FORSVARSDEPARTEMENTET

HØRINGSNOTAT

FORSLAG TIL FORSKRIFTER TIL NY SIKKERHETSLOV

2. juli 2018

Høringsfrist 1. oktober 2018

Innhold

1 Innledning

Forsvarsdepartementet foreslår tre forskrifter til lov om nasjonal sikkerhet (sikkerhetsloven). Forskriftene regulerer henholdsvis myndighetenes ansvar og roller for forebyggende sikkerhet, virksomhetens arbeid med forebyggende sikkerhet og klarering av personell og leverandører. Departementet arbeider med sikte på at forskriftene fastsettes, og ny sikkerhetslov trer i kraft, fra 1. januar 2019. Departementet bemerker at regelverkets funksjonelle innretning gjør det nødvendig at det utarbeides veiledere av Nasjonal sikkerhetsmyndighet og myndigheter med sektoransvar i de aktuelle sektorene. Regelverket forutsetter også at det etableres gode arenaer for dialog mellom myndighetene og virksomheter som underlegges loven.

I høringsnotatet benyttes «sikkerhetsloven» som betegnelse på lov om nasjonal sikkerhet som enda ikke er trådt i kraft. Der hvor det vises til gjeldende sikkerhetslov vil det fremgå uttrykkelig.

Departementet ber høringsinstansenes være oppmerksom på at det fremgår i merknadene til de enkelte bestemmelsene hvor departementet særlig ønsker høringsinstansenes innspill. Departementet vil i forbindelse med høringen fortsette med lovteknisk gjennomgang av forskriftene, men vil ikke endre det materielle innholdet i bestemmelsene før høringsinnspillene foreligger.

2 Bakgrunn

Lov om nasjonal sikkerhet (sikkerhetsloven) ble vedtatt av Stortinget 6. mars 2018, og i det vesentlige slik den ble fremmet av regjeringen i Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet (sikkerhetsloven)*. Proposisjonen baserte seg på anbefalingen fra det regjeringsoppnevnte sikkerhetsutvalgets utredning som forelå høsten 2016 i rapporten NOU 2016: 19 *Samhandling for sikkerhet.*

2.1 Arbeidsform og involvering

Arbeidet med forskriftene har foregått som et prosjekt med prosjektmedarbeidere fra Forsvarsdepartementet (FD), Justis- og beredskapsdepartementet (JD) og Nasjonal sikkerhetsmyndighet (NSM). Prosjektet har fått første utkast til bestemmelser fra NSM. Prosjektet har også innhentet innspill fra en arbeidsgruppe bestående av Avinor, Direktoratet for forvaltning og IKT, Direktoratet for samfunnssikkerhet og beredskap, Forsvaret, Forsvarsmateriell, Forsvarsbygg, Finanstilsynet, Helsedirektoratet, Helsetilsynet, Kystverket, Legemiddelverket, Luftfartstilsynet, Nasjonal kommunikasjonsmyndighet, Norges Bank, Norges vassdrags- og energidirektorat, Oljedirektoratet, Petroleumstilsynet, Politidirektoratet, Politiets sikkerhetstjeneste, Statens vegvesen, Statens strålevern, Valgdirektoratet og Utenriksdepartementet. Etatene anses å være de mest sentrale myndighetene som har en rolle i arbeidet med sikkerhet og beredskap i de enkelte samfunnssektorene.

Det har vært gjennomført fire møter med arbeidsgruppen der prosjektet har lagt frem forslag til bestemmelser, og deltagerne har kunnet stille spørsmål og diskutere alternative forslag til innretninger. Det har også vært anledning til å gi skriftlige innspill i etterkant. Hvordan innspillene fra etatene i arbeidsgruppen har blitt vurdert, har blitt lagt frem for en referansegruppe bestående av representanter fra Arbeids- og sosialdepartementet (ASD), Finansdepartementet (FIN), Helse- og omsorgsdepartementet (HOD), Kommunal- og moderniseringsdepartementet (KMD), Nærings- og fiskeridepartementet (NFD), Olje- og energidepartementet (OED), Samferdselsdepartementet (SD), Utenriksdepartementet (UD) og Statsministerens kontor (SMK).

Departementene i referansegruppen og etatene i arbeidsgruppen har blitt oppfordret til å involvere private virksomheter og interesseorganisasjoner i sin sektor i arbeidet, og prosjektet har gjennom dette fått verdifulle innspill. Det ble 22. mars 2018 avholdt et informasjonsmøte hvor alle instanser som ble hørt i forbindelse med høringen av NOU 2016:19 var invitert, og hvor det ble åpnet for spørsmål og innspill til arbeidet.

Departementet mener at prosessen har gitt et godt grunnlag for å komme frem til en form og et nivå på bestemmelsene som gjør at forskriftene vil bidra til å bedre det forebyggende sikkerhetsarbeidet i alle samfunnssektorene.

3 Om forslaget

3.1 Virkeområde

Ny sikkerhetslov vil gjelde for alle statlige, fylkeskommunale og kommunale organer. Loven vil også gjelde for leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser. Det vil si anskaffelser der leverandøren, eller personell fra leverandøren, får tilgang til eller tilvirker sikkerhetsgradert informasjon, eller får tilgang til et skjermingsverdig objekt eller infrastruktur.

Loven vil i tillegg gjelde for virksomheter som behandler sikkerhetsgradert informasjon eller som råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for «grunnleggende nasjonale funksjoner». «Grunnleggende nasjonale funksjoner» er tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser, jf. sikkerhetsloven § 1-5 nr. 2. En forutsetning for at sistnevnte virksomheter omfattes av loven er imidlertid at det enkelte departement innenfor sitt ansvarsområdefatter vedtak om at loven skal gjelde for virksomheten, jf. sikkerhetsloven § 1-3.

Departementene skal i tråd med sikkerhetsloven til enhver tid ha oversikt over de virksomhetene som behandler sikkerhetsgradert informasjon, eller som råder over informasjonssystemer, objekter og infrastruktur som har betydning for Norges evne til å ivareta nasjonale sikkerhetsinteresser, jf. Prop. 153 L (2016–2017) kapittel 6. Departementene skal ha denne oversikten uavhengig av samfunnsutviklingen, og uavhengig av hvilke avhengighetsforhold som opprettes eller bortfaller på tvers av sektorene. Loven forutsetter at de enkelte departementene jevnlig oppdaterer oversikten over virksomheter.

Departementene skal identifisere og holde oversikt over «grunnleggende nasjonale funksjoner», jf. sikkerhetsloven § 2-1 bokstav a. Departementene må også identifisere virksomheter av «vesentlig» og «avgjørende» betydning for grunnleggende nasjonale funksjoner, og treffe vedtak om at loven gjelder virksomheter som er av avgjørende betydning for grunnleggende nasjonale funksjoner.

Det pågår et arbeid i departementene med å identifisere hvilke grunnleggende nasjonale funksjoner som opprettholdes i den enkelte sektor. Det arbeides også med å identifisere hvilke virksomheter som er av vesentlig og avgjørende betydning for grunnleggende nasjonale funksjoner. Dette vil være virksomheter som råder over informasjon, informasjonssystemer, infrastruktur og objekt som er av vesentlig eller avgjørende betydning for grunnleggende nasjonale funksjoner. Det vil være særlig viktig å kartlegge hvilke informasjonssystemer, infrastrukturer og objekter som har betydning for virksomheter i flere sektorer. Det tas utgangspunkt i at informasjon, objekter og infrastrukturer som er omfattet av gjeldende sikkerhetslov, i utgangspunktet vil være omfattet av ny sikkerhetslov. Det vil derfor være særlig fokus på å kartlegge hvilke informasjonssystemer, infrastruktur eller objekter som omfattes av den begrensede utvidelsen av lovens virkeområde. Tatt i betraktning de beslutningsmekanismer som følger av lovforslaget, vil det for de virksomheter som ikke allerede er

underlagt vil det kunne gå noe tid etter ikrafttredelse før virksomheten er utpekt. Offentlige myndigheters saksbehandlingskapasitet tilsier også at det vil måtte gjøres en gradvis vurdering av virksomheter og objekter. For disse virksomhetene vil det imidlertid det uansett måtte gis en rimelig frist for implementering av sikringstiltak, jf. kapittel 4.7.

I arbeidet med å kartlegge virkeområde ses det hen til det arbeidet som er gjort forbindelse med kartlegging av samfunnskritiske funksjoner i regi av Direktoratet for samfunnssikkerhet- og beredskap[1]. Slik departementet ser det vil det være stor grad av overlapp mellom de kritiske samfunnsfunksjonene, og grunnleggende nasjonale funksjoner. De grunnleggende nasjonale funksjonene vil være en delmengde av de samfunnskritiske funksjonene, men også omfatte funksjoner som ikke er omfattet av disse. Departementet vil vurdere om arbeidet med KIKS (Kritisk infrastruktur, kritiske samfunnsfunksjoner) og grunnleggende nasjonale funksjoner skal samordnes, slik at bidragene fra departementene i samfunnssikkerhetsarbeidet også kan benyttes inn i og dra vekselvirkninger på arbeidet med å kartlegge de grunnleggende nasjonale funksjonene.

Departementet bemerker at arbeidet med å kartlegge virkeområde er en kontinuerlig prosess, som forutsetter at oversikten over grunnleggende nasjonale funksjoner, og informasjon, informasjonssystemer, objekter og infrastrukturer som er av vesentlig og avgjørende betydning for grunnleggende nasjonale funksjoner, oppdateres jevnlig.

Sikkerhetsmyndigheten kan på eget initiativ fremme forslag overfor et departement om å fatte vedtak etter andre ledd. Dersom departementet ikke fatter vedtak i samsvar med sikkerhetsmyndighetens forslag, kan sikkerhetsmyndigheten bringe saken inn for endelig avgjørelse til det departementet som har overordnet ansvar for forebyggende sikkerhetsarbeid i sivil sektor eller det departementet som har overordnet ansvar for forebyggende sikkerhetsarbeid i forsvarssektoren.

Slik departementet ser det, er det på nåværende tidspunkt ikke nødvendig å forskriftsfeste ytterligere momenter som skal vektlegges i vurderingen av hvilke virksomheter loven skal gjelde for, utover de som allerede fremgår av Prop. 153 L (2016–2017), kapittel 6.4. Departementet ber likevel om høringsinstansenes syn på om det bør fremgå ytterligere momenter i forskriftene, og i så fall hvilke. Departementet ser at en slik momentliste vil kunne bidra til å klargjøre virkeområde til loven, og vil vurdere om det er behov for at det tas inn ytterligere momenter i forskriftene i forbindelse med høringsrunden.

3.2 Inndeling i forskrifter

Inndelingen i tre forskrifter skal gjøre det enklere for pliktsubjektene etter loven å finne sine plikter i forbindelse med det forebyggende sikkerhetsarbeidet.Hensikten er at virksomhetene i størst mulig grad skal finne sine plikter i en enkelt forskrift, i motsetning til slik det er i dag, der virksomhetene må forholde seg til opptil fem forskrifter for å finne frem til sine plikter.

Departementet foreslår på denne bakgrunn følgende tre forskrifter:

- forskrift om myndighetenes roller og ansvar for nasjonal sikkerhet (myndighetsforskriften)
- forskrift om klarering av leverandører og personell (klareringsforskriften)

[1] Samfunnets kritiske funksjoner, versjon 1.0, 2016, DSB.

- forskrift om virksomhetens arbeid med forebyggende sikkerhet (virksomhetsforskriften).

Myndighetsforskriften retter seg mot departementer, NSM og myndigheter med tilsynsansvar etter loven. Klareringsforskriften retter seg mot klareringsmyndighetene som Sivil klareringsmyndighet og FSA og andre virksomheter som klarer personell. Virksomhetsforskriften vil gjelde alle virksomheter som er underlagt loven. Krav som gjelder for alle virksomhetene som underlegges loven er plassert innledningsvis i forskriften. De krav som gjelder avhengig av graderingsnivået på den informasjonen eller klassifiseringsnivået på det objekt eller infrastruktur virksomheten råder over, er plassert fortløpende i den samme forskriften. De kravene som gjelder for alle virksomhetene som underlegges loven skal sikre et forsvarlig sikkerhetsnivå for informasjon gradert BEGRENSET, for ugradert skjermingsverdig informasjon og skjermingsverdige informasjonssystemer som ikke behandler sikkerhetsgradert informasjon høyere enn BEGRENSET.

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

3.3 Hva er nytt i forslaget

En vesentlig endring fra gjeldende forskrifter er at forslaget ikke er delt inn i de enkelte fagområdene som tidligere var omtalt som sikkerhetsadministrasjon, personellsikkerhet, sikkerhetsgraderte anskaffelser, objektsikkerhet og informasjonssikkerhet, der sistnevnte innbefattet dokumentsikkerhet, informasjonssystemsikkerhet, fysisk sikring og administrativ kryptosikkerhet. Inndelingen av bestemmelser i fagområder var hensiktsmessig, da forskriftene tidligere stilte detaljerte nominelle krav til sikkerhetstiltakene. Den som utøvde de enkelte fagområdene kunne da lese ut av forskriften hvilke tiltak som skulle gjennomføres innen det respektive fagområdet. Det har etter departementets vurdering ledet til at virksomheter har jobbet for lite med sammenhenger på tvers av fagområdene i det forebyggende sikkerhetsarbeidet, og ikke i tilstrekkelig grad balansert tiltak med et helhetlig, tverrfaglig perspektiv på sikring. Eksempelvis ved at det er lagt for mye vekt på fysisk sikring, uten at det er gjennomført et tilsvarende sikringsnivå for den elektroniske sikringen av IKT-systemene.

Forskriftene stiller krav til at forsvarlig sikkerhetsnivå skal oppnås gjennom en kombinasjon av menneskelige, elektroniske, fysiske og organisatoriske tiltak. Med menneskelige tiltak menes ikke bare klarering og autorisasjon, men også tiltak som opplæring og bevisstgjøring av medarbeidere, og hvordan sikkerheten ivaretas både under ansettelse og avslutning av arbeidsforhold. Med elektroniske tiltak menes også digitale/logiske tiltak. Dette kan være elektroniske alarm- og overvåkningssystemer av lokaler, men også tiltak gjort i IKT-systemer som brannmurer, passord og kryptering. Fysiske og elektroniske tiltak blir i enkelte sammenhenger omtalt under samlebetegnelsen teknologiske tiltak. Organisatoriske tiltak vil i all hovedsak dekkes av kravene til styringssystem for sikkerhet i virksomhetsforskriften. Kravene vil være en videreføring av de tidligere bestemmelsene om sikkerhetsadministrasjon, men i en oppdatert form som bedre samsvarer med andre bestemmelser i forskriftene og som harmonerer bedre med anerkjente standarder om styringssystemer (kalt «ledelsessystemer» i norske standarder).

Det er nytt at regelverket ikke bare omfatter informasjon og informasjonssystemer som er skjermingsverdige av hensyn til å beskytte informasjonens konfidensialitet, men at det også åpnes for at informasjon og informasjonssystemer vil kunne være skjermingsverdige ut i fra i hvilken grad tap av integritet og tilgjengelighet vil kunne påvirke de grunnleggende nasjonale funksjonene. Det vil derfor sannsynligvis bli flere informasjonssystemer som ikke behandler sikkerhetsgradert informasjon, men som på bakgrunn av hvilken funksjon de har, vil bli omfattet av regelverket.

Forskriftene åpner for at personer som bare skal gis tilgang til skjermingsverdige objekter og infrastruktur kan gis adgangsklarering eller utvidet adgangsklarering, se kapittel 4.4.3. Videre er det gjort endringer når det gjelder hvem som fører kontroll med leverandører for sikkerhetsgraderte anskaffelser.

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

Departementet bemerker at det i løpet av høringsrunden vil gjøre en lovteknisk gjennomgang av forskriftene, og vurdere om det skal gjøres endringer i bestemmelsene. Departementet legger imidlertid til grunn at det ikke vil bli gjort materielle endringer, før eventuelle innspill fra høringsinstansene.

3.4 Funksjonelle krav

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

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

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

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

4 Omtale av enkelte særskilte temaer

4.1 Objekt- og infrastruktursikkerhet

4.1.1 Innledning

Bestemmelsene om objektsikkerhet er i hovedsak en videreføring av eksisterende regelverk, men med noen endringer av kravene til beskyttelse. Bestemmelsene regulerer, som den nye loven, også infrastruktur, for tydeliggjøre og ivareta sikkerhet på et område som er av økende betydning for nasjonal sikkerhet. Departementet erkjenner imidlertid at infrastrukturer ofte er svært komplekse, og kjennetegnes av lange og uoversiktlige verdikjeder, som kan gjøre det vanskeligere å sikre en infrastruktur enn et objekt.

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

4.1.2 Arbeidet med identifisering, utpeking, klassifisering og sikring

Utpeking og klassifisering av skjermingsverdige objekter og infrastrukturer forutsetter at departementet først har identifisert grunnleggende nasjonale funksjoner, se kapittel 3.1 om virkeområdet. For å bestemme hvilke deler av objektene og infrastrukturene som skal klassifiseres og til hvilket nivå, må det vurderes hvilket tap man kan akseptere, som hvor mye av funksjonen det gjelder (kapasitet), for hvor lenge (varighet), og i hvilken grad innholdet i funksjonens leveranser forringes (kvalitet), før det får konsekvenser av avgjørende betydning for grunnleggende nasjonale funksjoner. Departementene skal ikke klassifisere større deler av infrastrukturene eller objektene, eller for en høyere klassifiseringsgrad, enn nødvendig. Loven legger opp til at et objekt eller deler av en infrastruktur kan få en høyere klassifiseringsgrad enn andre objekter eller infrastrukturen for øvrig.

Etter departementets syn vil det være nødvendig at det enkelte departement, i samarbeid med myndighetene i sektoren og de virksomhetene som råder over objektet eller infrastrukturen, bruker scenarier for å vurdere ulike typer konsekvenser av bortfall av funksjonen, og hvilke av disse konsekvensene som vil ha betydning for grunnleggende nasjonale funksjoner. Vurderingen skal basere seg på virksomhetenes vurdering av skadefølger ved bortfall av objektet eller infrastrukturens funksjon. Departementene bør minst årlig, og dersom det skjer vesentlige endringer i forholdene som ligger til grunn for klassifiseringen, oppdatere identifiseringen, utpekingen og klassifiseringen.

Der nye infrastrukturer og objekter utpekes eller klassifiseringsnivået endres, må departementene gi en frist for når virksomheten skal oppfylle kravene til et forsvarlig sikkerhetsnivå. Fristen må være

rimelig, ut i fra hvilke sikringstiltak som må iverksettes for at sikkerheten skal bli forsvarlig, se kapittel4.7. Før virksomheten har oppnådd et forsvarlig sikkerhetsnivå, bør det stilles krav om at det iverksettes kompenserende midlertidige tiltak slik at risiko så langt mulig reduseres tilstrekkelig, uten at dette blir uforholdsmessig krevende for virksomheten.

4.1.3 Departementenes ansvar

Basert på identifiseringen av grunnleggende nasjonale funksjoner, se nærmere kapittel 3.1, skal departementene utpeke, klassifisere og holde oversikt over skjermingsverdige objekter og infrastruktur, jf. § 7-1.

Objekter og infrastrukturer skal klassifiseres ut ifra hvor alvorlige skadefølger bortfall av funksjonen kan få for grunnleggende nasjonale funksjoner, jf. sikkerhetsloven § 7-2. I vurderingen skal momentene i myndighetsforskriften § 1 legges til grunn. Det vil særlig være av betydning i hvor stor grad grunnleggende nasjonale funksjoner er avhengige av objektet eller infrastrukturen, og hvorvidt bortfall av funksjonen vil ha betydning også for funksjoner i andre sektorer.

4.1.4 Virksomhetens ansvar

Skadevurdering

Grunnlaget for departementets vurdering vil være den informasjon departementet eller NSM har etter utpekingen, sammenholdt med virksomhetens skadevurdering, jf. forskrift om virksomhetens arbeid med forebyggende sikkerhet § 52. Bestemmelsen pålegger virksomheten å vurdere i hvilken grad bortfall eller reduksjon av et objekt eller en infrastruktur vil påvirke en eller flere grunnleggende nasjonale funksjoner.

Departementet står imidlertid fritt til å vurdere skadepotensialet som et annet enn det som følger av virksomhetens skadevurdering. Departementet kan ha bedre oversikt over hvordan de ulike virksomhetene i sektoren bidrar i helheten, enn det den enkelte virksomhet selv har, og må søke å harmonisere klassifiseringsnivået på tvers av ulike virksomheter i sektoren.

Forsvarlig sikkerhetsnivå

Virksomheten skal håndtere risikoen på en slik måte at den oppnår et forsvarlig sikkerhetsnivå for sine skjermingsverdige objekter og infrastruktur, jf. virksomhetsforskriften § 53, jf. § 12. Utgangspunktet for vurderingen vil være objektets eller infrastrukturens klassifiseringsgrad, og det er i forskriften gitt føringer for hva som regnes for et forsvarlig sikkerhetsnivå på de forskjellige klassifiseringsnivåene.

Virksomheten skal ved behov etablere nødvendige grunnsikringstiltak og planlegge påbygnings- og skadebegrensningstiltak, jf. virksomhetsforskriften § 13. Virksomheten skal også ha en plan for hvordan sikkerhetstilstanden til virksomheten skal gjenopprettes etter sikkerhetstruende virksomhet. Kravet til planene vil avhenge av hvilke trusler objektet eller infrastrukturen er utsatt for, jf. virksomhetsforskriften § 13 syvende ledd.

Hvilke sikkerhetstiltak som velges innenfor de ulike tiltakskategoriene vil være avhengig av objektets eller infrastrukturens klassifiseringsnivå, hvor lenge det er akseptabelt at objektet eller infrastrukturen svikter, muligheten til å gjenopprette eller erstatte funksjonalitet, og hvilke sårbarheter objektet eller infrastrukturen har, jf. virksomhetsforskriften §§ 11, 12 og 13 sammenholdt med §§ 52 og 53. Dette må vurderes opp mot hvilke trusler og scenarioer som anses relevante for objektet eller infrastrukturen. Basert på denne vurderingen må virksomheten etablere

de sikkerhets tiltakene som må til for å oppnå et forsvarlig sikkerhetsnivå for det aktuelle objektet eller infrastrukturen.

Denne vurderingen vil bidra til å avklare hva som er «vesentlig» funksjon, jf. virksomhetsforskriften § 53 første ledd bokstav a, og hvilke tiltak som må på plass for å begrense tap av denne funksjonen. Det understrekes at det er funksjonen, ikke objektet eller infrastrukturen som sådan, som skal unngås tapt eller overtatt. Det vil si at virksomheten kan komme frem til at tilstrekkelig redundans oppfyller kravet til at funksjonstap begrenses, eller at alternative løsninger som for eksempel tilstrekkelig nødstrømsaggregat som kompensasjon for strømtilførsel, i tilstrekkelig grad vil kunne avverge funksjonstap.

Trusselaktørene vil være interesserte i forskjellige typer objekter og infrastruktur, og vil være villig til å sette inn ulik mengde ressurser for å ødelegge disse, avhengig av hvilken stat eller organisasjon, aktøren kommer fra. Virksomheten må derfor vurdere hvilke kategorier trusselaktører virksomheten er utsatt for, og hvordan disse kategoriene av trusselaktører normalt vil gjennomføre sikkerhetstruende virksomhet. Departementet antar at det i de fleste tilfeller vil være relevant for virksomheten å etablere ulike scenarioer for denne kartleggingen. Scenarioene bør være basert på trussel- og risikovurderinger fra EOS-tjenestene, for å klargjøre hvilke kategorier trusselaktører sikringstiltakene skal være egnet til å beskytte mot, og hvilke tidsregnskap de forskjellige trusselaktørene skal vurderes mot.

4.2 NSMs tilsyns- og påleggskompetanse overfor sektormyndigheter med tilsynsansvar

NSM kan ilegge pålegg, tvangsmulkt og overtredelsesgebyr for å sikre etterlevelse av sikkerhetsloven med forskrifter, og for at forhold som er i strid med regelverket rettes. Dette gjelder overfor både departementer, sektormyndigheter som har fått tilsynsansvar og øvrige virksomheter sikkerhetsloven gjelder for. I påleggsbestemmelsen i loven § 3-6 er det eksplisitt fastsatt at NSM kan gi pålegg til andre tilsynsmyndigheter om å utføre tilsyn etter loven. Virkemiddelbestemmelsene i loven § 11-2 om tvangsmulkt og § 11-3 om overtredelsesgebyr fastsetter at disse virkemidlene kan anvendes ved overtredelse av pålegg gitt etter § 3-6.

I lovproposisjonen kapittel 8.4.7 er følgende inntatt:

> *Departementet mener likevel at sikkerhetsmyndigheten må ha denne sanksjonsmuligheten [pålegg] som virkemiddel, for å sikre at det gjennomføres tilsyn i samsvar med krav fastsatt i eller i medhold av loven i den aktuelle sektoren. Departementet legger til grunn at påleggskompetansen overfor myndigheter med tilsynsansvar bare vil bli benyttet der sektortilsynenes oppfølging av sikkerheten i sektoren er uforsvarlig. Dette kan for eksempel være hvis det ikke gjennomføres tilsyn eller at tilsynene ikke er gjennomført i tråd med de fastsatte kriteriene i eller i medhold av loven.*

NSM har således kompetanse til å gi pålegg og anvende tvangsmulkt og overtredelsesgebyr overfor tilsynsmyndigheter som ikke gjennomfører sine tilsynsoppgaver på en tilfredsstillende måte. I sektorer hvor det utpekes sektormyndigheter med tilsynsansvar, vil ikke NSM, med mindre det følger av internasjonale forpliktelser eller er tvingende nødvendig jf. sikkerhetsloven § 3-1 andre ledd andre punktum, kunne føre tilsyn med virksomheter som omfattes av sektortilsynets tilsynsansvar. Dette nødvendiggjør at NSM har de nødvendige virkemidler som sikrer at sektormyndigheters tilsyn med etterlevelse av sikkerhetsloven blir adekvat gjennomført i sektorer, jf. loven § 2-2 andre ledd bokstav a.

Påleggskompetansen vil bare bli benyttet der sektortilsynenes oppfølging av sikkerheten i sektoren er uforsvarlig. Departementet ser ikke for seg at anvendelse av disse reaksjonsformene vil være de

primære verktøyene som benyttes overfor de andre tilsynsmyndighetene. NSM vil legge til rette for at NSM og sektormyndigheter med tilsynsansvar vil kunne løse eventuelle utfordringer gjennom samarbeid. Avtale om samarbeid mellom NSM og sektormyndigheter med tilsynsansvar skal ha som formål å bidra til godt samarbeid og sikre tilstrekkelig grad av enhetlig, helhetlig, samordnet og tverrsektoriell tilnærming til forebyggende sikkerhet. Det vil også bli benyttet andre virkemidler før NSM eventuelt gir pålegg til et sektortilsyn, blant annet dialog mellom NSM og sektortilsynet, eller ved å løfte eventuelle uenigheter mellom NSM og sektortilsynet til departementene.

Omfanget av det tilsyn som sektortilsynet er forventet å ha ansvar for å gjennomføre, og med hvilken støtte det kan forvente fra NSM i gjennomføringen, vil bli regulert gjennom samarbeidsavtaler og arenaer for opplæring og informasjonsutveksling. Samarbeidsavtalen blir et viktig verktøy for hvordan disse oppgavene skal fordeles mellom NSM og sektormyndigheten. Formålet med fordelingen er å unngå dobbeltarbeid og unødvendig dublering av kompetansemiljøer. For eksempel vil NSM kunne bistå i planlegging og forberedelse av tilsyn med fagkompetanse på områder som sektormyndigheten ikke har, og NSM kan også delta på tilsyn som fageksperter eller gjøre revisjoner på særlige fagområder. Dette vil gjøre at på de områdene hvor det ikke er hensiktsmessig at man bygger opp egen kompetanse i sektortilsynene, kan sektortilsynene dra veksler på fagmiljøene i NSM. NSMs opplæring av sektormyndighetene i fag og tilsynsmetodikk og hvilke samarbeidsarenaer og kontaktflate det skal være vil også være områder det er aktuelt å etablere forutsigbarhet om. Det kan også avtales at oppgaver delegeres fra NSM til sektormyndigheten, for eksempel knyttet til godkjenning av informasjonssystemer, der det er hensiktsmessig. Videre vil det være aktuelt å avtale hvordan NSM best kan tilrettelegge for at sektormyndighetene får tilgang på relevant informasjon om trusler og sårbarheter slik at disse kan legges til grunn i sektormyndighetenes tilsyns- og rådgivningsoppgaver.

Det er viktig å understreke at der hvor det er blitt utpekt sektormyndighet med tilsynsansvar er det sektormyndigheten som har ansvaret for alle slike tilsyn i sektoren. Det vil si at de må være ansvarlige for å planlegge med tilstrekkelig tilsyn og at det gjennomføres tilsyn etter en vurdering av risiko i sektoren. Om NSM bidrar inn i forberedelse eller gjennomføring av tilsyn vil det være under ledelse av sektormyndigheten. Dette for at det ikke skal skapes tvil, hverken ovenfor tilsynsobjektene, myndighetene eller departementene hvor ansvaret ligger.

Departementet kan gjennom instruks gjøre nødvendige tilpasninger i særlige tilfeller. Eksempelvis gjelder det tilsyn med Etterretningstjenesten, hvor det i dag foreligger en departementsfastsatt instruks om systemrettet tilsyn med begrensninger og prosedyrer som ivaretar Etterretningstjenestens særlige skjermingsbehov. Det legges til grunn at Etterretningstjenesten ikke vil bli underlagt tilsyn fra sektormyndighet i forsvarssektoren, og at NSM fortsatt vil føre tilsyn med e-tjenesten i medhold av gjeldende instruks.

4.3 Utveksling av trusselvurderinger og annen sikkerhetsinformasjon

Overgangen fra gjeldende sikkerhetslov til ny sikkerhetslov, med endring fra nominelle til funksjonelle bestemmelser, innebærer at den enkelte virksomhet selv må ta større ansvar for egen forebyggende sikkerhet, herunder vurdering av risiko og valg av sikkerhetstiltak, jf. ny sikkerhetslov § 4-2 og § 4-3. For å kunne foreta en reell vurdering av risiko er imidlertid virksomheten avhengig av tilgang til trusselvurderinger og andre opplysninger av betydning for det forebyggende sikkerhetsarbeidet. For å sikre dette er NSM gitt i oppgave å legge til rette for tilgang til slik informasjon, jf. sikkerhetsloven § 2-3 første ledd.

Nasjonale trussel- og risikovurderinger utarbeides i hovedsak av Politiets sikkerhetstjeneste (PST), Etterretningstjenesten, NSM og Direktoratet for samfunnssikkerhet og beredskap (DSB). Det er

presisert i Prop. 153 L (2016–2017) kapittel 19.2 at informasjonsutvekslingen må skje innenfor rammene av lovbestemt taushetsplikt og innenfor rammene av den enkelte aktørs lovmessige adgang til å til dele slik informasjon. Det innebærer at det fortsatt vil være slik at ikke all informasjon kan deles med alle.

Av lovproposisjonen, og § 2-3 andre ledd, fremgår det videre at mye av tilretteleggingsansvaret kan ivaretas gjennom etablering av nødvendige arenaer for informasjons- og erfaringsutveksling, eller som felles arrangementer med øvrige relevante myndigheter. Sektormyndigheter som er gitt tilsynsansvar vil ha en sentral rolle innen sektorene de har et ansvar for, og det må legges til rette for at de får den nødvendige informasjonen tilpasset sin sektor til at de kan ivareta sine oppgaver.

Departementet ser at ulike virksomheter og sektorer vil ha ulik grad av informasjonsbehov, avhengig av hvilke verdier virksomheten forvalter og i hvilken grad virksomheten vurderes å være et interessant mål for trusselaktører. For de fleste virksomhetene vil det trolig være tilstrekkelig med de ugraderte trussel- og risikovurderingene som er tilgjengelig i dag, blant annet fra Etterretningstjenesten, PST og NSM. Enkelte virksomheter vil imidlertid ha et informasjonsbehov ut over dette.

Hvilke arenaer som etableres eller utvikles vil være avhengig av virksomhetenes informasjonsbehov, hvilken informasjon EOS-tjenestene har tilgjengelig, i hvilken grad og på hvilket nivå informasjonen kan deles, og i hvilken grad virksomhetene kan håndtere sikkerhetsgradert informasjon. Dette vil kunne endre seg over tid og tilsier at det er behov for en dynamisk tilnærming.

Spesifikk trussel- og sikkerhetsinformasjon vil kunne gis direkte til den enkelte virksomhet eller til flere virksomheter samtidig – avhengig av informasjonens relevans for den enkelte, og avhengig av informasjonens graderingsnivå. Noen virksomheter vil motta slik informasjon direkte fra NSM, mens andre vil få det via sektormyndigheten i den aktuelle sektoren. Trussel- og sikkerhetsinformasjon vil være en del av grunnlaget for sektormyndighetenes råd om risikovurdering og -håndtering, og tilsvarende grunnlag for tilsyn.

Innen den enkelte sektor vil det trolig være flere virksomheter med likt eller tilsvarende informasjonsbehov, og det kan være hensiktsmessig at det etableres eller videreutvikles fellesarenaer innen den enkelte sektor. En differensiering av ulike fellesarenaer og målgrupper vil kunne bidra til informasjonsdeling og erfaringsutveksling på riktig nivå, og samtidig ivareta behov for skjerming av informasjon.

Departementet har foreløpig kommet til at loven og forarbeidene gir tilstrekkelige føringer for hvordan NSMs plikt til å tilrettelegge for informasjonsutveksling skal løses, og har derfor ikke funnet behov for å presisere dette ytterligere i forskrift. Departementet ser klart behovet for at det etableres helhetlige rammeverk for risikovurderinger, og for utveksling av trusselvurderinger, men ser som nevnt ikke behov for ytterligere føringer for dette i forskriftene.

Forsvarsdepartementet og Justis- og beredskapsdepartementet vil gjennom etatsstyringen kunne følge opp hvordan NSM ivaretar denne oppgaven.

4.4 Adgangsklarering

4.4.1 Innledning

Etter ny sikkerhetslov § 8-3 kan det enkelte departement fatte vedtak om krav til adgangsklarering for adgang til hele eller deler av skjermingsverdige objekter eller infrastruktur innen sitt

ansvarsområde. Hva adgangsklarering skal være, og hva som skal være forskjellen mellom adgangsklarering og sikkerhetsklarering skal fastsettes i forskrift.

4.4.2 Virksomhetenes behov

Departementet har vurdert mange forslag til hva adgangsklarering skal være. Innspill til forskriftsarbeidet har tydeliggjort at ulike virksomheter og sektorer har ulike behov og preferanser knyttet til adgangsklarering. Forskjellene omhandler blant annet hva slags type trusler som adgangsklareringen skal beskytte mot, og hvilke registre personkontrollen skal basere seg på. For noen virksomheter er det terrortrusselen som er fremtredende, for andre er det fremmedstatlig sabotasje og etterretning. De ulike trusselscenarioene legger føringer for både hvilke kilder som er relevante ved personkontrollen, og for hvilke vurderingskriterier som er hensiktsmessige. Dette påvirker kompleksiteten i saksgrunnlaget og forventet saksbehandlingstid. Departementet har etter dette funnet det hensiktsmessig med to typer adgangsklarering: «Adgangsklarering» og «utvidet adgangsklarering».

4.4.3 Adgangsklarering og utvidet adgangsklarering

Adgangsklarering er mindre omfattende enn utvidet adgangsklarering og skal i hovedsak være egnet til å forebygge mot terror. Ved vanlig adgangsklarering vil personkontrollen omfatte færre kilder, egenopplysninger og samlet sett være færre vurderingskriterier enn for utvidet adgangsklarering. Det legges imidlertid opp til at det også ved vanlig adgangsklarering vil hentes inn opplysninger om andre kriminelle forhold, for å vurdere risikoen for skadeverk med annet motiv enn terror. Departementet forutsetter at det vil legges til rette for rask og effektiv saksbehandling.

Ved utvidet adgangsklarering vil det hentes inn informasjon fra flere kilder i personkontrollen, være et større omfang av egenopplysninger og vurderingskriterier i vurdering. Formålet med utvidet adgangsklarering er at kontrollen, i tillegg til terror, skal forebygge mot fremmedstatlig sabotasje og etterretning. For utvidet adgangsklarering vil tilknytning til andre stater være et relevant vurderingskriterium. Lojalitet til Norge og norske sikkerhetsinteresser, samt sårbarhet for press fra andre staters etterretningstjenester, vil i større grad være gjenstand for den kontroll som skal gjennomføres ved utvidet adgangsklarering.

Både adgangsklarering og utvidet adgangsklarering kan benyttes uavhengig av klassifiseringsgraden til et skjermingsverdig objekt eller infrastruktur. Departementene må ta stilling til om adgangsklarering eller utvidet adgangsklarering er egnede sikkerhetstiltak for det konkrete objektet eller infrastrukturen. Departementet understreker at kravet om forholdsmessighet er et styrende prinsipp for hvorvidt det velges adgangsklarering eller utvidet adgangsklarering.

En adgangsklarering vil være gyldig for tilgang til alle skjermingsverdige objekter og infrastrukturer der det er fattet vedtak om krav om adgangsklarering. Tilsvarende gjelder for utvidet adgangsklarering, men en utvidet adgangsklarering vil også gi tilgang der det bare kreves adgangsklarering.

4.4.4 Forholdet til sikkerhetsklarering

Personell som er sikkerhetsklarert, uavhengig av nivå, er også klarert for adgang til skjermingsverdige objekter eller infrastrukturer der det er fattet vedtak om adgangsklarering eller utvidet adgangsklarering. Forslaget innebærer at nivået på sikkerhetsklarering for tilgang til de høyest klassifiserte skjermingsverdige objektene senkes fra HEMMELIG til KONFIDENSIELT. Det vises til gjeldende forskrift om objektsikkerhet § 3-6 andre ledd om at dersom det kreves sikkerhetsklarering for adgang til skjermingsverdig objekt klassifisert MEGET KRITISK kreves sikkerhetsklarering for

HEMMELIG eller høyere. Departementet vurderer at en slik endring er forsvarlig. Det vises til at kildegrunnlaget og vurderingskriteriene som inngår i sikkerhetsklarering for KONFIDENSIELT omfatter alt det som også inngår ved adgangsklarering og utvidet adgangsklarering.

Departementet legger til grunn at nærstående har mindre betydning for sikkerhetsmessig skikkethet for klarering for adgang til skjermingsverdig objekt eller infrastruktur, enn for tilgang til gradert informasjon. Det vises til at personkontrollen av nærstående er begrunnet i at sikkerhetsgradert informasjon lett gjøres tilgjengelig for nærstående dersom den som er klarert ikke overholder taushetsplikten (f.eks. informasjon som gis muntlig eller tas med hjem i dokumentform). Terskelen for at en nærstående skal kunne skade et objekt eller en infrastruktur er derimot høyere, fordi den nærstående da først må skaffe seg adgang til objektet eller infrastrukturen. Departementet foreslår derfor at ved nærstående kan kontrolleres, men da bare ved utvidet adgangsklarering der det foreligger opplysninger som gir grunn til å anta at nærstående kan påvirke personens pålitelighet, lojalitet eller dømmekraft. Det innebærer at terskelen for å kontrollere nærstående ved utvidet adgangsklarering vil tilsvare terskelen for å kontrollere nærstående ved sikkerhetsklarering for KONFIDENSIELT. Det vises samtidig til at det i loven gis hjemmel til å gjennomføre personkontroll av nærstående i særlige tilfeller, uavhengig av klareringsnivå for både sikkerhetsklarering og adgangsklarering.

4.5 Klarering av utenlandske statsborgere

4.5.1 Innledning

Det kan i noen tilfeller være behov for å klarere utenlandske statsborgere, blant annet der en person har kompetanse som ikke er tilgjengelig i Norge, som en virksomhet er helt avhengig av for at skjermingsverdig objekt eller infrastruktur skal kunne fungere.

Utenlandsk statsborgere med manglende tilknytning til Norge kan ikke forventes å ha samme lojalitet til norske sikkerhetsinteresser som en norsk statsborger. En klarering vil derfor innebære økt risiko for at informasjon benyttes på en måte som er i strid med norske sikkerhetsinteresser. Norske myndigheter vil heller ikke alltid ha tilgang til personkontrollopplysninger som grunnlag for klareringen. Graden av tilknytning til Norge, hjemlandet og hjemlandets sikkerhetsmessige betydning er derfor sentrale vurderingsmomenter i avgjørelsen av om en utenlandsk statsborger skal gis klarering.

Slik departementet ser det gir ny lov § 8-7, sammenholdt med gjeldende forskrifter, tilstrekkelig fleksibilitet i disse tilfellene. Departementet erkjenner imidlertid at praktisering av gjeldende rett har vært for snever. Departementet foreslår derfor en forsiktig oppmykning av praksis, ved at handlingsrommet i § 8-7 benyttes i større grad, slik at det i større grad vil være mulig å klarere utenlandske statsborgere, også de uten tilknytning til Norge. Departementet legger opp til at gjeldende forskriftsbestemmelser videreføres, men at oppfølgingen og praktiseringen i større grad vil være i tråd med lovens formål. Det foreslås imidlertid en dispensasjonsadgang i særskilte tilfeller hvor det ikke er grunnlag for å klarere personen, eller det som følge av sikkerhetsmessig samarbeid ikke er behov for eller gjelder særlige regler for klareringen, se kapittel 4.5.4 nedenfor. Det gjelder også særlig regler for personell som inngår i en sikkerhetsgradert anskaffelse, se kapittel 4.6.1 nedenfor.

Det følger av ny sikkerhetslov § 8-7 at

> *En person som har utenlandsk statsborgerskap, kan etter en konkret helhetsvurdering få klarering, dersom det ikke er rimelig grunn til å tvile på at personen er sikkerhetsmessig skikket. I*

> *tillegg til forholdene i § 8-4 skal det i vurderingen legges vekt på hjemlandets sikkerhetsmessige betydning, personens tilknytning til hjemlandet og tilknytningen til Norge.*
>
> *Ved klarering av en person med utenlandsk statsborgerskap, skal det vurderes særskilt om bruk av vilkår, som for eksempel stillingsklarering, kan være et risikoreduserende tiltak.*

Bestemmelsen er en videreføring av gjeldende lov § 22, jf. Prop. 153 L (2016–2017) kapittel 19.8 s. 187. Når det gjelder behovet for å kunne klarere utenlandske statsborgere uten tilknytning til Norge følger det av kapittel 12.5.2 på s. 132:

> *Det kan likevel være et særskilt behov for å klarere en utenlandsk statsborger uten tilknytning til Norge, eksempelvis dersom personen besitter særlig kompetanse som er av betydning for nasjonale sikkerhetsinteresser eller andre spesifikke nasjonale interesser. Ordlyden i departementets forslag gir tilstrekkelig handlingsrom til å kunne klarere personer som ikke har tilknytning til Norge, der særskilte grunner gjør dette nødvendig. Departementet mener imidlertid i likhet med NSM at klarering av personer uten noen form for tilknytning til Norge bare bør skje unntaksvis.*

Departementet mener at § 8-7 gir tilstrekkelige føringer for den helhetsvurderingen klareringsmyndigheten skal gjøre, og har derfor ikke sett det som nødvendig at det gis ytterligere bestemmelser om selve vurderingen i forskrift, utover §§ 14 og 16 i klareringsforskriften, om personhistorikk og tilknytning. Departementet ber imidlertid om høringsinstansenes innspill på om det er behov for en bestemmelse som konkretiserer vurderingstemaene ytterligere, og vil vurdere en slik bestemmelse i lys av høringsinnspillene.

4.5.2 Tilknytning

I vurdering av graden av tilknytning vil det særlig være personens juridiske og personlige tilknytning til Norge, og til hjemlandet, som vil være relevant. Det avgjørende vil være hvorvidt det foreligger forhold som en annen stat kan bruke for å påvirke en persons pålitelighet, lojalitet og dømmekraft, f.eks. eiendom, gjeld eller familieforhold i hjemlandet. Dette gjør at det vil være forskjell på de tilfellene der personen kun skal gjøre et oppdrag i Norge, kontra et langvarig ansettelsesforhold som innebærer at personen ikke lenger har økonomiske interesser, eller eiendom eller personlig tilknytningsforhold i hjemstaten.

