg til de nye varslingsreglene, uten at de fra før er pålagt å følge regler om offentlige anskaffelser.

Kostnader forbundet med saksbehandling ved varsling
Der en virksomhet sender varsel til et departement vil det kreve ressursbruk hos departementet som mottar varselet og hos de offentlige myndighetene som blir anmodet om å avgi rådgivende uttalelser om leveransens risikopotensiale og leverandørens sikkerhetsmessige pålitelighet. Samlet ressursbruk vil være antallet varslinger multiplisert med ressursbruk til saksbehandlingen. På kort sikt antas varslingsplikten primært å kunne bli utløst innenfor ekomsektoren.

Mulige effekter av at enkeltleverandører eventuelt ikke gis adgang til markedet
De klart største konsekvensene antas å kunne komme dersom Kongen i statsråd eventuelt vedtar å utestenge én eller flere leverandører fra et marked. Basert på situasjonen innenfor de ulike sektorene, er det spesielt innenfor ekomsektoren det vil kunne være aktuelt at varslingsplikten utløses på kort sikt. Forutsatt at et varsel medfører at Kongen i statsråd vedtar å utestenge én eller flere leverandører fra ekommarkedet, er et anslag fra BDO at endringen

kan medføre en kostnadsdrivende effekt på investeringer innenfor sektoren mellom 1 og 10%, 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.

3.5 Forslag til ny bestemmelse om varsling mv. ved risiko for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser

Konsulentselskapet BDO har foretatt en vurdering av de økonomiske og administrative konsekvensene av forslag til ny bestemmelse om varsling mv. ved risiko for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, jf. omtale av forslaget til ny bestemmelse i pkt. 2.8 over.

BDO peker på at det er en betydelig utfordring at virkningen av forslaget til ny § 5 a vil være lite kvantifiserbar. BDO mener det ikke vil være forsvarlig å sette en kroneverdi på dette. På denne bakgrunn har ikke BDO gjennomført en kost-nytteanalyse i tradisjonell forstand. BDO har derfor forsøkt å redegjøre for de kostnadsmessige virkningene av å innføre bestemmelser om varslingsplikt og kompetanse for Kongen i statsråd til å fatte nødvendige vedtak.

Departementet antar at det kan være nødvendig og hensiktsmessig å utforme en veileder eller instruks som forklarer bestemmelsen, og som bidrar til at de aktuelle virksomhetene kan gjøres kjent med, og eventuelt selv utarbeide og implementere, relevante varslingsrutiner mv. i sin virksomhet. Departementet vurderer de økonomiske og administrative konsekvensene av varslingsplikten som små.

Forslaget i andre ledd om muligheten for Kongen i statsråd til å fatte nødvendige vedtak er en unntaksbestemmelse. Saksbehandlingsaktivitet knyttet til varslinger, herunder uttalelser fra relevante organer, forventes ikke å inntreffe på jevnlig basis, og omfanget vurderes derfor som svært lite. BDO vurderer de økonomiske og administrative konsekvensene av denne delen av bestemmelsen som beskjedne. På bakgrunn av disse vurderingene legger departementet til grunn at den beskjedne aktiviteten som ventes å komme som følge av første og andre ledd i den nye bestemmelsen, løses innenfor den enkelte virksomhets eksisterende rammer.

Det er videre foretatt en vurdering av om regelendringen vil kunne gjøre Norge til et mindre attraktivt marked å investere i for globale aktører. BDO peker på at det er vanlig praksis for globale investorer å vurdere regulatorisk og politisk risiko ved investeringer i det globale markedet. Tilstedeværelsen av denne type bestemmelse kan tolkes til å bidra til uforutsigbarhet i noen enkelte prosesser, men samtidig peker BDO på at investorer i land som Norge har et sikkerhetsmessig samarbeid med, med høy grad av sannsynlighet vil kunne forutsette at bestemmelsen ikke vil gjøres gjeldende overfor potensielle investeringer. Snarere blir utenlandske investeringer i Norge i praksis trygget av det arbeidet som norske sikkerhetsmyndigheter gjør for å sikre landets selvstendighet og trygghet. I lys av dette kan

det argumenteres for at utenlandske investorer ser på den nye bestemmelsen som positiv og at den bidrar til å gjøre det norske markedet mer attraktivt å investere i.

Departementet vurderer med bakgrunn i dette at forslaget til ny § 5 a om varslingsplikt mv. vil ha beskjedne økonomiske og administrative konsekvenser. Det legges derfor til grunn at aktiviteten som kan forventes som følge av forslag til ny bestemmelse, løses innenfor den enkelte virksomhets eksisterende rammer.

4 Forslag til lovendringer

Departementet foreslår at § 2 skal lyde:

§ 2. Lovens generelle virkeområde

Loven gjelder for forvaltningsorganer. Som forvaltningsorgan regnes i loven ethvert organ for stat eller kommune. Kongen kan i tvilstilfelle bestemme om et organ er å regne som forvaltningsorgan. Kongen kan også bestemme at et forvaltningsorgan helt eller delvis skal være unntatt fra loven når det foreligger særlige grunner for det, og kan da i stedet fastsette særlige regler.