Det er ikke et absolutt vilkår, verken i gjeldende sikkerhetslov eller i den nye loven, at utenlandske personer må ha tilknytning til Norge for å kunne bli sikkerhetsklarert. Graden av tilknytning til Norge må imidlertid vurderes mot hjemlandets sikkerhetsmessige betydning.

4.5.3 Hjemlandets sikkerhetsmessige betydning

De aller fleste stater driver etterretning mot andre land, mot forskjellige mål, med forskjellige metoder. I vurderingen av hjemlandets sikkerhetsmessige betydning er det derfor sentralt å vurdere hvor stor etterretningstrusselen er fra det aktuelle landet, mot hvilke mål, og med hvilke metoder. Denne vurdering må holdes opp mot hva den utenlandske statsborgeren skal klareres for. Videre har Norge et sikkerhetssamarbeid med mange nasjoner, men dette varierer noe i art og omfang. Arten og omfanget av sikkerhetssamarbeidet sier noe om graden av tillitt til at personell fra den aktuelle staten vil behandle norsk sikkerhetsgradert informasjon i tråd med norske sikkerhetsinteresser. Sikkerhetssamarbeidet vil dessuten kunne gjøre det mulig å innhente personkontrollopplysninger fra personens hjemland, eller legge personens klarering fra hjemlandet til grunn som tilstrekkelige personkontrollopplysninger. Det vil f.eks. være større grunn til å klarere en person med tilknytning til en stat som gjennom NATO-medlemskap regnes som en nær alliert av Norge, enn en person med tilknytning til en stat som ikke er en nær alliert av Norge, og som norske myndigheter er klar over at har høy etterretningsaktivitet mot mål i Norge.

Departementet mener det bør foreligge et sikkerhetssamarbeid av et visst omfang for at den utenlandske statsborgeren skal kunne gis klarering, dersom personen har ingen eller liten grad av tilknytning til Norge. Uten sikkerhetssamarbeid med personens hjemland vil ikke norske myndigheter ha tilgang til registeropplysninger om personen fra hjemlandet, og Norge vil heller ikke kunne legge til grunn en klarering fra hjemlandet, i forbindelse med personkontroll, jf. loven § 8-5 og forskriften § 14. For de tilfellene hvor det ikke foreligger et sikkerhetssamarbeid med hjemlandet mener departementet at det må stilles krav om tilknytning til Norge før det kan gis klarering.

Departementet mener videre at klarering av utenlandske statsborgere med liten eller ingen tilknytning til Norge kun bør skje unntaksvis, i de tilfeller der hensynet til nasjonale sikkerhetsinteresser eller andre spesifikke nasjonale interesser veier tyngre enn risikoen ved å gi tilgang til norsk sikkerhetsgradert informasjon. Hvor mye tilknytning som kreves og hvilket behov som er tilstrekkelig, vil måtte avklares gjennom praktiseringen av bestemmelsen.

Departementet vil bemerke at selv om det foreligger et sikkerhetssamarbeid med hjemlandet, må personen som skal klareres i Norge likevel oppfylle de øvrige kravene til sikkerhetsklarering, jf. § 8-4 fjerde ledd.

4.5.4 Unntak fra krav om sikkerhetsklarering i særskilte tilfeller

Departementet finner grunn til å bemerke at det ikke vil være nødvendig å klarere utenlandsk personell der personellet inngår i et stat-til-stat sikkerhetssamarbeid, f.eks. knyttet til en militærøvelse, et konkret prosjekt eller i møter i forbindelse med NATO-samarbeidet og personellet har klarering på tilsvarende nivå fra hjemlandet. I disse tilfellene vil det følge av avtale mellom Norge og staten hvilken informasjon, informasjonssystem, infrastruktur eller objekt det skal gis tilgang til, og hvilke personer som skal gis tilgangen. For at det skal være mulig å følge opp denne type avtale, ser departementet behovet for en bestemmelse som gir mulighet til å gjøre unntak fra kravet om klarering og autorisasjon av utenlandske statsborgere.

Det vil heller ikke være nødvendig å klarere personell som inngår i en sikkerhetsgradert anskaffelse, og sikkerhetssamarbeidet gjør at klareringen fra personens hjemland kan legges til grunn for tilgang til norsk sikkerhetsgradert informasjon som det skal gis tilgang til gjennom anskaffelsen. Det aktuelle sikkerhetssamarbeidet gjør det også mulig å be sikkerhetsmyndighetene i hjemlandet til personen om å klarere vedkommende, se kapittel 4.6.3.

Departementet ser også at det i særskilte tilfeller vil kunne oppstå behov for å gi norsk sikkerhetsgradert informasjon til personer som ikke vil kunne få klarering gjennom den klareringsprosessen som er beskrevet over. Dette vil eksempelvis kunne være tilfelle for personer som kommer fra et land Norge ikke har sikkerhetssamarbeid med og det ikke foreligger tilstrekkelig tilknytning til Norge, men der funksjonaliteten til et sikkerhetsgradert informasjonssystem eller skjermingsverdig infrastruktur eller objekt, er helt avhengig av den aktuelle kompetansen, og det vil være uforholdsmessig byrdefullt å få kompetanse fra et land vi har sikkerhetssamarbeid med.

Departementet foreslår etter dette en unntaksbestemmelse i myndighetsforskriften § 11, som gir sikkerhetsmyndigheten mulighet til å gjøre unntak fra kravet til klarering og til at klareringsmyndigheten skal samtykke før autorisasjon av utenlandske statsborgere til BEGRENSET. En forutsetning for å benytte bestemmelsene er at risikoen forbundet med tilgangen veies opp av behovet for å gi tilgang. Risikoen ved å gi tilgang vil kunne variere ut i fra etterretningsaktivitet fra det aktuelle landet, det sikkerhetspolitiske samarbeidet med staten og hva personellet gis tilgang til. Det er, som nevnt, også en forutsetning at funksjonaliteten til den skjermingsverdige verdien blir

skadelidende dersom kompetansen ikke gjøres tilgjengelig, og det vil være uforholdsmessig byrdefullt å få kompetanse fra ett land vi har sikkerhetssamarbeid med.

I førstnevnte tilfeller, hvor Norge har et stat-til-stat samarbeid, forutsetter departementet at risikoen forbundet med tilgangen er veid mot behovet for å gi tilgang, og at risikoen er akseptert av Norge gjennom sikkerhetssamarbeidet med hjemstaten.

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

4.6 Krav til sikkerhet i anskaffelser

En anskaffelse til en skjermingsverdig verdi vil kunne føre til økt risiko for sikkerhetstruende virksomhet mot verdien, ved at leverandører får tilgang til eller leverer komponenter til verdien. Det er også en risiko forbundet ved å la funksjonen til en skjermingsverdig verdi være avhengig av en leverandør, ettersom leverandøren ved f.eks. økonomiske problemer eller påvirkning fra andre stater ikke lenger vil kunne levere tjenesten funksjonen er avhengig av. Forskriftene stiller derfor krav til at virksomheten må opprettholde et forsvarlig sikkerhetsnivå ved anskaffelser til den skjermingsverdige verdien.

4.6.1 Sikkerhetsgraderte anskaffelser

En sikkerhetsgradert anskaffelse er en anskaffelse som innebærer at leverandøren av varen eller tjenesten kan få tilgang til eller tilvirker sikkerhetsgradert informasjon, eller får tilgang til et skjermingsverdig objekt eller infrastruktur, jf. sikkerhetsloven § 9-1. Formålet med reglene for sikkerhetsgraderte anskaffelser er å sikre at leverandøren eller personell fra leverandøren oppfyller de samme krav til sikkerhet som gjelder for den virksomheten eller personell hos virksomheten som gjennomfører anskaffelsen. Kravene til leverandøren vil derfor avhenge av hva leverandøren får tilgang til, og hvordan denne tilgangen gis. Skal personell fra leverandøren få tilgang til sikkerhetsgradert informasjon eller skjermingsverdig infrastruktur eller objekt hos virksomheten, må kravene til autorisasjon og klarering som gjelder for den aktuelle tilgangen være oppfylt. Skal leverandøren behandle eller oppbevare sikkerhetsgradert informasjon, eller gis tilgang til skjermingsverdig infrastruktur eller objekt, i eller fra egne lokaler, må leverandøren oppfylle de krav loven og forskriftene stiller til virksomheter med tilsvarende mulighet til å råde over samme informasjon, objektet eller infrastruktur. Departementet bemerker at også underleverandører med samme tilgang vil måtte oppfylle kravene i sikkerhetsloven og forskrifter.

4.6.2 Forholdet til regelverket om offentlig anskaffelser

For offentlige oppdragsgivere, og enkelte andre virksomheter i forsyningssektorene, vil reglene om sikkerhetsgraderte anskaffelser komme i tillegg til reglene som gjelder for offentlige anskaffelser, jf. lov om offentlige anskaffelser (anskaffelsesloven) LOV 2016-06-17-73 med tilhørende forskrifter. Det innebærer at en offentlig oppdragsgiver i anbudsprosessen også må vurdere om og i hvilken grad leverandøren skal ha tilgang til gradert informasjon eller skjermingsverdig objekt eller infrastruktur, og ta hensyn til dette i anskaffelsesprosessen. Det kan f.eks. innebære at det må stilles som krav i konkurransegrunnlaget at leverandøren må være i stand til å behandle sikkerhetsgradert informasjon i sine lokaler. Det kan også innebære at leverandøren og/eller personell hos leverandøren må kunne

autoriseres og eventuelt klareres for det graderingsnivået som er på informasjonen eller for adgang til objekt og infrastruktur for å kunne delta i konkurransen.

Det kan også være at hele eller deler av anskaffelsen må unntas regelverket for anskaffelser av hensyn til nasjonale sikkerhetsinteresser, jf. f.eks. EØS-avtalen artikkel 123. Departementet bemerker at sikkerhetsloven og forskrifter bare stiller krav til behandling av informasjon, og beskyttelse av informasjonssystemer, objekter eller infrastruktur som anses å være av sentral betydning for nasjonale sikkerhetsinteresser.

Departementet bemerker at sikkerhetsavtalen senest må foreligge før leverandøren får tilgang til informasjon, infrastruktur eller objekt. For at en offentlige oppdragsgiver skal unngå å måtte heve kontrakten med leverandør, bør oppdragsgiveren sørge for at sikkerhetsavtalen, jf. § 9-2 i loven, er inngått før eller senest som en del av den kontrakten som inngås med leverandøren. Det samme gjelder for autorisasjon eller klarering av personellet som gis tilgang som en del av anskaffelsen.

Departementet vil samarbeide med NFD om utarbeidelse av veiledningsmateriell som vil gjøre det enklere å se sammenhengen mellom de ulike regelsettene.

4.6.3 Leverandører med lokaler utenfor norsk jurisdiksjon og utenlandske leverandører

Skal en leverandøren oppbevare eller behandle sikkerhetsgradert informasjon, eller gis tilgang til skjermingsverdig infrastruktur eller objekt fra egne lokaler utenfor norsk jurisdiksjon må det foreligge et sikkerhetssamarbeid med den staten som har jurisdiksjon der lokalene ligger. Det samme gjelder der leverandøren driver sin virksomhet fra en annen stats jurisdiksjon. Bakgrunnen for kravet er at norske myndigheter i disse tilfellene ikke vil ha tilgang til de opplysninger som inngår i en leverandørklarering, jf. virksomhetsforskriften § 74, og norske myndigheter vil ikke kunne føre kontroll med at leverandøren oppfyller kravene i sikkerhetsloven og forskriftene. Ettersom sikkerhetssamarbeidene variere i art og omfang har departementet sett det som hensiktsmessig å stille krav om at sikkerhetsavtalen mellom Norge og den andre staten som minimum må regulerer hvem av statene som skal kontrollere leverandøren.

Dersom utenlandsk personell fra en leverandør som driver sin virksomhet utenfor norsk jurisdiksjon skal få tilgang til skjermingsverdig informasjon, informasjonssystem, infrastruktur og objekt hos oppdragsgiveren, må personellet oppfylle kravene til autorisasjon og klarering som gjelder for den aktuelle tilgangen. Dersom personellet er klarert i et land Norge har et sikkerhetssamarbeid med, vil det som regel følge av avtalen mellom Norge og det aktuelle landet, at klarering fra det aktuelle landet kan legges til grunn i Norge for tilgang til norsk sikkerhetsgradert informasjon i forbindelse med den aktuelle anskaffelsen. Der personellet ikke har klarering kan NSM be sikkerhetsmyndigheten i det aktuelle landet om å klarere personellet for den aktuelle anskaffelsen eller selv klarere personellet basert på registeropplysninger fra det aktuelle landet. Slik departementet ser det gir i §§ 9-2 og 9-3 i ny lov, kapittel 5 i klareringsforskriften og kapittel 10 i virksomhetsforskriften tilstrekkelig hjemmel til å følge opp de ulike avtalene om sikkerhetssamarbeid og sikkerhetsgraderte anskaffelser. NSM kan også klarere personellet med hjemmel i § 8-7, beskrevet i kapittel 3 over. Når det gjelder behovet for kompetanse som Norge ikke har tilstrekkelig tilgang på nasjonalt, antar departementet at denne som utgangspunkt kan anskaffes som en sikkerhetsgradert anskaffelse fra land Norge har et sikkerhetssamarbeid med.

4.6.4 Varslingsplikt

Varslingsplikten etter sikkerhetsloven § 9-4 gjelder anskaffelser til skjermingsverdig informasjonssystem, objekt eller infrastruktur hvor det er en ikke ubetydelig risiko for at verdien kan bli rammet av eller brukt til sikkerhetstruende virksomhet gjennom anskaffelsen.

Oppdragsgiver må vurdere hvorvidt anskaffelsen elektronisk eller fysisk gir leverandøren mulighet til å gjennomføre sikkerhetstruende virksomhet. En slik risiko vil blant annet kunne oppstå i anskaffelser som medfører at en leverandør gis tilgang til oppdragsgivers skjermingsverdige informasjonssystemer, eller der hvor anskaffelsen dreier seg om kjøp av kritiske komponenter til de skjermingsverdige verdiene. I sistnevnte tilfelle kan det oppstå en ikke ubetydelig risiko for at det er lagt inn en bakdør i komponentene som vil kunne gi tilgang til systemet, objektet eller infrastrukturen på et senere tidspunkt. Det bør også vurderes om det er mulig gjennom anskaffelsen å forstyrre skjermingsverdige informasjonssystemer, objekter eller infrastrukturer gjennom å stoppe leveranser av drift og vedlikehold eller leveranser av deler eller forbruksmateriell.

Varslingsplikten inntrer ikke dersom virksomheten håndterer risikoen på en slik måte at den blir ubetydelig. Virksomheten kan f.eks. gjennomføre anskaffelsen ved bruk av klarert personell og eventuelt også en klarert leverandør, jf. kapittel 4, eller ha oppsyn med personell som skal levere tjenester slik at man sikrer seg at de ikke gjennom oppdraget kan utføre skade, f.eks. gjennom logging av aktivitet i et informasjonssystem.

Virksomheten kan også sørge for kontroll av komponenter gjennomført av tiltrodd tredjepart for å oppdage om det f.eks. er lagt inn en bakdør i en komponent. Virksomheten kan også benytte forskjellige leverandører fra forskjellige land for å sikre at ikke en enkelt trusselaktør alene kan påføre skade.

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

Det vises for øvrig til Prop. 97 L (2015–2016) kapittel 13.4.5 på side 75-77 for nærmere omtale av varslingsplikten og plikten til å vurdere risiko etter § 9-4.

4.6.5 Klareringsmyndighet for leverandørklarering

Etter gjeldende regelverk er det NSM som er klareringsmyndighet for leverandørklareringer. Ny sikkerhetsloven legger opp til at det skal være én klareringsmyndighet for leverandørklarering, jf. § 9-3 sjette ledd. Antallet saker om leverandørklarering, som ifølge NSM er mellom 15 og 20 hvert år, tilsier at det ikke er behov for mer enn én leverandørklareringsmyndighet. Muligheten for å beholde og utvikle god fagkompetanse, og for effektive løsninger, blir også bedre med én klareringsmyndighet, enn om myndigheten blir spredt på flere.

Dersom NSM fortsatt skal ha leverandørklareringsmyndighet, vil NSM ikke kunne føre uavhengig tilsyn med denne myndighetsutøvelsen. Videre må departementet da fortsatt være klageinstans på vedtak om leverandørklarering, i stedet for NSM som ved klarering av personer. Det er riktignok

svært få klager på vedtak om leverandørklarering. Når bestemmelsene om sikkerhetsgraderte anskaffelser med ny lov og forskrift utvides til å gjelde langt flere virksomheter, og det samtidig blir gitt flere og tydeligere saksbehandlingsregler, må det imidlertid forventes flere klager enn det som har vært så langt.

Leverandørene er private rettssubjekter og sivile virksomheter. Det er derfor nærliggende å legge klareringsmyndigheten til et sivilt forvaltningsorgan. At klarering av personer inngår som en del av leverandørklareringer, tilsier at Sivil klareringsmyndighet peker seg ut som en mulig kandidat. Klareringsarbeidet kan da samles i ett og samme organ. Det kan gi gode faglige og administrative synergier, og det vil være enkelt for pliktsubjektene som da bare behøver å forholde seg til ett klareringsorgan.

Det er ikke praktisk mulig å endre hvilket forvaltningsorgan leverandørklareringsmyndigheten skal legges til allerede innen 1. januar 2019, som er tidspunktet for planlagt fastsettelse av nye forskrifter. Behovet for en nærmere vurdering av de økonomiske og administrative konsekvensene av en slik endring, og tid til å gjennomføre eventuelle endringer, tilsier at NSM i første omgang fortsatt bør være leverandørklareringsmyndighet. Departementet ber om høringsinstansenes syn på hvem som bør være klareringsmyndighet for leverandørklarering.

4.6.6 Ansvar for kontroll av leverandørens oppfyllelse av sikkerhetskrav i fm. leverandørklarering

En leverandørklarering er en form for tredjepartskontroll med en leverandør. Hensikten med tredjepartskontroller i forhold til andre typer kontroller, er at den som foretar kontrollen og fatter eventuelle avgjørelser er mest mulig uavhengig av den vedtaket gjelder.

I sikkerhetsgraderte anskaffelser vil oppdragsgiver stå i et visst avhengighetsforhold til leverandøren, i den forstand at oppdragsgivers primære interesse ligger i at anskaffelsen gjennomføres. Det kan lett tenkes tilfeller der leverandørens manglende oppfyllelse av sikkerhetskravene burde få konsekvenser for leverandørklareringen, men der en tilbakekalling av leverandørklareringen vil komme i konflikt med oppdragsgivers interesse i at leveransene ikke uteblir. En slik interessekonflikt kan være egnet til å påvirke oppdragsgivers vurdering av leverandørens oppfyllelse av sikkerhetskravene eller hvordan dette rapporteres til leverandørklareringsmyndigheten.

Mange av leverandørene vil levere til flere oppdragsgivere, som alle er omfattet av loven. Det vil være uheldig om flere oppdragsgivere skal utføre nærmest parallelle kontroller av samme leverandør. I dag er dette løst med at NSM utpeker én av oppdragsgiverne som «sikkerhetsmessig ansvarlig» (kontrollansvarlig) for leverandørens oppfyllelse av sikkerhetskravene i forhold til alle leverandørens oppdragsgivere. Med ny lov vil oppdragsgiver kunne være private rettssubjekter, noe de ikke kan etter gjeldende lov. Dersom en privat eier av f.eks. skjermingsverdig infrastruktur skal føre kontroll på vegne av andre private eiere av lignende infrastruktur i samme sektor, vil det kunne gi tilgang til andre oppdragsgiveres informasjon som disse av konkurransehensyn ønsker å beskytte mot innsyn fra den som foretar kontrollen. Dette kan medføre situasjoner som ikke lar seg forene med behovet for å ivareta forretningshemmeligheter.

På grunnlag av nevnte forhold foreslår departementet at ansvaret for kontrollene av om leverandørene oppfyller sikkerhetskravene i sikkerhetsloven med forskrifter, legges til klareringsmyndigheten for leverandørklarering. Hvordan en slik kontroll skal utøves vil avhenge av en vurdering av risiko. Det kan være å innhente dokumentasjon fra virksomheten for å vurdere om de etterlever kravene til styringssystem for sikkerhet, stedlig revisjon av deres styringssystem og at de etterlever dette eller inspeksjoner av at sikkerhetstiltak er i henhold til regelverket.

4.7 Ikrafttredelse

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

Departementene skal fatte enkeltvedtak om hvilke virksomheter loven skal gjelde for, jf. sikkerhetsloven § 1-3. Virksomhetene vil da ha behov for tid til å tilpasse seg kravene i lov og forskrifter. Hvor mye tid virksomheten trenger for å tilpasse seg vil imidlertid være individuelt. Det er derfor naturlig at det som del av vedtaket om at sikkerhetsloven skal gjelde for virksomheten også fastsettes hvor mye tid virksomheten får til å tilpasse seg kravene til sikring av den informasjon, informasjonssystem, infrastruktur eller objekt virksomheten råder over. Departementet vurderer hvorvidt det er nødvendig med en bestemmelse som fastsetter kriterier som skal vektlegges når fristen for oppfyllelse skal settes. Disse kriteriene vil blant annet kunne være behov for sikkerhetsfagligkompetanse i virksomheten, hva gjenstår før virksomheten har et forsvarlig sikkerhetsnivå, kostnader forbundet med å implementere sikkerhetstiltak, herunder f.eks. plassering av et eventuelt objekt, risikoen virksomheten er utsatt for og graderings eller klassifiseringsnivået til informasjonen, infrastrukturen eller objektet.

Det samme gjelder når departementene utpeker og klassifiserer skjermingsverdige objekter og infrastrukturer. Da bør også her gis en rimelig frist for å oppfylle sikkerhetstiltak basert på en vurdering av hva som er forsvarlig og mulig å oppnå. I tilfeller hvor man ser at det er nødvendig kan det gis en relativt kort frist for å iverksette kompenserende tiltak som styrket vakthold og overvåkning inntil virksomheten har fått på plass permanente tiltak.

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

4.8 Overgangsregler

Departementet ser behov for overgangsregler som sikrer at objekter som er klassifisert og informasjon som er gradert beholder sitt gradering- eller klassifiseringsnivå regelverk til det gjøres en ny vurdering etter nytt regelverk. Det samme gjelder informasjonssystemer, kryptosystemer, rom, oppbevaringsenheter og destruksjonsmåter som er godkjent etter dagens regelverk. Det legges også opp til at personell som er klarert etter gjeldende regelverk beholder sin klarering inntil disse løper ut eller forutsetningene for at klareringen er gitt ikke lenger er til stede. En eventuell klage på klareringsavgjørelse avgjøres etter reglene på vedtakstidspunktet.

Departementet legger til grunn at sikkerhetstiltak som oppfyller kravene i gjeldende sikkerhetslov, som utgangspunkt også vil oppfylle kravene i nytt regelverk. Endringer kan tenkes som følge av revurderinger av klassifiserings eller graderingsnivået på den infrastruktur eller objekt virksomheten råder over, eller der nye objekter eller infrastruktur blir utpekt som følge av den begrensede utvidelsen av lovens virkeområde. I begge disse tilfellene vil det måtte gis en ny frist for implementering av sikkerhetstiltak, jf. avsnittet om ikrafttredelse. Videre vil virksomhetens risikovurderinger etter nytt regelverk, og de revisjoner som virksomheten skal foreta av sikkerhetstilstanden i virksomheten, kunne føre til at det etterhvert må iverksette nye sikkerhetstiltak.

5 Økonomiske og administrative konsekvenser

5.1 Bakgrunn

Formålet med ny regulering av forebyggende nasjonalt sikkerhetsarbeid er ifølge lovens § 1-1 å bidra til å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser. Videre skal reguleringen bidra til å forebygge, avdekke og motvirke sikkerhetstruende virksomhet. Reguleringen skal også bidra til at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn. Ny sikkerhetslov medfører en begrenset utvidelse av gjeldende lovs virkeområde, slik at både nye virksomheter og større deler av allerede underlagte virksomheters infrastruktur og systemer kan bli underlagt regelverkets krav til forebyggende sikkerhetsarbeid.

I Prop. 153 L (2016–2017) ble det lagt til grunn at det ikke er mulig å angi konkret de økonomiske konsekvensene av lovforslaget før loven har trådt i kraft og alle departementer har vurdert hvilke virksomheter som skal omfattes av loven. Det ble også poengtert at kravene virksomhetene må forholde seg til ikke vil være endelig fastlagt før forskriftsarbeidet er gjennomført, virkeområde klarlagt og virksomhetene har fått tid til å innrette seg etter regelverket.

5.2 Vurdering av utgifter

Utvidelsen av sikkerhetslovens virkeområde vil få økonomiske og administrative konsekvenser for virksomhetene som underlegges loven, myndigheter med sektoransvar, klareringsmyndighetene, departementene, NSM og PST. Utgiftene vil være knyttet til blant annet sikkerhetstiltak, administrative og organisatoriske oppgaver, IKT-utstyr, personell og kompetanse. Regelverket legger opp til en større aktivitetsplikt for både departementer og virksomheter, gjennom krav til å dokumentere, rapportere, kartlegge, analysere og gjennomføre risikovurderinger. Det vil også kunne bli utgifter knyttet til bytte av leverandører eller underleverandører, som følge av krav om at leverandøren eller leverandørens personell må klareres. Departementet legger imidlertid til grunn at for virksomheter som er omfattet av gjeldende regelverk, og som oppfyller gjeldende krav til sikring av informasjon, informasjonssystem, objekt og infrastruktur, vil nytt regelverk i utgangspunktet ikke medføre økte utgifter til arbeidet med forebyggende sikkerhet i virksomheten.

For de virksomheter som ikke er underlagt dagens regelverk, vil utgiftene knyttet til nytt regelverk kunne bli betydelige. Størrelsen på utgiftene vil imidlertid avhenge av hvor stort endringsbehovet for virksomhetene er som følge av nytt regelverk, og det må særlig ses hen til det sikringsnivået som allerede er etablert i virksomheten, gjerne som følge av krav i gjeldende sektorregelverk. F.eks. vil allerede etablerte teknologiske barrierer og rutiner for behandling av sensitiv informasjon kunne oppfylle krav i ny sikkerhetslov og forskrifter.

I de sektorene som har stor utenlandsk kontaktflate og som er særlig avhengig av utenlandsk ekspertise og kompetanse, som for eksempel kraft, petroleum, samferdsel og finanssektoren, vil krav til klarering ved anskaffelser kunne gi relativt høye økonomiske og administrative konsekvenser for virksomhetene. De faktiske utgiftene avhenger blant annet av i hvilken grad det er behov for å dele sikkerhetsgradert informasjon, gi tilgang til skjermingsverdig infrastruktur eller objekt, sikkerhets- eller adgangsklarere norsk og/eller utenlandsk personell, samt i hvilken grad virksomheten er avhengig av utenlandske leveranser.

De funksjonelle kravene, og begrensningen i lovens § 4-3 om at kostnadene ved sikkerhetstiltak skal stå i et rimelig forhold til det som kan oppnås med tiltaket, gjør at virksomhetene ikke skal ha flere eller mer omfattende sikkerhetstiltak enn det som er nødvendig for å oppnå et forsvarlig sikkerhetsnivå. Det legges opp til at sektormyndighetene, på bakgrunn av kunnskap om egen sektor

og basert på rådgivning fra NSM, skal legge føringer for hva som er et forsvarlig sikkerhetsnivå. Den enkelte virksomhet må imidlertid selv vurdere hvilke konkrete sikkerhetstiltak som er nødvendige for å oppnå og opprettholde et forsvarlig sikkerhetsnivå, og til å vurdere hva som er akseptabel restrisiko holdt opp mot utgiften ved tiltakene.

5.2.1 Innspill fra øvrige departementer

I forbindelse med forskriftsarbeidet har Forsvarsdepartementet innhentet innspill fra de departementene som forventes å bli mest berørt av den nye reguleringen. Flere av disse har hentet informasjon fra sine underliggende virksomheter. Det er mottatt svar fra Arbeids- og sosialdepartementet (Petroleumstilsynet, bransjeorganisasjonen Norsk olje og gass), Finansdepartementet (Finanstilsynet, Norges Bank), Helse- og omsorgsdepartementet, Kommunal- og moderniseringsdepartementet, Olje- og energidepartementet, Samferdselsdepartementet, Utenriksdepartementet og Justis- og beredskapsdepartementet. Tilbakemeldingene viser stor grad av variasjon i estimerte utgifter, og samtlige understreker usikkerhet knyttet til tallmaterialet.

Ett av usikkerhetsmomentene er i hvor stor grad lovens virkeområde vil bli utvidet, siden departementene ennå ikke har identifisert grunnleggende nasjonale funksjoner, og virksomheter som har vesentlig og avgjørende betydning for disse funksjonene. Andre usikkerhetsmomenter knytter seg til utgiftene for den enkelte virksomhet og i hvilken grad myndigheter med sektoransvar skal gjennomføres tilsyn etter ny lov.

5.2.2 Variasjon og usikkerhet knyttet til estimatene

Basert på innspillene legger Forsvarsdepartementet til grunn at utgiftsnivået for den enkelte virksomhet vil variere ut i fra i hvilken grad en virksomheten skal håndtere lav- eller høygradert informasjon, hvilke fasiliteter som kreves for at denne informasjonen skal håndteres forsvarlig, om virksomheten har skjermingsverdige objekter eller infrastruktur, og hvilket klassifiseringsnivå disse har eller vil få. Det stilles lavere krav til sikring for virksomheter som kun skal håndtere informasjon gradert BEGRENSET enn til virksomheter som skal håndtere høyere gradert informasjon. Hvilke sikkerhetstiltak som er nødvendige vil også avhenge av hvilke trusselaktører og metoder virksomheten er utsatt for. Hva som er et forsvarlig sikkerhetsnivå for virksomheten må vurderes ut ifra graderings- eller klassifiseringsnivået på informasjon, objektet eller infrastrukturen, holdt opp mot hvor stor risiko virksomheten er utsatt for, og hvilke grad av restrisiko som bør aksepteres.

5.2.3 Besparelser og samfunnsøkonomisk nytte

Få virksomheter har vektlagt potensiale for besparelser som følge av å bli underlagt sikkerhetsloven. Slik departementet ser det, vil et bedre forebyggende sikkerhetsarbeid i virksomhetene kunne spare samfunnet for store uforutsette kostnader. Identifisering av grunnleggende nasjonale funksjoner, og kartlegging av avhengigheter på tvers av samfunnssektorene, forventes å gi bedre oversikt over sårbarheter og sikkerhetsarbeidet i den enkelte sektor. Bedre oversikt av avhengigheter kan bidra til mer målrettede sikkerhetstiltak. Videre vil felles rammeverk kunne gi muligheter for besparelser ved at det etableres enhetlige risikovurderinger og rapporteringssystemer i forvaltningen.

Prop. 153 L (2016–2017) legger opp til at det skal benyttes kost-effektive løsninger for å sikre utpekte verdier. Dette understrekes i ny sikkerhetslov § 4-3 andre ledd som fastsetter at kostnadene ved et sikkerhetstiltak skal stå i et rimelig forhold til det som kan oppnås ved tiltaket. Videre er det først og fremst virksomhetenes egne vurderinger av risiko som skal legges til grunn for de sikkerhetstiltakene som implementeres.

Departementet vil bemerke at behovet for ny sikkerhetslov er grundig utredet. Formålet med loven og tilhørende forskrifter er å styrke arbeidet med forebyggende sikkerhet på tvers av samfunnssektorene. Regelverket skal gi bedre oversikt over hvilke informasjonssystemer, objekter og infrastruktur som er av sentral betydning for nasjonal sikkerhet, hvilke trusler og sårbarheter disse er utsatt for, og hvilke sikkerhetstiltak som er nødvendige for at disse skal være forsvarlig sikret. Departementet vil understreke at konsekvensene av manglende sikkerhet, herunder manglende oversikt over hvilke virksomheter Norge er avhengig av for å sikre nasjonale sikkerhetsinteresser, vil kunne bli betydelige. Departementet viser eksempelvis til den pågående Helse Sør-Øst saken, hvor en fremmedstatlig aktør fikk tilgang til store deler av IKT systemene til Helse Sør-Øst. Saken har påført det norske samfunnet betydelige utgifter i forbindelse med kartlegging av skadene og gjenoppretting av funksjonen til systemene. Det er samtidig usikkert i hvilket omfang informasjon har blitt kjent for uvedkommende. Det er verdt å merke seg at skadene kunne blitt vesentlig større om forholdet ikke hadde blitt avdekket, tatt i betraktning den tilgang den fremmedstatlige aktøren hadde til systemene.

Departementet viser også til «WannaCry»-angrepet mot det britiske helseforetaket NHS i september 2017, hvor man fem måneder senere ikke hadde full oversikt over hvor mye angrepet kostet selskapet. Departementet viser også til «NotPetya»-saken, og angrepene mot farmasiselskapet Merck og shippingselskapet Maersk, som anslås å ha kostet hvert av selskapene opp under 300 millioner dollar.

5.2.4 Konkretisering av utgifter

Det vil variere fra sektor til sektor hvor mange virksomheter som underlegges sikkerhetsloven, og i hvilken grad disse virksomhetene får særskilte utgifter. Virksomhetene som underlegges loven vil få administrative utgifter, og utgifter i forbindelse med etablering og drift av sikkerhetstiltak.

Fra finanssektoren opplyses det at det er noen funksjoner som har så høy grad av kritikalitet at de kvalifiserer for å være skjermingsverdige objekter, men som ikke er underlagt gjeldende sikkerhetslov. Noen av disse er allerede svært godt fysisk og logisk sikret også i konteksten av nasjonal sikkerhet, og det antas derfor at det ikke vil være forbundet med høye utgifter om disse underlegges ny sikkerhetslov. Andre funksjoner i finanssektoren anses i dag som godt sikret, men antas likevel å måtte gjennomføre betydelige oppgraderinger som følge av ny sikkerhetslov. Dette kan f.eks. være tilfelle dersom store systemer i store foretak må sikres vesentlig annerledes enn i dag. Det samme gjør seg gjeldende i andre sektorer som opplyser at kostnadene ved innføring av sikkerhetslovens krav kan bli svært store.

Eksempelvis er det i finanssektoren anslått administrative utgifter i spennet mellom 0,5 til 2,5 millioner kroner pr. virksomhet i etableringsfasen, avhengig av i hvilken grad virksomheten skal ha graderte informasjonssystemer og kryptorom, og ca. 0,5 millioner kroner i årlige driftsutgifter pr. virksomhet i forbindelse med bl.a. identifisering og oppfølging av skjermingsverdige informasjonssystemer er det antatt etableringskostnader på 0,45 millioner kroner, med tilhørende årlige driftskostnader på 0,2 millioner kroner.

Samferdselssektoren har oppgitt et anslag for flertallet av nye virksomheters administrative utgifter i etableringsfasen vil være på ca. 2–3 millioner kroner, og 2–3 millioner kroner i årlige økte utgifter pr. virksomhet. SD anslår videre at totale etableringskostnader i sektoren vil ligge på mellom 550 og 900 millioner kroner, mens totale årlige driftskostnader er anslått til 90–150 millioner kroner. Anslagene er basert på at det vil være mellom 20-30 nye virksomheter som faller inn under ny sikkerhetslov, og en økning på mellom fem og 10 nye skjermingsverdige fysiske objekter i sektoren. Kostnadene knyttet til sikring av logiske objekter inngår også i anslagene.

Departementet vil imidlertid understreke at estimatene over er usikre, basert på tidlige utkast av forskriftene. Slik departementet ser det vil kostnadene også kunne bli vesentlig mindre, avhengig av hvilke sikkerhetstiltak som er etablert, og hvordan virksomheten velger å oppnå et forsvarlig sikkerhetsnivå.

JD anslår at nytt regelverk vil kunne medføre et investeringsbehov i justissektoren, avhengig av hvilke krav som til slutt stilles til virksomhetene. PST har anslått økt ressursbehov i forbindelse med oppfølging av virksomhetene som underlegges loven.

I forsvarssektoren, med unntak av NSM, er det som angitt i Prop. 153 L (2016–2017) særlig krav om beskyttelse av informasjonssystemer som er skjermingsverdige, men ugraderte, som vil medføre økte utgifter. For NSM antas det at sikkerhetsloven og de nye forskriftene får konsekvenser for ansvarsområde og virksomheten til NSM. Det samlede økonomiske merbehovet NSM vurderes imidlertid å være i tråd med estimatene angitt i Prop. 153 L (2016–2017).

Statens utgifter til implementering av forskriftene skal i utgangspunktet dekkes innenfor berørte departementers gjeldende budsjettrammer.

6 Merknader til forskrift om myndighetenes roller og ansvar for nasjonal sikkerhet (myndighetsforskriften)

Forskrift om ansvar og myndighet for nasjonal sikkerhet retter seg først og fremst mot departementene, sikkerhetsmyndigheten og myndigheter som fører tilsyn etter sikkerhetsloven med forskrifter. Det er de overordnede roller, ansvar og oppgaver disse myndighetene har etter sikkerhetsloven, som forskriften skal regulere. De samme myndighetene har, i kraft av myndighetsrollen, likevel enkelte roller, ansvar og oppgaver som enten direkte eller indirekte følger av bestemmelser i andre kapitler og i andre forskrifter til sikkerhetsloven. Dette er gjerne roller, ansvar og oppgaver som er mer spesifikt knyttet til bestemte forhold, som f.eks. myndighetsforskriften § 8 fjerde ledd siste punktum og forskrift om klareringsforskriften § 13 siste punktum hvor det fremgår at ved eventuell uenighet mellom NSM og PST om bruk av opplysninger, skal saken avgjøres av Justis- og beredskapsdepartementet. Departementene, sikkerhetsmyndigheten og tilsynsmyndighetene er for øvrig underlagt bestemmelser i sikkerhetsloven med forskrifter på lik linje med andre virksomheter som eier eller råder over skjermingsverdig informasjon, objekter mv.

Departementet vil vurderer hvorvidt følgende bestemmelser skal fremgå av en egen instruks for departementene og etatene, og hvorvidt noen av bestemmelsene skal flyttes til virksomhets, eller klareringsforskriften.

6.1 Til kapittel 1 Departementenes rolle og oppgaver

6.1.1 Til § 1 Klassifisering av skjermingsverdige objekter og infrastruktur

I forslaget til § 1 første ledd bokstav a og b er det angitt kriterier som departementene eller NSM skal legge vekt på ved klassifisering av skjermingsverdige objekter og infrastruktur. Bestemmelsen må ses i sammenheng med de kriteriene som skal vektlegges for virksomhetenes skadevurdering etter forslaget til virksomhetsforskriften § 52 første ledd bokstav a til e.

Ettersom formålet er å komme frem til hvilken betydning objektet eller infrastrukturen har for grunnleggende nasjonale funksjoner, har departementet valgt å ta utgangspunkt i den metodiske tilnærmingen i KIKS-modellen for vurdering av samfunnskritiske funksjoner. Det har blitt gjort enkelte tilpasninger for å tilpasse modellen til sikkerhetsloven, for å ta høyde for at de grunnleggende nasjonale funksjonene er en delmengde av de samfunnskritiske funksjonene, men og så vil være funksjoner utover de samfunnskritiske funksjonene.

Som etter KIKS-modellen må det i vurderingen av avhengigheten til et objekt eller infrastruktur, også inngå en vurdering av om det finnes gode alternativer til objektet eller infrastrukturen, for å løse de oppgavene som infrastrukturen understøtter (f.eks. transport på jernbane versus transport på vei). Der et annet objekt eller infrastruktur, eller en manuell løsning, kan løse samme oppgave helt eller delvis, kan det gjøre at objektet eller infrastrukturen ikke skal klassifiseres, eller klassifiseres på et lavere nivå.

Videre må det som etter KIKS-modellen også vurderes om det er en tett kobling mellom objektet eller infrastrukturen og de oppgavene som skal løses. Dvs. i hvor stor grad feil eller skader i et objekt eller ett sted i infrastrukturen fører til konsekvenser et annet sted, og spesielt hvor hurtig eller umiddelbart det skjer (f.eks. et styringssystem for lastebiltransport versus for togtransport). Jo tettere koblingen er, dess større grunn er det til å klassifisere objektet eller infrastrukturen.

Redundans er ikke nevnt eksplisitt som en eget vurderingstema i første ledd. Graden av redundans i en infrastruktur vil imidlertid være en av flere faktorer som påvirker resultatet av departementets vurdering etter myndighetsforskriften § 1 første ledd. Se også merknaden til virksomhetsforskriften § 52.

Departementet ber om høringsinstansenes syn på om ovennevnte kriterier er tilstrekkelige for at departementene skal kunne beslutte et klassifiseringsnivå etter sikkerhetsloven § 7-1.

6.1.2 Til § 2 Bruk av adgangsklarering.

Adgangsklarering er en ny type klarering, jf. sikkerhetsloven § 8-3. Departementet har foreslått å presisere at adgangsklarering kan benyttes som sikkerhetstiltak dersom fysisk eller elektronisk tilgang til hele eller deler av et klassifisert objekt eller infrastruktur gjør det mulig å skade grunnleggende nasjonale funksjoner. Slik skade kan skje ved at objektets eller infrastrukturens funksjonalitet reduseres, eller ved at den utsettes for skadeverk, ødeleggelse eller rettsstridig overtakelse.

Hvor omfattende eller nær tilgangen må være for at den skal kunne begrunne krav om adgangsklarering beror på en vurdering av i hvilken grad den tilgangen som gis, gir mulighet til å utføre sikkerhetstruende virksomhet. Det må også vurderes hvilket skadepotensiale vilkårlig tilgang kan ha. Se nærmere om dette i lovproposisjonens merknader til § 8-2.

Departementet antar at vurderingene normalt vil være knyttet til det konkrete objektet eller den konkrete infrastrukturen, men vil ikke utelukke at det f.eks. kan være relevant å vurdere om tilgang til ett konkret skjermingsverdig objekt, vil kunne utgjøre et skadepotensiale også for andre skjermingsverdige objekter eller infrastrukturer som er avhengig av hverandres funksjoner.

Generelt må *tilgang* i en sikkerhetssammenheng forstås som at en eller flere personer gis mulighet til å gjøre skade på objektet eller infrastrukturen. Dermed må all tilgang som kan misbrukes på en slik måte at det kan skade grunnleggende nasjonale funksjoner, kunne kontrolleres på ett eller annet vis.

Etter *andre ledd første punktum* kan det fattes vedtak om *adgangsklarering* der objektet eller infrastrukturen kan være et mål for terror, attentat eller annen alvorlig kriminalitet. Etter *andre punktum* kan det fattes vedtak om *utvidet adgangsklarering* dersom objektet eller infrastrukturen i stedet eller i tillegg kan være mål for spionasje eller sabotasje fra annen stat. Ved utvidet adgangsklarering vil personkontrollen være mer omfattende enn ved ordinær adgangsklarering, se nærmere i merknaden til kapittel 2 om personkontroll i forskrift om klarering av personell og leverandører.

6.2 Til kapittel 2 Nasjonal sikkerhetsmyndighets roller og ansvar

6.2.1 Til § 3 Iverksettelse av inntrengingstesting, kommunikasjons- og innholdskontroll og testing av sikkerhetstiltak

Bestemmelsens *første punktum* tilsvarer gjeldende krav om at NSM *kan* iverksette inntrengingstesting, kommunikasjons- og innholdskontroll og testing av sikkerhetstiltak når virksomhetens leder ber om det. En anmodning om at slike tester mv. blir gjennomført innebærer m.a.o. ikke en plikt for NSM om å iverksette. Det er således opp til NSM selv å vurdere om de har nødvendige ressurser og kapasitet til å iverksette slike tester, eller om det vurderes som mer hensiktsmessig å prioritere ressursene på andre områder. At slike tester mv. først kan iverksettes etter at virksomhetens leder ber om det, innebærer at NSM ikke av eget tiltak kan iverksette testing uten at virksomhetens leder samtykker. Det er likevel ikke av avgjørende betydning om det er virksomhetens leder eller NSM som foreslår at dette gjennomføres.

I henhold til *andre punktum* skal det inngås en avtale med virksomheten om hvilket personell som skal stå for testingen og kontrollen, og hva testingen og kontrollen skal omfatte.

6.2.2 Til § 4 Iverksettelse av tekniske sikkerhetsundersøkelser

I likhet med forslaget til § 3 foreslås det i *§ 4 første ledd første punktum* at også tekniske sikkerhetsundersøkelser (TSU) kan iverksettes av NSM når virksomhetens leder ber om det. Etter *andre punktum* skal det som for testing og kontroll etter § 3 også her inngås en avtale med virksomheten om hvilket personell som skal stå for undersøkelsen, og hva undersøkelsen skal omfatte.

Etter *andre ledd* skal PST forhåndsvarsles om at tekniske sikkerhetsundersøkelser skal gjennomføres. PST skal imidlertid ikke varsles der slike undersøkelser gjennomføres i Forsvaret.

Etter *tredje ledd* er det angitt enkelte momenter som NSM skal legge vekt på i vurderingen av om tekniske sikkerhetsundersøkelser skal gjennomføres.

6.2.3 Til § 5 Fellesregler for tekniske sikkerhetsundersøkelser, inntrengningstesting, testing av sikkerhetstiltak og kommunikasjons- og innholdskontroll av informasjonssystemer

I *første ledd* er det angitt at resultater fra undersøkelser, testing og kontroller skal rapporteres til virksomheten og den myndigheten som fører tilsyn etter loven. Slike rapporter skal ikke unødig inneholde informasjon som identifiserer enkeltpersoner som har begått eventuelle sikkerhetsbrudd.

Etter *andre ledd* skal informasjon fra undersøkelser mv. slettes senest innen tre måneder etter at oppdraget er avsluttet. I likhet med gjeldende § 11-6 i forskrift om informasjonssikkerhet, er det også foreslått at informasjonen kan bevares lenger enn tre måneder dersom det er nødvendig for å håndtere sårbarheter eller sikkerhetstruende hendelser, og dersom det er nødvendig av hensyn til kontrollvirksomheten til EOS-utvalget.

6.2.4 Til § 6 Bruk av tredjepart til å utføre tekniske sikkerhetsundersøkelser, inntrengingstesting, testing av sikkerhetstiltak og kommunikasjon- og innholdskontroll av informasjonssystemer

I *første ledd* angis det at NSM kan utpeke virksomheter til å utføre tekniske sikkerhetsundersøkelser, inntrengingstesting, testing av sikkerhetstiltak og kommunikasjon- og innholdskontroll av informasjonssystemer. Med utvidet virkeområde vil det kunne være behov for at flere enn NSM kan utføre slike undersøkelser, tester og kontroller. Det skal imidlertid som hovedregel være NSM som skal stå for utføringen, og dersom andre skal kunne gjøre dette på vegne av NSM må de være utpekt for dette.

Av *andre ledd* fremgår det et sett med kriterier som NSM skal basere seg på når de utpeker en virksomhet. Hensikten er å skape en viss forutberegnelighet for virksomhetene som eventuelt ønsker å utføre oppgaven og for å fastsette en ramme for NSM sin vurdering av virksomheter. Det sentrale er at virksomheten er sikkerhetsmessig skikket, og at den er kompetent til å utføre de undersøkelser mv. som er aktuelle. Utpeking av virksomheter vil f.eks. kunne skje ved at NSM, etter tilbudskonkurranse, tildeler kontrakt til kvalifiserte virksomheter.

Departementet ber høringsinstansenes syn på om bestemmelsen gir tilstrekkelige føringer for å benytte tredjeparter til disse oppgavene, og ønsker særlig tilbakemelding på om det bør fremgår ytterligere kriterier, og i så fall hvilke, som bør fremgå av forskrift for bruk av tredjeparter i disse tilfellene.

Tredje ledd pålegger virksomheter som utpekes å utføre undersøkelser, tester og kontroller i samsvar med de kriterier for utføring som fastsettes av NSM. Hensikten med dette er å sikre at dette gjøres i tråd med NSM sine føringer for dette, ettersom utføringen skjer på vegne av dem.

6.2.5 Til § 7 Om kryptosikkerhetstjenester

Bestemmelsen beskriver den rolle og det ansvaret NSM har når det gjelder kryptosikkerhetstjenester. Bestemmelsen bidrar også til å ivareta Norges forpliktelser overfor NATOs regelverk gjennom å beskrive og plassere ansvar for konkrete roller som de enkelte medlemsland skal ivareta.

Første ledd legger til grunn en videreføring av dagens praksis der NSM ivaretar rollen som nasjonal distribusjonsmyndighet for nasjonalt kryptomateriell samt kryptomateriell mottatt fra fremmede stater og internasjonale organisasjoner, og at NSM skal ha regnskapsmessig oversikt over kryptomateriell.

Nasjonal distribusjonsmyndighet innebærer å føre sentralt regnskap over kryptomateriell, å være nasjonale mottaker og forvalter av kryptomateriell fra NATO og andre samarbeidspartnere, produserer nøkkelmateriell til nasjonale kryptosystemer og distribuerer nasjonalt nøkkelmateriell og nøkkelmateriell fra NATO og andre samarbeidspartnere til brukere i Norge og utenrikstjenesten.

Andre ledd viser den rolle NSM skal ha som nasjonalt kontaktpunkt mot distribusjonsmyndigheter i andre stater og internasjonale organisasjoner.

Tredje ledd beskriver det overordnede ansvaret NSM har for at bruk, forvaltning, produksjon av kryptomateriell og regnskapsmessig kontroll med kryptomateriell, utføres i samsvar med sikkerhetsloven med forskrifter.

6.2.6 Til § 8 Register over avgjørelser om personklarering

Bestemmelsen er en videreføring av gjeldende personellsikkerhetsforskrift § 4-7. I bestemmelsens *første ledd bokstav a-e* er det imidlertid foreslått å gjøre det tydelig hva registeret skal inneholde informasjon om.

Forsvarsdepartementet har vurdert om den klarertes autorisasjonsstatus, jf. første ledd *bokstav e*, alltid skal registreres i registeret. Et slikt krav fordrer etter departementets syn at det først må utvikles en god og tilgjengelig elektronisk løsning som autorisasjonsansvarlige kan benytte for å registrere autorisasjonsstatus. I mangel av en slik løsning er det derfor valgt å angi at registeret *kan* inneholde informasjon om autorisasjonsstatus, *når den er tilgjengelig*. Det følger samtidig av sikkerhetsloven § 8-9 tredje ledd at sikkerhetsmyndigheten kan kreve at virksomheten skal holde sikkerhetsmyndigheten orientert om hvilke personer som er autorisert.

Av *tredje ledd* fremgår det at NSM, på forespørsel fra PST, skal utlevere informasjon fra registeret i samsvar med sikkerhetsloven § 8-12, og at NSM av hensyn til nasjonale sikkerhetsinteresser kan utlevere slike opplysninger til PST på eget initiativ. Forespørsel om og utlevering av opplysninger skal skje skriftlig.

Bestemmelsens *fjerde ledd* er ny og stiller krav om at NSM i avtale med PST skal fastsette kriterier for bruk av opplysninger fra registeret, og at kriteriene som minimum skal regulere hvordan hensynet til det opprinnelige formålet med opplysningene skal avveies mot hensynet til PSTs bruk av opplysningene etter politiloven og NSMs bruk av opplysningene i en klareringssak. Bestemmelsen er tilnærmet identisk med forslaget i klareringsforskriften § 13 om bruk av opplysninger fra registre hos politiet og PST. Ved uenighet mellom NSM og politiet/PST om bruk av opplysninger fra registeret, skal uenigheten løftes til Justis- og beredskapsdepartementet.

Departementet har i tillegg vurdert om det er behov for å fastsette at PST, og eventuelt også andre myndigheter, skal være pliktig til å melde fra til NSM dersom de blir kjent med forhold som kan ha betydning for om en klarering skal tilbakekalles, nedsettes eller suspenderes etter sikkerhetsloven § 8-8. Det måtte i tilfelle gjøres unntak fra en slik plikt der meldingen kommer i konflikt med PSTs samfunnsoppdrag, som f.eks. i konkrete etterforsknings- eller etterretningsoppgaver. Etter departementets vurdering er det likevel mer naturlig at en slik plikt eventuelt fastsettes i eller med hjemmel politiloven kapittel III a om *Politiets sikkerhetstjeneste. Organisering, oppgaver og forebyggende bruk av tvangsmidler.* Departementet viser samtidig til at PST, med hjemmel i politiloven § 17 b første ledd nr. 1, har som oppgave å forebygge og etterforske overtredelser av sikkerhetsloven. Det følger også av politiregisterloven § 30 at taushetsplikt ikke er til hinder for at opplysninger utleveres til andre offentlige organer i deres interesse, dersom dette er nødvendig for å fremme mottakerorganets oppgaver etter lov eller for å hindre at virksomhet blir utøvd på en uforsvarlig måte. I medhold av denne bestemmelsen er det i politiregisterforskriften § 9-6 første ledd nr. 11 fastsatt at det kan utleveres opplysninger til NSM og klareringsmyndighetene til formål personkontroll. Departementet ser det derfor som naturlig at PST i slike tilfeller vil varsle sikkerhetsmyndigheten om slike forhold når dette ikke kommer i konflikt med PSTs andre oppgaver.

6.2.7 Til § 9 Register over leverandørklareringer og sikkerhetsgraderte anskaffelser

Bestemmelsen er en videreføring av gjeldene § 6-1 i forskrift om sikkerhetsgraderte anskaffelser. I likhet med § 11, er det i § 12 *første ledd bokstav a til d* foreslått å tydeliggjøre hvilke opplysninger om leverandørklareringer registeret skal inneholde.

Bestemmelsens *andre ledd* fastsetter at NSM skal føre et register over alle sikkerhetsgraderte anskaffelser. Videre at registeret skal inneholde opplysninger som oppdragsgiver har innmeldt i samsvar med forslaget til forskrift om virksomhetens arbeid med forebyggende sikkerhet § 76. I henhold til den bestemmelsen skal oppdragsgiver årlig sende oversikt over egne sikkerhetsgraderte anskaffelser til klareringsmyndigheten og NSM.

6.2.8 Til § 10 Utlevering av opplysninger om klarering og personkontroll til andre staters myndigheter eller internasjonale organisasjoner

Bestemmelsens del om personkontroll og klarering av personer er i det vesentlige en videreføring av gjeldende forskrift om personellsikkerhet § 3-6. Det er i forhold til gjeldende forskrift lagt til at NSM også kan opplyse om leverandørklareringer.

Bestemmelsen er gitt for at NSM skal ha en tydelig hjemmel for hva de kan opplyse andre staters sikkerhetsmyndigheter og internasjonale organisasjoner om. Bestemmelsen setter samtidig begrensninger for hva det kan opplyses om, av hensyn til personvernet.

6.2.9 Til § 11 Unntak fra krav om sikkerhetsklarering og autorisasjon

Bestemmelsens *første ledd første punktum* gir NSM mulighet for i særlige tilfeller å gjøre unntak fra kravet om klarering etter sikkerhetsloven § 8-1, og unntak fra kravet i klareringsforskriften § 26 om samtykke fra klareringsmyndigheten for å autorisere utenlandske statsborgere for BEGRENSET. Etter *andre punktum* er det foreslått at et departementet som har fattet vedtak om adgangsklarering etter loven § 8-3, selv kan dispensere fra eget vedtak. Etter Forsvarsdepartementets syn kan det være behov for å tydeliggjøre dette i bestemmelsen.

Departementet ser det som viktig at det dispensasjon etter første ledd kun skjer unntaksvis, og at «listen» for slike dispensasjoner ikke blir for lav. I bestemmelsens *andre ledd* er det derfor angitt at det i vurderingen av *særlig behov* skal legges vekt på om behovet for tilgang er større enn risikoen

manglende klarering eller samtykke vil innebære for nasjonale sikkerhetsinteresser. En forutsetning for å benytte bestemmelsene at risikoen forbundet med tilgangen veies opp av behovet for å gi tilgang.

Risikoen ved å gi tilgang vil kunne variere ut i fra etterretningsaktivitet fra det aktuelle landet, det sikkerhetspolitiske samarbeidet og personellet som gis tilgang. Det er også en forutsetning at virksomhetens funksjon blir skadelidende dersom kompetansen ikke gjøres tilgjengelig, og det vil være uforholdsmessig krevende å få kompetanse fra et land vi har sikkerhetssamarbeid med.

Unntakene skal praktisere snevert og kun brukes i særlige tilfeller. Departementet har vurdert om NSM også skulle kunne gjøre tilsvarende unntak for tilgang til objekt eller infrastruktur som et departement har fattet vedtak om krav om adgangsklarering, jf. sikkerhetsloven § 8-3. Departementet er imidlertid av den oppfatning at et slikt vedtak i tilfelle bør fattes av det samme departementet som har fattet vedtak etter loven § 8-3.

Departementet vil vurdere hvorvidt bestemmelsen heller skal fremgå av virksomhetsforskriften eller klareringsforskriften, ettersom bestemmelsen sier noe om i hvilke tilfeller en virksomhet likevel kan benytte utenlandsk personell, selv om det ikke er mulig å klarere dem.

6.3 Til kapittel 3 Nasjonal responsfunksjon og nasjonalt varslingssystem for digital infrastruktur

6.3.1 Til § 12 Utøvelse av nasjonal responsfunksjon for alvorlige digitale angrep og nasjonalt varslingssystem for digital infrastruktur

Bestemmelsens første ledd fastsetter at det er NSM som skal drive responsfunksjonen og varslingssystemet for digital infrastruktur (VDI). Denne oppgaven ligger til NSM i dag, og sikkerhetsloven § 2-4 har ikke ment å innebære noen materiell endring fra gjeldende sikkerhetslov.

I andre ledd fremgår det nærmere hva som er hovedoppgaven til responsfunksjonen og VDI.

For nærmere omtale om nasjonal responsfunksjon og VDI henviser departementet til Prop. 97 L (2015–2016) om endringer i sikkerhetsloven kapittel 6 hvor temaet er inngående behandlet.

Ettersom det er et klart behov for bedre VDI dekning for å gi en bedre oversikt over digitale angrep mot sentrale virksomheter, vurderer departementet NSM skal gis mulighet til å pålegge VDI tilknytning for de virksomhetene som blir underlagt loven. Departementet ber om høringsinnstansenes syn på en slik påleggskompetanse, og eventuelt hvilke rammer en slik påleggskompetanse bør ha. For mer om VDI se kapittel 7.9.

6.3.2 Til § 13 Informasjonsbehandling og -deling

Felles cyberkoordineringssenter (FCKS) er et samarbeid mellom Etterretningstjenesten, Kripos, NSM og PST som er opprettet for å styrke evnen til å motvirke truslene i det digitale rom.

Bestemmelsen gir NSM hjemmel til å dele informasjon med partene i FCKS når dette er av betydning for å sikre nasjonale sikkerhetsinteresser. Hensikten med dette er å sikre informasjonsflyt mellom de hemmelige tjenestene og på den måten bidra til å oppfylle formålet med FCKS.

6.4 Til kapittel 4 Tilsyn

Til kapittelet om tilsyn bemerker departementet at flere av disse bestemmelsene snarere kan gis gjennom instruks fremfor forskrift. Departementene ber høringsinstansene om deres synspunkter på

innholdet i bestemmelsene og ønsker også synspunkter på om det er noe av dette som bør stå i forskrift av hensyn til forutberegnelighet for de som blir gjenstand for tilsyn.

6.4.1 Til § 14 Tildeling av tilsynsansvar

Det følger av loven § 3-1 at departementet *kan* bestemme at «myndigheter med sektoransvar som fører tilsyn med beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur skal føre tilsyn med virksomheter som er omfattet av loven». Det er tilstrekkelig at sektormyndigheten fører tilsyn innenfor et eller flere av disse fagområdene. Det forutsettes at sektormyndigheten har tilsynskompetanse. Det tas utgangspunkt i forståelsen av begrepet tilsyn fra St.meld. nr. 17 (2002-2003) Om statlige tilsyn:

> *Tilsynsbegrepet kan i vid forstand forstås som et fellesbegrep for all aktivitet eller virkemiddelbruk som iverksettes for å følge opp et lovverks intensjoner. Kjernen i tilsynsrollen er imidlertid den konkrete kontrollen av pliktsubjektenes etterlevelse av en norm som allerede er fastsatt ved lov, forskrift eller enkeltvedtak, samt reaksjoner ved avvik.*

Det vil si at sektormyndigheten som får et tilsynsansvar vil få et helhetlig ansvar for å følge opp sikkerhetslovens krav i sin sektor. Det vil også si ansvar for å gi råd, veiledning og informasjon til virksomhetene i sin sektor og områdeovervåkning i betydningen av å samle inn og systematisere ulike former for kunnskap om reguleringsområdet.

Samarbeidsavtalen blir et viktig verktøy for hvordan disse oppgavene skal fordeles mellom NSM og sektormyndigheten. Formålet med fordelingen må være å unngå dobbeltarbeid og unødvendig dublering av kompetansemiljøer. Det bør også vurderes om sektormyndighetene skal gis ansvar for godkjenninger og dispensasjoner i sektoren.

Ettersom sektormyndigheten som får tilsynsansvar allerede har tilsynsoppgaver, jf. sikkerhetsloven § 3-1, legges det til grunn som en forutsetning for tildeling av tilsynsansvar at sektormyndigheten allerede har kompetanse innen utøvelse av tilsynsfunksjonen, som for eksempel kompetanse innen risikovurdering og systemrevisjon. Sektormyndigheten må også ha den nødvendige sikkerhetsfaglige kompetanse og ressurser. Uttalelsen fra NSM som skal innhentes i forbindelse med helhetsvurderingen som skal gjøres, må særlig berøre i hvilken grad sektormyndigheten har eller vil kunne tilegne seg denne kompetansen, og på hvilke områder det vil være hensiktsmessig at NSM bistår med forberedelse eller gjennomføring av tilsyn.

6.4.2 Til § 15 Avtale om samarbeid mellom Nasjonal sikkerhetsmyndighet og andre myndigheter med tilsynsansvar

Sektormyndighet som har fått tildelt tilsynsansvar har som hovedregel ansvar for tilsyn i sin sektor. Samarbeidsavtalen som inngås med NSM vil nærmere presisere om det er områder NSM skal bistå med, men ansvaret ligger hos sektormyndigheten. Det er kun der det er tvingende nødvendig, grunnet konkrete sikkerhetsinteresser eller fordi det er nødvendig av hensyn til internasjonale avtaler, at dette kan fravikes i sektorer hvor sektormyndighet har tilsynsansvar.

I henhold til lovens § 2-2 skal NSM utarbeide og vedlikeholde grunnleggende kriterier for tilsyn. Det bør i avtalen fremkomme hvordan det er forventet at sektormyndigheten legger disse til grunn for sine tilsyn. Eventuelle tilpasninger som må gjøres bør fremkomme etter dialog mellom NSM og sektormyndigheten slik at dette ikke får utilsiktede effekter som kan gå på bekostning av nasjonale sikkerhetsinteresser.

Det kan og bør avtales hvordan NSM skal sikre at sektormyndigheten kan opparbeide seg og vedlikeholde den nødvendige kompetansen gjennom opplæring og veiledning av sektormyndigheten innen sikkerhetsfaget og NSMs kriterier for tilsyn.

Fremfor å lære opp sektormyndigheten, bør det på enkelte områder hvor det ikke er hensiktsmessig å bygge opp egen kompetanse hos sektormyndigheten avtales at NSM bidrar med forberedelse og gjennomføring av tilsyn. Dette kan være innenfor områder som kryptosikkerhet eller personellsikkerhet hvor NSM har særlig kompetanse. Slik medvirkning kan for eksempel være å utarbeide sjekklister eller planer for tilsynet, gjennomgå innhentet dokumentasjon eller selv å være med for å gjennomføre intervjuer eller verifikasjoner innenfor fagområdene hvor NSM har særlig kompetanse.

For at sektormyndigheten fullt ut skal kunne ivareta sitt ansvar, er det viktig at den har tilgang på trusselinformasjon og annen sikkerhetsrelevant informasjon. Det bør i avtalen berøres hvilken informasjon sektormyndigheten kan forvente og hvordan denne skal gjøres tilgjengelig, og om det for eksempel skal benyttes egne informasjonssystemer for dette. På samme måte bør det avtales hvordan informasjon skal sendes fra sektormyndigheten til NSM både etter tilsyn og ved rapportering om hendelser.

Normerende vedtak som godkjenninger og dispensasjoner følges ofte opp gjennom tilsyn. Det bør i avtalen berøres om NSM, der det er anledning, skal bemyndige sektormyndigheten til å være godkjennings- og dispensasjonsmyndighet. Videre bør det avtales hvordan informasjon om slike godkjenninger og dispensasjoner deles mellom NSM og sektormyndigheten og forventningen til hvordan disse følges opp.

Videre er det viktig at sektorspesifikk kompetanse tilbakeføres til NSM for å gjøre dem bedre i stand til å ivareta sitt nasjonale sektorovergripende ansvar. Dette kan gjelde særlige forhold i sektoren som kan være av betydning for nasjonale sikkerhetsinteresser.

6.4.3 Til § 16 Tilsynsmyndighet for leverandører i sikkerhetsgraderte anskaffelser

Som hovedregel skal NSM være tilsynsmyndighet overfor leverandører i sikkerhetsgraderte anskaffelser. Bakgrunnen er at mange leverandører ikke faller inn under én sektor ved at de kan være leverandører til oppdragsgivere i forskjellige sektorer. Dette vil medføre at forskjellige sektormyndigheter ville kunne fått tilsynsansvar, avhengig av hvor leverandøren for tiden hadde sine oppdrag. Videre er Norge forpliktet gjennom sikkerhetsavtaler med andre land til å følge opp leverandører som er klarert og som har andre lands sikkerhetsgraderte informasjon i sin besittelse på bakgrunn av oppdrag til andre land. Det vil således være et enklere og mer forutsigbart regime, og i mange tilfeller nødvendig, at NSM har tilsynsansvaret for leverandører. Det vil kunne avtales at sektormyndigheter har tilsynsansvar for leverandører som er i deres sektor, dersom om det likevel er mer hensiktsmessig, og internasjonale forpliktelser ikke er til hinder.

6.4.4 Til § 17 Om tilsyn med virksomheter underlagt lov om nasjonal sikkerhet

NSM har allerede begynt etableringen av samarbeidsforum for tilsynsvirksomheter. Disse arenaene vil, sammen med løpende dialog og samarbeidsavtalene, være det viktigste verktøyet for å harmonisere og sikre rett kvalitet på tilsyn på tvers av sektorene. Det er viktig å understreke at tilsyn skal ha en positiv effekt, ikke utelukkende påvise avvik fra reglene. Det sentrale er at det blir påpekt avvik på rett nivå i virksomheten slik at man får insentiver til å rette opp bakenforliggende forhold. For eksempel kan manglende tiltak skyldes at det mangler ressurser og kompetanse på overordnet

nivå. Tilsynsmyndigheten må derfor ivareta at virksomheten settes i stand til å utbedre forhold både når rapporter og pålegg utformes og gjennom å tilby påfølgende rådgivningen og veiledningen.

Etter *andre ledd* skal tilsyn skal gjennomføres planlagt og systematisk og skal følge et program som er utarbeidet på bakgrunn av risiko og vesentlighet. Det vil si at tilsynsobjekter, temaer og metodikk skal benyttes slik at det gir størst mulig effekt for ivaretagelsen av nasjonale sikkerhetsinteresser over tid.

Da regelverket er funksjonelt skal tilsyn i tråd med *tredje ledd* som hovedregel gjennomføres som systemrevisjon. NSM legger i dag den internasjonale standarden ISO 19011til grunn for sin tilsynsmetodikk. Standarden er vel etablert og anerkjent, og det finnes mange opplæringsprogrammer for innføring i denne. Det er derfor nærliggende også for andre tilsyn å legge til grunn for sitt tilsynsarbeid etter dette regelverket. Forskriften åpner likevel for at sektormyndigheten kan legge andre tilnærminger til grunn, så fremt disse er egnet til å føre tilsyn med kravene i eller i medhold av sikkerhetsloven.

6.4.5 Til § 18 Rapport etter tilsyn

For å kunne ivareta sine tverrsektorielle oppgaver, må NSM ha kjennskap til sikkerhetstilstanden også i de sektorene hvor det er utpekt sektormyndigheter med tilsynsansvar. Sektormyndigheter med tilsynsansvar må derfor gjøre NSM kjent med rapporter fra tilsyn. På hvilken måte og form avtales i samarbeidsavtalen. For eksempel er det ikke noe til hinder for at sektormyndighetene sammenfatter aktuelle rapporter til en årlig rapport til NSM om det er ønskelig for begge partene. Det er kun opplysninger som er relevant for tilsyn etter sikkerhetsloven som NSM etter bestemmelsen skal ha tilgang til. Dette betyr at opplysninger som kun er relevant for tilsyn etter annet sektorregelverk, kan holdes utenom i den rapporten NSM skal ha tilgang til.

Bestemmelsen angir for øvrig krav om at tilsynsmyndigheten skal forelegge virksomheten en foreløpig rapport til uttalelse, og at endelig rapport skal sendes virksomheten og NSM.

6.4.6 Til § 19 Tvangsmulkt

Det er i § 22 foreslått at tvangsmulkt kan fastsettes som engangsmulkt eller løpende for hver dag, uke eller måned, etter at fristen for å rette forholdet er gått ut. Det er også foreslått at tilsynsmyndigheten kan frafalle påløpt tvangsmulkt.

Forsvarsdepartementet har også vurdert om det er behov for å fastsette krav i forskrift om overtredelsesgebyr. Da lovteksten er relativt detaljert og dekkende, er det ikke vurdert som nødvendig å utarbeide dette. Enhetlig praksis innenfor en sektor vurderes også å være viktigere enn enhetlig praksis med hensyn til samtlige tilsynsobjekter.

Det er heller ikke foreslått å regulere utmåling da dette er et forhold hvor det typisk vil være stor variasjon fra sektor til sektor.

6.5 Til kapittel 5 Andre bestemmelser

6.5.1 Til § 20 Melding om erverv av kvalifisert eierandel i virksomhet underlagt sikkerhetsloven

Det fremgår av Prop. 153 L (2016–2017), kapittel 14.4 s. 151, at «departementet vil utrede behovet for nærmere krav til innholdet i meldingen i det videre forskriftsarbeidet.» Videre har utenriks- og forsvarskomiteen under behandlingen etterlyst forutberegnelighet for virksomhetene som underlegges loven. Slik departementet ser det ivaretar forslaget til bestemmelse, sammenholdt med

merknadene i proposisjonen, tilstrekkelig forutberegnelighet for virksomhetene. Det er ved utformingen av bestemmelsen sett hen til finansforetaksregelverket og reglene om leverandørklarering i gjeldende og ny sikkerhetslov. Det er også lagt opp til meldingen etter § 9-4 i loven, vil være tilnærmet lik meldingen etter § 10-1.

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

Departementet har heller ikke sett det som hensiktsmessig med et tydeligere gjennomføringsforbud, utover at det følger av § 10-2 at departementet skal gi melding til erverver innen 60 dager om at ervervet er godkjent eller ikke.

Når det gjelder forholdet til Norges folkerettslige forpliktelser viser departementet til de vurderinger som ble gjort på s. 152, i kapitel 14.4 i proposisjonen. Slik departementet ser det vil bestemmelsen kun benyttes unntaksvis, i de tilfellene hensynet til nasjonale sikkerhetsinteresser veier tyngre enn de negative konsekvensene for de involverte aktørene. Departementet vil vurdere forholdet til våre folkerettslige forpliktelser i lys av høringsinnspillene.

Departementet ber om høringsinstansenes innspill til bestemmelsen, og vil vurdere behovet for ytterligere bestemmelser om eierskapskontroll i lys av høringsinstansenes innspill. Departementet vil også vurdere om det er mer hensiktsmessig at bestemmelsen fremgår av virksomhetsforskriften.

6.5.2 Til § 21 Oppnevning av advokater etter sikkerhetsloven § 8-15

Det foreslås at Forsvarsdepartementet oppnevner advokater og at sikkerhetsklarering og autorisasjon foretas av Sivil klareringsmyndighet.

7 Merknader til forskrift om virksomhetens arbeid med sikkerhet (virksomhetsforskriften)

7.1 Innledning

Virksomhetens plikt til å sikre sine skjermingsverdige verdier er nærmere regulert i forskrift om virksomhetens arbeid med forebyggende sikkerhet. Begrepet *skjermingsverdig verdi* er en samlebetegnelse på skjermingsverdig informasjon, informasjonssystem, objekt og infrastruktur.

Forskriften er innrettet på en slik måte at det først stilles krav til virksomhetens styringssystem for sikkerhet. Styringssystemet for sikkerhet utgjør rammen for hvordan virksomheten oppfyller kravene til forebyggende sikkerhet. Et velfungerende styringssystem for sikkerhet, skal gjøre at sikkerhetsarbeidet planlegges, gjennomføres og kontinuerlig utvikles på en systematisk måte. Videre stilles det enkelte generelle krav til beskyttelse av skjermingsverdige verdier og noen krav som gjelder spesifikt for de konkrete verdiene.

Kapittel 2 om generelle krav til beskyttelse av skjermingsverdige verdier danner utgangspunktet og rammen for virksomhetens håndtering av risiko. De generelle kravene vil gjelde for alle virksomheter som blir underlagt loven, uavhengig av hva slags verdier som skal beskyttes. De generelle kravene må utfylles av og ses i sammenheng med de mer spesifikke kravene for beskyttelse av informasjon, informasjonssystemer, infrastruktur og objekt som fremgår av kapittel 3 til 7.

Bakgrunnen for innretningen er at vi lever i et samfunn preget av en omfattende teknologisk utvikling og et vesentlig mer komplekst trusselbilde enn for bare få år siden. Trusselaktørene blir mer sofistikerte, samtidig som systemene og infrastrukturen vår er mer kompleks og sammensatt enn tidligere. Det stilles dermed økte krav til kompetanse om både egne verdier, sårbarheter, trusselaktører og tilgjengelige sikkerhetstiltak for å oppnå et forsvarlig sikkerhetsnivå.

Det er også viktig at virksomheten tenker sikkerhet på tvers av de verdiene virksomheten råder over. Det sentrale er ikke hvorvidt det er et informasjonssystem, infrastruktur eller et objekt, men hvordan man sikrer at informasjonssystemet, objektet eller infrastrukturen har et forsvarlig sikkerhetsnivå, sett hen til de sårbarheter verdien har, holdt opp mot den til enhver tid rådende trusselen mot virksomheten. Dette er også lagt til grunn i Prop. 153 L (2016–2017) punkt 11.4 på side 111 hvor det bl.a. sies at «innenfor mange av de funksjonene og systemene som vil falle inn under sikkerhetsloven, vil det være påkrevet å se bestemmelsene om informasjonssikkerhet, informasjonssystemsikkerhet og objekt- og infrastruktursikkerhet i nær sammenheng.»

7.1.1 Forsvarlig sikkerhetsnivå

Virksomheten skal i henhold til loven sørge for et *forsvarlig sikkerhetsnivå* for sine skjermingsverdige verdier slik at de fungerer slik de skal, ikke blir kjent for uvedkommende, går tapt eller blir endret, blir utilgjengelig, blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse. For å tilpasse kravet til styringssystem til anerkjente standarder og rammeverk for styring, har departementet valgt å kalle disse kravene for *sikkerhetsmål*.

Virksomheten skal i henhold til forskriften planlegge hvordan sikkerhetsmålene i sikkerhetsloven §§ 4-3, 5-2, 6-2 og 7-3 skal nås. Ut fra hvor viktig de skjermingsverdige verdiene er for grunnleggende nasjonale funksjoner og/eller nasjonale sikkerhetsinteresser, holdt opp mot hva slags sikkerhetstruende virksomhet verdien er utsatt for, skal virksomheten fastsette hva som er et forsvarlig sikkerhetsnivå for virksomheten.

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

Hva som er forsvarlig vil variere, avhengig av hva slags skjermingsverdige verdier virksomheten har, hvilken sektor og bransje virksomheten tilhører og hva slags type funksjon den enkelte virksomhet har. På enkelte områder er det i forskriften, og til en viss grad direkte i loven, fastsatt krav om tiltak som er forholdsvis konkrete. Det gjelder spesielt ved beskyttelse av sikkerhetsgradert informasjon. På mange andre områder er det imidlertid ikke gitt slike konkrete krav. Det er derfor nødvendig at virksomhetene som råder over de skjermingsverdige verdiene, konkretiserer hva som anses forsvarlig for sine verdier.

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

7.1.2 Beskyttelse av skjermingsverdig informasjon

I lov om nasjonal sikkerhet (sikkerhetsloven) § 5-1 etableres samlebetegnelsen skjermingsverdig informasjon om all informasjon som skal beskyttes etter loven. Dette medfører en utvidelse sammenlignet med gjeldende lov og forskrift som kun omtaler skjermingsverdig informasjon som sikkerhetsgradert informasjon. Nå stilles det krav til beskyttelse av informasjon også av hensyn til integritet og tilgjengelighet, ikke bare av hensyn til konfidensialitet. Dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen ikke er tilgjengelig, plikter altså virksomheten etter loven å sørge for at den er tilgjengelig. Informasjonen vil være ugradert skjermingsverdig dersom det kan skade nasjonale sikkerhetsinteresser hvis informasjonen går tapt, blir endret, eller blir utilgjengelig ved tjenstlig behov.

Forskrift om virksomhetens arbeid med forebyggende sikkerhet kapittel 3 stiller funksjonelle krav til sikringsnivået for ugradert skjermingsverdig informasjon og til sikkerhetsgradert skjermingsverdig informasjon. Videre stilles det enkelte krav til destruering av dokumenter, til evakuering og destruering i nødsituasjoner og til utlevering av sikkerhetsgradert informasjon til fremmede stater og internasjonale organisasjoner.

Dersom det behandles sikkerhetsgradert informasjon på et informasjonssystem, vil reglene i kapittel 6 om beskyttelse av informasjonssystemer gjelde i tillegg. Det er derfor viktig at de ulike bestemmelsene leses i sammenheng.

7.2 Til kapittel 1 Sikkerhetsstyring

7.2.1 Til § 1 Definisjoner

Departementet har sett det som hensiktsmessig å definere begrepene i bestemmelsen for å klargjøre hva som menes med disse i forskriften. Departementet ber om høringsinstansenes syn på om definisjonene i bestemmelsen er nødvendig, og på om det er andre begreper som bør defineres.

7.2.2 Til § 2 Styringssystem for sikkerhet

Styringssystemet for sikkerhet utgjør rammen for hvordan virksomheten oppfyller kravene til forebyggende sikkerhet. Et velfungerende styringssystem for sikkerhet skal gjøre at sikkerhetsarbeidet planlegges, gjennomføres og kontinuerlig utvikles på en systematisk måte.

Formålet med å stille krav om styringssystem er at virksomhetene i større grad skal tenke helhetlig i det forebyggende sikkerhetsarbeidet. Virksomheter som allerede har et eksisterende styringssystem for f.eks. virksomhetsstyring, IKT-sikkerhet eller HMS kan bygge videre på dette for å ivareta kravene i forskriftene. Slik departementet ser det vil de fleste virksomheten gjør endringer for å oppfylle kravene i forskriften om virksomhetens arbeid med forebyggende sikkerhet.

Kravene i forskriften §§ 3 til 10 har mange fellestrekk med innholdet i gjeldende forskrift om sikkerhetsadministrasjon. Bestemmelsene er imidlertid mer funksjonelt utformet, med færre detaljerte krav enn i gjeldende forskrift. Bestemmelsene er i stor grad basert på strukturen og de viktigste prinsippene i standarden ISO/IEC 27001 om ledelsessystem for informasjonssikkerhet. Innholdet er imidlertid utformet slik at det skal passe for sikkerhet etter loven, og ikke bare informasjonssikkerhet. Denne tilnærmingen vil etter departementets syn gjøre det lettere å integrere styringssystemet for sikkerhet i virksomhetsstyringen for øvrig, jf. sikkerhetsloven § 4-1 første ledd, ettersom mange virksomheter allerede i dag baserer sine styringssystemer på anerkjente standarder.

Omfanget av styringssystemet den enkelte virksomhet må ha, vil variere ut ifra bl.a. hvilke skjermingsverdige verdier virksomheten har og hvilke deler av virksomheten som har tilgang til verdiene.

Hvordan risiko skal vurderes og håndteres er en sentral del av et styringssystem for sikkerhet. Departementet har imidlertid valgt å plassere kravene til vurdering og håndtering av risiko i kapittel 2, for å gi bedre sammenheng med de generelle kravene til beskyttelse av skjermingsverdige verdier.

7.2.3 Til § 3 Styringsdokument for det forebyggende sikkerhetsarbeidet

Bestemmelsen er ny, men har visse likhetstrekk med bestemmelsen om grunnlagsdokument for sikkerhet i gjeldende forskrift om sikkerhetsadministrasjon § 3-3. Styringsdokumentet etter § 3 skal imidlertid i større grad være på et overordnet nivå og kortfattet. Dokumentet skal gi den ytre rammen og vise retningen for virksomhetens sikkerhetsarbeid, og tilsvarer det som i ISO/IEC 27001 kalles *sikkerhetspolicy*.

Bestemmelsen er begrunnet i behovet for at det gis noen sentrale føringer fra øverste ledelse for å ha et utgangpunkt for det videre sikkerhetsarbeidet. Videre har øverste ledelses uttalte forpliktelser stor betydning for at medarbeidere forholder seg lojalt til kravene etter sikkerhetsloven.

Med «prinsipper» i *første ledd bokstav c* menes overordnede føringer som er felles for mye av sikkerhetsarbeidet i virksomheten. Det kan bestå av hvilke overordnede mål virksomheten skal oppfylle, jf. § 4, et sett med føringer om virksomhetens styring med sikkerhet, eller en kort henvisning til en eller flere standarder eller rammeverk som virksomheten skal legge til grunn for styringssystemet. Hvilke prinsipper som fastsettes i styringsdokumentet må tilpasses virksomhetens størrelse og kompleksitet.

Selv om plikten til å fastsette styringsdokumentet er lagt til virksomhetens leder, er det ikke departementets intensjon at bestemmelsen skal gjøre inngrep i ansvarsforholdene som følger av selskapsretten og annen organisasjonsrett. Dersom virksomheten f.eks. er et selskap eller statsforetak der styret ikke har delegert myndigheten til å fastsette styringsdokumentet til daglig leder, er det styret som har ansvaret etter første ledd.

7.2.4 Til § 4 Sikkerhetsmål

Bestemmelsen er ny. Målstyring er imidlertid en sentral prosess i mange modeller for styringssystemer for å oppfylle eksterne og interne krav og forventninger. Det gjelder f.eks. ISO/IEC

27001 om ledelsessystem for informasjonssikkerhet og ISO 31000 om risikostyring, Balanced Scorecard (balansert målstyring), COSO Internal Control og COSO ERM. Direktoratet for økonomistyring har for eksempel basert seg på COSO-modellen i sine veiledere om hvordan statlige virksomheter kan oppfylle styringskravene i statens økonomiregelverk.

De overordnede sikkerhetsmålene er formulert i lovens § 4-3 første ledd, § 5-2 første ledd, § 6-2 første ledd og § 7-3 første ledd, og det er derfor vist til disse bestemmelsene i forskriften § 4. Fordi de overordnede sikkerhetsmålene ikke er konkrete nok til å alene gi gode nok føringer for hva som skal gjøres, må virksomheten planlegge hvordan oppfyllelsen skal skje. Planleggingen innebærer at virksomheten først må bryte de overordnede sikkerhetsmålene ned i delmål, eller angi måleparametere og måleindikatorer for hvert mål, som er konkrete nok til at graden av måloppnåelse senere kan måles.

Hvordan sikkerhetsmålene etter sikkerhetsloven skal integreres i virksomhetenes målstyring vil variere ut ifra virksomhetenes valg av prosess for mål- og resultatstyring, vesentlighet, risiko og det samlede målbildet. I enkelte virksomheter er det naturlig at sikkerhetsmålene etter loven plasseres øverst i målhierarkiet, men for andre er det tilstrekkelig at sikkerhetsmålene fremgår delmål under andre strategiske mål. Sikkerhetsmålene kan f.eks. være delmål under et strategisk mål om etterlevelse av eksterne krav og forpliktelser, eller delmål under et strategisk mål om å ivareta sikkerhet generelt (utover bare sikkerhetslovens krav). Hvorvidt sikkerhetsmålene står i et strategisk målbilde, et dokument for oppdragsstyringen i virksomheten, lederkontrakter med den enkelte eller i annen form, er ikke avgjørende. Det sentrale er at styringen av sikkerhetsmålene skal være integrert i målstyringen for øvrig, og på det nivået og i den formen som er hensiktsmessig for at kravene etter sikkerhetsloven skal bli oppfylt.

Planleggingen av *konkrete tiltak* kan først skje når også vurdering og håndtering av risiko er gjort, jf. forskriften §§ 11 og 12. Hvor detaljert og omfattende virksomheten må planlegge for oppfyllelse av sikkerhetsmålene, vil variere fra virksomhet til virksomhet, basert på virksomhetens skjermingsverdige verdier, størrelse og kompleksitet.

7.2.5 Til § 5 Roller og ansvar i det forebyggende sikkerhetsarbeidet

Bestemmelsen regulerer kravet til at det forebyggende sikkerhetsarbeidet fordeles på nødvendige roller i virksomheten. Til forskjell fra gjeldende forskrift om sikkerhetsadministrasjon § 2-5 stilles det ikke spesifikke krav til *hvilke* roller som skal etableres, heller ikke at det skal etableres en sikkerhetsorganisasjon. Sikkerhetsloven får et bredt nedslagsfelt med alt fra små virksomheter, til leverandører og store statlige og private aktører. Det fremstår derfor som lite hensiktsmessig å stille konkrete krav til hvilke roller den enkelte virksomhet bør etablere. Det bør utarbeides veiledningsmateriale fra tilsynsmyndigheten eller sikkerhetsmyndigheten som kan brukes i vurderingen av hvilke roller som vil være tilstrekkelig i det enkelte tilfelle.

Med roller menes i bestemmelsen ikke bare styrende og kontrollerende roller, som typisk ivaretas av stabsfunksjoner («andrelinje»), men også utøvende roller («førstelinje»). Dvs. at det også må være fastsatt hvilket ansvar linjeorganisasjonen har for å ivareta sikkerheten i utførelsen av de daglige oppgavene, og i utvikling av nye løsninger i interne fellesfunksjoner og i virksomhetens kjernefunksjoner.

For å sikre en mest mulig uavhengig og objektiv kontroll av styringssystemet følger det av tredje ledd at personer med kontrollerende roller ikke bør være de samme som har styrende eller utøvende roller i det forebyggende sikkerhetsarbeidet. Kravet er ikke gjort absolutt, da kostnaden for små

virksomheter ofte vil kunne være uforholdsmessig store i forhold til gevinsten for det forebyggende sikkerhetsarbeidet.

7.2.6 Til § 6 Ressurser og kompetanse

Det er avgjørende for oppfyllelsen av kravene etter sikkerhetsloven med forskrifter at det settes av nok personell og økonomiske ressurser til å gjennomføre tiltakene.

Bestemmelsen er i stor grad en videreføring av gjeldende forskrift om sikkerhetsadministrasjon §§ 2-1 andre ledd, 2-2 og 2-3, men er noe forenklet og har et oppdatert språk. Det stilles heller ikke eksplisitt krav til «den foresattes ansvar». Departementets vurdering er at dette fremgår av § 6 andre ledd, hvor det stilles krav til alle som utfører arbeid eller tjenester, uavhengig om du er mellomleder, «vanlig» ansatt eller innleid personell. Det vil være opptil virksomheten å identifisere hvilken kompetanse og hvilket ansvar som er nødvendig for at medarbeidere og innleide skal være i stand til å ivareta sikkerheten i virksomheten.

Kravet i *andre ledd* om hva personellet skal kjenne til eller ha kompetanse om, er avgrenset til det som er relevant for den enkelte. En person som skal jobbe med f.eks. drift av informasjonssystemer har behov for fagkompetanse om sårbarheter og sikkerhetstiltak i informasjonssystemer, mens personellet for øvrig bare trenger å vite hvordan de skal bruke informasjonssystemene på en sikker måte.

Med relevante sikkerhetsbestemmelser i *andre ledd bokstav e* menes de bestemmelser i lov, forskrift, internt instruksverk, prosedyrebeskrivelser eller andre føringer innen sikkerhet, som gjelder for den aktuelle personen.