Loven gjelder også for ethvert rettssubjekt som ikke er forvaltningsorgan og som er leverandør av varer eller tjenester til et forvaltningsorgan i forbindelse med en sikkerhetsgradert anskaffelse.

Kongen kan bestemme at loven helt eller delvis også skal gjelde for ethvert annet rettssubjekt, herunder enkeltpersoner, foreninger, stiftelser, selskaper og privat og offentlig næringsvirksomhet,

a. som eier eller på annen måte har kontroll over eller fører tilsyn med skjermingsverdig objekt, eller

b. som av et forvaltningsorgan gis tilgang til sikkerhetsgradert informasjon.

Kongen kan bestemme at § 29 a skal gjelde for 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.

Loven gjelder ikke for Stortinget, Riksrevisjonen, Stortingets ombudsmann for forvaltningen og andre organer for Stortinget. *Bestemmelsene gitt i og i medhold av lovens kapittel 6 om personellsikkerhet gjelder ikke for regjeringens medlemmer.*

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

Departementet foreslår at ny § 5 a skal lyde:

§ 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.

Departementet foreslår at ny § 6 a skal lyde:

§ 6 a *Gebyr*

Kongen kan fastsette nærmere forskrift om gebyr for tjenester som utføres med hjemmel i denne lov. Gebyret må være formålstjenlig, og gebyret skal ikke overstige kostnadene ved ytelsen.

Departementet foreslår at § 9 skal lyde:

§ 9. Nærmere om oppgavene

Nasjonal sikkerhetsmyndighet skal

a. innhente og vurdere informasjon av betydning for gjennomføringen av forebyggende sikkerhetstjeneste,

b. søke internasjonalt samarbeid, herunder med andre lands og organisasjoners tilsvarende tjenester, når dette tjener norske interesser,

c. føre tilsyn med sikkerhetstilstanden i virksomheter, herunder kontrollere at den enkeltes plikter i eller i medhold av loven her overholdes, og eventuelt gi pålegg om forbedringer,

d. bidra til at sikkerhetstiltak utvikles, herunder iverksette forskning og utvikling på områder av betydning for forebyggende sikkerhetstjeneste,

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

f. gi informasjon, råd og veiledning til virksomheter, og

g. for øvrig utføre de oppgaver som fremgår av bestemmelsene i og i medhold av loven her.

Kongen kan gi nærmere bestemmelser om Nasjonal sikkerhetsmyndighets utøvelse av oppgavene.

Departementet foreslår at ny § 10 a skal lyde:

§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.

Departementet foreslår at ny § 13 a skal lyde:

§ *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.

Departementet foreslår at § 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 *autorisasjonssamtale* er avholdt. Nasjonal sikkerhetsmyndighet gir nærmere regler om autorisasjon og om hvem som er autorisasjonsansvarlig.

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 foreslår at § 28 skal lyde:

§ 28. Leverandørklarering

Før en leverandør kan få tilgang til skjermingsverdig informasjon sikkerhetsgradert KONFIDENSIELT eller høyere, eller dersom det av andre grunner anses nødvendig, skal leverandøren ha gyldig leverandørklarering for angitt sikkerhetsgrad. *Kongen fastsetter den generelle gyldighetstid for leverandørklareringer.* Nasjonal sikkerhetsmyndighet er klareringsmyndighet.

Leverandørklarering skal ikke gis dersom det foreligger rimelig tvil om leverandørens sikkerhetsmessige skikkethet. Ved avgjørelse om sikkerhetsmessig skikkethet skal det bare

legges vekt på forhold som er relevante for å vurdere leverandørens evne og vilje til å utøve forebyggende sikkerhetstjeneste etter bestemmelsene i eller i medhold av loven her. I vurderingen skal inngå personkontroll av personer i leverandørens styre og ledelse.

Leverandøren skal gi alle opplysninger som antas å kunne være av betydning for klareringsspørsmålet.

Leverandøren skal uten ugrunnet opphold orientere Nasjonal sikkerhetsmyndighet om endringer i styre eller ledelse, forandringer i eierstrukturen, flytting av lokaliteter og utstyr, åpning av gjeldsforhandling eller begjæring om konkurs og andre forhold som kan ha betydning for leverandørens sikkerhetsmessige skikkethet. Anses slike forhold å representere en sikkerhetsrisiko og risikoen ikke kan elimineres gjennom å utøve forebyggende sikkerhetstjeneste, kan Nasjonal sikkerhetsmyndighet inndra leverandørklareringen. Skjermingsverdig informasjon eller objekt kan ikke overføres til ny eier eller inngå i bobehandling ved gjeldsforhandling eller konkurs, med mindre Nasjonal sikkerhetsmyndighet har samtykket til dette.

For øvrig gjelder reglene i kapittel 6, herunder reglene om begrunnelse og klage, så langt de passer.

Departementet foreslår følgende overskrift i kapittel 7:

Kapittel 7. Sikkerhetsgraderte anskaffelser *og anskaffelser til kritisk infrastruktur*

Departementet foreslår at ny § 29 a skal lyde:

§ 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.