Tredje ledd er tatt inn for å sørge for at virksomheten ivaretar sikkerheten også i avslutningsfasen av et arbeids- eller tjenesteforhold. For eksempel vil en ansatt i den nærmeste tiden før avgang kunne utgjøre en større sikkerhetsrisiko enn ellers i ansettelsesforholdet, samt etter at arbeidsforholdet er avsluttet. Det er da viktig at virksomheten iverksetter nødvendige tiltak for å redusere risikoen til et forsvarlig sikkerhetsnivå.

7.2.7 Til § 7 Tiltak ved sikkerhetstruende virksomhet, avvik og kompromittering av sikkerhetsgradert informasjon

Bestemmelsen er delvis en videreføring av gjeldende § 5-1 i forskrift om sikkerhetsadministrasjon.

I *første ledd* fastsettes det funksjonelle krav til hvordan en virksomhet skal håndtere sikkerhetstruende virksomhet og avvik. Bestemmelsen stiller krav til håndtering i fire faser: Umiddelbare tiltak, gjenoppretting og konsekvensvurdering. I tillegg skal forholdet rapporteres. Rapporteringen kan måtte skje flere ganger ettersom hvordan saken utvikler seg.

For å sikre at tilvirker av den sikkerhetsgraderte informasjonen får informasjon om brudd på konfidensialiteten til sikkerhetsgradert informasjon, fastsettes det i *andre ledd* en bestemmelse som pålegger virksomheten å underrette utsteder om dette. Bestemmelsen er begrunnet i at det er tilvirker av informasjon som normalt er best skikket til å vurdere hvilken skade kompromitteringen av informasjonen kan føre til, og om det finnes skadereduserende tiltak.

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

begrep som i loven. Departementet ber om høringsinstansenes syn på bruken av begrepet «sikkerhetstruende virksomhet».

7.2.8 Til § 8 Evaluering og øvelser

Bestemmelsens første ledd stiller krav til at virksomheten jevnlig skal evaluere hvorvidt sikkerhetsmålene nås. At målene er nådd er ikke en statisk tilstand som man kan evaluere med fastsatte tidsintervaller, men er noe som må vurderes kontinuerlig. At det foreligger et forsvarlig sikkerhetsnivå den ene dagen, betyr ikke nødvendigvis at man har det den neste dagen.

Evaluering i denne sammenheng skal forstås som et vidt begrep. Det kan benyttes ulike metoder både for målingen som kan utgjøre et datagrunnlag for evalueringen, og for evaluering som sådan. Modenhetsmodeller, sammenligning (benchmarking), statistikk om standardavvik innen kvalitetsstyring, selvevaluering med sjekklister, øvelser og ekspertvurderinger er noen eksempler på metoder for evaluering.

Deler av eller hele evalueringen kan gjennomføres som en internrevisjon. Bruk av internrevisjon skal imidlertid ikke føre til at evaluering som utføres av første- eller andrelinje skal opphøre.

Bestemmelsens andre ledd er plassert i forlengelsen av evaluering generelt, da øvelser som metode anses som både en form for måling og en form for evaluering. Andre ledd understreker at øvelser skal være med på å sikre sikkerhetstiltakenes effektivitet.

7.2.9 Til § 9 Virksomhetens leders gjennomgang av det forebyggende sikkerhetsarbeidet

Bestemmelsen er i hovedsak en videreføring av gjeldende forskrift om sikkerhetsadministrasjon § 4-4 om «ledelsens evaluering». Fordi uttrykket «evaluering» i § 8 brukes om beslutningsgrunnlaget for ledelsens gjennomgang, og heller ikke samsvarer bruken av uttrykket i ISO/IEC 27001, har departementet valgt å endre uttrykket i § 9 til «gjennomgang». Gjennomgangen skal føre til nødvendige beslutninger om tiltak.

7.2.10 Til § 10 Dokumentasjon om styringssystemet for sikkerhet

Bestemmelsen er utformet som en fellesbestemmelse for de ulike kravene til styringssystemet, og er derfor plassert til slutt. En slik plassering avviker fra strukturen i ISO/IEC 27001, men er gjort for å unngå at det må tas inn krav til dokumentasjon i hver eneste paragraf.

7.3 Til kapittel 2 Generelle krav til beskyttelse av skjermingsverdige verdier

7.3.1 Til § 11 Plikt til å vurdere risiko

Bestemmelsen tilsvarer til en viss grad gjeldende forskrift om sikkerhetsadministrasjon § 4-2 om risikovurdering. Bestemmelsens materielle innhold og språk er imidlertid endret en del.

Departementet har i innretningen av bestemmelsen valgt å legge til grunn samme forståelse av risikobegrepet som i ISO Guide 73 og ISO 31000 om risikostyring. Risiko er der definert som «virkningen av usikkerhet knyttet til mål», der «virkning» er forklart som bl.a. avvik fra det forventede. Uttrykket «mål» er ikke brukt i bestemmelsen, men det følger av *første ledd* at det er oppfyllelsen av lovens krav om et forsvarlig sikkerhetsnivå som er gjenstand for vurderingen.

Kravet i *første ledd* om at vurderingen skal bestå av å identifisere, analysere og evaluere risikoene, følger med hensikt samme prosessorienterte tilnærming som i ISO 31000 om risikostyring, ISO/IEC 27001 om ledelsessystem for informasjonssikkerhet og ISO/IEC 27005 om styring av informasjonssikkerhetsrisiko.

Når det gjelder *første ledd* er formålet med *identifiseringen* å lage en liste over potensielle hendelser som kan utløse konsekvenser som ikke er i samsvar med virksomhetens mål, jf. § 4. Eksempler på potensielle hendelser er terroranslag mot virksomhetens skjermingsverdige infrastruktur som gjør at den får redusert funksjonalitet, eller at sikkerhetsgradert informasjon blir kjent for uautorisert personell gjennom spionasje fra fremmed etterretning.

Analysen handler om å utvikle en forståelse av risikoene. Formålet er å kunne fastslå mulig konsekvens av og tilhørende sannsynlighet for potensielle hendelser identifisert i forrige steg. Analysen omfatter en vurdering av årsakene og kildene til hendelsene, hvor sårbar virksomhetens verdier er mot hendelsene (scenarioer), hvilke konsekvenser det kan få, og hvilke mål som da kan bli påvirket.

Evalueringen består i å sammenligne risikonivået som ble avdekket i analysen, med virksomhetens kriterier for hvilken risiko som kan aksepteres for at målet om et forsvarlig sikkerhetsnivå, jf. § 4, skal nås. Formålet med evalueringen er å fremskaffe et beslutningsgrunnlag for hvordan risikoene skal håndteres, jf. § 12, og, dersom håndteringen består av sikkerhetstiltak, hva tiltakene skal gå ut på, jf. § 13.

Departementet legger til grunn at virksomheten har, eller vil få tilgang til, nødvendig informasjon om relevante trusselaktører og hvordan disse opererer, for å kunne fastsette hva som er et forsvarlig sikkerhetsnivå for virksomhetens verdier, se nærmere omtale om temaet i punkt 4.3.

Formålet med kravet i *andre og tredje ledd* er å sikre at virksomhetens risikoforståelse er oppdatert, for igjen å kunne ta stilling til om risikoen må håndteres på en annen måte enn før.

Formålet med kravet i *fjerde ledd* er å gi ansvarlig departement en oversikt over avhengighetene i sin sektor og eventuelt på tvers av sektorer. På den måten vil departementet få et bedre grunnlag for å avgjøre hvilke virksomheter som er av betydning for grunnleggende nasjonale funksjoner.

7.3.2 Til § 12 Plikt til å håndtere risiko

Etter gjennomført vurdering av risiko skal det vurderes hvordan risiko skal håndteres. Det er ulike alternativer for risikohåndtering. Risikoen kan håndteres helt eller delvis ved at virksomheten unngår risikoen f.eks. ved å avhende en skjermingsverdig verdi, eller aksepterer den, f.eks. fordi kostnadene ved sikkerhetstiltak ikke står i et rimelig forhold til risikoreduksjonen. En annen måte å håndtere risikoen på er å sørge for at infrastrukturen er tilstrekkelig redundant. Bruk av sikkerhetstiltak vil være den mest vanlige måten å håndtere risiko, og vil nesten i ethvert tilfelle være en forutsetning for å oppnå et forsvarlig sikkerhetsnivå.

Det sentrale er imidlertid ikke *på hvilken måte* risiko håndteres, men *at* den håndteres på en slik måte at virksomheten oppnår et forsvarlig sikkerhetsnivå. Bestemmelsen inneholder et generelt krav til at risiko skal håndteres og må leses i sammenheng med kravene som stilles til de konkrete verdiene i §§ 20, 32, 45 og 53. Det vil være den skjermingsverdige verdiens betydning for grunnleggende nasjonale funksjoner (klassifiserings- og graderingsnivået) som vil være dimensjonerende for hva som er et forsvarlig sikkerhetsnivå og derav også hvilke krav som stilles til håndteringen.

Vi ber særlig om høringsinstansenes syn på denne innretningen. Departementet vil vurdere hensiktsmessigheten og utformingen av denne bestemmelsen.

7.3.3 Til § 13 Grunnsikringstiltak, påbyggingstiltak og tiltak for skadebegrensning og gjenopprettelse.

Dersom virksomheten, på bakgrunn av sin vurdering av risiko, velger å håndtere risikoen med bruk av sikkerhetstiltak skal det etableres grunnsikringstiltak. I tillegg skal virksomheten ha en plan for påbygningstiltak og tiltak for skadebegrensning og gjenopprettelse. Hvor stor betydning de skjermingsverdige verdien har for grunnleggende nasjonale funksjoner vil være avgjørende for hvilke grunnsikringstiltak som er nødvendig for å oppnå et forsvarlig sikkerhetsnivå, holdt opp mot den risiko virksomheten er utsatt for. Det innebærer at graderingsnivå på informasjonen, og klassifiseringsnivå av objekt eller infrastruktur, er sentralt hvor terskelen for å etablere tiltak ligger.

Formålet med å presisere dette i bestemmelsen er for å skape en tydeligere sammenheng mellom virksomhetens risikovurdering og kravene til håndtering av risiko i det generelle kapittelet og i kapitlene som regulerer de spesielle kravene som gjelder beskyttelse av informasjon, informasjonssystem, objekt eller infrastruktur.

Grunnsikringstiltak er sikkerhetstiltak som skal bidra til å ivareta det forsvarlige sikkerhetsnivået i en normaltilstand. Departementet har i *andre ledd bokstav a* valgt å inndele grunnsikringstiltakene på samme måte som i loven (fysiske, elektroniske, menneskelige og organisatoriske). Dette tilsvarer inndelingen av tiltak i NS 5830, men med den forskjell at det som i NS 5830 er nevnt som teknologiske tiltak, her er delt opp i hhv. fysiske og elektroniske tiltak.

Departementet mener at disse kravene til grunnsikringstiltak gjør seg like gjeldende for beskyttelse av informasjon og informasjonssystemer, og de bør derfor være overordnede krav til grunnsikringstiltakene til virksomheten.

Bestemmelsens *tredje ledd* gir virksomheten plikt til å tenke sikkerhet i alle stadier – fra planlegging og etablering, til avvikling og destruering. For virksomheter som planlegger for grunnsikringen *etter* at objektet er realisert, vil det kunne påløpe store kostnader. Det er vesentlig mer kostbart å bytte ut veggene i et rom, fordi det eksempelvis ikke egner seg for å behandle sikkerhetsgradert informasjon, etter at det allerede er satt opp. På samme måte må virksomheten sørge for planlegging av sikkerhet i forbindelse med utvikling og implementering av systemet, ikke etter at systemet er implementert i virksomheten.

Ved avvikling, enten det er et objekt som skal avhendes eller et system som skal tas ned eller destrueres, er det viktig å opprettholde et forsvarlig sikkerhetsnivå. Hensikten med å presisere dette er for å gjøre virksomheten bevisst på at det også er en fare for kompromittering dersom en annen virksomhet skal overta et objekt eller dersom man leverer fra seg systemer eller lagringsmedier til andre.

Fjerde ledd stiller krav om at virksomheten skal planlegge påbyggingstiltak som kan iverksettes dersom risikoen øker utover det som kan håndteres av grunnsikringstiltakene. Påbyggingstiltak er tiltak som kan iverksettes dersom det skjer en endring i risiko som virksomheten ikke har tatt høyde for i grunnsikringen. Planen vil normalt ha ulike nivåer alt ettersom hvor mye risikoen øker med. Plan for påbygningstiltak vil normalt omfattes av det som i dag inngår i beredskapsplaner.

Et eksempel kan være at virksomheten bruker sikre dører med et avansert elektronisk låssystem til alle adgangspunkter. Dette er et grunnsikringstiltak, og i en normalsituasjon er det tilstrekkelig at de ansatte åpner døren med sitt adgangskort. Dersom risikoen øker til nivå 1 (hvis virksomheten har nivåinndeling i sin plan for påbyggingstiltak) vil det innføres PIN-kode for å åpne dørene. Ved økning av risiko til et høyere nivå, vil det i tillegg innføres adgangsbegrensning. Ansatte får eksempelvis kun adgang til egne kontorer, og ikke andre steder i virksomheten.

Et annet eksempel kan være at terrorfaren øker betydelig for offentlige regjeringsbygg. Da kan det være at det blir utplassert sikringsstyrker fra Forsvaret eller politiet. Sikringsstyrker står imidlertid i en særstilling og er ikke noe en virksomhet skal planlegge for uten videre, men det illustrerer at påbyggingstiltak er noe som er ment å være midlertidig og noe ekstra utover det normale sikringsnivået.

Dersom det er grunn til å tro at den økte risikoen er varig, f.eks. som følge av trusselen virksomheten er utsatt for, eller det er svakheter i virksomhetens sikringstiltak, skal virksomheten vurdere om påbyggingstiltakene skal inngå i grunnsikringen. I visse tilfeller kan påbyggingstiltakene være kostnadskrevende, og kravet er ikke til hinder for at virksomheten heller iverksetter andre tiltak som skal inngå i grunnsikringen.

Femte ledd stiller krav til at virksomheten planlegger for tiltak for skadebegrensning og gjenopprettelse dersom en sikkerhetstruende hendelse til tross for grunnsikrings og påbygningstiltakene. Tiltakene må være egnet til å redusere skade, og gjenopprette sikringsnivået forut for den sikkerhetstruende hendelsen, jf. § 7.

7.3.4 Til § 14 Prinsipper ved valg og utforming av sikkerhetstiltak

Prinsippene i bestemmelsen er hovedsakelig en videreføring av prinsippene i kapittel 5 i forskrift om informasjonssikkerhet. Prinsippene gjelder per i dag kun for sikring av informasjonssystemer. Departementet er imidlertid av den oppfatning at dette er gode sikkerhetsprinsipper som bør gjelde generelt for sikring av alle skjermingsverdige verdier.

Prinsippet om minimalisme innebærer at virksomheten ikke skal iverksette tiltak som har annen funksjonalitet eller som er mer komplekse enn det som er nødvendig. For eksempel bør systemer for adgangskontroll ikke i unødvendig grad kobles til andre administrative systemer enn de som er nødvendige for å ivareta sikkerheten, rom som skal benyttes for sikker oppbevaring eller gradert tale bør ikke benyttes til å oppbevare materiell eller ha møter som ikke krever dette sikkerhetsnivået. Når sikre informasjonssystemer skal designes, vil det være lettere å sikre disse dersom det er tydelig gjennom prosessen hva systemene skal benyttes til og at de ikke designes for også å løse oppgaver som ikke krever et like høyt sikkerhetsnivå. Økt kompleksitet kan på sin side medføre økt sårbarhet.

Prinsippet om minste privilegium innebærer at det ikke skal gis mer omfattende tilgang til en skjermingsverdig verdi enn det som er strengt nødvendig for å ivareta en funksjon, eller for å gi tilgang til informasjon. Tjenstlig behov for tilgang skal være styrende. For eksempel skal ikke den jevne bruker av et informasjonssystem gis administratorrettigheter. Prinsippet er like viktig ved maskin til maskin kommunikasjon. I en fysisk sammenheng tilsier prinsippet i mange tilfeller at ikke alle ansatte i en bedrift skal ha tilgang til alle områder og kontorer hos virksomheten. Se for øvrig merknadene til myndighetsforskriften § 5 om adgangsklarering hvor betydningen av *tilgang* omtales nærmere.

Prinsippet om sikring i dybden innebærer at det skal være flere sikkerhetstiltak for å beskytte det samme. Formålet med prinsippet er at sikkerheten ikke skal være avhengig av bare ett sikkerhetstiltak. Det klassiske eksempelet er bruk av soner for beskyttelse av sikkerhetsgradert informasjon.

Prinsippet om motstandsdyktighet skal sikre at det ikke er mulig å svekke eller sette ut av funksjon flere sikkerhetstiltak med samme type handling.

Prinsippet om balansert styrke tilsier de ulike veiene til en skjermingsverdig verdi skal beskyttes like sterkt. F.eks. skal ikke et informasjonssystem med krav til passord for innlogging være tilgjengelig ved bruk av adgangskort alene.

Siste ledd har sitt utgangspunkt i lovens § 1-1 bokstav c om at «sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn». Med grunnleggende rettsprinsipper menes blant annet hensynet til den enkeltes personvern og rettssikkerhet. Presiseringen i bestemmelsen er for å tydeliggjøre at det kun skal brukes sikkerhetstiltak som er nødvendige og forholdsmessige. I dette ligger det en plikt til å vurdere alternative og mindre inngripende tilnærminger. Virksomheten må også dokumentere hvilke avveininger som er gjort mot personvernet til den enkelte i disse tilfellene.

7.3.5 Til Feil! Fant ikke referansekilden.§ 15 Krav om bruk av evaluerte produkter og tjenester

Enkelte typer tekniske produkter eller tjenester må evalueres før de kan tas i bruk. Formålet med evalueringen er å hindre at uvedkommende kan endre, fjerne eller få tilgang til høygradert informasjon eller skjermingsverdig objekt eller infrastruktur. Hensikten med dette er å sikre at virksomheten kan ha tillit til at de produktene eller tjenestene som *i seg selv har avgjørende betydning* for personer ikke skal få tilgang til informasjon i tråd med § 15 bokstav a eller b, eller skal kunne overta eller sette ut av drift infrastruktur eller objekter i tråd med bokstav c. Eksempler på dette vil blant annet være dioder, filtre, krypteringsmekanismer, adgangskontrollsystemer.

Evaluering gjennomføres ved bruk av forskjellige typer tester og undersøkelser. Omfanget av testene og undersøkelsene vil avhenge av i hvor høy gradering eller klassifiseringsnivå tjenesten eller produktet skal beskytte. F.eks. vil det være krav til grundige tester og undersøkelser for adgangskontrollsystemer som muliggjør tilgang til kjernefunksjonalitet i skjermingsverdig objekt eller infrastruktur, direkte tilgang til høyere gradert informasjon, eller til de krypteringsmekanismene som benyttes til å beskytte informasjon når det overføres over internettet.

7.3.6 Til § 16 Hvem som evaluerer produkter og tjenester

En evaluering av produkter eller tjenester må gjøres av en uavhengig tredjepart med nødvendig kompetanse. Departementet har derfor vurdert at evalueringen skal gjennomføres etter internasjonalt anerkjente kriterier og metoder som sikrer at alle trinn i prosessen blir gjennomført på korrekt måte. Det laboratorium som benyttes, skal være akkreditert av Norsk akkreditering før det kan gjennomføres evaluering.

For produkter eller tjenester som skal evalueres for flere brukere kan det være grunn til å dokumentere evalueringen ved bruk av sertifikat. Sertifikatet vil suppleres med en rapport som gir nærmere beskrivelser av sikkerhetsfunksjonalitet produktet eller tjenesten er evaluert ut i fra, hvilke tester og undersøkelser som er gjort og under hvilke forutsetninger sertifikatet er gitt.

7.3.7 Til § 17 Krav til sikkerhet i anskaffelser

Bestemmelsen stiller krav om at virksomheten må sørge for et forsvarlig sikkerhetsnivå i anskaffelser som gir leverandøren, eller personell fra leverandøren, mulighet til påvirke funksjonen til informasjonssystemet, objektet eller infrastrukturen. Det samme gjelder hvor det gis tilgang til skjermingsverdig informasjon.

Virksomheten må da avtale med leverandøren at denne forplikter seg til å følge de samme kravene for beskyttelse som gjelder for informasjonen, informasjonssystemet, infrastrukturen eller objektet som gjelder for virksomheten. Avtalen må også gi virksomheten mulighet til i undersøke om

leverandøren opprettholder kravene til beskyttelse. Bestemmelsen tilsvarer kravet til sikkerhetsavtale i § 9-2, men gjelder i tillegg for anskaffelser hvor leverandøren ikke i utgangspunktet skal få tilgang, men hvor leverandøren eksempelvis leverer komponenter eller lignende som skal inngå i et skjermingsverdig informasjonssystem objekt eller infrastruktur.

Bestemmelsen innebærer også at virksomheten må vurdere hvilken risiko det er forbundet med å la en leverandør f.eks. drifte og vedlikeholde et informasjonssystem. Virksomheten vil da risikere at funksjonen til systemet blir skadelidende, dersom leverandøren ikke kan levere vedlikeholdet, f. eks fordi denne går konkurs, eller der en utenlandsk leverandør blir nektet å levere tjenesten av myndighetene i sitt hjemland.

Dersom virksomheten kommer til at anskaffelsen vil medføre en ikke ubetydelig risiko, skal virksomheten varsle til departementet, jf. § 9-4 i loven, i tråd med § 18. Varslingsplikten inntrer ikke dersom virksomheten håndterer risikoen på en slik måte at den blir ubetydelig, se nærmere kapittel 4.6.4.

7.3.8 § Til § 18 Varslingsplikt om anskaffelser til skjermingsverdig informasjonssystem, objekt og infrastruktur

Bestemmelsen skal gi grunnlag for departementet til å vurdere den risikoen anskaffelsen innebærer for det aktuelle informasjonssystemet, objektet eller infrastrukturen, vurdere om denne er akseptabel holdt opp mot betydningen av informasjonssystemet, objektet eller infrastrukturen, og se hen til konsekvensene for virksomheten som er underlagt sikkerhetsloven. For den konkrete vurderingen departementet skal foreta vises det til sikkerhetsloven § 9-4, og Prop. 97 L (2015–2016), side 75-77. Relevante vurderingsmomenter vil bl.a. være om vi har et sikkerhetssamarbeid med det landet leverandøren kommer fra, hvilken tilknytning det er mellom leverandøren og hjemlandet, hvilke tilganger leverandøren eller personell fra leverandøren får til den skjermingsverdige informasjonen, infrastrukturen eller objektet, klassifiserings eller graderingsnivå til informasjonen, infrastrukturen og objektet, hvilke økonomiske konsekvenser stans av anskaffelsen vil få for virksomheten og om et stans av anskaffelsen vil gjøre det uforholdsmessig vanskelig å opprettholde funksjonen til informasjonssystemet, objektet eller infrastrukturen.

Det vil f.eks. kunne være aktuelt å benytte bestemmelsen ved kjøp av kritiske komponenter til skjermingsverdige informasjonssystemer, hvor leverandøren ikke skal få tilgang som gjør anskaffelsen til en sikkerhetsgradert anskaffelsen, men hvor komponenten kan inneholde en bakdør som vil kunne gi tilgang til systemet på et senere tidspunkt.

7.3.9 Til § 19 Unntak fra sikkerhetskrav

Bestemmelsen åpner for at det i særlige tilfeller kan gis unntak fra kravene til sikkerhet i denne forskriften, jf. sikkerhetsloven §§ 5-2 andre ledd og 6-2 andre ledd. Det er på nåværende tidspunkt uklart hvordan kravene i forskriften vil treffe de ulike sektorene, og i enkelte tilfeller kan det for eksempel være behov for å gjøre konkrete tilpasninger mellom ulike eksisterende sikkerhetsregimer som gjør det nødvendig å gjøre unntak fra kravene i forskriftene.

Første ledd fastsetter terskelen for når det vil være aktuelt med unntak. Dersom oppfyllelsen av kravene i forskriften vil være *uforholdsmessig byrdefullt*, kan det gjøres unntak. Dette vil for eksempel kunne være de tilfellene hvor oppfyllelsen av sikkerhetskravene medfører at det går så hardt ut over virksomheten at den ikke lenger kan fungere slik den skal. Det fremgår av lovproposisjonen kapittel 10.5.2.2 at behovet for unntak må begrunnes godt, og det må vurderes

kompenserende tiltak. Hensikten er ikke å lempe på sikkerhetskravene, men å gjøre det mulig å få til tilpassede løsninger.

Både NSM og sektortilsyn kan gi slike unntak. For unntak fra sikkerhetskrav knyttet til beskyttelse av sikkerhetsgradert informasjon er imidlertid denne kompetansen lagt til sikkerhetsmyndigheten.

7.4 Til kapittel 3 Beskyttelse av skjermingsverdig informasjon

7.4.1 Til § 20 Forsvarlig sikkerhetsnivå for skjermingsverdig informasjon

Bestemmelsens *første ledd* stiller krav til hva som vil være et forsvarlig sikkerhetsnivå for sikring av skjermingsverdig informasjon. Informasjonen skal beskyttes slik at den ikke med enkle midler kan endres, gå tapt, gjøres utilgjengelig eller bli kjent for uautoriserte personer. Første ledd første punktum dreier seg om beskyttelse av integritet og tilgjengelighet, mens andre punktum dreier seg om beskyttelse av konfidensialitet.

Første ledd andre punktum vil i praksis først og fremst gjelde for informasjon som er gradert BEGRENSET, ettersom høyere gradert informasjon skal sikres bedre, jf. tredje ledd. Informasjon som ikke sikkerhetsgraderes, jf. loven § 5-3, kan ha behov for konfidensialitetsbeskyttelse av andre grunner enn nasjonal sikkerhet, men dette reguleres ikke av sikkerhetsloven. Dette innebærer at virksomheten må håndtere risikoen på en slik måte at en trusselaktør ikke kan kompromittere informasjon enten ved vilkårlig tilgang, eller ved å kun ta i bruk utstyr, teknikker eller tjenester som ikke er spesielt tilpasset virksomheten som er målet for den sikkerhetstruende virksomheten. Motsetningen til dette vil for eksempel være der fremmed etterretning benytter en skadevare de har tilpasset for å trenge inn i systemene til den konkrete virksomheten de skal ramme.

Hva som er enkle midler vil imidlertid kunne være ulikt ut fra hva slags type sikkerhetstruende virksomhet virksomheten må beskytte seg mot. Det er for eksempel forskjell på hvilke midler som benyttes ved utøvelse av sabotasje og for spionasje. Det er viktig at bestemmelsen leses i forlengelsen av de generelle kravene i kapittel 2 og særlig kravet til vurdering av risiko, jf. § 11. Det er virksomhetens vurdering av risiko som vil være avgjørende for hvilke tiltak som er nødvendig for å oppnå et forsvarlig sikkerhetsnivå. Virksomheten må basert på dette tilstrebe en symmetri mellom verdiene, sikkerhetstiltakene og truslene. Det vil si at tiltakene må stå i et rimelig forhold til de trusselaktørene og deres metoder som virksomheten mener de bør beskytte verdiene mot.

Det er i den sammenheng viktig å påpeke at også trusselaktører vil ha begrensede ressurser og måtte gjøre prioriteringer. Trusselaktøren vil også vurdere hvor stor risiko de må ta for å lykkes. Sikkerhetstiltakene bør optimalt sett være på et slikt nivå at trusselaktørene opplever kostnaden som større enn nytten ved å kompromittere informasjonen.

Sikkerhetsloven § 5-3 opererer med grader av konfidensialitetsbehov. Integritets- og tilgjengelighetsbehov er ikke tilsvarende gradert i loven. Det følger likevel av lovens og forskriftens system at sikkerhetstiltakene skal være tilpasset den konkrete risikoen. Er det viktig nok at en viss type informasjon skal være tilgjengelig, må sikringsnivået være deretter. Det innebærer at også ved beskyttelse av tilgjengelighet kan det være nødvendig å sikre seg mot avanserte aktører. Det vil antakelig kunne være særlig aktuelt i en digital kontekst der det er svært viktig at et kommunikasjonssystem eller informasjonssystem fungerer som det skal.

Bestemmelsens *andre ledd* er et uttrykk for lovens intensjon om at informasjonens konfidensialitet, integritet og tilgjengelighet må ses i sammenheng og avveies mot hverandre. Sikkerhetsloven sidestiller i større grad enn i dag behovet for å beskytte disse tre egenskapene. Det vil kunne forekomme tilfeller hvor behovet for tilgjengelighet er større enn behovet for konfidensialitet.

Virksomheten må foreta en konkret helhetsvurdering av de ulike hensynene og spørre seg hva som totalt sett er viktigst av hensyn til nasjonal sikkerhet. Dette kan innebære at deling av informasjonen er så viktig at skjermingskravene som gjelder for det aktuelle sikkerhetsgraderingsnivået ikke kan følges fullt ut.

Til forskjell fra dagens forskrift om informasjonssikkerhet stilles det ikke ytterligere detaljerte krav for beskyttelse av informasjon gradert BEGRENSET. Det har vært ulikt syn i arbeidsgruppen på hvorvidt det bør være mer detaljerte krav for å unngå at sikkerhetsgradert informasjon får et for lavt sikringsnivå. Sikkerhetsloven får et bredere nedslagsfelt enn tidligere, noe som medfører at flere private virksomheter blir underlagt og mer informasjon blir gradert BEGRENSET. Med detaljerte krav øker faren for at virksomhetene unngår å sikkerhetsgradere informasjonen i takt med antall virksomheter. Departementet mener derfor at virksomhetene bør gis større grad av fleksibilitet for beskyttelse av informasjon på det laveste graderingsnivået, for å sikre at virksomhetene gjør den vurderingen av risiko og iverksetter de tiltak som er nødvendig. Dette har også sammenheng med at den teknologiske utviklingen gjør det vanskelig å fastsette flere detaljerte krav på dette nivået.

Departementet vil imidlertid understreke at dette ikke er ment å være en realitetsendring sammenlignet med dagens krav til BEGRENSET. Det vil imidlertid bli opp til virksomheten hvilke tiltak som må være på plass for å sikre denne typen informasjon. Departementets vurdering er at det vil gi tilstrekkelig føring for virksomheten at informasjonen, basert på en vurdering av risiko, skal sikres mot kompromittering ved bruk av enkle midler med tiltak som velges og utformes i tråd med prinsippene i § 14.

7.4.2 Til § 21 Destruering av dokumenter og lagringsmedier med sikkerhetsgradert informasjon

Bestemmelsen er i all hovedsak en videreføring av gjeldende § 4-34 og § 4-36 om tilintetgjøring og metoder for tilintetgjøring. Kravet er nå funksjonelt beskrevet og ikke så detaljert som tidligere. Virksomheten kan selv bestemme hvilken metode som benyttes for å destruere informasjon gradert BEGRENSET, så lenge kravet i bestemmelsen oppfylles. For destruering av informasjon gradert KONFIDENSIELT eller høyere må imidlertid virksomheten bruke en metode som er godkjent av NSM.

7.4.3 Til § 22 Evakuering og ekstraordinær destruering i nødsituasjoner

Bestemmelsen er i hovedsak en videreføring av gjeldende § 4-35 i forskrift om informasjonssikkerhet, men er vesentlig mindre detaljert enn dagens bestemmelse. Virksomheten må lage en plan for evakuering og destruering av eventuelle dokumenter og lagringsmedier med skjermingsverdig informasjon i en nødsituasjon. Hensikten er å sikre at sikkerhetsgradert informasjon ikke blir kjent for uvedkommende, for eksempel hvis en utenriksstasjon blir overtatt av en fremmed stat.

Hvilke dokumenter og lagringsmedier som bør prioriteres og hvilke nødsituasjoner virksomheten skal ta utgangspunkt i for sin plan, må basere seg på en vurdering av risiko.

7.4.4 Til § 23 Utlevering av sikkerhetsgradert informasjon til fremmede stater og internasjonale organisasjoner

Bestemmelsen er en videreføring av gjeldende § 3-2 i forskrift om informasjonssikkerhet.

Hva en stat er forpliktet til å følge opp overfor en annen stat, skal fremgå av en avtale med den andre staten. Det er imidlertid noe ulike sikkerhetskrav i ulike land, og dermed ikke et identisk sikkerhetsnivå mellom landene, selv for samme graderingsnivå. Innholdet i slike avtaler vil derfor variere noe. De viktigste nasjonale sikkerhetskravene vil imidlertid følge av avtalene. Det er f.eks.

praksis at det i slike avtaler fremgår at sikkerhetsklareringer gitt av den ene staten kan legges til grunn for tilgang til den andre statens sikkerhetsgraderte informasjon, samt krav til hvordan dokumenter og informasjonssystemer med sikkerhetsgradert informasjon skal beskyttes.

Bestemmelsen stiller krav til at det må foreligge en sikkerhetsavtale mellom Norge og den aktuelle staten eller organisasjonen dersom det skal gis tilgang til sikkerhetsgradert informasjon. I tillegg må det å gi tilgang være i samsvar med nasjonale sikkerhetsinteresser. Et eksempel er der utenlandske militære styrker, for å kunne delta på en øvelse i Norge med det norske forsvaret, må ha tilgang til informasjon om øvelsen som har norsk sikkerhetsgradering. Et annet eksempel er der norske myndigheter i et møte eller løpende strategisk samarbeid med en annen stat skal utveksle sikkerhetsgradert informasjon om sikkerhetspolitiske forhold.

Andre ledd stadfester at det er sikkerhetsavtalen mellom landende som er utgangspunktet for hvordan myndighetene, en virksomhet eller internasjonal organisasjon i en annen stat skal behandle informasjonen.

Tredje ledd åpner for at det kan gjøres unntak fra krav til sikkerhetsavtale ved deling av informasjon med fremmed stat eller internasjonale organisasjoner. Det foreligger noen særlig behov i forsvars- og justissektoren som medfører at det kan være aktuelt å dele informasjon med land som Norge ikke har sikkerhetsavtale med. For eksempel vil det forekomme tilfeller hvor EOS-tjenestene må dele etterretningsinformasjon med andre land av hensyn til nasjonale sikkerhetsinteresser.

7.4.5 Til § 24 Korresponderende sikkerhetsgrader

Bestemmelsens *første ledd* pålegger virksomheten å ha prosedyrer som sikrer at utenlandsk informasjon som er sikkerhetsgradert, blir sikret like godt som norsk sikkerhetsgradert informasjon.

Andre ledd er en videreføring av gjeldende § 2-8 i forskrift om informasjonssikkerhet.

7.4.6 Til § 25 Kryptering

Bestemmelsen stiller krav til at virksomheten skal kryptere sikkerhetsgradert informasjon som sendes elektronisk ut av område virksomheten kontrollerer. Dette innebærer at dersom informasjonen på et tidspunkt befinner seg utenfor virksomhetens område, enten fordi det er lagret i sky eller er i transitt mellom to lokasjoner, så skal den krypteres.

Andre ledd stiller krav til at virksomheten som hovedregel også skal kryptere sikkerhetsgradert informasjon som er lagret hos virksomheten, det vil si, innenfor området virksomheten kontrollerer. Dette kravet gjelder imidlertid ikke dersom virksomheten har etablert andre sikkerhetstiltak som sikrer informasjonen på en tilstrekkelig måte. Bruk av godkjent kryptering for lagring av sikkerhetsgradert informasjon vil si at dette kan lagres som om det var ugradert og slik kompensere for behov for andre tiltak som adgangskontroll og fysiske barrierer.

Tredje ledd stiller krav til sikring av kryptomateriellet. Kryptomateriellet inkluderer hardware eller software som krypterer og dekrypterer informasjonen, kryptoalgoritmen, kryptonøkkelen og eventuell dokumentasjon som beskriver dette. Kryptomateriellet skal sikres i tråd med verdien på informasjonen, som materiellet er ment å beskytte. Det vil i enkelte tilfeller ikke være nok å se til graderingsnivået på informasjonen, man må også vurdere omfanget av informasjonen som er beskyttet og at en trusselaktør vil kunne få tilgang til dette over lang tid om krypteringen er kompromittert. Dette betyr at kravet må leses i sammenheng med bestemmelsene i kapittel 2 om generelle krav til sikring, kapittel 3 om beskyttelse av skjermingsverdig informasjon, kapittel 5 om beskyttelse av informasjon gradert KONFIDENSIELT eller høyere og kapittel 6 om beskyttelse av

informasjonssystemer. Utgangspunktet for sikring av kryptomateriell vil være virksomhetens vurdering av risiko, jf. § 11. Der hvor materiell er sikret i seg selv gjennom manipulasjonssikring eller lignende mekanismer, kan det kompensere for andre sikringstiltak.

Kryptosystemet skal godkjennes av NSM, jf. sikkerhetsloven § 5-6 første ledd. Som nasjonal forvalter av kryptomateriell skal NSM, som en del av godkjenningen, stille krav til hvordan materiellet skal brukes, driftes og forvaltes. Bakgrunnen for dette er at det finnes mange forskjellige kryptosystemer, som vil kunne ha ulike krav til bruk, drift og forvaltning. Hvilke krav som bør stilles vil også kunne avhenge av hvordan materiellet er implementert i informasjonssystemet og sikkerhetsgraderingen og omfanget av informasjonen som skal beskyttes.

Dersom virksomheten skal kryptere informasjon gradert KONFIDENSIELT eller høyere ser departementet det som nødvendig at NSM bestemmer hvilke materiell som benyttes, både av hensyn til bruk av nasjonalt kryptomateriell, og NATOs krav til kryptering av gradert materiell. For informasjon gradert BEGRENSET kan det godkjennes kommersielle software- eller hardwareprodukter på bakgrunn av at de har nødvendig sertifisering og implementeres etter NSMs anbefalinger.

7.5 Til kapittel 4 Sikkerhetsgradering og merking

7.5.1 Til § 26 Merking av dokumenter og lagringsmedier som inneholder sikkerhetsgradert informasjon

Bestemmelsen *første ledd* stiller krav til merking av de graderte dokumentene. Det som er viktig er at det er tydelig for de som leser/hører/ser informasjonen hvilket nivå det er gradert på og at det er gjenkjennbart for alle som skal håndtere informasjonen. Det er også hensiktsmessig at det står hvor lenge graderingen varer.

Bestemmelsens *andre ledd* er hovedsakelig en videreføring av krav i gjeldende forskrift om informasjonssikkerhet § 2-3 første ledd, men med en mer funksjonell innretning. Delgradering innebærer at virksomheten må vurdere om innholdet i eksempelvis forskjellige kapitler, avsnitt eller vedlegg gjør at disse må graderes med forskjellige graderingsnivå.

I motsetning til gjeldende rett er det ikke tatt inn et eksplisitt krav om at journaler ikke skal sikkerhetsgraderes høyere enn nødvendig. Departementet mener at dette følger av hovedregelen om at informasjon ikke skal sikkerhetsgraderes høyere enn nødvendig.

I *tredje ledd* fremgår det at sikkerhetsgradert informasjon skal merkes før utlevering til andre stater eller internasjonale organisasjoner. Hensikten med bestemmelsen er dels at det skal fremgå tydelig hvilken informasjon som kan utleveres i slike tilfeller. Hvem som kan beslutte utlevering er ikke fastsatt eksplisitt i bestemmelsen, da det er avhengig av hvilken type informasjon det gjelder og hvem motparten er. Normalt vil dette være virksomhetens leder. I noen tilfeller for eksempel der det følger av internasjonale avtaler, vil det kunne være nødvendig med tillatelse fra departementet e.l.

7.5.2 Til § 27 Sikkerhetsgradering ut over 30 år

Bestemmelsen er i hovedsak en videreføring av gjeldende rett om unntak for automatisk avgradering i forskrift om informasjonssikkerhet § 2-6.

Hovedregelen i sikkerhetsloven er at sikkerhetsgraderingen skal tidsbegrenses, og at informasjonen blir automatisk avgradert etter 30 år dersom ikke annet er bestemt.

Det foreligger imidlertid tilfeller hvor det kan være behov for beskyttelse utover 30 år. Dette kan være der informasjonen dreier seg om forholdet til fremmede makter, kritisk infrastruktur, beredskapsplaner, kryptosikkerhet, og kilder og metoder i etterretnings-, overvåkings- og sikkerhetstjeneste. For å sikre at ikke virksomheten kan bestemme å sikkerhetsgradere et dokument på ubestemt tid, videreføres plikten til å revurdere sikkerhetsgraderingen hvert tiende år.

Departementet har ikke funnet det hensiktsmessig å videreføre gjeldende rett om tidsbegrenset gradering i forskrift om informasjonssikkerhet § 2-4. Sikkerhetsloven stiller krav til at informasjon ikke skal sikkerhetsgraderes for lengre tid enn det som er nødvendig. Det innebærer at virksomheten i hvert enkelt tilfelle må vurdere hvor lang tid den aktuelle informasjonen skal være sikkerhetsgradert. Det er ikke ønskelig å angi en hovedregel slik det gjøres i dagens bestemmelse med henvisning til normal tidsangivelse for sikkerhetsgradering i 2-5 år. Hovedregelen er «ikke lenger enn nødvendig», noe som kan være en dag, en uke, ett år eller 10 år.

7.5.3 Til § 28 Omgradering av sikkerhetsgradert informasjon

Bestemmelsen er i hovedsak en videreføring av gjeldende § 2-10 i forskrift om informasjonssikkerhet og stiller krav til når virksomheten skal vurdere om den sikkerhetsgraderte informasjon skal gis et høyere eller lavere nivå, eller om informasjonen skal avgraderes.

7.5.4 Til § 29 Hvem som kan omgradere

Bestemmelsen er i hovedsak en videreføring av gjeldende § 2-11 i forskrift om informasjonssikkerhet og stiller krav til hvem som kan omgradere informasjonen.

7.5.5 Til § 30 Plikt til å informere om behov for eller avgjørelse om omgradering

Bestemmelsen er i hovedsak en videreføring av gjeldende § 2-12 i forskrift om informasjonssikkerhet og stiller krav til at virksomheten skal underrette utsteder dersom sikkerhetsgraderingen er feil.

7.5.6 Til § 31 Prosedyrer ved henvendelse om innsyn etter offentleglova eller forvaltningsloven

Bestemmelsen er i hovedsak en videreføring av gjeldende § 2-13 i forskrift om informasjonssikkerhet og stiller krav til prosedyrer ved henvendelse om innsyn i sikkerhetsgradert informasjon.

7.6 Til kapittel 5 Beskyttelse av informasjon gradert KONFIDENSIELT eller høyere

7.6.1 Innledning

Kapittelet må leses i forlengelsen av de generelle kravene i kapittel 2 og de mer generelle regler for beskyttelse av skjermingsverdig informasjon i kapittel 3. I dette kapittelet stilles det noen særskilte krav til virksomheten dersom den behandler informasjon som er gradert KONFIDENSIELT eller høyere. Det innebærer at kravene i dette kapittelet *ikke* kommer til anvendelse dersom en virksomhet bare har informasjon gradert BEGRENSET eller dersom informasjon er skjermingsverdig, men ikke sikkerhetsgradert.

7.6.2 Til § 32 Forsvarlig sikkerhetsnivå for informasjon gradert KONFIDENSIELT eller høyere

Bestemmelsens stiller krav til hva som vil være et forsvarlig sikkerhetsnivå for sikring av informasjon gradert KONFIDENSIELT eller høyere.

Tiltakene for beskyttelse av informasjon gradert KONFIDENSIELT skal være egnet til at virksomheten oppdager at informasjonen er kompromittert. Det må altså etableres tiltak som gjør det mulig å oppdaget om en trusselaktør har fått tak i informasjonen. Et eksempel på dette vil kunne være

videoovervåking eller fysiske eller elektroniske barrierer som etterlater tydelige spor dersom noen har kommet seg forbi disse.

For informasjon gradert HEMMELIG skal virksomheten i tillegg til å oppdage at kompromittering har skjedd, også gjøre slik at virksomheten oppdager kompromitteringen i tide til å begrense skadefølgene. Dette innebærer ikke et absolutt krav til at virksomheten faktisk skal klare å begrense skadefølgene, men *tiltakene* må sette virksomheten i stand til å gjøre dette. For eksempel innebærer dette at virksomheten må ha tiltak som varsler virksomheten om at noe uønsket er i ferd med å skje, slik at virksomheten rekker å reagere i tide. Dette kan være et alarmsystem eller lignende.

For informasjon gradert STRENGT HEMMELIG skal det ikke være mulig for en trusselaktør å få tak i informasjonen. Dette kan oppnås ved at man har en kombinasjon av barrierer, deteksjon, verifikasjon og reaksjon som til sammen setter virksomheten i stand til å avverge kompromittering, for eksempel ved at destruksjon av dokumenter eller lagringsmedier vil kunne iverksettes og utføres før en trusselaktører har brutt seg gjennom barrierene eller at man kan reagere med vaktstyrker i tide til å stoppe eller forsinke kompromittering. Tidsregnskap og øvelser vil være viktige virkemidler for å kunne verifisere at man har de nødvendige tiltakene.

Hvor omfattende tiltak en virksomhet må etablere for å ha et forsvarlig sikkerhetsnivå må vurderes på bakgrunn av vurderingen av risiko som gjøres i forkant.

7.6.3 Til § 33 Sending av informasjon gradert KONFIDENSIELT eller høyere

All fysisk forsendelse av informasjon gradert KONFIDENSIELT eller høyere skal sendes med kurer. Dette er en reell innstramming fra gjeldende rett. Dagens § 4-19 i forskrift om informasjonssikkerhet åpner for forsendelse ved registrert postsending både av HEMMELIG og KONFIDENSIELT informasjon. Dette anses ikke lenger som sikkert nok. Når gjeldende forskrift om informasjonssikkerhet trådte i kraft i 2001 ble posten driftet fullt og helt av staten. Siden den gang har postverket utviklet seg, og i 2016 ble det norske postmarkedet åpnet for full konkurranse. Videre henter de fleste posten på sin nærmeste dagligvarebutikk, noe som medfører betydelig grad av usikkerhet knyttet til håndtering av dokumenter eller lagringsmedier som inneholder høyere gradert informasjon. På bakgrunn av dette har departementet kommet til at eneste metode for fysisk forsendelse av denne typen er med kurer, også ved forsendelse til utlandet. Ved forsendelse til utlandet gjelder imidlertid noen tilleggskrav som følger av bestemmelsen om krav til forsendelse med kurer.

Dersom det er mulig å sende informasjonen elektronisk via et godkjent informasjonssystem vil det i mange tilfeller være å foretrekke.

7.6.4 Til § 34 Pakking av informasjon gradert KONFIDENSIELT eller høyere

Bestemmelsen er i hovedsak en videreføring av gjeldende § 4-20 i forskrift om informasjonssikkerhet. Den er imidlertid noe mindre detaljert og funksjonelt utformet og gjelder kun ved forsendelse av informasjon gradert KONFIDENSIELT eller høyere. Bestemmelsen gjelder ikke for informasjon gradert BEGRENSET. Det betyr imidlertid ikke at denne typen informasjon kan sendes helt åpent med posten, men det blir opp til virksomheten å vurdere hva som i det enkelte tilfelle vil være et forsvarlig sikkerhetsnivå ved forsendelse av BEGRENSET informasjon.

7.6.5 Til § 35 Krav til oversikt over informasjon gradert KONFIDENSIELT eller høyere

Bestemmelsen gjelder i tillegg til bestemmelser om journalføringsplikten i arkivlova med tilhørende forskrift. Departementet er imidlertid av den oppfatning at det ikke er behov for å presisere dette i forskriften, slik det gjør i dagens forskrift om informasjonssikkerhet § 4-10.

Bestemmelsen går bort fra dagens detaljerte bestemmelser om journalføring i dagens forskrift om informasjonssikkerhet kapittel 4 del B. Det sentrale er at virksomheten til enhver tid har oversikt over hvor deres høyere gradert informasjon befinner seg. Om dette føres i en egen journal eller ikke er opp til virksomheten, men vil nok være det mest naturlige for mange.

For ut- og inngående dokumenter i offentlig forvaltning følger journalføringsplikten i tillegg av arkivlova. Arkivlova gjelder imidlertid ikke for private virksomheter eller interne dokumenter. Dette er en endring fra dagens krav om journalføring av inn- og utgående dokumenter gradert BEGRENSET og for interne dokumenter gradert KONFIDENSIELT. Det stilles heller ikke noe eksplisitt krav til et medieregister. Departementets vurdering er at dette dekkes av kravet til å ha oversikt. Det innebærer at virksomheten nødvendigvis må ha oversikt over hvilken informasjon som til enhver tid befinner seg på de ulike lagringsmediene.

7.6.6 Til § 36 Soneinndeling av informasjon gradert KONFIDENSIELT eller høyere

Bestemmelsen er i hovedsak en videreføring av gjeldende rett § 6-3 i forskrift om informasjonssikkerhet og stiller krav til etablering av soner. Kravet til soneinndeling gjelder imidlertid ikke for informasjon som er skjermingsverdig, men ikke sikkerhetsgradert eller for informasjon gradert BEGRENSET, slik det er i dag. Hensikten med dette er både å legge seg nærmere NATO, som ikke stiller krav til soner for NATO RESTRICTED. I tillegg fremstår det som noe uhensiktsmessig å pålegge denne typen detaljerte krav for lavere gradert informasjon. Det er i den sammenheng viktig å påpeke at det blant annet fortsatt gjelder krav til både tilgangskontroll og autorisasjon også for BEGRENSET, jf. prinsippet om minste privilegium og sikkerhetsloven § 8-1.

Alle virksomheter som oppbevarer eller tilvirker informasjon gradert KONFIDENSIELT eller høyere plikter å dele inn sine lokaler i soner. Områdene skal defineres som henholdsvis kontrollert, beskyttet eller sperret – hvorav kontrollert er det minst vitale og sperret mest sensitivt. Kravet til sperret sone gjelder imidlertid ikke uten videre. Det er kun dersom virksomheten har et område hvor det gis direkte tilgang til informasjon gradert KONFIDENSIELT eller høyere at det skal etableres en sperret sone.

Inndeling i avgrensede soner er av grunnleggende betydning for å kunne ivareta kravene til sikring på en hensiktsmessig måte. Det er av stor viktighet at denne inndelingen, som blant annet innebærer restriksjoner for den enkeltes adgangsrettigheter, er vel forankret i virksomheten og at den er hensiktsmessig utformet slik at administrasjonen av tilgangsrettigheter blir oversiktlig og enklest mulig.

7.6.7 Til § 37 Kontrollert sone

Bestemmelsen er i hovedsak en videreføring av forskrift om informasjonssikkerhet § 6-7. Kontrollert sone vil typisk være et område som omgir beskyttet og sperret sone. Kontrollert sone fungerer ofte som en buffersone mellom område med allmenn ferdsel og de rom hvor det behandles gradert informasjon ved at adgang skal begrenses til de som har et tjenstlig behov for opphold.

7.6.8 Til § 38 Beskyttet sone

Bestemmelsen er i hovedsak en videreføring av forskrift om informasjonssikkerhet § 6-8.

Første ledd stiller krav om at sonen skal ha en fysisk avgrensning der sikkerhetstruende virksomhet skal kunne oppdages. En slik avgrensning vil normalt være en bygning, men kan (spesielt i Forsvaret) også være en kontainer, et telt, et rom på et fartøy eller et kjøretøy. Et uteområde bare omgitt av et

gjerde vil antakelig ikke tilfredsstille kravet fordi det vil være mulig å få adgang over gjerdet eller fra luften.

Den vanligste formen for beskyttet område er kontorlokaler der personellet behandler sikkerhetsgradert informasjon. Den sikkerhetsgraderte informasjonen skal ivaretas av den enkelte, og papirer eller harddisker låses inn i godkjente oppbevaringsenheter når brukeren ikke er tilstede. En godkjent oppbevaringsenhet kan for eksempel være et skap godkjent for informasjon gradert KONFIDENSIELT. Disse vil ofte være av et visst materiale og ha en personlig kode slik at det kun er den enkelte som har mulighet til å komme inn i skapet.

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

Personer med permanent adgang til beskyttet sone vil for eksempel være de med egen nøkkel-/adgangskort og som kan ferdes fritt alene.

Fjerde ledd stiller krav til at virksomheten skal ha kontroll med adgangen til beskyttet sone. Dette innebærer ikke nødvendigvis at virksomheten må installere et elektronisk adgangskontrollsystem, men at man har et system/rutine som sikrer at ikke andre enn de som skal ha tilgang, som får tilgang. At det skal være synlig hvem som har permanent adgang til området vil for eksempel kunne gjøres ved å ha ulike fargekoder på adgangskort.

7.6.9 Til § 39 Sperret sone

Sperret sone defineres i forskriften som sone hvor adgang gir direkte tilgang til informasjon gradert KONFIDENSIELT eller høyere. Det vil si at dersom virksomheten har et område hvor det er mulig å få en slik direkte tilgang skal det etableres som en sperret sone, og beskytte det deretter.

Typiske sperrede soner er arkiver og dokumenthvelv, operasjonsrom, kommunikasjons- og serverrom eller lokaler der det lages sikkerhetsgraderte produkter. Dette er altså rom hvor sikkerhetsgradert informasjon er åpent eller lett tilgjengelig for den som har adgang. Felles for disse rommene er at det personellet som gis adgang skal være sikkerhetsklarert og autorisert for den informasjonen og det utstyret som er i rommet.

I motsetning til gjeldende § 6-9 i forskrift om informasjonssikkerhet, stilles det ingen detaljerte krav til hvordan informasjonen skal beskyttes i sonen. Kravet til sikring av sonen må leses i lys av de generelle kravene for beskyttelse av informasjon gradert KONFIDENSIELT eller høyere, jf. § 32.

Fjerde ledd stiller krav til at virksomheten skal ha kontroll med adgangen til beskyttet sone. Dette innebærer ikke nødvendigvis at virksomheten må installere et elektronisk adgangskontrollsystem, men at man har et system/rutine som sikrer at ikke andre enn de som skal ha tilgang, som får tilgang.

7.6.10 Til § 40 Behandling av informasjon gradert KONFIDENSIELT eller høyere

Bestemmelsen stiller krav til at sikkerhetsgradert informasjon som hovedregel skal behandles i beskyttet sone eller sperret sone.

Det vil imidlertid være tilfeller hvor det ikke er mulig for virksomheten å behandle informasjonen i de aktuelle sonene. Dette vil særlig være aktuelt i militære øvelser eller operasjoner. Bestemmelsen åpner derfor for at den sikkerhetsgraderte informasjonen kan tas med utenfor sonene dersom

virksomheten, basert på en vurdering av risiko, finner det tilrådelig. Dersom virksomheten beslutter at informasjonen kan tas med utenfor sonene skal det iverksettes kompenserende tiltak som ivaretar informasjonens konfidensialitet, integritet og tilgjengelighet i tråd med forslaget til § 32.

Selv om *første ledd* kun gjelder for dokumenter eller lagringsmedier med sikkerhetsgradert informasjon så vil *andre ledd* også gjelde for de tilfellene hvor informasjonen befinner seg på et informasjonssystem. Det er ikke et eksplisitt krav om at systemet må oppbevares i beskyttet eller sperret sone, men dersom man behandler informasjonen utenfor, også på et system, må virksomheten iverksette nødvendige kompensatoriske tiltak.

Tredje ledd bestemmer at virksomheten kun kan ta med dokumenter eller lagringsmedier med informasjon utenlands dersom det er til NATO-land eller land Norge har sikkerhetsavtale med, og det er mulig å deponere informasjonen på en norsk utenriksstasjon. Dersom informasjonen skal tas med til land utenfor NATO eller som vi ikke har sikkerhetsavtale med, må den sendes med kurer som diplomatisk post, jf. forslaget til § 43. Dersom informasjonen befinner seg på et informasjonssystem i utlandet, vil det være godkjenningen av informasjonssystemet som angir hvordan informasjonen i systemet skal behandles.

7.6.11 Til § 41 Særlige krav for informasjon gradert HEMMELIG eller høyere

Bestemmelsen stiller noen særlige krav til dokumenter eller lagringsmedier med informasjon gradert HEMMELIG eller STRENGT HEMMELIG. Når dokumenter eller lagringsmedier skal fordeles eller lånes ut skal låntaker bekrefte at den er mottatt. Det er viktig at virksomheten til enhver tid har oversikt over hvem som har informasjonen slik at denne ikke kommer på avveie.

Andre ledd stiller krav ved destruering. Dersom virksomheten skal destruere informasjon gradert HEMMELIG eller STRENGT HEMMELIG, skal denne kontrolleres og bekreftes av minst to personer. Bakgrunnen for dette er i likhet med kravet i første ledd at virksomheten skal ha oversikt over informasjonen. At det skal være to personer som skal kontrollere og bekrefte har sammenheng med at NATO stiller dette som krav for destruering av NATO SECRET informasjon.

7.6.12 Til § 42 Rapportering av informasjon gradert STRENGT HEMMELIG

Bestemmelsen er i hovedsak en videreføring av forskrift om informasjonssikkerhet § 4-39.

7.6.13 Til § 43 Krav til forsendelse med kurer

Bestemmelsen viderefører delvis tilsvarende krav i gjeldende forskrift på området.

Det som er endret er at bestemmelsen i gjeldende forskrift på området om at NSM skal godkjenne virksomheter som utfører kurerposttjeneste, ikke videreføres. Begrunnelsen for endringen er at så lenge virksomheter sender kurerposten i samsvar med kravene for øvrig i paragrafen, anser prosjektgruppen at det ikke er nødvendig at sikkerhetsmyndigheten i tillegg må godkjenne virksomheten som utfører tjenesten. Det er også slik at virksomhetens ansatte selv kan utføre kurertransporten så lenge kurersertifikatet er utstedt av rette myndighet.

Når det gjelder den delen av bestemmelsen som gjelder godkjenning av private virksomheter som utfører kurerposttjenester, er begrunnelsen for ikke å videreføre bestemmelsen, at tilvarende gjeldende bestemmelse, så vidt departementet er kjent med, ikke har blitt anvendt noen gang i løpet av de 17 årene den har eksistert. Et eventuelt fremtidig behov for kommersielle kurerposttjenester kan håndteres ved å heller anvende bestemmelsene for sikkerhetsgraderte anskaffelser til å stille krav til utførelsen av tjenesten.

7.6.14 Til § 44 Beskyttelse av rom og lokaler for tale gradert KONFIDENSIELT eller høyere

Bestemmelsen er i hovedsak en videreføring av beskyttelsesnivået i dagens regelverk, men det stilles funksjonelle krav til beskyttelse av rommet eller lokalet. Kravet bør sees i sammenheng med kravene i kapittelet om styringssystem for sikkerhet og bestemmelsene i §§ 37-41 om etablering og behandling av informasjon i soner.

Andre ledd stiller krav om at virksomheten skal føre oversikt over hvilke personer som har selvstendig tilgang til rommet eller lokalet. I andre ledd annet punktum stilles det også krav om at virksomheten skal føre oversikt over besøkende til rommet eller lokalet. Hensikten er blant annet å sikre sporbarhet for de tilfellene hvor man oppdager en kompromittering av rommet.

Tredje ledd stiller krav til at lokalene skal være tydelig merket med hvilket graderingsnivå det tillates å tale i rommet og lokalet. Hensikten med dette er at det ikke skal omtales informasjon av høyere gradering i rommet eller lokalet enn det dette er beskyttet for.

Fjerde ledd er en kodifisering av dagens praksis, der virksomheten skal be NSM om teknisk sikkerhetsundersøkelse før rom eller lokaler for tale gradert KONFIDENSIELT eller høyere tas i bruk. NSM beslutter om det er nødvendig med en teknisk sikkerhetsundersøkelse.

7.7 Kapittel 6 Beskyttelse av skjermingsverdige informasjonssystemer

7.7.1 Innledning

Kapittel 6 må leses i forlengelsen av og i sammenheng med andre kapitler i forskriften, særlig kapitlene om sikkerhetsstyring, risikovurdering og om beskyttelse av skjermingsverdig informasjon. I mange tilfeller må kapittel 6 også leses i sammenheng med kapittelet om personellsikkerhet, sikkerhetsgraderte anskaffelser og objekt- og infrastruktursikkerhet.

Prinsippene for sikring av informasjonssystemer har for så vidt ikke endret seg siden den tidligere forskriften om informasjonssikkerhet ble utformet. Imidlertid er det betydelige forskjeller mellom tidligere og ny sikkerhetslov, samt tilhørende forskrifter, slik at kapittelet om informasjonssystemsikkerhet ikke enkelt kan sammenlignes med tidligere regler om sikring av informasjonssystemer. For eksempel gjelder nå prinsippet om minste privilegium som generelt prinsipp for all sikring, og det er derfor ikke lenger en del av bestemmelsene om informasjonssystemsikkerhet. Videre har blant annet forholdet mellom infrastruktur og informasjonssystemer og det at informasjonssystemer nå favner mer enn kun systemer som behandler sikkerhetsgradert informasjon, gjort det nødvendig med endringer.

7.7.2 Til § 45 Forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer

Første ledd fastsetter hvilke egenskaper ved et skjermingsverdig informasjonssystem som skal ivaretas for at virksomheten skal kunne sies å ha et forsvarlig sikkerhetsnivå og for at informasjonssystemet skal bli godkjent, jf. § 48. Bokstav a til c gjelder egenskaper som allerede følger av kravet i lovens § 6-2, men er tatt inn for helhetens skyld og for å presisere at det, avhengig av informasjonssystemet, kan være behov for å beskytte både data og tjenester. Med «data» menes her noe mer enn bare informasjon i tradisjonell forstand. «Data» omfatter også, men er ikke begrenset til, for eksempel et tallmateriale eller et register som i seg selv kanskje ikke gir særlig mening, men som det kan utledes informasjon ut ifra.

Hensikten med *bokstav a* er å kontrollere tilgangen til data og tjenester som har et behov for beskyttelse mot uautorisert eksponering. Med begrepet «uønsket» menes det som ofte ellers kalles uautorisert. «Uønsket» er valgt for å unngå uriktig kobling til begrepet «autorisasjon» som brukes

andre steder i forskriften. «Uønsket lesing» i bokstav a omfatter alle former for uautorisert lesing av data og informasjon, inkludert for eksempel TEMPEST. «Uønsket bruk» i bokstav a omfatter all form for uautorisert buk av en tjeneste.

Hensikten med *bokstav b* er å kontrollere endringer av tjenester eller data som har behov for beskyttelse mot uautorisert modifikasjon eller manipulasjon. Begrepet «uønsket modifikasjon og manipulasjon» i bokstav b vil for eksempel omfatte at en tjeneste endres eller manipuleres slik at den utfører uautoriserte eller utilsiktede operasjoner.

Hensikten med *bokstav c* er å oppnå tidsriktig og pålitelig leveranse av data og tjenester. Bokstav c omfatter blant annet beskyttelse mot elektromagnetisk puls (EMP). Tap av tilgjengeligheten til informasjon kan for eksempel inntreffe ved at data slettes uautorisert eller tapes ved et diskhavari. Tilgjengeligheten til en tjeneste kan eksempelvis tapes ved komponentfeil, feilaktig oppsett eller tjenestenektangrep.

Bokstavene d til g gjelder henholdsvis egenskapene autentisering, sporbarhet og tillit.

Hensikten med *bokstav d* er å kontrollere tilgangen til informasjon og systemer. For å hindre uønsket lesing, modifikasjon eller sletting av informasjon er det nødvendig å vite hvem som er autorisert til å kjenne til og lese, endre og slette spesifikke data, eksempelvis et dokument. For å hindre uønsket bruk av en tjeneste er det nødvendig å vite hvem som er autorisert til å kjenne til og benytte, modifisere eller stoppe, strupe eller hindre oppstart av tjenesten. Dette inkluderer også kildekode og konfigurasjon av tjenester.

Hensikten med *bokstav e* er å forhindre introduksjon av falske data og tjenester. Informasjonssystemene skal også beskyttes mot at falske data og tjenester introduseres ved at det stilles krav til ektheten til data. Dette kommer i tillegg til et krav om integritet (umanipulert), siden falske data fra en uautorisert bruker introdusert i systemet godt kan ivareta dets integritet mens det behandles i informasjonssystemet. Tilsvarende kan data fra en autorisert kilde (ikke-falske data) mangle integriteten ved at de er manipulert mens de behandles i informasjonssystemet. I kravet om å forhindre ligger det implisitt et krav om at slike handlinger skal stanses før handlingen har skjedd.

Hensikten med *bokstav f* er å ivareta behovet for å kunne ha oversikt over aktiviteter i informasjonssystemet og kunne ansvarliggjøre brukere for de handlinger som gjøres i informasjonssystemet. Med dette skal man oppnå bevissthet om de aktiviteter i informasjonssystemet som leder frem til en sikkerhetstruende hendelse slik at hendelsen kan oppdages og brukere kan holdes ansvarlige for deres handlinger. I dette ligger også et behov for å sikre logger i informasjonssystemet slik at disse ikke modifiseres eller slettes slik at handlinger i informasjonssystemet kan rekonstrueres. I tillegg til å ansvarliggjøre brukere, er intensjonen med bokstav f å kunne forhindre sikkerhetstruende hendelser gjennom oppdagelse og tidlig varsling, samt skadeevaluering og -begrensning i tillegg til gjenoppretting.

Hensikten med *bokstav g* er å oppnå tillit til at sikkerhetsfunksjonaliteten i informasjonssystemer og dets produkter ivaretar sikkerheten i nødvendig og tilstrekkelig grad, og at de implementeres og opereres i henhold til hensikten.

Andre ledd bestemmer at virksomheten skal legge sin verdivurdering av informasjonssystemet til grunn ved vurderingene av hvordan risikoen skal håndteres for å oppnå et forsvarlig sikkerhetsnivå. Dette innebærer forutsetningsvis at virksomheten må ha gjort en vurdering av hvilken betydning informasjonssystemet har for grunnleggende nasjonale funksjoner.

Tredje ledd bestemmer i hvilke tilfeller det er krav om automatisering av sikkerhetstiltakene, blant annet for å spare tid og for å unngå manuelle feil. Eksempler på funksjonalitet det vil være naturlig å automatisere er funksjoner for å håndtere forvaltning av informasjonssystemer, som utrulling av oppdateringer, konfigurasjonsstyring, systemovervåkning, brukerhåndtering og sikkerhetskonfigurasjon og verifikasjon.

Fjerde ledd bestemmer at det må foretas en konkret helhetsvurdering av det enkelte informasjonssystem for å kunne velge, utforme og iverksette passende sikkerhetstiltak. Det er viktig at beskyttelse av de ulike egenskapene i første ledd ses i sammenheng og at vektingen av dem baseres på en risikovurdering. Denne helhetsvurderingen skal, gjennom risikovurderinger som beskrevet i § 11 tredje ledd, vedlikeholdes gjennom hele systemets levetid slik at bokstav a til g ivaretas.

Departementet vil vurdere om bestemmelsen er hensiktsmessig utformet i løpet av høringsrunden.

7.7.3 Til § 46 Plikt til å sørge for godkjenning av skjermingsverdige informasjonssystemer

Bestemmelsen konkretiserer plikten som følger av sikkerhetsloven § 6-3. Godkjenning er en formell bekreftelse på at risiko forbundet med å ta et skjermingsverdig informasjonssystem i bruk er identifisert, erkjent og tilfredsstillende håndtert. Om et system skal forhåndsgodkjennes eller ikke har dermed ingen innvirkning på virksomhetens generelle plikt etter loven § 6-2.

Andre ledd inneholder en informasjonsplikt for de tilfellene hvor virksomheten har besluttet å utvikle et system som det ikke er åpenbart at skal godkjennes av virksomheten selv. Denne informasjonsplikten retter seg hovedsakelig mot de tilfellene hvor virksomheten skal utvikle et system som skal behandle sikkerhetsgradert informasjon. Hensikten er å sikre at NSM blir involvert så tidlig som mulig i prosessen slik at virksomheten, ved behov, kan få bistand fra fagmyndigheten i hvordan virksomheten bør sikre systemet for å oppnå et forsvarlig sikkerhetsnivå.

7.7.4 Til § 47 Godkjenningsmyndighet

Første ledd bestemmer at det som hovedregel er virksomheten selv som godkjenner skjermingsverdige informasjonssystemer. NSM er godkjenningsmyndighet når det er særlig behov for det, jf. andre og tredje ledd.

Hensikten med *første ledd andre punktum* er at NSM og relevante tilsynsmyndigheter skal kunne ha oversikt over alle skjermingsverdige informasjonssystemer i henholdsvis hele landet og den enkelte sektor. I tillegg gir det grunnlag for NSM til å vurdere om de skal godkjenne informasjonssystemet. Informasjonsplikten inntrer når det er fastslått at et informasjonssystem er skjermingsverdig eller når det er besluttet å utvikle et skjermingsverdig informasjonssystem.

Andre ledd gjelder informasjonssystemer som er særlig viktige. Dette vil typisk være systemer som har en så viktig rolle at dersom informasjonssystemet slutter å fungere så har det stor negativ innvirkning på funksjonaliteten i objektet eller infrastrukturen. For denne kategorien informasjonssystemer vil det antakelig være behov for tett samhandling mellom NSM, sektormyndigheten og virksomheten.

Tredje ledd tilsvarer i all hovedsak tidligere forskrift § 5-28 andre ledd, men med motsatt tilnærming. I stedet for å sette kriterier for hvilke systemer virksomheten selv kan godkjenne, er det nå satt kriterier for hvilke systemer NSM skal godkjenne.

Bokstav b og c gjelder elektronisk overføring av sikkerhetsgradert informasjon via infrastruktur virksomheten ikke kontrollerer gjennom eierskap eller avtale som gir full sikkerhetsmessig kontroll.

NSM vil normalt ha mer trusselinformasjon og kunnskaper fra flere tilsvarende godkjenninger, som kan brukes som grunnlag for vurderingen av risiko, sammenlignet med den enkelte virksomhet.

Mens *bokstav d* gjelder for informasjonssystemer som har brukere som ikke er *sikkerhetsklarert* for det aktuelle graderingsnivået, gjelder *bokstav e* tilfeller der brukerne ikke er *autorisert* for den aktuelle informasjonen. *Bokstav f* gjelder for alle systemer som behandler STRENGT HEMMELIG informasjon, selv om alle brukerne har korrekt sikkerhetsklarering og autorisasjon.

Begrunnelsen for at NSM skal godkjenne disse informasjonssystemene er for det første at de har særlig god kunnskap om aktuelle trusselvurderinger. For det andre har de særlig god kunnskap om sikkerhetsavtaler og sikkerhetssamarbeid med andre land og andre myndigheter. Normalt vil NSMs saksbehandling være særlig rettet mot de elementene som etter bestemmelsen gjør at ikke virksomheten selv kan godkjenne systemet. Eksempelvis når det gjelder *bokstav c* så vil tilkoblingen mellom kontrollert og ikke kontrollert område normalt være av særlig interesse for NSM.

Etter *fjerde ledd* kan det departement som har utpekt objektet eller infrastrukturen bestemme at det er myndigheten med tilsynsansvar som skal gjennomføre godkjenningen etter andre ledd, og ikke NSM. Hensikten er å åpne for at sektortilsynet, som allerede fører tilsyn med informasjonssystemer og infrastruktur etter sektorregelverk, også skal kunne godkjenne informasjonssystemene etter sikkerhetsloven dersom de har kompetansen som trengs. Det kan også tenkes at det følger enkelte krav til disse systemene i sektorregelverk, noe som gjør det lite hensiktsmessig at NSM skal være godkjenningsmyndighet for disse.

7.7.5 Til § 48 Godkjenningen

Godkjenning er en formell bekreftelse på at risiko forbundet med å ta et skjermingsverdig informasjonssystem i bruk er identifisert, erkjent og tilfredsstillende håndtert, jf. §§ 11, 12 og 45. En godkjenning indikerer at man kan ha tillitt til at informasjonssystemet kan brukes til det systemet er godkjent for. Godkjenningen kan imidlertid ikke tas som en garanti på at kravet til forsvarlig sikkerhetsnivå er oppfylt.

At godkjenning skal skje ved en «planlagt» gjennomgang menes at systematikken skal være fastlagt på forhånd og tilpasset oppgaven som skal løses. Det vil si at ikke hver godkjenning blir en utprøving av godkjenningsmetodikken. Med "systematisk" menes en samling av nødvendige aktiviteter i en logisk sammenheng/rekkefølge.

Godkjenningen omfatter gjennomgang av de sikkerhetsmessige forhold som er særskilte for informasjonssystemer og informasjonssystemsikkerheten. *Første ledd bokstav a til e* angir disse forholdene i logisk rekkefølge, både som beskrivelse av en godkjenningsprosess og som hovedelementer ved utvikling av et sikkert informasjonssystem. Opplistingen er således et utvalg av virksomhetens forpliktelser etter forskriften.

Godkjenningens omfang og detaljeringsgrad skal stå i et rimelig forhold til risiko for sikkerhetstruende virksomhet. Det vil si at det skal være sammenheng mellom sikkerhetsgodkjenningens grundighet og behovet for tillit til beskyttelsen. Det vil være forskjell på en godkjenning av et system som skal brukes til å behandle informasjon gradert HEMMELIG i utlandet med mange brukere, og et system for informasjon gradert BEGRENSET med få brukere.

Departementet ber om innspill på om godkjenningsbestemmelsen er hensiktsmessig utformet. Departementet vil vurdere om denne skal oppdateres for å bedre synliggjøre forholdet mellom godkjenningen og kravene i § 45.

7.7.6 Til § 49 Godkjenningens varighet

En regodkjenning dreier seg i hovedsak om vurdering av de endringene som har skjedd, og vil ta utgangspunkt i den forrige godkjenningen. En regodkjenning vil normalt være mindre omfattende enn en første godkjenning.

En «vesentlig endring» vil antakelig som oftest være en endring som berører § 48 første ledd bokstav a om informasjonssystemets funksjon og operative miljø. Videre kan det være endringer som påvirker sikkerhetsteknologi – dvs. at valgte tiltak ikke lenger oppfyller § 48 første ledd bokstav d.

7.7.7 Til § 50 Midlertidig brukstillatelse

Bestemmelsen fastsetter i hvilke tilfeller et system kan benyttes uten at kravene om godkjenning er oppfylt. Det er først og fremst når de prosessuelle kravene ikke er tilfredsstilt at dette er aktuelt. Er det grunn til å tro at sikkerhetskravene ikke er oppfylt, skal det ikke gis midlertid brukstillatelse.

Ved særskilte behov som når informasjonssystemet skal benyttes i en svært kritisk aktivitet eller når det å sette systemet i drift er eneste mulighet for utprøving, kan det være nødvendig å gi midlertidig brukstillatelse for å ta informasjonssystemet i bruk. Forutsetningen er at beskyttelsesbehovet er kjent, at manglende grunnlag for sikkerhetsgodkjenning er kompensert og at det foreligger en plan for å oppnå nødvendig grunnlag for godkjenning.

Tre typetilfeller der bestemmelsen vil kunne få anvendelse er for det første er et system er under utvikling og det er behov for testing med faktiske og ikke fiktive data. For det andre kan det være behov for slik tillatelse rett i etterkant av endrede sikkerhetspolitiske forhold. For det tredje kan det være slikt behov ved enkeltstående feltmessig utprøving av informasjonssystemer. Dette er imidlertid kun mulige eksempler. Bestemmelsen er utformet generelt slik at det kan tenkes mange andre *særlige tilfeller.* Vurderingen må som hovedregel knyttes opp mot hensyn som ivaretar lovens formål.

Bestemmelsen gjelder for alle skjermingsverdige informasjonssystemer, men vil antakelig ha størst praktisk betydning for systemer som skal behandle sikkerhetsgradert informasjon.

Etter *andre ledd* kan NSM dispensere fra vilkårene i bokstav a til c når det er tvingende nødvendig å ta informasjonssystemet i bruk.

7.7.8 Til § 51 Sammenkobling av informasjonssystemer som behandler sikkerhetsgradert informasjon

Bestemmelsen er i noen grad en videreføring av tidligere forskrift § 5-8 om sammenkobling av informasjonssystemer. Hvilke systemer som omfattes er endret mens kravet til det dedikerte sammenkoblingssystemet er det samme. Avtalekravet videreføres også.

Første ledd pålegger en plikt til å ha et eget informasjonssystem for sammenkobling av informasjonssystemer som behandler høyt sikkerhetsgradert informasjon. Hensikten er å ha kontroll med informasjonsflyten mellom de ulike systemene og hvem som har tilgang. Blir kompleksiteten stor nok, vil det være helt nødvendig å ha et dedikert sammenkoblingssystem for å kunne ha tilstrekkelig kontroll på informasjonsflyten.

Forskriften oppstiller ikke en tilsvarende plikt ved sammenkobling av andre informasjonssystemer. Det kan likevel være at en konkret risikovurdering tilsier at en også i andre tilfeller enn de som reguleres i denne bestemmelsen bør ha egne informasjonssystemer for sammenkoblinger.

Det vil måtte bero på en risikovurdering når kompleksiteten i sammenkoblingene og de sikkerhetsmessige avhengighetene mellom informasjonssystemene blir så omfattende at plikten inntrer. I noen tilfeller kan det være at plikten inntrer allerede ved tre sammenkoblede informasjonssystemer.

7.8 Til kapittel 7 Beskyttelse av skjermingsverdig objekter og infrastruktur

7.8.1 Til § 52 Skadevurdering i forbindelse med klassifisering av skjermingsverdig objekt eller infrastruktur

Formålet med bestemmelsen er å gi departementet tilstrekkelig grunnlag for å klassifisere objektet eller infrastrukturen, jf. myndighetsforskriften § 1. Vurderingen vil også være utgangspunktet for vurderingen av hvilke sikkerhetstiltak som må på plass for å oppnå et forsvarlig sikkerhetsnivå, jf. § 53.

Bokstav a stiller krav om at virksomheten skal gjennomføre en vurdering av hvilken betydning bortfall eller reduksjon av objektets eller infrastrukturens funksjonalitet vil ha for de grunnleggende nasjonale funksjonene. F.eks. hvor stor betydning vil tap av en stor trafostasjon ha for virksomhetens totale leveranse av strøm. Det kan være krevende for en virksomhet å vite hvilken betydning den har for de grunnleggende nasjonale funksjonene. Det vil derfor være sentralt med en god dialog med ansvarlig departement. Bestemmelsen forutsetter at virksomheten har de nødvendige forutsetninger for å vite hvilken betydning virksomhetens funksjon og leveranser har for de grunnleggende nasjonale funksjonene. *Bokstav b* stiller krav om at virksomheten skal gjennomføre en vurdering av hvor lenge objektet eller infrastrukturen kan være satt ut av funksjon før det får betydning for grunnleggende nasjonale funksjoner. F.eks. vil det ta kort tid fra et bortfall eller funksjonssvikt til det får betydning for virksomhetens leveranse ved tett kobling. For andre objekter eller infrastrukturer med mindre tett kobling, vil betydningen for virksomhetens leveranser kunne oppstå senere. Eksempler på leveranser med tett kobling er f.eks. elektroniske finanstransaksjoner eller forholdet mellom en radar og det militære luftbildet.

Bokstav a og b speiler myndighetsforskriften § 1 første ledd bokstav a. I myndighetsforskriftens bestemmelse tas det utgangspunkt i den grunnleggende nasjonale funksjonen, for så å ta stilling til hvilke objekter eller infrastruktur funksjonen er avhengig av. F.eks. kan én funksjon være avhengig av to eller flere objekter eller infrastrukturer. I virksomhetsforskriften § 52 bokstav a og b, som retter seg mot virksomhetene, tas det derimot utgangspunkt i objektet eller infrastrukturen til virksomheten, for så å ta stilling til hvilken betydning disse har for grunnleggende nasjonale funksjoner. F.eks. kan ett objekt ha betydning for to eller flere funksjoner. Se også merknaden til myndighetsforskriften § 1.

Bokstav c stiller krav om at virksomheten skal gjennomføre en vurdering av i hvilken grad objektet- eller infrastrukturens funksjon kan gjenopprettes eller erstattes. F.eks. hvor lang tid det vil ta å reparere et linjebrudd eller hvorvidt en leveranse som forutsetter jernbanetransport kan erstattes med veitransport.

Departementet bemerker at graden av redundans i en infrastruktur vil være en av flere faktorer som bør vurderes etter bokstav a, b eller c.

Bokstav d stiller krav om at virksomheten skal gjennomføre en vurdering av hvilke andre skjermingsverdige objekter eller infrastrukturer som er avhengige av objektet eller infrastrukturen. F.eks. en vurdering av hvilke andre skjermingsverdige objekter eller infrastrukturer som vil være avhengig av Nødnettet. Bestemmelsen skal ikke forstås som at det foreligger en plikt til å undersøke

eller utrede hvem andre som er avhengig av egne objekter eller infrastruktur. Hensikten med bestemmelsen er at der den som råder over objektet eller infrastrukturen har blitt informert av en annen virksomhet om at denne objekt eller infrastruktur er avhengig av førstnevntes objekt eller infrastruktur, skal det tas hensyn til i skadevurderingen.

Bokstav e stiller krav om at virksomheten skal gjennomføre en vurdering av i hvilken grad rettstridig overtakelse av objektet- eller infrastrukturen kan påvirke befolkningens grunnleggende sikkerhet. F.eks. hvor stor grad kan det påvirke befolkningens grunnleggende sikkerhet om en aktør tar kontroll over et anlegg som inneholder spesielt farlige stoffer som kan benyttes i en terrorhandling. Etter *tredje ledd* skal en virksomhet som ikke selv kan redusere sin avhengighet av annet objekt eller infrastruktur, varsle virksomheten som råder over den andre objektet eller infrastrukturen. Hensikten er at virksomheten som mottar varselet da kan benytte informasjonen i sin egen skadevurdering. Bestemmelsen er imidlertid ikke ment å regulere hvilke av de to virksomhetene som plikter å iverksette tiltak i en slik situasjon. Normalt vil dette være virksomheten som er avhengig av dem andre, men dette vil kunne variere ut i fra krav i sektorlovgivningen, konsesjonsvedtak, leveranseavtalen mellom virksomhetene og andre relevante rettskilder.

Fjerde ledd innebærer en plikt for virksomheten til å gjennomføre en ny vurdering dersom det skjer en endring av forhold som er relevante for vurderingen etter første ledd. Dette kan eksempelvis være ved etablering av redundans for virksomhetens leveranser, ved endring av teknologi eller etablering av flere eller reduksjon av relevante aktører i markedet.

Femte ledd bestemmer at virksomheten skal varsle det departement som har utpekt objektet eller infrastrukturen dersom virksomheten råder over andre skjermingsverdige objekter eller infrastruktur. Det kan eksempelvis være tilfeller hvor virksomheten ved sin vurdering etter første ledd kommer til at flere av objektene som virksomheten råder over enn de som departementet har pekt ut, bør omfattes av loven. NSM skal varsles dersom virksomheten ikke har et ansvarlig departement.

Sjette ledd stiller krav om at skadevurderingen og informasjon om klassifiseringsnivået skal graderes. Bakgrunnen for dette er at det antas at denne informasjon vil være av stor interesse for fremmed etterretning.

7.8.2 Til § 53 Forsvarlig sikkerhetsnivå for klassifiserte objekter og infrastruktur

Den klassifiseringsgrad departementet vedtar for objektet eller infrastrukturen vil legge føringer for hva som er et forsvarlig sikkerhetsnivå.

Bestemmelsen må leses i forlengelsen av plikten til å vurdere og håndtere risiko, jf. §§ 11 og 12. Det er denne vurderingen som er utgangspunktet for om det er nødvendig å iverksette ytterligere tiltak for å nå et forsvarlig sikkerhetsnivå.

Første ledd bokstav a gir føringer om hva som et minimum må til for å opprettholde funksjonaliteten til objekt eller infrastruktur klassifisert VIKTIG. Virksomheten må definere hva som er å regne som vesentlige funksjoner ved objektet eller infrastrukturen. Virksomheten må også beskrive hvor stor grad av tap eller ødeleggelse som kan aksepteres slik at det kan vurderes om målet om å begrense tapet er oppnådd. Alternativer til funksjonen, redundans og tiltak for hurtig gjenoppretning kan være mulige måter å oppnå målet som alternativ til eller i kombinasjon med sikkerhetstiltak.

Bokstav b legger føringer for hva som minimum må til for å opprettholde funksjonaliteten av objekt eller infrastruktur klassifisert KRITISK. Det er ikke bare vesentlige, men alle funksjoner til objektet eller infrastrukturen som det skal begrenses tapet ved forsøk på ødeleggelse eller skadeverk.

Bokstav c bestemmer at tap av funksjonalitet skal kunne avverges ved forsøk på å skade eller ødelegge objekter eller infrastruktur klassifisert MEGET KRITISK. Slik avverging av funksjonstap kan ved siden av eller i tillegg til å være redundans eller gjenoppretning være en kombinasjon av barrierer, overvåkning og reaksjon hvor det i sum vil ta kortere tid for virksomheten å iverksette reaksjon enn det tar å påføre skade eller ødelegge verdien. Dette kan gjøres gjennom et tidsregnskap. Alternativer til funksjonen som har tilsvarende kapasitet og som ikke enkelt kan settes ut samtidig som den opprinnelige funksjonen kan også avverge funksjonstap. MEGET KRITISK er den høyeste klassifiseringsgraden med de strengeste kravene til beskyttelse. Departementet vurderer at det ikke vil være mange objekter eller infrastrukturer med denne klassifiseringsgraden. Det vil være staten som råder over de aller fleste objekter eller infrastrukturer med denne klassifiseringsgraden

Bokstav d bestemmer at virksomheten i tillegg til bokstav b og c, må sørge for at den kan avverge at vesentlige funksjoner rettstridig overtas for skjermingsverdige objekter og infrastruktur klassifisert KRITISK og MEGET KRITISK. Det er funksjonen som det skal hindres overtagelse av. Dersom det finnes alternativer til den delen av objektet eller infrastrukturen som det er aktuelt å overta, kan et tiltak være å ødelegge denne eller koble den fra nettet.

IKT-dimensjonen er viktig å se til både når det gjelder å hindre tap av funksjonalitet og rettstridig overtagelse, da mange objekter og infrastrukturer styres gjennom prosesskontrollsystemer eller andre IKT-baserte styringssystemer. Disse systemene vil sannsynligvis utgjøre skjermingsverdige informasjonssystemer og må sikres deretter.

7.8.3 Til § 54 Bruk av sikringsstyrker

Sikringsstyrker er kapasiteter fra politiet og Forsvaret til beskyttelse av et objekt eller infrastruktur. Hvor stor kapasitet politiet og Forsvaret har vil kunne variere over tid. Det ligger derfor til Forsvaret og politiet å bestemme hvilke skjermingsverdige objekter- og infrastruktur som skal beskyttes ved hjelp av sikringsstyrker. Det vil forhåndsplanlegges for bruk av sikringsstyrker på kun et lite antall objekter og infrastruktur.

For å sikre hensiktsmessig bruk av sikringsstyrkene foreslår departementet en plikt for virksomhetene til å tilrettelegge for bruk av sikringsstyrker, og at det skal utarbeides en plan i samarbeid med politiet og Forsvaret i de tilfellene at et objektene eller infrastrukturen som virksomheten råder over er blitt prioritert for dette. Bruk av sikringsstyrker er et påbygningstiltak og forberedelse til å ta imot disse bør inngå i beredskapsplaner og øves.

7.8.4 Til § 55 Behovet for bruk av adgangsklarering

Dersom virksomhetens vurdering av risiko viser at det ikke vil være mulig å redusere risikoen tilstrekkelig ved hjelp av andre egnede tiltak, kan virksomheten be ansvarlig departement eller NSM om å fatte vedtak om adgangsklarering for tilgang til skjermingsverdig objekt eller infrastruktur. Søknaden må redegjøre for hvorfor virksomheten har behov for adgangsklarering som del av sitt forebyggende sikkerhetsarbeid.

Departementet legger til grunn at en adgangsklarering er en nivåklarering. Det vil si at en gitt klarering er gyldig for adgang ikke bare til det objektet eller den infrastrukturen som den opprinnelig ble gitt for, men kan også benyttes til å bli autorisert for adgang til *andre* objekter eller infrastruktur med krav om adgangsklarering på samme nivå eller lavere.

7.9 Til kapittel 8 Nasjonalt varslingssystem for digital infrastruktur

7.9.1 Innledning

Varslingssystem for digital infrastruktur er opprettet for å ivareta nasjonale sikkerhetsinteresser. Varslingssystemets primærfunksjon er ikke å håndtere virksomhetens risiko, men å detektere og varsle om hendelser som kan ha betydning for nasjonale sikkerhetsinteresser. Gjennom dette vil NSM imidlertid også varsle virksomheten om hendelser av betydning for virksomhetens risiko. Tilknytning til varslingssystemet gir ikke nødvendigvis virksomheten prioritet ved hendelseshåndtering, og er noe som vil måtte reguleres i avtalen mellom NSM og de ulike virksomhetene.

7.9.2 Til § 56 Tilknytning til varslingssystemet for digital infrastruktur

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

For at tilknytningen til VDI skal få mest mulig effekt, er det sentralt at kapasitetene blir plassert på den mest hensiktsmessige måten. Partene må derfor gjennom avtalen regulere hvor og hvordan deteksjonskapasitetene og andre VDI-kapasiteter skal utplasseres hos virksomheten. Deteksjonskapasitetene vil ofte være sensorer som varsler NSM når unormal aktivitet forekommer i virksomhetens systemer.

Hensikten med utplasseringen er å oppdage alvorlige digitale angrep, slik at disse kan håndteres, som utgangspunkt av virksomheten selv eller med bistand fra et responsmiljø. Dette kan være sektorvise responsmiljøer eller det kan være NSM NorCERT. Det må i avtalen reguleres hvilken rolle virksomheten har, og hvilken rolle NSM har dersom et slikt angrep inntreffer. Dette innebærer at det må avtales nærmere i hvilke tilfeller NSM vil håndtere hendelsen, og hvordan virksomheten eventuelt skal bistå i håndteringen. Hvis det finnes et hendelseshåndteringsmiljø for den konkrete sektoren som virksomheten tilhører, bør også forholdet til det sektorvise hendelseshåndteringsmiljøet omfattes av avtalen.

Dersom det samles inn personopplysninger gjennom tilknytningen skal det reguleres i hvilket omfang dette kan skje, og hvordan disse skal behandles. Blant annet vil det være naturlig å avtale nærmere deling av informasjon med tredjeparter, hvordan den registrertes rettigheter ivaretas og avviksrutiner. For nærmere omtale av de rettslige rammene for behandling av personopplysninger vises det til Prop. 97 L (2015–2016) om endringer i sikkerhetsloven kapittel 7.

Det skal også i avtalen reguleres nærmere hvordan NSM skal behandle og håndtere annen informasjonen som VDI-kapasitetene gir. Eksempler på slike tilfeller kan være der det innhentes informasjon fra organ med ulike konstitusjonelle roller eller der dataene kan være underlagt taushetsplikt i annet regelverk eller i samarbeidsavtaler med andre stater. Trafikkmengde, sikkerhetsmekanismer i systemene, og eventuell fiendtlig aktivitet vil ofte være å anse som sensitiv informasjon, uten at det nødvendigvis er skjermingsverdig etter sikkerhetsloven, som vil være nødvendig å håndtere med varsomhet av NSM.

For øvrig vises det til Prop. 97 L (2015–2016) om endringer i sikkerhetsloven kapittel 6 for en nærmere beskrivelse av VDI.

7.9.3 Til § 57 Virksomhetens rett til innsyn

Bestemmelsen gir virksomhetene rett til innsyn i hvordan kapasitetene for deteksjon og sårbarhetsreduksjon som brukes i virksomheten er konfigurert, og i dataene som NSM mottar fra virksomhetens kapasiteter. Hensikten med dette er å sikre åpenhet rundt NSMs bruk av varslingssystemet.

7.10 Til kapittel 9 Personellsikkerhet

7.10.1 Til § 58 Vilkår for å gi autorisasjon

Bestemmelsen er basert på gjeldende forskrift om personellsikkerhet § 5-2. En del av opplistingen av vilkår i gjeldende rett er tatt ut da departementet finner disse ivaretatt i andre deler av regelverket. Bestemmelsens *første ledd tredje punktum* er ny og fastsetter at dersom det er gitt klarering på vilkår skal autorisasjonsansvarlig beslutte hvordan vilkårene skal følges opp før autorisasjon kan gis.

Bestemmelsens *andre ledd* tilsvarer i hovedsak gjeldende forskrift om personellsikkerhet § 5-2 andre ledd, men med språklige forenklinger.

7.10.2 Til § 59 Autorisasjonssamtale

Bestemmelsen tilsvarer i hovedsak gjeldende forskrift om personellsikkerhet § 5-5, men med språklige forenklinger.

I bestemmelsens *andre ledd* har departementet funnet det hensiktsmessig å være tydeligere på hva autorisasjonsansvarlig skal berøre autorisasjonssamtalen, enn i gjeldende forskrift. Momenter som er tatt inn i bestemmelsen er at den som skal autoriseres skal forstå sin rolle i sikkerhetsarbeidet, forstå eventuelle egne sårbarheter og tiltak som kan iverksettes for å redusere risiko.

7.10.3 Til § 60 Autorisasjon av autorisasjonsansvarlig hos leverandøren

Bestemmelsen tilsvarer gjeldende praksis og henviser til det tillitsforholdet som må avklares mellom oppdragsgiver og autorisasjonsansvarlig hos leverandøren. Departementet har funnet det hensiktsmessig å kodifisere denne praksisen.

7.10.4 Til § 61 Autorisasjon av utenlandske statsborgere

Bestemmelsen er utledet av gjeldende forskrift om personellsikkerhet § 2-2. Se for øvrig merknad til klareringsforskriften § 26.

7.10.5 Til § 62 Nødautorisasjon

Bestemmelsen er utledet av gjeldende forskrift om personellsikkerhet § 5-3. Ved nødrett, jf. straffeloven § 17, kan en person autoriseres uten å ha nødvendig klarering. Autorisasjonsansvarlig skal i den grad det er hensiktsmessig ut i fra situasjonen, følge de prosedyrer og bestemmelsens som gjelder for autorisasjon. Særlig relevant er autorisasjonssamtalen.

Departementet har ikke funnet det hensiktsmessig å videreføre gjeldende forskrift om personellsikkerhet § 5-3 andre ledd, om at nødautorisasjon for høyeste nivå kun kan gis dersom personen er klarert for et lavere nivå. Departementet mener at når det foreligger nødrett kan det ikke stilles et slikt vilkår, og anser at autorisasjonsansvarlig vil være best egnet til foreta avveiningen mellom den risiko som er forbundet med å gi autorisasjon på det høyeste nivået, og konsekvensene ved å ikke gi slik autorisasjon i det enkelte tilfellet.

Departementet har ikke videreført gjeldende forskrift om personellsikkerhet § 5-3 tredje ledd andre punktum om at autorisasjonsansvarlig uten ugrunnet opphold skal be om klarering for en person som er gitt nødautorisasjon. Autorisasjonsansvarlig må i etterkant av nødsituasjonen, ut ifra de alminnelige bestemmelsene om når det kreves klarering, vurdere om det er grunnlag for å be om at personen blir klarert.

7.10.6 Til § 63 Oversikt over personell med autorisasjon

Bestemmelsen er utledet av gjeldende forskrift om personellsikkerhet § 5-6 om autorisasjonsliste. I bestemmelsens *første ledd bokstav a* fremgår det at opplysninger om statsborgerskap og tjenestested er en del av oversikten. Dette er nytt og viser til ny lov § 8-12 om utlevering av informasjon til Politiets sikkerhetstjeneste. Det vises til at NSM etter ny lov § 8-9 tredje ledd kan kreve at virksomheten skal holde NSM orientert om hvilke personer som er autoriserte. Dette er nødvendig for at PST skal kunne be om opplysninger etter § 8-12. Opplysninger om nødautorisasjon og eventuelle vilkår for klareringen er også lagt inn som en del av oversikten som autorisasjonsansvarlige skal føre.

7.10.7 Til § 64 Dokumentasjon på autorisasjon

Bestemmelsen tilsvarer i hovedsak gjeldende forskrift om personellsikkerhet § 5-7 om autorisasjonsbevis, men med språklige forenklinger. I bestemmelsen fastsettes det at i tillegg til graderingsnivå på informasjon, skal også klassifiseringsnivå for objekt og infrastruktur inngå dersom det er gitt autorisasjon for adgang til skjermingsverdig objekt eller infrastruktur.

7.10.8 Til § 65 Nedsettelse, suspensjon og tilbakekallelse av autorisasjon

Bestemmelsen tilsvarer i hovedsak gjeldende forskrift om personellsikkerhet § 5-8 om ufordelaktige autorisasjonsavgjørelser, men med språklige forenklinger.

I *første ledd* fastsettes det at autorisasjonsansvarlige skal dokumentere en eventuell revurdering av autorisasjon og at dokumentasjonen skal oppbevares sammen med øvrig dokumentasjon om autorisasjon og klarering. Steg for steg beskrivelsen av prosessen ved revurdering av autorisasjon i gjeldende forskrift om personellsikkerhet § 5-8 første ledd er imidlertid ikke videreført i forslaget. Departementet finner en slik detaljert beskrivelse overflødig i en forskrift, og viser til blant annet NSMs håndbok om autorisasjon for utfyllende beskrivelse av denne prosessen.

Med innmeldte opplysninger i bestemmelsens *tredje ledd*, menes de forhold som autorisasjonsansvarlige meldte inn til klareringsmyndigheten som grunnlag for en ny vurdering av sikkerhetsmessig skikkethet. Autorisasjonsansvarlige står fritt til å revurdere autorisasjon dersom det fremkommer forhold som klareringsmyndigheten ikke er kjent med.

7.10.9 Til § 66 Begrunnelse og dokumentasjon ved forespørsel om klarering

Bestemmelsen tilsvarer gjeldende forskrift om personellsikkerhet § 3-1 første ledd annet punktum og første ledd tredje punktum.

I bestemmelsens første ledd første punktum er det fastsatt at ved en klareringsforespørsel skal behovet begrunnes og dokumenteres. Hensikten med bestemmelsen er å unngå at det bes om klarering og igangsettes personkontroll, i tilfeller der det ikke foreligger et behov. Det er ikke tilstrekkelig dokumentasjon at det i et skjema for forespørselen bare står at personen skal ha tilgang til sikkerhetsgradert informasjon. Det må gis en kort forklaring på hva slags funksjon eller type arbeid det er som gjør at personen må gis en slik tilgang, som f.eks. at vedkommende skal drifte sikkerhetsgraderte informasjonssystemer, forberede forvaltningsvedtak der deler av

saksopplysningene består av sikkerhetsgradert informasjon, eller utarbeide sikkerhetsgraderte beredskapsplaner. Det må ikke nødvendigvis vedlegges en nærmere redegjørelse eller en stillingsbeskrivelse ved hver enkelte klareringsanmodning. Kravet er ment å være funksjonelt og kan oppfylles også ved henvisningsteknikk. For eksempel er det tilstrekkelig for å oppfylle dokumentasjonskravet at det vises til en instruks eller et vedtak om at det for tilgang til det angitte skjermingsverdige objektet kreves adgangsklarering, så lenge klareringsmyndigheten tidligere har mottatt en slik instruks eller dokument om vedtaket.

7.10.10 Til § 67 Merking av personopplysninger for klarering og autorisasjon

Bestemmelsens er utledet av gjeldende forskrift om personellsikkerhet § 6-2. Er et dokument sikkerhetsgradert skal det i tillegg merkes i samsvar med ny sikkerhetslov § 5-3. Formålet med en egen type merking for slike opplysninger er å tydeliggjøre at dette er opplysninger som det skal være streng kontroll med tilgangen til og som det gjelder egne behandlingsregler for.

7.10.11 Til § 68 Beskyttelse av personopplysninger for klarering og autorisasjon

Bestemmelsens *første ledd* er utledet av gjeldende forskrift om personellsikkerhet § 6-4 første ledd. Den som utpeker hvilket personell som har tjenstlig behov, er i forslaget endret til den autorisasjonsansvarlige fra virksomhetens leder i gjeldende forskrift om personellsikkerhet. Det vises til at det er autorisasjonsansvarlig, uavhengig om det er virksomhetens leder eller om det er delegert til en annen person, som beslutter om autorisasjon skal gis.

Departementet ha valgt å ikke foreslå egne bestemmelser om beskyttelse av personopplysninger for klarering og autorisasjon. Dersom personopplysningene er sikkerhetsgraderte, gjelder bestemmelsene i forskriften kapittel 3 og 5. I tillegg stilles det i ny personopplysningslov krav om at den enkelte virksomhet selv plikter å vurdere konsekvenser for personvernet og risikoen, som grunnlag for hvordan opplysningene bør beskyttes.

7.10.12 Til § 69 Bevaring og kassasjon av opplysninger i saker om autorisasjon og klarering

Bestemmelsen er utledet fra gjeldende forskrift om personellsikkerhet § 6-9 om kassasjon, og fra gjeldende bestemmelser om bl.a. kassasjon som er fastsatt av NSM og godkjent av Riksarkivaren.

Bestemmelsens *første ledd* regulerer behandling av personopplysninger i forbindelse med autorisasjon og klarering innhentet fra søkere som ikke blir tilsatt, engasjert eller opptatt på skoler eller kurs. For denne gruppen er behovet for klarering og autorisasjon bortfalt og personopplysningene skal kasseres eller returneres uten ugrunnet opphold. Nytt er at dokumenter som kun inneholder personkontrollopplysninger gitt av personen selv kan returneres til den personen disse gjelder. Eksempelvis hvis personen ber om å få returnert personopplysningsblanketten.

Bestemmelsens *andre ledd første punktum* er ny. Hensikten med bestemmelsen er at opplysningene i autorisasjonssaken oppbevares i ett år etter at autorisasjonen er utløpt. Departementet finner at denne type opplysninger bør oppbevares i en gitt tidsperiode slik at opplysningene kan videreformidles til autorisasjonsansvarlig ved ny virksomhet dersom det er autorisasjonsbehov.

7.11 Til kapittel 10 Sikkerhetsgraderte anskaffelser

7.11.1 Til § 70 Vurdering av graderingsnivået for ulike deler av en sikkerhetsgradert anskaffelse

Bestemmelsen tilsvarer i hovedsak gjeldende forskrift om sikkerhetsgraderte anskaffelser § 2-1. I bestemmelsen fokuseres det imidlertid mer på at vurderingen skal skje for de ulike stadiene, enn i gjeldende forskrift der fokuset er hvilken type informasjon det dreier seg om.

I mange tilfeller vil det kun være nødvendig å sikkerhetsgradere kravspesifikasjoner fra oppdragsgiver. I noen anskaffelser der leverandøren skal tilvirke informasjon som ledd i å utvikle eller produsere et produkt for oppdragsgiver, vil imidlertid ikke all informasjon som skal vurderes foreligge på forhånd. (Produktet kan f.eks. være knyttet til skjermingsverdig objekt eller infrastruktur.) Dette fordi en del av informasjonen om produktet tilvirkes under eller i etterkant av utviklingen eller produksjonen. Fastsettelsen av graderingsnivået før anskaffelsesform velges og sikkerhetskrav stilles, vil derfor ofte måtte skje ut ifra en kvalifisert vurdering av verdien av informasjonen som senere tilvirkes. For at riktige sikkerhetstiltak skal kunne brukes på riktig stadium i anskaffelsesprosessen, er det derfor viktig at oppdragsgiver tidlig i anskaffelsesprosessen fastsetter graderingsnivået på dokumentene i de ulike stadiene i prosessen. Oversikten over hva som er gitt hvilket graderings- eller klassifiseringsnivå, vil utgjøre mye av grunnlaget for valg av anskaffelsesform og den senere sikkerhetsavtalen, jf. § 71 andre ledd.

7.11.2 Til § 71 Krav til sikkerhetsavtalen etter sikkerhetsloven § 9-2 når leverandøren skal ha sikkerhetsgradert informasjon eller tilgang til skjermingsverdig objekt eller infrastruktur i eller fra sine egne lokaler

Med informasjonssystem for tilgang til skjermingsverdig objekt eller infrastruktur i *andre ledd bokstav d*, menes f.eks. et driftskontrollsystem (SCADA-system) for styring av infrastrukturen. Det kan også være et IKT-basert anlegg for fysisk sikring av et objekt, der man ved hjelp av IKT-systemet kan slå av og på alarmer og låser i et objekt. Et informasjonssystem kan altså være tett integrert i kjernefunksjonaliteten i en infrastruktur, eller bare være et støttesystem for sikring av et objekt.

Departementet bemerker at sikkerhetsavtalen senest må foreligge før leverandøren får tilgang til informasjon, infrastruktur eller objekt.

7.11.3 Til § 72 Unntak fra krav til sikkerhetsavtalen etter sikkerhetsloven § 9-2

Bestemmelsen fastsetter at der personell fra leverandøren er under oppsyn av oppdragsgiveren, er det ikke krav om sikkerhetsavtale. Med «oppsyn» menes at en representant for oppdragsgiveren, f.eks. en ansatt eller innleide vektere, har kontroll med hvor i lokalene leverandørens personell til enhver tid oppholder seg, eller hvilke operasjoner leverandørens personell gjør i et informasjonssystem for behandling av sikkerhetsgradert informasjon. En slik kontroll kan f.eks. bestå av at leverandørens personell ledsages, eller at det ikke er gitt administratorrettigheter i informasjonssystemet, samtidig som systemet overvåkes i samsvar med sikkerhetsloven § 6-4. Det er en forutsetning at den som holder oppsyn har tilstrekkelig autorisasjon og klarering for den informasjon eller det informasjonssystem, infrastruktur eller objekt personell fra leverandøren får tilgang til.

7.11.4 Til § 73 Tilbakelevering av sikkerhetsgradert informasjon

I *andre ledd* er det presisert at også service- og garantitid skal regnes som en del av kontraktsforholdet. Dersom det er nødvendig å beholde sikkerhetsgradert informasjon etter at et

produkt er levert for å kunne utføre service eller foreta rettelser i garantitiden, behøver altså informasjonen ikke å tilbakeleveres før service- og garantitiden er over.

7.11.5 Til § 74 Krav om leverandørklarering

I *første ledd* er det gitt utfyllende bestemmelser til sikkerhetsloven § 9-3 første ledd om i hvilke tilfeller det er krav om leverandørklarering. Bestemmelsen stiller krav om leverandørklarering i tilfeller der beskyttelsen av tilgangen eller andre sikkerhetstiltak i realiteten er helt eller delvis under leverandørens kontroll. *Bokstav a, b og c* er presiseringer for å utfylle loven.

Bokstav b er ment å gjelde der leverandøren f.eks. bruker et informasjonssystem de selv råder over til å styre infrastrukturen. Et annet eksempel er der leverandøren låner en klientmaskin tilhørende oppdragsgiver til å kartlegge infrastrukturen, og gjør det fra leverandørens egne lokaler.

Bokstav c er ment å gjelde der leverandøren har objektet eller infrastrukturen i sin besittelse. Ved elektronisk styring av et objekt eller en infrastruktur vil bestemmelsen kunne overlappe delvis med bokstav b. Bokstav c gjelder imidlertid også der det dreier som om kun *fysisk* rådighet, f.eks. at leverandøren håndterer radioaktivt materiale som eies av oppdragsgiver.

Leverandørklareringen må foreligge senest før informasjonen skal behandles eller tilgang gis fra leverandørens lokaler. Leverandørklarering må derfor gjøres til et krav i konkurransegrunnlaget, og bør senest foreligge før oppdragsgiveren signerer kontrakten. Dersom leverandøren allerede i konkurransefasen skal behandle eller gis tilgang fra sine lokaler, må leverandørklarering foreligge allerede i konkurransefasen.

7.11.6 Til § 75 Leverandører med lokaler utenfor norsk jurisdiksjon og utenlandske leverandører

Bestemmelsens *første ledd* gjelder uavhengig av om leverandøren, som skal bruke den norske sikkerhetsgraderte informasjonen i utlandet, er norsk eller utenlandsk. Også der en leverandør skal behandle informasjonen i en tredjestat, vil bestemmelsen gjelde. Bestemmelsen kommer imidlertid ikke til anvendelse der norsk sikkerhetsgradert informasjon behandles av en leverandør på en norsk utenriksstasjon eller en militær base i utlandet der Norge er gitt jurisdiksjon.

En sikkerhetsavtale kan være bi- eller multilateral og omhandler statenes gjensidige forpliktelse til å beskytte hverandres sikkerhetsgraderte informasjon. For store prosjekter utarbeides det ofte en såkalt Project Security Instructions (PSI) der avtalevilkårene kan konkretiseres og tilpasses det enkelte oppdrag. Avtalevilkårene vil typisk gjelde hvilke sikkerhetsgrader som skal benyttes, krav om sikkerhetstiltak, hvem som er kompetent myndighet og kontaktpunkt for vedtak om leverandørklarering og kontroll av leverandører, samt prosedyrer for informasjonsutveksling og besøk som omhandlet i § 78.

I *andre ledd* er det fastsatt at ved behov for leverandørklarering av en utenlandsk leverandør, skal klareringsmyndigheten innhente nødvendig informasjon fra sin motpart i utlandet om leverandøren har eller kan gis en leverandørklarering. Det er en forutsetning at klareringsmyndigheten blir kjent med behovet av oppdragsgiver.

7.11.7 Til § 76 Forespørsel om leverandørklarering

Bestemmelsen tydeliggjør at det er oppdragsgiveren, og ikke leverandøren, som skal be om en leverandørklarering. Bakgrunnen for bestemmelsen er at det er oppdragsgiver som er nærmest til å begrunne behovet for klareringen.

7.11.8 Til § 77 Oversikt over sikkerhetsgraderte anskaffelser

Bestemmelsen fastsetter at oppdragsgiveren skal føre oversikt over egne sikkerhetsgraderte anskaffelser. Bestemmelsen må sees i sammenheng med myndighetsforskriften § 9 om at NSM skal føre et sentralt register over sikkerhetsgraderte anskaffelser og klareringsavgjørelser basert på oversikten. Oversikten er tenkt å fungere som beslutningsgrunnlag for om klareringsmyndigheten skal foreta ny kontroll av om leverandøren oppfyller sikkerhetskravene, jf. klareringsforskriften § 33 andre ledd, og i vurderingen av om det skal føres tilsyn hos virksomheten eller hos leverandøren.

7.11.9 Til § 78 Prosedyrer for besøk fra utlandet

Bestemmelsen er i hovedsak en videreføring av forskrift om sikkerhetsgraderte anskaffelser § 4-3.

Det er i sikkerhetsavtaler med andre stater og internasjonale organisasjoner vanlig med avtalevilkår om prosedyrer for besøk mellom partene. Hensikten er å kunne kontrollere at de besøkende har et legitimt behov for besøket, at de er den de gir seg ut for og representerer en av partene, og at de har tilstrekkelig klarering. Sikkerhetsavtalene er imidlertid ikke åpne for offentlig innsyn eller alminnelig kjent for alle oppdragsgivere og leverandører, og leverandører er heller ikke et direkte pliktsubjekt etter avtalene. For at pliktene i sikkerhetsavtalen skal bli ivaretatt av oppdragsgivere eller leverandører i Norge, foreslår derfor departementet en bestemmelse om at besøk skal gjennomføres i samsvar med besøksprosedyrene i eller med hjemmel i sikkerhetsavtalen med staten. I store prosjekter utarbeides det ofte egne besøksprosedyrer i en såkalt Project Security Instructions (PSI) som fastsettes med hjemmel i sikkerhetsavtalen.

Bestemmelsen gjelder også for norske oppdragsgivere og leverandører.

7.11.10 Til § 80 Overgangsregler

Overgangsreglene fastsetter at gjeldende graderinger, klassifiseringer og godkjenninger videreføres som forutsatt også etter at lov om nasjonal sikkerhet trer i kraft 1. januar 2019. Hensikten er å sikre en videreføring for f.eks. informasjonssystemer og objekter som allerede er klassifisert, slik at ikke disse må vurderes på nytt med en gang den nye loven trer i kraft. En gradvis vurdering av systemer og objekter etter nye regler, vil være innenfor myndighetenes saksbehandlingskapasitet.

Dersom en virksomhet klager på en avgjørelse om klassifisering, eller på en godkjenning av et informasjonssystem, kryptosystem, destrueringsmetode eller oppbevaringsenhet så skal regelverket som gjelder på vedtakstidspunktet for klagen legges til grunn. Dette innebærer at en klage høsten 2018, men som først blir avgjort i 2019, skal avgjøres etter reglene i den nye sikkerhetsloven.

Det understrekes at det kun er godkjenning, klareringen, graderingen og klassifiseringen som videreføres, og ikke bestemmelsene knyttet til sikring etter gjeldende sikkerhetslov. Det innebærer at det fra lovens ikrafttredelse vil være et krav om forsvarlig sikkerhetsnivå for de objektene og informasjonen som er gradert og klassifisert i dag. Det antas at dersom virksomheten oppfyller krav til sikring etter gjeldende lov, så vil kravet til forsvarlig sikkerhetsnivå anses å være oppfylt med mindre virksomhetens risikovurdering etter nytt regelverk skulle tilsi noe annet.

8 Merknader til forskrift om klarering av leverandører og personell (klareringsforskriften)

8.1 Til kapittel 1 Generelle bestemmelser om sikkerhetsklarering og adgangsklarering

8.1.1 Til § 1 Klareringsmyndighet

Første ledd fastsetter hvem som er klareringsmyndighet jf. ny sikkerhetslov § 8-16 første ledd. Innholdet samsvarer med vedtak fattet etter endringene fra 1. januar 2017 i gjeldende sikkerhetslov, om hvilke virksomheter som skal være klareringsmyndighet. For ikke å gripe inn i Forsvarets interne organisering, er myndigheten for forsvarssektoren lagt til Forsvaret som etat, og ikke direkte til Forsvarets sikkerhetsavdeling. Dersom Forsvaret skal fortsette å benytte Forsvarets sikkerhetsavdeling til å utøve klareringsmyndighet, må Forsvarsdepartementet eller Forsvaret opprettholde vedtaket om det i samsvar med organisasjons- og instruksjonsmyndigheten for egen etat.

Andre ledd er ny og åpner for at de ulike klareringsmyndighetene i enkeltsaker kan avtale hvem som skal være klareringsmyndighet. Det kan eksempelvis være aktuelt dersom formelle eller praktiske årsaker tilsier at en annen klareringsmyndighet bør klarere det aktuelle personellet, for eksempel grunnet inhabilitet eller andre interne forhold hos den enkelte klareringsmyndighet. Dette kan også vurderes i tilfeller hvor begge klareringsmyndigheter er enige om at den som allerede har klarert personen, for eksempel den militære klareringsmyndigheten, også reklarerer personen selv om denne er i et engasjement i sivil sektor for en periode, og at klareringsmyndighetene da slipper unødvendig administrasjon med å overføre saken.

Tredje ledd tilsvarer forskrift om personellsikkerhet § 4-1 sjette ledd. Bestemmelsen er gitt av effektivitetshensyn, slik at tvil og uklarhet om hvem som er rett myndighet ikke forsinker saken unødig.

Fjerde ledd tilsvarer forskrift om personellsikkerhet § 4-1 niende ledd og fastsetter at den som utøver klareringsmyndighet må ha klarering for det høyeste klareringsnivået vedkommende skal gis fullmakt til å fatte vedtak om. Bestemmelsen er begrunnet i at det er uheldig om den som fatter vedtak om klarering skal vurdere om andre er sikkerhetsmessig skikket til å ha et høyere klareringsnivå, enn det vedkommende selv har. Det kan argumenteres for at en slik føring strengt tatt ikke behøver å forskriftsfestes, men er et kvalifikasjonskrav som heller kan reguleres innen rammen av arbeidsgivers styringsrett. For å unngå ulik praksis mellom klareringsmyndighetene på dette området, har departementet valgt å foreslå det forskriftsfestet. Departementet ber om høringsinstansene syn på femte ledd.

8.1.2 Til § 2 Definisjoner

For å oppnå forutsigbarhet og åpenhet om hvem som kontrolleres i klareringssaker, og unngå usaklig forskjellsbehandling mellom sakene, er det viktig at det er tydelig hvilke personkategorier som inngår i personkontrollen. Departementet har derfor valgt å definere hvem som er å anse som nærstående og enkelte undergrupper av nærståendebegrepet. Det er videre regelteknisk praktisk å ha definisjoner om personkategoriene som det kan henvises til, i stedet for å måtte liste opp i flere bestemmelser hvem som inngår i kontrollen.

Definisjonene tilsvarer i hovedsak definisjoner i gjeldende forskrift om personellsikkerhet. Departementet har i paragrafens bokstav d om annen nær tilknytning gått noe lenger i å presisere hvem andre enn nær familie som kan inngå i kontrollen. Dette vil i hovedsak være personer som den

som klareres har tilsvarende tilknytningsforhold til som til nær familie eller samboer, f.eks. et tett personlig forhold til og som vedkommende har regelmessig privat omgang med. Forholdet må imidlertid ha betydning for om en person er sikkerhetsmessig skikket, jf. bokstav a.

8.1.3 Til § 3 Forholdet mellom adgangsklaring og sikkerhetsklarering

Bestemmelsen er redegjort nærmere for i høringsnotatets kapittel om adgangsklarering.

8.1.4 Til § 4 Hvem som kan be om klarering

Bestemmelsen er ny og fastsetter i *første ledd* at det bare er virksomhetens autorisasjonsansvarlig som kan be klareringsmyndigheten om klarering av personell. Fordi klarering er et inngripende tiltak knyttes retten til å be om klarering til rollen som autorisasjonsansvarlig. Denne myndigheten kan imidlertid ved behov delegeres.

Andre ledd omhandler personell som skal klareres som en del av leverandørklareringsprosessen. For å unngå tvil om hvem av avtalepartene som i slike tilfeller kan be om klarering, er det fastsatt at det er oppdragsgiver som skal be klareringsmyndigheten om klarering. En grunn til dette er at oppdragsgiver bør føre en viss grad av kontroll med at omfanget av klareringsforespørsler samsvarer med oppdragets størrelse, tatt i betraktning klareringens inngripende karakter.

8.2 Til kapittel 2 Personkontroll

8.2.1 Til § 5 Kontroll og avvisning av forespørsel om personkontroll

Bestemmelsen tilsvarer gjeldende forskrift om personellsikkerhet § 3-1 siste punktum.

Bestemmelsen skal ikke forstås som at klareringsmyndigheten står ansvarlig for at behovet for klarering er reelt, men at personkontroll bare iverksettes der begrunnelsen gir rimelig grunn til å tro at det foreligger et reelt behov for klarering.

Når det gjelder hvordan kravet om dokumentasjon skal forstås, viser departementet til merknaden til virksomhetsforskriften § 66.

8.2.2 Til § 6 Personer som inngår i personkontrollen

Bestemmelsen regulerer hvilke personer som inngår i personkontrollen. Med ny sikkerhetslovs utvidelse av begrepet nærstående kan det nå gjøres personkontroll for en videre krets av personer.

Bestemmelsens *første ledd* tilsvarer gjeldende forskrift om personellsikkerhet § 3-2 og angir de personkategorier som omfattes av personkontroll ved sikkerhetsklarering for de ulike nivåene.

Bestemmelsens *andre ledd* fastsetter at det kan gjennomføres personkontroll av andre nærstående, enn de som er angitt i første ledd, dersom klareringsmyndigheten sitter på opplysninger, eller det fremgår av opplysninger som er innhentet fra personen, som tilsier at det er grunn til å anta at vedkommende kan påvirke pålitelighet, lojalitet eller dømmekraften til den som skal klareres. Hvorvidt det er adgang til å gjennomføre personkontroll av andre nærstående vil måtte bero på en konkret helhetsvurdering av *hvor* nærstående personen er til den som skal klareres, og de opplysningene som klareringsmyndigheten har om den nærstående. For eksempel kan betydelige økonomiske forpliktelser overfor en venn, som private lån eller sameie i en bolig, tilsi at vennen kan påvirke den som skal klareres. Det samme gjelder der det foreligger betydelig sosial kontroll. For eksempel at man tilhører en forening, et gjengmiljø eller annet sosialt fellesskap der forutsetningen for å delta er at lojaliteten til venner i fellesskapet settes foran plikten til å overholde lovpålagte krav.

Spesielt dersom det forventes at man utfører kriminelle handlinger eller ikke varsler om alvorlig kriminalitet, og der brudd med forventningene fører til represalier fra vennene.

8.2.3 Til § 7 Sikkerhetsklarering – krav til egenopplysninger

Bestemmelsen er ny. For å få en effektiv og lik innmelding av opplysninger fra den som skal klareres, er det nødvendig at de som skal klareres benytter et fast skjema. For at private rettssubjekter skal kunne pålegges av myndighetene å benytte bestemte skjemaer, må enten skjemaet som sådan eller hvilke typer opplysninger som kan inngå i skjemaet, være fastsatt i forskrift.

Departementet vil vurdere om det er hensiktsmessig å kreve at den som klareres skal måtte gi slike opplysninger eller om det er tilstrekkelig at klareringsmyndighet innhenter slike opplysninger fra offentlige registre. I sistnevnte tilfeller kan det tenkes at klareringsmyndigheten bare ber den som skal klareres om opplysninger der disse ikke kan innhentes fra registre. På den andre siden er det å be om å få slike opplysninger fra den som klareres en måte å kunne kontrollere pålideligheten til den som skal klareres. Et alternativ til å gi en uttømmende liste er en generell plikt til å opplyse om forhold som den klarete antar er av betydning for om han eller hun er sikkerhetsmessig skikket knyttet til lovens § 8-4 fjerde ledd. Departementet ønsker høringsinstansenes innspill på hvordan plikten til å gi egenopplysninger bør reguleres.

Første ledd skal ikke forstås slik at det må gis fullstendige opplysninger om alle temaene som er listet opp. For å f.eks. oppfylle bokstav e om utdanning, kan det være tilstrekkelig at det opplyses om høyeste utdanning. NSM kan presisere nærmere i skjemaet hvilken type opplysninger som skal opplyses om. For å oppfylle bokstav p om referanser er det normalt tilstrekkelig å opplyse om en person som kjenner vedkommende privat, og en som kjenner vedkommende gjennom arbeid.

8.2.4 Til § 8 Adgangsklarering – krav til egenopplysninger

Bestemmelsen er ny og fastsetter hvilke egenopplysninger som skal gis i forbindelse med adgangsklarering. Det er behov for langt færre opplysninger ved adgangsklarering enn ved sikkerhetsklarering. Hensikten er at prosessen ved adgangsklarering skal være forholdsvis enkel og ta kortere tid enn sikkerhetsklarering. Dersom personkontrollen gir funn som gjør at klareringsmyndigheten, for å kunne opplyse saken tilstrekkelig, må innhente flere opplysninger enn det som fremgår av skjemaet, kan klareringsmyndigheten likevel innhente ytterligere opplysninger.

Ved utvidet adgangsklarering, jf. *andre ledd,* er også kravet til egenopplysninger noe utvidet.

8.2.5 Til § 9 Registre for personkontroll ved sikkerhetsklarering

Bestemmelsen er utledet fra gjeldende forskrift om personellsikkerhet § 3-4 og gir en liste over relevante registre NSM kan kreve å få registeropplysninger fra som ledd i den innledende personkontrollen. Det er gjort noen tilføyelser for å komplettere tilfanget av informasjon på forhold som kan tillegges vekt og for å kunne effektivisere klareringsprosessen. Det følger av omtalen i lovproposisjonen til sikkerhetsloven § 8-5 sjette ledd at det med *«relevante registre»* også omfattes opplysninger som virksomheten har lagret på annen måte, eksempelvis i elektroniske saksarkiv. Det er således ikke av avgjørende betydning hvordan opplysningene er lagret i virksomheten.

Bokstav a henviser til politiets registre. Dette vil bl.a. omfatte det som i gjeldende forskrift er benevnt som reaksjonsregisteret og straffesaksregisteret. Det vil også omfatte politiets arbeids- og etterretningsregistre, slik praksis er i dag, og andre registre eller saksarkiv. Det er samtidig gitt ytterligere bestemmelser i § 13 om hvordan opplysningene kan brukes og i § 21 om innsyn.

Det sentrale folkeregisteret og registre ved Statens innkrevingssentral som er listet i gjeldende personellsikkerhetsforskrift, inngår i registre ved Skattedirektoratet som er liste i *bokstav c*.

Arbeidsgiver- og arbeidstakerregisteret i *bokstav e* er også nytt i listen. Registeret vil gi klareringsmyndigheten informasjon om en persons arbeidshistorikk. Registeret er også viktig for å kunne få oppdaterte opplysninger om nye arbeidsforhold under klareringens gyldighetstid.

I *bokstav g* er namsmyndighetene lagt til i listen over relevante registre. Dette omfatter både de alminnelige namsmenn og særnamsmyndigheter. Også Kartverkets registre og Brønnøysundregistrene er nye, jf. bokstav h og i. Fra disse virksomhetene kan det blant annet innhentes opplysninger fra Gjeldsordningsregisteret, Konkurskaranteneregisteret og tinglysingsregistrene.

Bestemmelsens *andre ledd* tilsvarer gjeldende bestemmelse i forskrift om personellsikkerhet § 3-4 tredje ledd. Det er imidlertid foretatt nødvendige tilpasninger grunnet endring av hvilke registre som er relevant for personkontroll.

8.2.6 Til § 10 Registre for personkontroll ved adgangsklarering

Bestemmelsen er utledet av § 9, men med færre registre. Hvilke registre som er relevante er utledet fra vurderingsgrunnlaget ved adgangsklarering. Registre ved Brønnøysundregistrene og kommersielle registre med inkasso- og kredittopplysninger er følgelig ikke relevante ved adgangsklarering.

Bestemmelsens *tredje ledd* er ny og lister registre som avleses for nærstående som inntas i personkontrollen for utvidet adgangsklarering. Hvilke registre som inngår i listen er tilpasset til hvilke temaer som skal inngå i vurderingsgrunnlaget etter § 14.

8.2.7 Til § 11 Innhenting av personkontrollopplysninger fra andre stater

Bestemmelsen tilsvarer langt på vei gjeldende forskrift om personellsikkerhet § 3-5.

Bestemmelsen tydeliggjør at tilsvarende opplysninger for personkontroll kan innhentes fra andre staters myndigheter. Av hensyn til både nasjonale sikkerhetsinteresser og personvernet avgrenses hvilke opplysninger som da kan gis til den andre staten.

Formuleringen i gjeldende forskrift om personellsikkerhet § 3-5 om at NSM kan benytte annet forvaltningsorgan til å innhente personkontrollopplysninger fra utlandet, er ikke videreført i denne paragrafen, uten at det er ment å innebære en realitetsendring. Begrunnelsen for at den delen av bestemmelsen ikke er videreført, er at departementet mener NSM ikke trenger hjemmel i forskrift for å gi et annet forvaltningsorgan fullmakt til å utføre en slik oppgave. NSM har derfor mulighet til å fortsatt benytte PST til å innhente personkontrollopplysninger fra utlandet, dersom NSM og PST finner det hensiktsmessig.

8.2.8 Til § 12 Behandlingsansvarliges plikter ved utlevering av opplysninger

Bestemmelsen tilsvarer gjeldende bestemmelse i forskrift om personellsikkerhet § 3-4 fjerde ledd. Bestemmelsen må sees i sammenheng med ny sikkerhetslovs § 8-4 niende ledd om at behandlingsansvarlig skal legge til rette for digital overføring av opplysningene.

8.2.9 Til § 13 Bruk av opplysninger fra registre hos politiet og Politiets sikkerhetstjeneste

Bestemmelsen er ny og søker å ivareta hensynet til operative og forebyggende behov hos politiet/PST og NSM/ klareringsmyndighetene. Kriteriene som avtales vil kunne ha betydning for om og hvordan NSM og klareringsmyndigheten behandler opplysninger fra de nevnte registrene og i

hvilken grad slike opplysninger eventuelt kan videreformidles til en person som er vurdert klarert i forbindelse med begrunnelse og innsyn. De avtalte kriteriene skal balansere flere hensyn, bl.a. behovet for beskyttelse av opplysningene, kildene, de operative og forebyggende behovene og personers rett til innsyn i egen klareringssak.

For å tydeliggjøre at eventuell uenighet mellom politiet/PST og NSM skal løftes til departementet, er det tatt inn en bestemmelse om at ved uenighet skal bruken av opplysningene avgjøres av Justis- og beredskapsdepartementet.

8.2.10 Til § 14 Personhistorikk

Bestemmelsens *første ledd* tilsvarer gjeldende bestemmelse i forskrift om personellsikkerhet § 3-7 første ledd.

Andre ledd er nytt og stiller krav til personhistorikk for begge typer adgangsklarering. Adgangsklarering skal være en mindre inngripende klarering enn sikkerhetsklarering. Departementet foreslår derfor at krav til personhistorikk er kortere for adgangsklarering (5 år) enn for sikkerhetsklarering som er omhandlet i første ledd (10 år).

Fjerde ledd gir mulighet til å gjøre unntak fra kravet om personhistorikk dersom bakgrunnen for at det ikke foreligger personhistorikk er årsaker i stor grad veier opp for risikoen ved å klarere personen. Dette kan f.eks. være aktuelt der personen har oppholdt seg i et land vi ikke har sikkerhetssamarbeid med i forbindelse med tjeneste for den norske stat, humanitære organisasjoner, eller har hatt et studieopphold i det aktuelle landet. Det kan også være aktuelt å bruke bestemmelsen der en norsk statsborger som skal klareres for HEMMELIG er gift med en person fra et land vi ikke har sikkerhetsmessig samarbeid med, og hvor det da ikke er tilgang på personkontrollopplysninger, men hvor etterretningstrusselen fra det aktuelle landet er lav. Momentene som skal vektlegges er forhold som gjør at vi kan vite hvor personen har vært og hvorfor vedkommende. Departementet mener at et slikt unntak er nødvendig i et mer og mer globalisert samfunnet der personell flytter seg mellom land i mye større grad enn tidligere.

Bestemmelsen forutsetter imidlertid at det gjøres en helhetsvurdering der risikoen forbundet med å gi klarering basert på manglende tilgang til personkontrollopplysninger må holdes opp mot de andre opplysningene som foreligger om personen, jf. § 8-4 fjerde ledd, og i hvilken grad klarering kan gis på vilkår. Det kan også vurderes om det finnes andre måter, f.eks. kontakt med arbeidsgivere, utdanningsinstitusjonen vedkommende hevder å ha vært student ved, eller andre for å verifisere at oppholdet har funnet sted for det angitte formålet, og med det kompensere for den manglende tilgangen på personopplysninger. Det må i de tilfellene inngå i vurderingen hvilken tillitt man kan ha til kildene.

Femte ledd slår fast at en klarering fra en annen stat kan legges til grunn i stedet for tilgang til personkontrollopplysninger fra den andre staten. Bestemmelsen gjelder for de tilfellene hvor det skal gis en *norsk* sikkerhetsklarering til en person som allerede har en utenlandsk klarering, og den utenlandske klareringen gjør det unødvendig å innhente personkontrollopplysninger fra staten som har utstedt klareringen. Klareringsmyndigheten må likevel vurdere om det er behov for å innhente ytterligere personkontrollopplysninger, f.eks. dersom den utenlandske klareringen er såpass gammel at det kan foreligge nye forhold som det bør innhentes opplysninger om.

8.3 Til kapittel 3 Sikkerhetsklarering og adgangsklarering

8.3.1 Til § 15 Vurderingsgrunnlaget for adgangsklarering

Bestemmelsen er ny. *Første ledd* fastsetter hvilke vurderingskriterier og forhold etter ny sikkerhetslovs 8-4 fjerde ledd det kan legges vekt på i vurderingen av om adgangsklarering kan gis. I vurderingen etter bokstav a er det foretatt en avgrensing av vurderingstemaene. Hensikten er å få frem at formålet med adgangsklarering i hovedsak omhandler forebygging mot forberedelser til og forsøk på terror. Avgrensingen er imidlertid ikke absolutt. Dersom tilknytning til spionasje eller sabotasje for fremmed stat likevel skulle fremkomme, kan også det legges vekt på. For øvrig kan det legges vekt på forhold etter bokstav b, d, l og m.

I bestemmelsens *andre ledd* fastsettes hvilke vurderingskriterier og forhold etter lovforslagets § 8-4 fjerde ledd det kan legges vekt på i vurderingen av om utvidet adgangsklarering kan gis. Ved utvidet adgangsklarering er det ingen avgrensing av vurderingstemaene i bokstav a. Vurderingsgrunnlaget omhandler, i tillegg til terror, i like stor grad forebygging mot spionasje og sabotasje. For øvrig kan det i tillegg til sikkerhetsloven § 8-4 bokstav b, d, l, legges vekt på bokstav k om økonomiske forhold og bokstav n om tilknytning til andre stater.

8.3.2 Til § 16 Vurderingsgrunnlaget for tilknytning til andre stater

Bestemmelsen tilsvarer materielt sett gjeldende forskrift om personellsikkerhet § 3-3 tredje ledd. Hensikten er å regulere at klareringsmyndighetene benytter samme relevante og autorative kilde som grunnlag for å vurdere tilknytning til andre stater. Bestemmelsen forutsetter at NSM fortsatt utarbeider konkrete personellsikkerhetsmessige vurderinger av andre stater. Departementet ber om høringsinstansenes innspill på bestemmelsen, herunder om momentene i tilknytningsvurderingen bør fremgå tydeligere av forskriftene.

8.3.3 Til § 17 Klareringsintervju

Bestemmelsen tilsvarer gjeldende bestemmelse i forskrift om personellsikkerhet § 4-2, men med enkelte endringer.

I bestemmelsens *overskrift* og *første ledd* er begrepet «sikkerhetssamtale» erstattet med «klareringsintervju» av pedagogiske hensyn til personen som skal vurderes klarert. Erfaring fra klareringsmyndighetene viser at enkelte som har blitt innkalt til sikkerhetssamtale, der uttrykket «sikkerhetssamtale» har blitt brukt, har misforstått hva samtalen skulle handle om. Disse har oppfattet at dialogen innholdsmessig skulle omhandle sikkerhetsbestemmelser eller sikkerhetsrisiko, og foregå i form av likeverdig mulighet for å styre dialogen og gjensidig forsøk på å forstå hverandre. At dialogen i stedet benevnes som intervju i forbindelse med en klareringssak, vil gjøre det tydeligere at det er klareringsmyndigheten som styrer dialogen i den hensikt at den intervjuede skal bidra til å opplyse klareringssaken.

Bestemmelsens *andre ledd* er ny og viser til formålet med intervjuet og den rettslige rammen for hvilke temaer klareringsmyndigheten kan vektlegge under intervjuet følger av ny sikkerhetslov § 8-4 fjerde ledd. Rammen skal ikke forhindre deltakerne i intervjuet å snakke om øvrige forhold, men dette faller da utenfor vurderingen klareringsmyndigheten gjør i etterkant av intervjuet.

I *tredje ledd* er dokumentasjonskravet endret fra skriftlighet til lydopptak av hensyn til rettssikkerhet og effektivitet i saksbehandlingen. Samtykkekravet ved bruk av audiovisuelt opptak er endret slik at det kreves positivt samtykke fra personen. Departementet mener et krav om positivt samtykke vil styrke personvernet, samtidig som det er til liten byrde for klareringsmyndighetene å be om det. Bestemmelsen angir ikke formkrav til samtykke, men det forutsettes at samtykket dokumenteres.

Bestemmelsens *fjerde og femte ledd* tilsvarer gjeldende bestemmelse om bisitter, men med en ny regel om at bruk av bisitter og bisitters identitet må være innmeldt til klareringsmyndigheten i forkant av samtalen. Kravet om melding må sees i sammenheng med avgrensningen om hvem som kan stille som bisitter i andre punktum og avvisningsmuligheten i tredje punktum, samt hensynet til klareringsmyndighetens planlegging av intervjuet og effektiv saksgang.

Bestemmelsens *sjette ledd* er ny.

8.3.4 Til § 18 Vurdering av om lavere klareringsnivå kan gis og bruk av vilkår

Bestemmelsens *første ledd* tilsvarer bestemmelsen i gjeldende forskrift om personellsikkerhet § 4-3.

I *andre ledd* oppstilles prinsippet for bruk av vilkår for klarering. At vilkåret skal være tilstrekkelig risikoreduserende fremgår av motivene til sikkerhetsloven § 8-6, og er tatt inn i forskriften av pedagogiske hensyn. Departementet bemerker at eventuelle vilkår skal være kontrollerbare, samtidig som de er realistiske og ikke uforholdsmessig inngripende for personen det gjelder. Dette vil bidra til en effektiv og rimelig oppfølging av vilkårene.

8.3.5 Til § 19 Karantene før ny klareringsvurdering

Bestemmelsen tilsvarer gjeldene bestemmelse i forskrift om personellsikkerhet § 4-4 andre ledd andre til femte punktum. Hensikten med å sette en karantene er å gi den klarerte en indikasjon på hvor lenge det minimum vil ta før vedkommende igjen kan bli vurdert klarert. I tillegg vil en karantene gjøre at klareringsmyndigheten ikke blir belastet unødig med stadige forespørsler om klarering for en person som nylig har fått avslag på tilsvarende forespørsel fremsendt av en annen autorisasjonsansvarlig. Det er gjort enkelte endringer i ordlyden, blant annet er uttrykket «observasjonstid» erstattet med «karantene».

8.3.6 Til § 20 Melding om klareringsavgjørelse

Bestemmelsens *første og andre ledd* om melding tilsvarer gjeldene bestemmelser i forskrift om personellsikkerhet § 4-4 første og tredje ledd, med presisering om at både eventuell karantene og vilkår skal følge meldingen. Begrepet «melding» er valgt i stedet for «klareringsbevis» for å gjøre bestemmelsen tilpasningsdyktig til eventuell utvikling i måten klareringsmyndigheten svarer virksomheten på forespørsel om klarering.

Melding kan fortsatt gis i listeform, jf. gjeldende forskrift § 4-4 første ledd andre punktum, men bestemmelsens *andre ledd* presiserer at melding om *avslag* på forespørsel ikke kan gis i listeform.

Bestemmelsens *tredje ledd* tilsvarer gjeldende bestemmelse i forskrift om personellsikkerhet § 4-5 første ledd. I sammenheng med ny bestemmelse i § 15 om avtale om bruk av opplysninger fra politiet og PST, vil innhenting av tillatelse til videreformidling av opplysninger i praksis være aktuelt der klareringsmyndigheten ikke har fått informasjon om vilkår i avtale mellom NSM og registereier om videreformidling av opplysningene.

8.3.7 Til § 21 Innsyn i klareringssak

Bestemmelsens *første ledd* er ny og gjenspeiler prinsippet i § 20 siste ledd om at tillatelse må innhentes fra visse virksomheter for å beskytte blant annet kilder og pågående operasjoner, dersom slike vilkår ikke fremkommer av avtale mellom NSM og registereier som er gjort tilgjengelig for klareringsmyndigheten.

Bestemmelsens *andre ledd* er utledet av gjeldende sikkerhetslov § 25 a første ledd annet punktum og tredje ledd annet punktum og presiserer hvordan innsyn med hjemmel i ny sikkerhetslov § 8-14 i de

elektroniske lagringsmediene av klareringsintervju skal gis. Innsyn i eventuell skriftlig dokumentasjon avgjøres etter de generelle reglene om innsyn i lovens § 8-14.

8.3.8 Til § 22 Gyldighetstid for sikkerhetsklarering og adgangsklarering

Bestemmelsens *første ledd* tilsvarer gjeldende bestemmelse i forskrift om personellsikkerhet § 4-8 første ledd første punktum. I tillegg tas høyde for at internasjonale avtaler eller regler som Norge har forpliktet seg til, kan sette begrensninger i gyldighetstiden på enkelte typer klareringer. Det er i *andre punktum* tilført en regel om utvidelse av gyldighetstid for en klarering i særskilte tilfeller. Slik utvidelse kan være ønskelig der det foreligger et fortsatt klareringsbehov og en pågående klareringssak (reklarering) ikke kan avsluttes før gyldighetstiden på gjeldende klarering utløper. Det forutsettes likevel at utvidelse etter denne regelen kun skjer der det foreligger særskilte omstendigheter og der utvidelsen er nødvendig. For eksempel der forespørsel om klarering er innsendt i tide, men saken er forsinket av grunner virksomheten eller klareringsmyndigheten ikke rår over. Det forutsettes også at klareringsmyndigheten gjør en vurdering av om det er sikkerhetsmessig forsvarlig med slik forlengelse. Bestemmelsen vil også harmonisere med NATOs bestemmelser om utvidelse av gyldighetstiden for sikkerhetsklarering for NATO-gradert informasjon.

I *andre ledd* videreføres gjeldende bestemmelse i forskrift om personellsikkerhet § 4-8 fjerde ledd, men med endret ordlyd. Opplysninger om endring i sivil status som angitt i bestemmelsen gir grunnlag for ny personkontroll med hjemmel i sikkerhetsloven § 8-5 tredje ledd. Omfanget av personkontrollen vurderes av klareringsmyndigheten. For eksempel kan det bare foretas personkontroll av personer som er nye i kontrollomfanget.

I *tredje ledd* er det tydeliggjort at opprettholdelse av gjeldende klareringer ikke får til følge at gyldighetstiden på klareringen endres eller forlenges. Dette fordi det forventes at en forlengelse av gyldighetstiden følges av en begrunnelse for klareringsbehov av virksomhetens autorisasjonsansvarlig. I tredje ledd annet punktum fastsettes det at ved en ny klareringsavgjørelse basert på en fullstendig personkontroll settes gyldighetstid etter første ledd.

8.3.9 Til § 23 Betydningen av forhold som ble vurdert ved en tidligere klareringsavgjørelse

Bestemmelsen tilsvarer gjeldende bestemmelse i forskrift om personellsikkerhet § 4-8 første ledd andre punktum, men med mindre endringer i ordlyden.

8.3.10 Til § 24 Bevaring, kassasjon og avlevering av dokumenter i klareringssaker

Det er nødvendig å fastsette bestemmelser om bevaring, kassasjon og avlevering av dokumenter i klareringssaker. Departementet anser imidlertid at bestemmelser om slike arkivfaglige forhold ikke er bestemmende for rettigheter eller plikter for personene som klareres. Bestemmelsene vil bare gjelde for klareringsmyndighetene, som alle er forvaltningsorganer, og kan bli forholdsvis detaljerte. Departementet foreslår derfor at NSM gis rett og plikt til å fastsette slike bestemmelser i en instruks som skal gjelde for klareringsmyndighetene, klageinstansene og NSM selv i rollen som personkontrollinstans.

8.3.11 Til § 25 Dekning av kostnader ved klarering

Bestemmelsen tilsvarer gjeldende bestemmelser i forskrift om personellsikkerhet § 6-11, men med noe endret ordlyd.

8.4 Til kapittel 4 Samtykke til å autorisere utenlandske statsborgere for BEGRENSET

8.4.1 Til § 26 Samtykke til å autorisere utenlandske statsborgere for begrenset

Bestemmelsen er ny og gjelder krav til samtykke fra klareringsmyndigheten til autorisasjon av utenlandske statsborgere for BEGRENSET, og hva autorisasjonsansvarlig skal opplyse om. Formålet med bestemmelsen er å unngå at det gis tilgang til gradert informasjon i større grad enn hva det strengt tatt er behov for, og at det ikke gis autorisasjon uten at risikoen knyttet til etterretningstrusselen fra personellet hjemstat er vurdert. Autorisasjonsansvarlig vil ikke ha tilgang til NSMs personellsikkerhetsmessige landvurderinger, slik klareringsmyndigheten vil ha.

Bestemmelsene i kapittel 4 skal også sikre at klareringsmyndigheten har oversikt over utenlandsk personell som skal gis tilgang til BEGRENSET informasjon.

Autorisasjonsansvarlig må opplyse om hvilken stilling vedkommende skal ha, og hvorfor det er nødvendig å gi tilgang til BEGRENSET informasjon for personer som har denne stillingen.

Departementet har ikke foreslått egne klagebestemmelser for saker der NSM i vedtaket ikke gir samtykke. Departementet legger til grunn at for private rettssubjekter gjelder de alminnelige bestemmelsene om klage i forvaltningsloven kapittel VI.

Departementet ser at de bestemmelsene som foreslås i kapittel 4 kan bli i overkant omstendelige å gjennomføre i praksis, tatt i betraktning den risiko autorisering av personell for BEGRENSET innebærer for nasjonale sikkerhetsinteresser. Departementet ber derfor om høringsinstansenes innspill, og vil vurdere etter høringsrunden hvorvidt det er hensiktsmessig å videreføre bestemmelsene i kapittel 4. Et alternativ er at virksomhetene blir gjort kjent med NSMs vurdering av andre stater, jf. § 16.

8.4.2 Til § 27 Egenopplysninger

Bestemmelsen fastsetter rammen for hvilke opplysninger klareringsmyndigheten kan kreve av utenlandske statsborgere for avgjørelse om tillatelse for autorisasjon for BEGRENSET. De opplysningene som innhentes antas å være egnet til å vurdere risikoen forbundet må å gi den utenlandske statsborgeren tilgang til BEGRENSET informasjon.

8.4.3 Til § 28 Saksbehandling og avgjørelse om samtykke til autorisasjon

Bestemmelsen skal legge til rette for at autorisasjon gis på bakgrunn av klareringsmyndighetens tilgang til NSMs personellsikkerhetsmessige landvurderinger, og autorisasjonsansvarliges vurdering av personellet, slik at samtykke gis på bakgrunn av en helhetlig forståelse av risikoen forbundet med å gi tilgang til BEGRENSET informasjon. Det vil være relevant å legge vekt på hvor mange utenlandske statsborgere som er autorisert i en virksomhet.

Departementet forutsetter at det bare vil skje helt unntaksvis at samtykke ikke kan gis f.eks. der risikoen ved å gi tilgang er så stor at den ikke vil kunne reduseres gjennom den tilgangskontroll autorisasjonsprosessen gir.

8.5 Til kapittel 5 Leverandørklarering

8.5.1 Til § 29 Klareringsmyndighet for leverandørklarering

Det er i gjeldende praksis for sikkerhetsavtaler mellom stater ikke vanlig at det tas inn en hjemmel til å kontrollere leverandører som holder til i den andre staten. I stedet legges det opp til at statenes sikkerhetsmyndigheter bare skal kontrollere leverandører som holder til på statens eget territorium. Av den grunn er også leverandørklareringsmyndigheten lagt til sikkerhetsmyndigheten i staten der leverandøren holder til. Det er i bestemmelsen derfor presisert at myndigheten bare gjelder norske leverandører. Utenlandske leverandører må klareres av sitt hjemlands sikkerhetsmyndigheter.

8.5.2 Til § 30 Egenopplysninger fra leverandøren

For å oppnå en effektiv saksbehandling og forutsigbarhet om hvilke opplysninger leverandøren skal gi til klareringsmyndigheten, er det behov for et skjema for formålet. Private rettssubjekter kan imidlertid ikke pålegges å gi opplysningene på en bestemt måte, uten at det er fastsatt i lov eller forskrift. Departementet foreslår derfor en ny bestemmelse i *første ledd* om at leverandøren skal benytte et skjema fastsatt av NSM.

Med «skjema» menes ikke at det nødvendigvis må være på papir. I prinsippet kan også elektronisk skjema benyttes, så lenge kravene til informasjonssystemet oppfyller kravene i sikkerhetsloven og eventuelt også personopplysningsloven.

I *andre ledd* er det fastsatt hvilke type opplysninger leverandøren skal gi i forbindelse med klareringssaken. Bestemmelsen er nødvendig som hjemmelsgrunnlag for hvilke opplysninger skjemaet skal inneholde. Opplysningene som er listet opp er i hovedsak de samme opplysningene som klareringsmyndigheten ber om etter gjeldende praksis, og innenfor rammen av sikkerhetsloven § 9-3 tredje ledd.

8.5.3 Til § 31 Vurderingsgrunnlaget for leverandørklarering

Paragrafen tilsvarer bestemmelsene i gjeldende forskrift om sikkerhetsgraderte anskaffelser § 3-2, men med enkelte språklige endringer.

Med «virksomhetens straffbare forhold» i *bokstav d* menes handlinger eller unnlatelser som kan kvalifisere til foretaksstraff. I likhet med vurdering av straffbare forhold ved klarering av personer, er det forholdets art og den betydning det har for leverandørens sikkerhetsmessige skikkethet, som er det sentrale i vurderingen etter bokstav e. Hvorvidt det er ilagt en straffereaksjon og hvor streng reaksjonen var, er et moment i vurderingen av forholdets relevans og vekt for klareringen, men er ikke avgjørende. Andre momenter det også må legges vekt på i vurderingen er bl.a. hvor lenge det er siden, årsaksforholdene og om det er gjentatte forhold. Også der det er mistanke og henleggelser skal en slik vurdering gjøres, jf. at beviskravet for straff er langt høyere enn i sivile saker og forvaltningsvedtak som dette er. Hvilken henleggelsesgrunn som er brukt kan ha betydning for vurderingen.

Andre og tredje ledd regulerer klarering av leverandørens øverste ledelse, som del av leverandørklareringen. Med virksomhetens leder menes den som i selskapsretten betegnes som daglig leder eller den med tilsvarende innflytelse over virksomhetens drift som daglig leder i selskapsrettens forstand. Daglig leder er normalt ansvarlig for styringssystemet for sikkerhet og beskyttelsen av de skjermingsverdige verdiene som leverandøren råder over. Daglig leder vil også ha en posisjon og innflytelse som gjør at vedkommende lett vil kunne tilegne seg tilgang til de

skjermingsverdige verdiene. Det er derfor naturlig at daglig leder klareres. Når det gjelder styremedlemmer, er bestemmelsen begrunnet i at disse, for å kunne ivareta sitt ansvar, har rett til å få innsyn i selskapets informasjon, herunder sikkerhetsgradert informasjon. Det er derfor krav om klarering også av leverandørens styremedlemmer. Dersom klarering ikke kan oppnås, må disse alternativt gi avkall på innsynsretten.

I et konsern er det den juridiske personen som forpliktes i kontrakten som er leverandøren i forskriftenes forstand. Avhengig av den juridiske konstruksjonen av konsernet, vil dette kunne være daglig leder av den leverandøren som forpliktes i kontrakten.

Kravet om klarering av leverandørens øverste ledelse kommer i tillegg til kravet om klarering og autorisasjon av personer som er ment å få tilgang til sikkerhetsgradert informasjon eller skjermingsverdig objekt og infrastruktur i forbindelse med anskaffelsen.

8.5.4 Til § 32 Kilder for leverandørkontroll

Bestemmelsen om hvilke kilder som inngår i leverandørkontrollen, er ny.

Departementet anser at det av hensyn til leverandørene som kontrolleres er viktig at det er fastsatt tydelig hvilke type registre som kontrolleres. Bestemmelsen vil også være en viktig føring for klareringsmyndigheten om hvilke type registre som kan kontrolleres. En slik tydeliggjøring bidrar til økt forutsigbarhet og til å unngå usaklig forskjellsbehandling i saksbehandlingen.

Bestemmelsen er formet etter mønster fra den lignende bestemmelsen om kilder for personkontroll. Kildene som er listet opp er i hovedsak en kodifisering av klareringsmyndighetens gjeldende praksis.

Registrene angitt i bokstav e omfatter registre der brukere kan kontrollere kvalitetssikret informasjon om leverandørene. f.eks. leverandørenes forsikringer, forpliktelse til å følge HMS- og kvalitetsstandarder, sertifiseringer, sikkerhetserklæringer og økonomiske forhold.

Registrene angitt i bokstav f omfatter registre hos inkassoforetak og kredittopplysningsforetak. I registrene er det opplysninger om bl.a. betalingsanmerkninger, inkassosaker og kredittvurderinger.

Registrene i bokstav e og f henter og sammenstiller i stor grad opplysninger fra ulike offentlige og private registre om foretak. Registrene kan også inneholde opplysninger fra kunder som benytter f.eks. inkassotjenester. Tilgang tilbys som en tjeneste gratis eller mot vederlag.

Opplysninger fra klareringsmyndighetens egne registre, som det vises til i bokstav g, kan f.eks. være opplysninger fra utførte tilsyn, klareringsmyndighetens kontroller i tidligere saker, innrapporterte sikkerhetstruende hendelser og avvik hos leverandøren, eller varslinger etter arbeidsmiljøloven om brudd på sikkerhetsloven.

8.5.5 Til § 33 Kontroll av om leverandøren oppfyller sikkerhetskravene

Første ledd fastsetter at kontroll av om leverandøren oppfyller sikkerhetskravene skal foretas før vedtak om leverandørklarering. Det brukes her begrepet «kontroll», ikke «tilsyn», da leverandørklareringsmyndigheten ikke nødvendigvis er et tilsynsorgan med påleggskompetanse. Kontrollen blir i dette tilfellet kun utført med hensyn på å innhente informasjon knyttet til om leverandørklarerings kan gis eller opprettholdes. Rent metodisk kan det legges til grunn samme type metodikk for innhenting av informasjon, systemrevisjoner og inspeksjoner som det gjøres for tilsyn. Resultatet av kontrollen vil inngå som en del av opplysningene det skal legges vekt på etter § 31. Kravet om slik kontroll tilsvarer gjeldende forskrift om sikkerhetsgraderte anskaffelser § 2-7 andre og tredje ledd, men gir noen flere føringer.

For funksjonelle krav, som de nye forskriftene i stor grad legger opp til, er systemrevisjon normalt en mer egnet måte å føre kontroll på enn inspeksjon. Det kan imidlertid ikke utelukkes at for enkelte typer krav i regelverket og etter uønskede hendelser er f.eks. inspeksjon et mer egnet virkemiddel.

Kravet i gjeldende forskrift om sikkerhetsgraderte anskaffelser om at ny kontroll skal gjennomføres hver minst hver 18. måned er ikke videreført. Departementet anser at det ikke bør være et fast tidsintervall for ny kontroll men at det gjøres etter en vurdering av risiko, men senest når ny leverandørklarering gis, f.eks. at klareringsmyndigheten blir kjent med ny trusselinformasjon, eller forhold hos leverandøren som tilsier at det bør gjøres en ny vurdering av leverandørens klarering.

Departementet foreslår i *fjerde ledd* at klareringsmyndigheten kan avtale at kontrollen skal gjennomføres av oppdragsgiver. Dersom en slik fullmakt gis, er det en forutsetning at oppdragsgiveren har tilstrekkelig fagkompetanse.

I *femte ledd* er det fastsatt et unntak fra hovedregelen i første ledd. Bestemmelsen er begrunnet i at enkelte stater kan kreve i sikkerhetsavtaler med Norge at NSM skal utføre kontrollen av om leverandører har oppfylt sikkerhetslovens krav.

8.5.6 Til § 34 Tilbakekall av leverandørklarering

Bestemmelsen åpner for at en klarering kan kalles tilbake dersom det oppdages avvik fra sikkerhetskravene etter at klareringen er gitt. Klareringsmyndigheten skal fastsette en rimelig frist for retting av avvikene. Hvor lang frist som skal gis vil avhenge av hvor omfattende avvikene er. Dersom det konstateres avvik som kan medføre en umiddelbar trussel mot nasjonale sikkerhetsinteresser, f.eks. at leverandøren ikke har tilstrekkelig adgangskontroll av personer som har tilgang til sikkerhetsgradert informasjon, kan klareringen trekkes tilbake dersom avviket ikke kan rettes umiddelbart.

8.5.7 Til § 35 Leverandørklareringens gyldighetstid

Bestemmelsen fastsetter at leverandørklareringen kan vare i inntil fem år. Bestemmelsen tilsvarer gjeldende forskrift om sikkerhetsgraderte anskaffelser § 3-1 fjerde ledd. Med uttrykket «inntil» fem år, åpnes det imidlertid for en viss fleksibilitet, f.eks. hvis det på klareringstidspunktet er åpenbart at leverandørklareringen ikke vil bli benyttet i fem år, eller leverandøren ikke ønsker å opprettholde sikkerhetstiltakene når oppdraget som utløser klareringsbehovet er ferdig.

8.5.8 Til § 36 Registrering av klareringsavgjørelser

Bestemmelsen fastsetter at avgjørelser skal registreres i det sentrale registeret over leverandørklareringer. Det er ikke fastsatt hvem som skal foreta registreringen. Departementet antar at det er naturlig og mest effektivt at dersom klareringsmyndigheten blir lagt til et annet organ, får dette organet tilgang av NSM til registeret for selv å foreta registreringen. Det er imidlertid ikke noe i veien for at klareringsmyndigheten bare rapporterer klareringsavgjørelsen til NSM, som er behandlingsansvarlig for registeret, og at NSM så foretar registreringen. Departementet antar at det normalt vil være mest hensiktsmessig av klareringsmyndigheten foretar registreringen i det felles informasjonssystem for behandling.

8.6 Til kapittel 6 Særbestemmelser for domstolene

8.6.1 Til § 37 Kapitlets virkeområde

Bestemmelsen er i hovedsak en videreføring av gjeldende forskrift om personellsikkerhet § 7-1. Uttrykket «lagrettemedlemmer» er imidlertid tatt ut som følge av at juryordningen er avskaffet fra

og med 1. januar 2018. Det legges til grunn at det ikke vil bli gjennomført straffesaker med jury etter 1. januar 2019. I motsatt fall må det etableres overgangsbestemmelse for lagrettemedlemmer.

8.6.2 Til § 38 Klareringsmyndighet og autorisasjonsansvarlig

Bestemmelsen tilsvarer i stor grad gjeldende forskrift om personellsikkerhet § 7-2, men med en viktig endring.

Etter gjeldende bestemmelser er det førstelagmannen i hver lagmannsrett som er klareringsmyndighet for lagmannsretten og lavere rettsinstanser. Det er meget få klareringssaker i domstolene. En slik spredning av klareringsmyndighet fører til at det er vanskelig for domstolene å over tid bygge opp og vedlikeholde god kompetanse om behandling av klareringssaker. Departementet viser til at begrunnelsen i Prop. 97 L (2015-2016) kapittel 9 for å samle øvrige klareringsmyndigheter hos i hovedsak to store klareringsmyndigheter, var hensynet til enhetlig saksbehandling, robuste fagmiljøer, individets rettssikkerhet og sikkerheten i sektoren. Departementet anser derfor at klareringsmyndigheten for domstolene med fordel kan samles hos én klareringsmyndighet. Domstolsadministrasjonen har imidlertid i brev til FD i 2016 gitt utrykk for at de ønsker at gjeldende særregler om hvem som er klareringsmyndighet for domstolene videreføres.

Departementet vil av hensyn til domstolenes uavhengighet, være varsom med å gjøre endringer i klareringsmyndigheten for domstolene. Spesielt dersom domstolene selv og Domstolsadministrasjonen ikke ønsker endringer i ordningen. Departementet ønsker imidlertid å legge til rette for at domstolene ved førstelagmannen får anledning til selv å avgjøre om de vil avtale med Sivil klareringsmyndighet at sistnevnte utøver deres klareringsmyndighet etter fullmakt. Vedtak i Sivil klareringsmyndighet fattet etter fullmakt fra førstelagmannen vil, hvis de påklages, fortsatt måtte behandles av Høyesterett ved justitiarius. Det at landets øverste domstol da fortsatt avgjør klagesakene, gjør at domstolenes uavhengighet kan sies å fortsatt være i behold også ved en slik ordning.

På bakgrunn av ovennevnte foreslår departementet en ny bestemmelse i tredje ledd, om at førstelagmannen og Sivil klareringsmyndighet kan avtale at klareringsmyndighet etter andre ledd utøves av Sivil klareringsmyndighet. For at det ikke skal være tvil om særbestemmelsene i kapittelet for øvrig også gjelder i slike tilfeller, er dette presisert i leddet. Det vil blant annet si at det i slike saker er Høyesterettsjustitiarius, og ikke NSM, som er klageinstans.

8.6.3 Til § 39 Forhåndsvalg av domstoler for enkeltstående rettergangsskritt i straffesaker

Bestemmelsen er en videreføring av gjeldende forskrift om personellsikkerhet § 7-3, med noen mindre språklige justeringer.

8.6.4 Til § 40 Sikkerhetsklarering og autorisasjon av meddommere

Bestemmelsen er en videreføring av gjeldende forskrift om personellsikkerhet § 7-4. Uttrykket «lagrettemedlemmer» er imidlertid tatt ut som følge av at juryordningen er avskaffet fra og med 1. januar 2018. Det legges til grunn at det ikke vil bli gjennomført straffesaker med jury etter 1. januar 2019. I motsatt fall må det etableres overgangsbestemmelse for lagrettemedlemmer. I tillegg er bestemmelsen kortet ned, uten at det er ment å innebære materielle endringer i bestemmelsen. Meddommere skal fortsatt trekkes ut etter de alminnelige bestemmelsene i domstolsloven kapittel 5.

8.6.5 Til § 41 Unntak fra sikkerhetslovens bestemmelser

Bestemmelsen er en videreføring av gjeldende forskrift om personellsikkerhet § 7-5, men der de aktuelle henvisninger er endret til nye bestemmelser i lov om nasjonal sikkerhet: § 3-1 Tilsyn med virksomheter, § 3-4 Adgangsrett og varslingsplikt ved stedlige tilsyn, og § 3-6 Pålegg.

8.6.6 Til § 43 Overgangsregler

Overgangsreglene fastsetter at gjeldende sikkerhetsklareringer videreføres som forutsatt også etter at lov om nasjonal sikkerhet trer i kraft 1. januar 2019. Hensikten er å sikre en videreføring for klareringer slik at ikke alle må vurderes på nytt når den nye loven trer i kraft.

Dersom en person klager på en avgjørelse om sikkerhetsklarering, så skal regelverket som gjelder på vedtakstidspunktet for klagen legges til grunn. Dette innebærer at en klage høsten 2018 i en klareringssak som først blir avgjort i 2019, skal avgjøres etter reglene i den nye sikkerhetsloven.

9 Utkast til forskrift om myndighetens roller og ansvar for nasjonal sikkerhet

Kapittel 1. Departementenes roller og oppgaver

§ 1 Klassifisering av skjermingsverdige objekter og infrastruktur

Når departementene eller Nasjonal sikkerhetsmyndighet klassifiserer skjermingsverdige objekter og infrastruktur etter sikkerhetsloven § 7-2, skal de legge vekt på

a) i hvor stor grad grunnleggende nasjonale funksjoner er avhengig av objektet eller infrastrukturen
b) virksomhetens skadevurdering, jf. virksomhetsforskriften § 52

Dersom forholdene som ligger til grunn for vurderingen, endrer seg, skal departementet vurdere om det skal fattes et nytt vedtak om klassifisering.

Klassifiseringsnivået, og grunnlaget for klassifiseringen, skal sikkerhetsgraderes minst BEGRENSET. En oversikt over samtlige eller et større antall klassifiserte objekter eller infrastrukturer, skal sikkerhetsgraderes minst KONFIDENSIELT.

§ 2 Bruk av adgangsklarering

Et departement eller Nasjonal sikkerhetsmyndighet kan fatte vedtak etter sikkerhetsloven § 8-3 om adgangsklarering dersom fysisk eller elektronisk tilgang til hele eller deler av et klassifisert objekt eller en klassifisert infrastruktur, gjør det mulig å skade grunnleggende nasjonale funksjoner ved å redusere objektets eller infrastrukturens funksjonalitet, eller utsette objektet eller infrastrukturen for skadeverk, ødeleggelse eller rettsstridig overtakelse.

Det kan fattes vedtak om adgangsklarering der objektet eller infrastrukturen kan være et mål for terror, attentat eller annen alvorlig kriminalitet. Kan objektet eller infrastrukturen i stedet eller i tillegg være mål for spionasje eller sabotasje fra en annen stat, kan det fattes vedtak om utvidet adgangsklarering.

Departementenes vedtak skal sendes Nasjonal sikkerhetsmyndighet.

Kapittel 2. Nasjonal sikkerhetsmyndighets roller og ansvar

§ 3 Iverksettelse av inntrengningstesting, kommunikasjons- og innholdskontroll og testing av sikkerhetstiltak

Når virksomhetens leder ber om det kan Nasjonal sikkerhetsmyndighet iverksette inntrengningstesting, kommunikasjons- og innholdskontroll og testing av sikkerhetstiltak. Det skal inngås avtale med virksomheten om hvilket personell som skal stå for testingen og kontrollen, og hva testingen og kontrollen skal omfatte.

§ 4 Iverksettelse av tekniske sikkerhetsundersøkelser

Når virksomhetens leder ber om det kan Nasjonal sikkerhetsmyndighet iverksette tekniske sikkerhetsundersøkelser. Det skal inngås avtale med virksomheten om hvilket personell som skal stå for undersøkelsen, og hva undersøkelsen skal omfatte.

Nasjonal sikkerhetsmyndighet skal forhåndsvarsle Politiets sikkerhetstjeneste om at tekniske sikkerhetsundersøkelser skal gjennomføres. Politiets sikkerhetstjeneste skal likevel ikke varsles ved gjennomføring av tekniske sikkerhetsundersøkelser i Forsvaret.

I vurderingen av om tekniske sikkerhetsundersøkelser skal gjennomføres, skal det legges vekt på

a) om virksomheten kontrollerer områdene som grenser til rommet

b) om dette befinner seg i utlandet
c) graderingsnivå på tale som skal forekomme i rommet
d) om det er risiko for at uvedkommende har hatt tilgang til rommet siden forrige tekniske sikkerhetsundersøkelse.

§ 5 Fellesregler for tekniske sikkerhetsundersøkelser, inntrengningstesting, testing av sikkerhetstiltak og kommunikasjons- og innholdskontroll av informasjonssystemer

Den som gjennomfører tester, kontroller og undersøkelser som nevnt i sikkerhetsloven §§ 5-5, 6-5, 6-6 og 7-4 skal rapportere resultatene til virksomheten og myndigheten som fører tilsyn etter loven. Rapporten skal ikke unødig inneholde informasjon som identifiserer enkeltpersoner som måtte ha begått sikkerhetsbrudd.

Informasjonen fra undersøkelser, testing og kontroller skal slettes senest innen tre måneder etter at oppdraget er avsluttet. Informasjonen kan likevel bevares lengre enn tre måneder, dersom dette er nødvendig for å håndtere sårbarheter eller sikkerhetstruende virksomhet. Det samme gjelder dersom det er nødvendig av hensyn til kontrollvirksomheten til Stortingets kontrollorgan for etterretnings-, overvåkings- og sikkerhetstjeneste.

§ 6 Bruk av tredjepart til å utføre tekniske sikkerhetsundersøkelser, inntrengningstesting, testing av sikkerhetstiltak og kommunikasjons- og innholdskontroll av informasjonssystemer

Nasjonal sikkerhetsmyndighet kan utpeke virksomheter til å utføre tekniske sikkerhetsundersøkelser, inntrengningstesting, testing av sikkerhetstiltak og kommunikasjons- og innholdskontroll av informasjonssystemer.

Utpekingen skal baseres på en vurdering av om virksomheten er sikkerhetsmessig skikket, og om virksomhetens personell har nødvendig klarering og kompetanse til å utføre undersøkelsene, testene og kontrollene.

Nasjonal sikkerhetsmyndighet skal stille krav om at utpekte virksomheter etter første ledd skal utføre undersøkelser, tester og kontroller i samsvar med kriterier for utføring som fastsettes av Nasjonal sikkerhetsmyndighet.

§ 7 Om kryptosikkerhetstjenester

Nasjonal sikkerhetsmyndighet skal ivareta rollen som nasjonal distribusjonsmyndighet for nasjonalt kryptomateriell samt kryptomateriell mottatt fra fremmede stater og internasjonale organisasjoner, og skal ha regnskapsmessig oversikt over kryptomateriell. Med kryptomateriell menes kryptodokumenter, kryptonøkler og kryptoutstyr.

Nasjonal sikkerhetsmyndighet er nasjonalt kontaktpunkt mot distribusjonsmyndigheter i andre stater og internasjonale organisasjoner.

Nasjonal sikkerhetsmyndighet har det overordnede ansvaret for at bruk, forvaltning, produksjon av kryptomateriell og regnskapsmessig kontroll med kryptomateriell utføres i samsvar med sikkerhetsloven med forskrifter.

§ 8 Register over avgjørelser om personklarering

Nasjonal sikkerhetsmyndighet skal opprette et register over alle klareringsavgjørelser. Registeret skal inneholde informasjon om

a) klareringsstatus
b) vilkår knyttet til klareringen
c) den klarertes tilknytning til andre stater
d) hvilken virksomhet som har bedt om klareringen
e) den klarertes autorisasjonsstatus, når den er tilgjengelig.

Opplysninger om klareringsstatus kan utleveres til klareringsmyndigheter og autorisasjonsansvarlige.

Nasjonal sikkerhetsmyndighet skal på forespørsel utlevere informasjon fra registeret til Politiets sikkerhetstjeneste i samsvar med sikkerhetsloven § 8-12. Anses det nødvendig av hensynet til nasjonale sikkerhetsinteresser, kan Nasjonal sikkerhetsmyndighet på eget initiativ utlevere registerinformasjonen til Politiets sikkerhetstjeneste. En forespørsel om og utlevering av opplysninger skal være skriftlig.

Nasjonal sikkerhetsmyndighet skal i avtale med Politiets sikkerhetstjeneste fastsette til hva og hvordan opplysningene som utleveres til tjenesten, skal brukes. Det skal minst fastsettes hvordan hensynet til det opprinnelige formålet med opplysningene skal avveies mot hensynet til at opplysningene kan brukes for å ivareta tjenestens oppgaver etter politiloven § 17 b og § 17 c nr. 1. Ved uenighet skal bruken av opplysningene avgjøres av Justis- og beredskapsdepartementet.

§ 9 Register over leverandørklareringer og sikkerhetsgraderte anskaffelser

Nasjonal sikkerhetsmyndighet skal føre et register over alle leverandørklareringer. Registeret skal inneholde informasjon om

a) klareringsstatus
b) vilkår knyttet til klareringen
c) leverandørens tilknytning til andre stater
d) hvilken oppdragsgiver som har bedt om klareringen.

Nasjonal sikkerhetsmyndighet skal føre et register over alle sikkerhetsgraderte anskaffelser. Registeret skal inneholde opplysningene som oppdragsgiver har innmeldt i samsvar med virksomhetsforskriften § 76.

§ 10 Utlevering av opplysninger om klarering og personkontroll til andre staters myndigheter eller internasjonale organisasjoner

Nasjonal sikkerhetsmyndighet kan informere annen stats myndigheter eller internasjonale organisasjoner om at en person eller en leverandør er gitt klarering, og eventuelt for hvilken sikkerhetsgrad. Opplysninger om vilkår knyttet til klarering, nekting, tilbakekalling, nedsettelse eller suspensjon av klarering skal bare gis dersom det er av sikkerhetsmessig betydning for det landet som spør, og Norge har sikkerhetsmessig samarbeid med staten eller organisasjonen.

Nasjonal sikkerhetsmyndighet kan utlevere personkontrollopplysninger om norske statsborgere, og om personer som har eller har hatt opphold i Norge, i forbindelse med personkontroll som foretas av myndigheten i et annet land eller en internasjonal organisasjon som Norge har et sikkerhetssamarbeid med.

§ 11 Unntak fra krav om sikkerhetsklarering og autorisasjon

Når det er særlig behov for det kan Nasjonal sikkerhetsmyndighet dispensere fra kravet om klarering etter sikkerhetsloven § 8-1 andre ledd, og fra kravet i klareringsforskriften § 26 om samtykke til å autorisere utenlandske statsborgere for BEGRENSET. Et departement som har fattet vedtak om krav til adgangsklarering etter loven § 8-3, kan på tilsvarende måte dispensere fra eget vedtak.

I vurderingen av om det foreligger et særlig behov skal det legges vekt på om behovet for tilgang er større enn risikoen manglende klarering eller samtykke vil innebære for nasjonale sikkerhetsinteresser.

Kapittel 3. Nasjonal responsfunksjon og nasjonalt varslingssystem for digital infrastruktur

§ 12 Utøvelse av nasjonal responsfunksjon for alvorlige digitale angrep og nasjonalt varslingssystem for digital infrastruktur

Nasjonal sikkerhetsmyndighet skal drive en nasjonal responsfunksjon for alvorlige digitale angrep og et nasjonalt varslingssystem for digital infrastruktur.

Den nasjonale responsfunksjonen og varslingssystemet for digital infrastruktur skal innhente, analysere og dele informasjon om digitale angrep.

§ 13 Informasjonsbehandling og -deling

Nasjonal sikkerhetsmyndighet kan dele informasjon med partene i Felles Cyberkoordineringssenter når delingen er innenfor lovens formål og avtale er inngått etter virksomhetsforskriften § 56 andre ledd.

Ved fare for alvorlige hendelser skal Nasjonal sikkerhetsmyndighet informere berørte nasjonale og internasjonale aktører om trusler, sårbarheter og mulige tiltak.

Kapittel 4. Tilsyn

§ 14 Tildeling av tilsynsansvar

Før departementet bestemmer at en myndighet med sektoransvar skal føre tilsyn etter sikkerhetsloven, skal det gjøre en helhetsvurdering av om sektormyndigheten har tilstrekkelig tilsyns- og sikkerhetsfaglig kompetanse til å føre tilsyn etter sikkerhetsloven innenfor sin sektor, eller kan få slik kompetanse uten uforholdsmessige store utgifter. Det vil være relevant å se hen til tilsynsmyndighetens kompetanse på risikovurderinger og systemrevisjon, og hvorvidt det er hensiktsmessig at Nasjonal sikkerhetsmyndighet bistår i forbindelse med tilsyn innenfor enkelte fagområder.

En uttalelse fra Nasjonal sikkerhetsmyndighet skal inngå i helhetsvurderingen.

§ 15 Avtale om samarbeid mellom Nasjonal sikkerhetsmyndighet og andre myndigheter med tilsynsansvar

Avtale om samarbeid mellom Nasjonal sikkerhetsmyndighet og sektormyndighet, jf. sikkerhetsloven § 3-2 første ledd, skal som et minimum omhandle

a) kriterier som skal ligge til grunn for tilsynet
b) Nasjonal sikkerhetsmyndighets opplæring og veiledning av sektormyndigheten
c) hvordan Nasjonal sikkerhetsmyndighet skal bidra til å forberede og gjennomføre sektormyndighetens tilsyn
d) hvordan Nasjonal sikkerhetsmyndighet skal dele relevant informasjon om trusselbildet og risiko med tilsynsmyndigheten
e) hvordan tilsynsmyndigheten skal rapportere til Nasjonal sikkerhetsmyndighet om planlagte tilsyn og resultater fra gjennomførte tilsyn
f) varsling, jf. sikkerhetsloven § 4-5
g) utøvelse av godkjennings- og dispensasjonsmyndighet i sektoren
h) hvordan sektormyndigheten skal dele spesifikk kompetanse med Nasjonal sikkerhetsmyndighet.

Myndighet som er tildelt tilsynsansvar etter sikkerhetsloven § 3-1 har ansvaret for tilsynet også i de tilfeller hvor Nasjonal sikkerhetsmyndighet medvirker til eller deltar på tilsynet.

Departementet har ansvar for at det inngås samarbeidsavtale mellom Nasjonal sikkerhetsmyndighet og myndigheten som tildeles tilsynsansvar.

§ 16 Tilsynsmyndighet for leverandører i sikkerhetsgraderte anskaffelser

Nasjonal sikkerhetsmyndighet skal føre tilsyn med norske leverandører i sikkerhetsgraderte anskaffelser med mindre annet er avtalt med sektormyndigheten som har tilsynsansvar overfor leverandøren.

§ 17 Om tilsyn med virksomheter underlagt lov om nasjonal sikkerhet

Tilsynet skal kontrollere at virksomhetene overholder kravene i sikkerhetsloven med forskrifter, og bidra til å forbedre virksomhetens arbeid med forebyggende sikkerhet.

Tilsyn skal planlegges på bakgrunn av risiko og vesentlighet og skal gjennomføres ofte nok og i stort nok omfang til å ivareta lovens formål.

Tilsyn skal som hovedregel gjennomføres som systemrevisjon.

For å kontrollere sikkerhetstilstanden til informasjonssystemer og infrastruktur, kan tilsynsmyndigheten benytte automatiserte metoder for å samle inn teknisk informasjon.

§ 18 Rapport etter tilsyn

Tilsynsmyndigheten skal utarbeide en foreløpig rapport som forelegges virksomheten det er ført tilsyn med til uttalelse. Endelig rapport skal sendes virksomheten og Nasjonal sikkerhetsmyndighet. Nasjonal sikkerhetsmyndighet kan gjøre tilsynsrapporter tilgjengelig for Politiets sikkerhetstjeneste. Tilsynsrapporter om leverandører i sikkerhetsgraderte anskaffelser kan også gjøres tilgjengelig for klareringsmyndigheten.

§ 19 Tvangsmulkt

Tvangsmulkt fastsatt med hjemmel i sikkerhetsloven § 11-2 kan fastsettes som engangsmulkt eller løpende for hver dag, uke eller måned, etter at fristen for å rette forholdet er gått ut. Tilsynsmyndigheten kan frafalle påløpt tvangsmulkt.

Kapittel 5. Andre bestemmelser

§ 20 Melding om erverv av kvalifisert eierandel i virksomhet underlagt sikkerhetsloven

Melding om erverv etter sikkerhetsloven § 10-1 skal inneholde:

a) navn, adresse og organisasjonsnummer til erverver og til virksomheten det gjøres erverv i
b) størrelsen på erververs eierandel etter at ervervet er gjennomført
c) erververs eierstruktur
d) styrets sammensetning
e) daglige ledelse
f) oversikt over eventuelle relasjoner mellom erverver og andre eksisterende eiere i virksomheten det gjøres erverv i
g) erververens eierinteresser i andre virksomheter underlagt sikkerhetsloven og i den aktuelle sektoren
h) erververs årsomsetning og årsregnskap siste fem år
i) andre forhold som erververen antar kan ha betydning for vurderingen av om ervervet er godkjent etter sikkerhetsloven § 10-2.

Opplysningene om eierstruktur skal omfatte eventuelle utenlandske eierinteresser i erververs virksomhet med angivelse av nasjonalitet, og med erververs eierinteresser i utlandet med angivelse av nasjonalitet

I opplysningene om styrets sammensetning og daglige ledelse skal oppgis navn, fødselsdato og nasjonalitet, og personlige næringsinteresser som ligger utenfor den aktuelle virksomheten.

Dersom erververen er en privat person skal meldingen, i stedet for første ledd bokstav a, inneholde erververens fulle navn, adresse og organisasjons- eller fødselsnummer. Utenlandske

statsborgere som ikke har norsk fødselsnummer eller D-nummer, skal opplyse om fødselsdato og nasjonalitet.

Erververen skal kunne legge frem opplysninger departementet anser som nødvendige for å vurdere saken.

§ 21 Oppnevning av advokater etter sikkerhetsloven § 8-15

Forsvarsdepartementet oppnevner advokater etter sikkerhetsloven § 8-15. Advokatene skal sikkerhetsklareres og autoriseres av Sivil klareringsmyndighet.

Kapittel 6. Avsluttende bestemmelser

§ 22 Ikrafttredelse

Denne forskriften trer i kraft 1. januar 2019.

10 Utkast til forskrift om virksomhetens arbeid med forebyggende sikkerhet

Kapittel 1. Sikkerhetsstyring

§ 1 Definisjoner

I forskriften menes med

a) skjermingsverdige verdier: skjermingsverdig informasjon, informasjonssystem, objekt og infrastruktur
b) dokument: en logisk avgrenset mengde med informasjon som er lagret på et medium for senere lesning, høring, visning eller overføring.
c) lagringsmedier: elektronisk eller fysisk medium til bruk for senere lesning, høring, visning eller overføring av informasjon.

§ 2 Styringssystem for sikkerhet

Virksomheten skal etablere et styringssystem for sikkerhet som skal sikre at virksomheten oppfyller kravene i eller med hjemmel i sikkerhetsloven.

§ 3 Styringsdokument for det forebyggende sikkerhetsarbeidet

Virksomhetens leder skal fastsette et styringsdokument som beskriver

a) hvilke deler av sikkerhetsloven med forskrifter som gjelder for virksomheten
b) roller og ansvar i virksomheten, jf. § 5
c) prinsipper for virksomhetens sikkerhetsarbeid.

Styringsdokumentet skal gjøres kjent og være tilgjengelig for ansatte, leverandører og andre eksterne samarbeidspartnere i den grad det er nødvendig for å bevisstgjøre om virksomhetens plikter etter sikkerhetsloven.

§ 4 Sikkerhetsmål

Virksomheten skal planlegge hvordan kravene til et forsvarlig sikkerhetsnivå i sikkerhetsloven § 4-3 første ledd, § 5-2 første ledd, § 6-2 første ledd og § 7-3 første ledd skal oppfylles, og fastsette hvordan den skal evaluere om kravene er oppfylt.

§ 5 Roller og ansvar i det forebyggende sikkerhetsarbeidet

Virksomhetens leder skal fordele det forebyggende sikkerhetsarbeidet på det antallet roller som er nødvendig for å ivareta krav gitt i eller med hjemmel i sikkerhetsloven. Rollenes ansvar og myndighet skal gjøres kjent i virksomheten.

Virksomhetens leder skal informeres om saker som er viktige for det forebyggende sikkerhetsarbeidet.

Kontroll av styringssystemet for sikkerhet skal om mulig utføres av andre enn de som har styrende eller utøvende oppgaver i det forebyggende sikkerhetsarbeidet.

§ 6 Ressurser og kompetanse

Virksomheten skal bruke tilstrekkelige ressurser til å forvalte og utvikle det forebyggende sikkerhetsarbeidet i virksomheten.

Virksomheten skal sørge for at den som kan få tilgang til skjermingsverdige verdier gjennom å utføre arbeid i, eller tjenester for, virksomheten,

a) har bekreftet identiteten sin med legitimasjon
b) er kjent med de delene av styringssystemet for sikkerhet som har betydning for egne oppgaver

c) har kompetanse om sikkerhet tilpasset egne oppgaver
d) blir informert om endringer i kravene til sikkerheten
e) kjenner til relevante sikkerhetstrusler og sikkerhetsbestemmelser og forstår sin rolle i sikkerhetsarbeidet.

Når et arbeidsforhold eller en tjeneste avsluttes, skal virksomheten sikre at den som slutter, ikke lenger har tilgang til skjermingsverdige verdier eller på annen måte utgjør en uakseptabel risiko. Den som slutter, skal informeres om at taushetsplikten etter sikkerhetsloven § 5-4 andre ledd også gjelder etter at arbeidsforholdet er endret eller avsluttet.

§ 7 Tiltak ved sikkerhetstruende virksomhet, avvik og kompromittering av sikkerhetsgradert informasjon

Ved sikkerhetstruende virksomhet eller avvik fra styringssystemet for sikkerhet skal virksomheten gjennomføre umiddelbare tiltak for å redusere skadeomfanget og tiltak som gjenoppretter sikkerhetstilstanden. Det skal rapporteres internt og til andre som er berørt av den sikkerhetstruende virksomheten. Virksomheten skal vurdere konsekvensene av den sikkerhetstruende virksomheten eller avviket.

Hvis sikkerhetsgradert informasjon kompromitteres skal virksomheten, i tillegg til å varsle i samsvar med sikkerhetslovens § 4-5, informere den som har tilvirket informasjonen om hendelsen.

§ 8 Evaluering og øvelser

Virksomheten skal jevnlig evaluere om kravet til forsvarlig sikkerhetsnivå er oppfylt, jf. § 4, og minst en gang i året evaluere om styringssystemet for sikkerhet er egnet til å sørge for at kravet oppfylles.

Virksomheten skal jevnlig gjennomføre øvelser for å kontrollere effekten av sikkerhetstiltakene i en normalsituasjon, og av tiltakene som er planlagt ved økt trusselnivå. Er virksomheten avhengig av andre virksomheter for å fungere slik den skal, skal øvelsen jevnlig inkludere de andre virksomhetene.

Resultatet av evalueringer og øvelser skal inngå i virksomhetens leders årlige gjennomgang, jf. § 9.

§ 9 Virksomhetens leders gjennomgang av det forebyggende sikkerhetsarbeidet

Virksomhetens leder skal årlig gjennomgå virksomhetens forebyggende sikkerhetsarbeid for å vurdere om styringssystemet for sikkerhet fungerer etter hensikten.

Dersom gjennomgangen viser at det er behov for det, skal virksomheten gjennomføre nødvendige forbedringer i det forebyggende sikkerhetsarbeidet og i styringssystemet for sikkerhet.

§ 10 Dokumentasjon om styringssystemet for sikkerhet

Virksomheten skal dokumentere at styringssystemet for sikkerhet og sikkerhetstiltakene gir et forsvarlig sikkerhetsnivå, jf. § 4.

Kapittel 2. Generelle krav til beskyttelse av skjermingsverdige verdier

§ 11 Plikt til å vurdere risiko

Virksomheten skal identifisere, analysere og evaluere risikoen for at kravet til et forsvarlig sikkerhetsnivå, jf. § 4, ikke nås. Når virksomheten vurderer risikoen, skal den ta hensyn til

a) hvilken sikkerhetstruende virksomhet de skjermingsverdige verdiene kan bli utsatt for
b) hvilke sårbarheter som er knyttet til de skjermingsverdige verdiene
c) i hvilken grad virksomheten er avhengig av andre virksomheter for å fungere som den skal.

Virksomheten skal minst årlig vurdere behovet for å for å gjennomføre en ny helhetlig vurdering av risiko.

Dersom endringer planlegges, gjennomføres eller inntreffer, skal virksomheten vurdere hvilken risiko endringene medfører.

Virksomheten skal sende en oversikt over hvilke virksomheter den er avhengig av for å fungere som den skal, jf. sikkerhetsloven § 4-2, til det departement som er ansvarlig for det forebyggende sikkerhetsarbeidet i sektoren, eller det departement som har fattet vedtak om at virksomheten skal omfattes av loven og Nasjonal sikkerhetsmyndighet.

§ 12 Plikt til å håndtere risiko

Virksomheten skal håndtere risiko for å oppnå et forsvarlig sikkerhetsnivå, jf. §§ 20, 32, 45 og 53.

§ 13 Grunnsikringstiltak, påbyggingstiltak og tiltak for skadebegrensning og gjenopprettelse

Dersom virksomheten vurderer det som nødvendig for å håndtere risikoen, skal den etablere grunnsikringstiltak, påbyggingstiltak og tiltak for skadebegrensning og gjenopprettelse.

Grunnsikringstiltak skal bidra til et forsvarlig sikkerhetsnivå i virksomheten i en normaltilstand. Når virksomheten vurderer hvilke grunnsikringstiltak som skal etableres, skal den ta utgangspunkt i hvilken betydning den skjermingsverdige verdien har for grunnleggende nasjonale funksjoner. Grunnsikringstiltakene kan være

a) fysiske, elektroniske, menneskelige eller organisatoriske barrierer
b) systemer som skal oppdage og varsle om aktiviteter eller hendelser
c) systemer og rutiner for å avklare aktiviteter og hendelser og bakgrunnen for dem
d) oppfølging av uønskede aktiviteter og uønskede hendelser, eller
e) en kombinasjon av tiltakene nevnt i bokstav a til d.

I god tid før en skjermingsverdig verdi etableres eller avvikles, skal virksomheten planlegge hvilke grunnsikringstiltak som skal beskytte den.

Virksomheten skal planlegge påbyggingstiltak som kan iverksettes dersom risikoen øker utover det grunnsikringstiltakene ivaretar. Påbyggingstiltakene skal kunne iverksettes i løpet av kort tid, og skal kunne avvikles dersom risikoen reduseres til opprinnelig nivå.

Dersom den økte risikoen varer, skal virksomheten vurdere om påbygningstiltakene skal inngå i grunnsikringen. I slike tilfeller skal virksomheten planlegge nye påbyggingstiltak.

Virksomheten skal planlegge skadebegrensningstiltak som kan iverksettes i situasjoner som ikke kan håndteres fullt ut med grunnsikrings- og påbyggingstiltakene.

Virksomheten skal ha en plan for å gjenopprette et forsvarlig sikkerhetsnivå i virksomheten.

§ 14 Prinsipper ved valg og utforming av sikkerhetstiltak

Når virksomheten velger ut og utformer sikkerhetstiltak, skal den vurdere prinsippene om

a) minimalisme: Sikkerhetstiltakene skal ikke ha annen funksjonalitet eller større kompleksitet enn det som er nødvendig.
b) minste privilegium: Det skal ikke gis mer omfattende tilgang enn det som er nødvendig.
c) sikring i dybden: Svikt i ett enkelt tiltak skal ikke kunne føre til kompromittering.
d) motstandsdyktighet: Det skal være tilstrekkelig uavhengighet mellom sikkerhetstiltak slik at flere sikkerhetstiltak ikke skal kunne svekkes eller settes ut av funksjon samtidig, for eksempel som følge av en enkelt feil eller en enkelt hendelse.
e) balansert styrke: Effekten av sikkerhetstiltakene skal være tilnærmet lik for alle skjermingsverdige verdier med samme sikkerhetsbehov.

Sikkerhetstiltakene skal være samordnet slik at de ikke fragmenteres eller dupliseres unødvendig.

Virksomheten skal ikke bruke mer inngripende sikkerhetstiltak enn det som fremstår som nødvendig for å håndtere den aktuelle risikoen. I vurderingen av hva som er nødvendig, skal virksomheten særlig ta hensyn til enkeltpersoners rettssikkerhet og personvern. Når sikkerhetstiltaket kan gripe inn i enkeltpersoners rettssikkerhet eller personvern, skal virksomheten kunne dokumentere vurderingen.

§ 15 Krav om bruk av evaluerte produkter og tjenester

Når virksomheten velger sikkerhetstiltak, skal den bruke evaluerte produkter og tjenester, jf. § 16, dersom produktets eller tjenestens funksjonalitet i seg selv er avgjørende for at

a) personer ikke får tilgang til informasjon gradert HEMMELIG eller STRENGT HEMMELIG de ikke har tjenstlig behov for
b) personer ikke får tilgang til sikkerhetsgradert informasjon de ikke er klarert for
c) personer ikke kan overta eller sette ut av drift infrastruktur eller objekter klassifisert KRITISK eller MEGET KRITISK.

Evalueringen skal gi tillit til at produktet eller tjenesten har den funksjonaliteten som er nødvendig for å sikre det aktuelle graderingsnivået. Evalueringen skal bestå av metodisk utvikling og testing, og være etterprøvbar.

§ 16 Evaluering av produkter og tjenester

Evalueringen skal utføres i samsvar med ISO- og IEC-standarder for evaluering av Nasjonal sikkerhetsmyndighet eller et akkreditert laboratorium som er utpekt av Nasjonal sikkerhetsmyndighet.

Dersom evalueringen dokumenteres gjennom sertifisering, skal sertifiseringen gis av Nasjonal sikkerhetsmyndighet eller et akkreditert sertifiseringsorgan utpekt av Nasjonal sikkerhetsmyndighet.

§ 17 Krav til sikkerhet i anskaffelser

Virksomheten har ansvaret for at kravet til forsvarlig sikkerhetsnivå ivaretas ved anskaffelser til, eller anskaffelser som gir tilgang til, skjermingsverdig informasjon, informasjonssystem, objekt eller infrastruktur.

Virksomheten skal avtale med leverandøren hvordan sikkerheten ivaretas i anskaffelsen. Avtalen skal gi virksomheten rett til å undersøke at leverandøren ivaretar sikkerheten i anskaffelsen.

§ 18 Varslingsplikt om anskaffelser til skjermingsverdig informasjonssystem, objekt og infrastruktur

Et varsel etter sikkerhetsloven § 9-4 skal inneholde opplysninger om

a) hva anskaffelsen gjelder
b) leverandørens navn, adresse, organisasjonsnummer, nasjonalitet, styremedlemmer og eiere
c) hvordan oppdragsgiveren vurderer risikoen for at informasjonssystemet, objektet eller infrastrukturen kan bli rammet av sikkerhetstruende virksomhet ved anskaffelsen
d) hvordan oppdragsgiveren vil håndtere risikoen
e) hvilken gjenstående risiko som ikke vil være ubetydelig etter at tiltak er iverksatt
f) hvorfor anskaffelsen likevel bør gjennomføres
g) andre forhold som oppdragsgiveren antar kan ha betydning for vurderingen av risikoen forbundet med anskaffelsen.

§ 19 Unntak fra sikkerhetskrav

Nasjonal sikkerhetsmyndighet kan gjennom enkeltvedtak gi unntak fra sikkerhetskrav i denne forskriften, dersom det blir uforholdsmessig byrdefullt for virksomheten å oppfylle kravene.

Et sektortilsyn kan også gi unntak etter første ledd fra de sikkerhetskravene som ikke gjelder for beskyttelse av sikkerhetsgradert informasjon.

Kapittel 3. Beskyttelse av skjermingsverdig informasjon

§ 20 Forsvarlig sikkerhetsnivå for skjermingsverdig informasjon

Når virksomheten håndterer risikoen knyttet til skjermingsverdig informasjon, jf. § 12, er kravet til et forsvarlig sikkerhetsnivå oppfylt dersom informasjonen ikke med enkle midler kan endres, gå tapt eller gjøres utilgjengelig. For informasjon som er sikkerhetsgradert, gjelder i tillegg et krav om at den ikke med enkle midler kan bli kjent for uautoriserte personer.

Behovet for å beskytte både konfidensialitet, integritet og tilgjengelighet må ses i sammenheng og avveies mot hverandre.

For informasjon som er gradert KONFIDENSIELT eller høyere, gjelder i tillegg reglene i Kapittel 5.

§ 21 Destruering av dokumenter og lagringsmedier med sikkerhetsgradert informasjon

Dersom dokumenter og lagringsmedier som inneholder eller har inneholdt sikkerhetsgradert informasjon, skal destrueres, skal det brukes en metode som ikke gjør det mulig å rekonstruere og lese informasjonen.

Dersom informasjonen er eller har vært gradert KONFIDENSIELT eller høyere, skal destrueringsmetoden være godkjent av Nasjonal sikkerhetsmyndighet.

§ 22 Evakuering og ekstraordinær destruering i nødsituasjoner

Virksomheten skal ha en plan for å evakuere og destruere dokumenter og lagringsmedier i nødsituasjoner.

§ 23 Utlevering av sikkerhetsgradert informasjon til fremmede stater og internasjonale organisasjoner

Fremmede stater og internasjonale organisasjoner kan bare gis tilgang til norsk sikkerhetsgradert informasjon dersom det

a) er i samsvar med nasjonale sikkerhetsinteresser
b) ikke er i strid med lovbestemt taushetsplikt og
c) foreligger en sikkerhetsavtale mellom Norge og den aktuelle staten eller den internasjonale organisasjonen.

Når myndigheter, virksomheter i andre stater eller internasjonale organisasjoner skal ha tilgang til sikkerhetsgradert informasjon, skal informasjonen behandles i samsvar med bestemmelsene i sikkerhetsavtalen som er inngått mellom Norge og den aktuelle staten.

I forsvars- og justissektoren kan Forsvarsdepartementet og Justis- og beredskapsdepartementet gjøre unntak fra kravet til sikkerhetsavtale, dersom det ikke er praktisk mulig å inngå en sikkerhetsavtale, og det likevel er i Norges interesse å utlevere informasjonen.

§ 24 Korresponderende sikkerhetsgrader

Informasjon med sikkerhetsgrad som er fastsatt av en fremmed stat eller internasjonal organisasjon, skal beskyttes på samme måte som informasjon med korresponderende norsk sikkerhetsgrad, jf. sikkerhetsloven § 5-3.

Nasjonal sikkerhetsmyndighet fastsetter hvilke sikkerhetsgrader utstedt av fremmede stater eller internasjonale organisasjoner som korresponderer med de norske sikkerhetsgradene i sikkerhetslovens § 5-3.

§ 25 Kryptering

Virksomheten skal kryptere sikkerhetsgradert informasjon som sendes elektronisk ut av et område virksomheten kontrollerer.

Sikkerhetsgradert informasjon som er lagret hos virksomheten, skal krypteres dersom informasjonen ikke er sikret med andre sikkerhetstiltak.

Kryptomateriellet som brukes til å kryptere informasjonen, skal sikres tilsvarende verdien på den informasjonen det beskytter.

Materiellet skal forvaltes i samsvar med kravene til implementering, bruk, drift og forvaltning som Nasjonal sikkerhetsmyndighet har fastsatt som en del av godkjenningen, jf. sikkerhetsloven § 5-6. Nasjonal sikkerhetsmyndighet bestemmer hvilket materiell som kan brukes til å kryptere informasjon gradert KONFIDENSIELT eller høyere.

Forsvarsdepartementet kan gi forskrift om krav til kryptering og beskyttelse av kryptomateriell.

Kapittel 4. Sikkerhetsgradering og merking

§ 26 Merking av dokumenter og lagringsmedier som inneholder sikkerhetsgradert informasjon

Dokumenter og lagringsmedier skal merkes med den høyeste sikkerhetsgraden som informasjon i dokumentet eller lagringsmediet er gradert til, og med hvor lenge graderingen varer. Merkingen skal være lett synlig eller hørbar ved avspilling, og gjenkjennelig for alle i og utenfor virksomheten som skal håndtere informasjonen.

Dersom ikke all informasjon i et dokument eller et lagringsmedium har samme sikkerhetsgradering, skal merkingen vise hvilke deler som har hvilken gradering.

Dokumenter og lagringsmedier med informasjon som utleveres til en annen stat eller internasjonal organisasjon, jf. § 23, skal være merket med hvilken stat eller organisasjon dokumentet eller lagringsmediet utleveres til.

§ 27 Sikkerhetsgradering ut over 30 år

Hvis det er behov for å beskytte informasjon ut over 30 år, jf. sikkerhetsloven § 5-3, skal avgradering vurderes 40 år etter utstedelsen og deretter hvert 10. år.

§ 28 Omgradering av sikkerhetsgradert informasjon

Virksomheten skal vurdere å omgradere sikkerhetsgradert informasjon dersom

a) den mottar et varsel om antatt feil gradering etter § 30
b) den mottar en henvendelse om innsyn som nevnt i § 31
c) den avleverer dokumenter til Arkivverket i medhold av arkivloven
d) det oppstår andre tilfeller som gir grunn til å tro at beskyttelsesbehovet for informasjonen endrer seg.

§ 29 Hvem som kan omgradere

Bare virksomheten som har utstedt informasjonen, en virksomhet overordnet denne, eller Nasjonal sikkerhetsmyndighet kan omgradere informasjon med norsk sikkerhetsgradering. Informasjon med utenlandsk sikkerhetsgradering kan bare omgraderes av den staten eller organisasjonen som har utstedt informasjonen, eller etter samtykke fra den.

§ 30 Plikt til å informere om behov for eller avgjørelse om omgradering

Den som mottar informasjon, skal informere utstederen dersom mottakeren antar at sikkerhetsgraderingen eller mangelen på sikkerhetsgradering er i strid med sikkerhetsloven § 5-3.

En virksomhet som omgraderer informasjon, skal informere alle som har mottatt informasjonen.

§ 31 Prosedyrer ved henvendelse om innsyn etter offentleglova eller forvaltningsloven

En utsteder av sikkerhetsgradert informasjon som mottar krav om innsyn etter offentleglova eller om partsinnsyn etter forvaltningsloven, skal uten ugrunnet opphold vurdere om den samlede informasjonen eller deler av den kan avgraderes, jf. § 28.

Dersom en annen virksomhet enn utstederen får henvendelsen om innsyn, skal virksomheten som får henvendelsen, uten ugrunnet opphold kontakte utstederen og informere om behovet for å vurdere avgradering. Utstederen skal uten ugrunnet opphold gi tilbakemelding om informasjonen kan avgraderes.

Virksomhetens leder kan autorisere en part for å gi partsinnsyn etter forvaltningsloven i informasjon gradert BEGRENSET, jf. forvaltningsloven § 2 første ledd bokstav b og e og § 19.

Kapittel 5. Beskyttelse av informasjon gradert KONFIDENSIELT eller høyere

§ 32 Forsvarlig sikkerhetsnivå for informasjon gradert KONFIDENSIELT eller høyere

Når virksomheten håndterer risikoen knyttet til sikkerhetsgradert informasjon, jf. § 12, er kravet til et forsvarlig sikkerhetsnivå oppfylt dersom

a) uautoriserte personer ikke kan få tilgang til informasjon gradert KONFIDENSIELT eller høyere uten at virksomheten oppdager det
b) uautoriserte personer ikke kan få tilgang til informasjon gradert HEMMELIG eller høyere uten at virksomheten oppdager det i tide og kan begrense skadefølgene
c) uautoriserte personer ikke kan få tilgang til informasjon gradert STRENGT HEMMELIG.

§ 33 Sending av informasjon gradert KONFIDENSIELT eller høyere

Når informasjon som er gradert KONFIDENSIELT eller høyere skal sendes fysisk, skal det brukes kurer. For informasjon gradert HEMMELIG eller STRENGT HEMMELIG skal i tillegg mottaker kvittere for at sendingen er mottatt.

Dersom informasjon med ulik sikkerhetsgradering sendes sammen, skal det ligge ved en liste med oversikt over informasjonen og dens sikkerhetsgrad.

§ 34 Pakking av informasjon gradert KONFIDENSIELT eller høyere

Når informasjon som er gradert KONFIDENSIELT eller høyere skal sendes fysisk, skal emballasjen være dobbel, ugjennomsiktig, av solid kvalitet og ikke kunne åpnes uten at det er sporbart. Den ytre emballasjen skal ikke vise at sendingen inneholder sikkerhetsgradert informasjon. Indre emballasje skal forsegles og merkes med sikkerhetsgrad.

§ 35 Krav til oversikt over informasjon gradert KONFIDENSIELT eller høyere

Virksomheten skal ha en oversikt over hvor dokumenter og lagringsmedier som er gradert KONFIDENSIELT eller høyere, til enhver tid befinner seg.

§ 36 Soneinndeling for informasjon gradert KONFIDENSIELT eller høyere

Virksomheter som har informasjon som er gradert KONFIDENSIELT eller høyere, skal etablere en kontrollert og beskyttet sone for å beskytte den sikkerhetsgraderte informasjonen.

Dersom virksomheten har et område med direkte tilgang til informasjon gradert KONFIDENSIELT eller høyere, skal det etableres en sperret sone.

§ 37 Kontrollert sone

En kontrollert sone skal være et tydelig avgrenset område der virksomheten skal kunne ha kontroll med personer og kjøretøy.

Ved særlig høy risiko skal adgang og ferdsel kontrolleres med en fysisk avgrensning.

§ 38 Beskyttet sone

En beskyttet sone skal ha en fysisk avgrensing der sikkerhetstruende virksomhet skal kunne oppdages.

I beskyttet sone skal dokumenter og lagringsmedier med informasjon som er gradert KONFIDENSIELT eller høyere lagres i en oppbevaringsenhet godkjent av Nasjonal sikkerhetsmyndighet, eller være under stedlig vakthold.

Personer som skal gis permanent adgang til en beskyttet sone skal være sikkerhetsklarert for KONFIDENSIELT. Dersom andre personer skal gis adgang, skal adgangen registreres, og personene skal følges av personell med permanent adgang.

Det skal være kontroll med adgangen til beskyttet sone og det skal være synlig hvem som har permanent adgang til området.

§ 39 Sperret sone

Sperret sone skal være tydelig merket med høyeste tillatte graderingsnivå.

Sperret sone skal sikres i samsvar med det høyeste tillatte graderingsnivået, jf. § 32.

Personer som skal gis permanent adgang til en sperret sone skal være sikkerhetsklarert og autorisert for informasjonen i området. Dersom andre personer skal gis adgang, skal adgangen registreres, og personene skal følges av personell som har permanent adgang.

Det skal være kontroll med adgangen til sperret sone og det skal være synlig hvem som har permanent adgang til området.

§ 40 Behandling av informasjon gradert KONFIDENSIELT eller høyere

Dokumenter eller lagringsmedier med informasjon som er gradert KONFIDENSIELT eller høyere skal bare oppbevares og behandles i beskyttet eller sperret sone.

Dokumentet eller lagringsmediet kan likevel oppbevares og behandles utenfor beskyttet eller sperret sone, når dette er godkjent av virksomheten på bakgrunn av en vurdering av risiko. Virksomheten skal holde oversikt over slike godkjenninger.

Dersom sikkerhetsgradert informasjon behandles eller oppbevares utenfor beskyttet eller sperret sone, skal virksomheten gjennomføre nødvendige tiltak for å beskytte informasjonen mot at den blir kjent for uautoriserte personer, blir slettet, endret eller gjort utilgjengelig.

Dokumenter eller lagringsmedier med informasjon gradert KONFIDENSIELT eller høyere kan tas med til et NATO-land eller en stat Norge har sikkerhetsavtale med, dersom en person tar vare på informasjonen gjennom hele reisen, og dersom det er mulig å deponere informasjonen ved en norsk utenriksstasjon eller et norsk kontrollert område ved ankomst.

Dersom informasjon gradert KONFIDENSIELT eller høyere lagres, overføres eller behandles på et informasjonssystem i utlandet, skal dette gjøres i samsvar med sikkerhetstiltakene i informasjonssystemet, jf. § 48.

§ 41 Særlige krav for informasjon gradert HEMMELIG eller høyere

Når dokumenter eller lagringsmedier gradert HEMMELIG eller høyere skal fordeles eller lånes ut internt i virksomheten, skal låntaker bekrefte mottaket.

Destruering av informasjon gradert HEMMELIG eller høyere skal kontrolleres og bekreftes av minst to autoriserte personer.

§ 42 Rapportering av informasjon gradert STRENGT HEMMELIG

Virksomheter som har dokumenter eller lagringsmedier med informasjon gradert STRENGT HEMMELIG, skal hvert år kontrollere at dokumentene og lagringsmediene er i virksomheten. Kontrollen skal foretas på grunnlag av journalen per 31. desember. Virksomheten skal innen utgangen av januar hvert år sende en oversikt over dokumenter og lagringsmedier med informasjon gradert STRENGT HEMMELIG til det departement som er ansvarlig for det forebyggende sikkerhetsarbeidet i sektoren. Departementet skal innen utløpet av februar sende Nasjonal sikkerhetsmyndighet en samlet oversikt over dokumenter og lagringsmedier med informasjon gradert STRENGT HEMMELIG i sin sektor. Oversiktene skal graderes HEMMELIG.

§ 43 Krav til forsendelse med kurer

Virksomheter som utfører kurerposttjeneste, skal sikre at informasjonen ikke blir kjent for uautoriserte personer. Avsenderen skal utstede kurersertifikat for hvert oppdrag og legge en plan for gjennomføringen. Kureren skal ha nødvendig sikkerhetsklarering.

Med mindre Nasjonal sikkerhetsmyndighet gir tillatelse til annet, skal kurerpost til utlandet sendes som diplomatisk post, eller med kurer fra Forsvaret eller utenrikstjenesten.

§ 44 Beskyttelse av rom og lokaler for tale gradert KONFIDENSIELT eller høyere

Virksomheten skal beskytte rom og lokaler for tale gradert KONFIDENSIELT eller høyere slik at sikkerhetsgradert informasjon ikke blir kjent for uautoriserte personer.

Virksomheten skal føre oversikt over hvilke personer som har selvstendig tilgang til rommet eller lokalet. Det skal føres en besøksoversikt over personell som har besøkt rommet eller lokalet.

Rommet eller lokalet skal være tydelig merket med hvilket graderingsnivå det er tillatt å tale der.

Virksomheten skal be Nasjonal sikkerhetsmyndighet vurdere om teknisk sikkerhetsundersøkelse skal gjennomføres før den tar i bruk rom eller lokaler for tale gradert KONFIDENSIELT eller høyere. Dersom Nasjonal sikkerhetsmyndighet mener det er nødvendig med en teknisk sikkerhetsundersøkelse, skal virksomheten legge Nasjonal sikkerhetsmyndighets rapport til grunn når den sikrer rommet eller lokalet før det blir brukt til sikkerhetsgradert tale. Virksomheten skal også be Nasjonal sikkerhetsmyndighet om teknisk sikkerhetsundersøkelse dersom det er vesentlige endringer i rom eller lokaler for sikkerhetsgradert tale, dersom det er mistanke om at informasjon er blitt kjent for uautoriserte, eller at uvedkommende har hatt adgang til rommet eller lokalene.

Kapittel 6. Beskyttelse av skjermingsverdige informasjonssystemer

§ 45 Forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer

Når virksomheten håndterer risikoen knyttet til skjermingsverdige informasjonssystemer, jf. § 12, skal den oppnå et forsvarlig sikkerhetsnivå ved å

a) beskytte data mot uønsket lesing og tjenester mot uønsket bruk
b) beskytte data mot uønsket modifikasjon og tjenester mot uønsket modifikasjon og manipulasjon
c) beskytte data mot uønsket sletting og tjenester mot uønsket reduksjon eller stans
d) identifisere og autentisere brukere som kan påvirke informasjonssystemets funksjon eller som kan få tilgang til data i systemet, før de gis tilgang til data og tjenester
e) forhindre at falske data og tjenester introduseres i informasjonssystemet
f) registrere bruk, misbruk og forsøk på misbruk av informasjonssystemet, tjenester og data

g) systematisk kontrollere at sikkerhetstiltakene er korrekt implementert og ivaretar sikkerheten på en effektiv og hensiktsmessig måte.

Når virksomheten vurderer hvordan risikoen skal håndteres, skal den ta utgangspunkt i hvilken betydning informasjonssystemet har for grunnleggende nasjonale funksjoner.

Sikkerhetstiltakene skal være tilpasset systemets totale omfang og kompleksitet gjennom hele systemets levetid.

Sikkerhetstiltak som skal virke hurtig, eller som lett kan utløse feil når de utføres manuelt, skal automatiseres.

§ 46 Plikt til å sørge for godkjenning av skjermingsverdige informasjonssystemer

Virksomheten skal sørge for at informasjonssystemer som skal behandle sikkerhetsgradert informasjon er godkjent før de tas i bruk. Andre skjermingsverdige informasjonssystemer skal være godkjent så fort som praktisk mulig. Virksomheten dekker kostnader med godkjenningen.

Virksomheten skal informere Nasjonal sikkerhetsmyndighet når den har besluttet å utvikle et skjermingsverdig informasjonssystem. Informasjonsplikten gjelder ikke dersom det er åpenbart at Nasjonal sikkerhetsmyndighet ikke trenger å godkjenne systemet, jf. § 47.

§ 47 Godkjenningsmyndighet

Virksomheten godkjenner skjermingsverdige informasjonssystemer som ikke er nevnt i andre eller tredje ledd. Nasjonal sikkerhetsmyndighet og relevante tilsynsmyndigheter skal informeres om slike informasjonssystemer.

Nasjonal sikkerhetsmyndighet godkjenner skjermingsverdige informasjonssystemer som er utpekt som, eller er av avgjørende betydning for funksjonaliteten i, et objekt eller en infrastruktur klassifisert KRITISK eller MEGET KRITISK.

Nasjonal sikkerhetsmyndighet godkjenner informasjonssystemer som behandler sikkerhetsgradert informasjon og som

a) skal brukes i utlandet
b) har forbindelse til informasjonssystemer i utlandet, eller til andre virksomheters informasjonssystemer
c) brukes eller har forbindelser utenfor områder virksomheten kontrollerer
d) har brukere som ikke er sikkerhetsklarert for det graderingsnivået som behandles i informasjonssystemet eller informasjonssystemer dette har forbindelse til
e) behandler informasjon som er gradert HEMMELIG, og som har brukere som ikke skal ha tilgang til all informasjon i informasjonssystemet eller de informasjonssystemer dette har forbindelse til
f) behandler informasjon som er gradert STRENGT HEMMELIG.

Departementet som har utpekt det skjermingsverdige objektet eller infrastrukturen kan bestemme at godkjenning av skjermingsverdige informasjonssystemer etter andre ledd skal gjøres av myndighet med tilsynsansvar. Det skal gjøres en helhetsvurdering av om myndigheten med tilsynsansvar har tilstrekkelig kompetanse til å godkjenne skjermingsverdige informasjonssystemer, eller kan få slik kompetanse uten uforholdsmessig store utgifter. En uttalelse fra Nasjonal sikkerhetsmyndighet skal inngå i vurderingen.

§ 48 Godkjenningen

Godkjenningen er en planlagt og systematisk gjennomgang av at virksomheten, for å oppnå et forsvarlig sikkerhetsnivå for informasjonssystemet, på en tilfredsstillende måte har vurdert og håndtert risiko ved å ha

a) identifisert behovet for beskyttelse basert på informasjonssystemets funksjon og operative miljø, jf. § 11,

b) fastsatt sikkerhetskrav utledet av behovet for beskyttelse, jf. bokstav a og § 45 andre ledd,
c) etablert sikkerhetstiltak som oppfyller sikkerhetskravene gjennom hele informasjonssystemets levetid, jf. bokstav b og § 45 første ledd bokstav a til f og tredje og fjerde ledd,
d) kontrollert at sikkerhetstiltakene fungerer etter sin hensikt, jf. § 45 første ledd bokstav g

§ 49 Godkjenningens varighet

Godkjenningen kan gis for inntil fem år. Hvis det oppstår en vesentlig endring som har betydning for beskyttelsen av informasjonssystemet og informasjonen, må informasjonssystemet godkjennes på nytt.

§ 50 Midlertidig brukstillatelse

Foreligger det et særlig behov for å ta i bruk et skjermingsverdig informasjonssystem før det er godkjent, kan godkjenningsmyndigheten gi midlertidig brukstillatelse dersom

a) behovet for beskyttelse er identifisert, basert på informasjonssystemets funksjon og operative miljø,
b) mangler forbundet med fastlegging av sikkerhetskrav, etablering av sikkerhetstiltak og sikkerhetstiltakenes funksjon er identifisert og håndtert med kompenserende tiltak, og
c) det foreligger en plan for å rette manglene.

Nasjonal sikkerhetsmyndighet kan i særlige tilfeller dispensere fra kravene i første ledd.

§ 51 Sammenkobling av informasjonssystemer som behandler sikkerhetsgradert informasjon

Dersom sammenkobling av flere informasjonssystemer som behandler informasjon gradert KONFIDENSIELT eller høyere medfører uoversiktlige sikkerhetsmessige avhengigheter, skal sammenkoblingen skje via et eget informasjonssystem.

Slike sammenkoblinger skal reguleres i avtaler mellom virksomhetene som avklarer roller og ansvar for sammenkoblingen og hvilken informasjon og hvilke tjenester som skal utveksles.

Kapittel 7. Beskyttelse av skjermingsverdig objekter og infrastruktur

§ 52 Skadevurdering i forbindelse med klassifisering av skjermingsverdig objekt eller infrastruktur

Virksomheten skal vurdere hvilke skadefølger det kan få for grunnleggende nasjonale funksjoner om de skjermingsverdige objektet eller infrastrukturen den råder over blir utsatt for skadeverk, ødeleggelse eller rettstridig overtakelse. I vurderingen skal virksomheten legge vekt på

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

Skadevurderingen skal sendes til det departementet som har utpekt det skjermingsverdige objektet eller infrastrukturen eller Nasjonal sikkerhetsmyndighet, jf. myndighetsforskriften § 1.

Dersom virksomheten ikke kan redusere sin avhengighet av objekt eller infrastruktur som en annen virksomhet råder over, skal virksomheten varsle den som råder over objektet eller infrastrukturen om avhengigheten.

Virksomheten skal gjøre en ny vurdering dersom det skjer en endring av forhold som er relevante for vurderingen etter første ledd.

Virksomheten skal varsle det departementet som har utpekt det skjermingsverdige objektet eller infrastrukturen eller Nasjonal sikkerhetsmyndighet dersom virksomheten råder over andre skjermingsverdige objekter eller infrastruktur som omfattes av sikkerhetsloven § 7-1.

Skadevurderingen skal graderes minst BEGRENSET.

§ 53 Forsvarlig sikkerhetsnivå for klassifiserte objekter og infrastruktur

Når virksomheten håndterer risikoen knyttet til skjermingsverdige objekter eller infrastruktur, jf. § 12, er kravet til et forsvarlig sikkerhetsnivå oppnådd dersom virksomheten kan

e) begrense tap av vesentlig funksjon ved skadeverk på eller forsøk på å ødelegge objekter og infrastruktur klassifisert VIKTIG
f) begrense tap av funksjon ved skadeverk på eller forsøk på å ødelegge objekter og infrastruktur klassifisert KRITISK
g) avverge tap av funksjon ved skadeverk på eller forsøk på å ødelegge objekter eller infrastruktur klassifisert MEGET KRITISK
h) avverge rettsstridig overtakelse av funksjonen til objektet eller infrastrukturen klassifisert KRITISK eller MEGET KRITISK.

§ 54 Bruk av sikringsstyrker

Dersom politiet eller Forsvaret har bestemt at det som et påbygningstiltak skal planlegges for bruk av sikringsstyrker ved et objekt eller en infrastruktur, skal virksomheten tilrettelegge og utarbeide plan for bruk av sikringsstyrkene i samarbeid med politiet eller Forsvaret.

§ 55 Behovet for bruk av adgangsklarering

En søknad om adgangsklarering, jf. sikkerhetsloven § 8-3, må redegjøre for hvorfor virksomheten ikke kan iverksette andre egnede sikkerhetstiltak. En adgangsklarering vil være gyldig for alle type objekter eller infrastruktur med krav om samme type adgangsklarering.

Kapittel 8. Nasjonalt varslingssystem for digital infrastruktur

§ 56 Tilknytning til varslingssystemet for digital infrastruktur

Ved tilknytning til varslingssystemet for digital infrastruktur skal det inngås en avtale mellom virksomheten og Nasjonal sikkerhetsmyndighet. Avtalen skal minimum regulere utplassering av deteksjonskapasiteter, hvordan alvorlige digitale angrep skal håndteres, og hvordan personopplysninger og opplysninger underlagt lovbestemt taushetsplikt skal behandles.

§ 57 Virksomhetens rett til innsyn

Virksomheter som er tilknyttet det digitale varslingssystemet har rett til innsyn i hvordan kapasitetene for deteksjon og sårbarhetsreduksjon som brukes i virksomheten er konfigurert. Virksomheten har også rett til innsyn i dataene som Nasjonal sikkerhetsmyndighet gjennom tilknytningen mottar fra virksomheten.

Kapittel 9. Personellsikkerhet

§ 58 Vilkår for å gi autorisasjon

Før autorisasjon gis skal personen ha signert taushetserklæring. Før det gis autorisasjon for COSMIC TOP SECRET skal også NATOs COSMIC-erklæring undertegnes. Dersom personen har

klarering på vilkår etter sikkerhetsloven § 8-6, skal autorisasjonsansvarlig før autorisasjon gis ha bestemt hvordan vilkårene skal følges opp.

En person som ikke er gitt sikkerhetsklarering, jf. sikkerhetsloven § 8-4, kan ikke autoriseres for BEGRENSET, uten tillatelse fra klareringsmyndigheten.

§ 59 Autorisasjonssamtale

Autorisasjonssamtale skal gjennomføres før autorisasjon finner sted, når personen selv ber om det, ved reklarering og når autorisasjonsansvarlig ellers finner grunn til det.

Autorisasjonsansvarlig skal gjennom autorisasjonssamtalen

a) forsikre seg om at personen kjenner til relevante sikkerhetstrusler og sikkerhetsbestemmelser og forstår sin rolle i sikkerhetsarbeidet til virksomheten
b) kontrollere at opplysningene fra den som autoriseres, er tilstrekkelige og oppdaterte
c) drøfte eventuelle sårbarheter personen har som er relevant for personellsikkerheten
d) drøfte tiltak som kan redusere personens sårbarheter eller som kan oppfylle vilkår som klareringsmyndigheten har gitt for klareringen.

Dersom personen har vært autorisert før, skal autorisasjonsansvarlig før samtalen hente inn opplysninger av betydning for autorisasjonen fra siste tidligere autorisasjonsansvarlig.

Personer som skal autoriseres for BEGRENSET, eller med kortvarig behov for autorisasjon for KONFIDENSIELT eller høyere, kan få en felles orientering om sikkerhetsmessige risikofaktorer og relevante krav til sikkerhet i stedet for en individuell autorisasjonssamtale. De skal likevel orienteres om sin rett til å kreve individuell autorisasjonssamtale.

Ved autorisasjon for STRENGT HEMMELIG, COSMIC TOP SECRET eller tilsvarende, skal autorisasjonssamtale gjennomføres minst hvert annet år.

§ 60 Autorisasjon av autorisasjonsansvarlig hos leverandøren

Oppdragsgiveren skal autorisere den autorisasjonsansvarlige hos leverandøren.

§ 61 Autorisasjon av utenlandske statsborgere

Dersom utenlandske statsborgere skal autoriseres for BEGRENSET, må autorisasjonsansvarlig innhente samtykke fra klareringsmyndigheten, jf. klareringsforskriften § 26.

Forespørselen om samtykke til autorisasjon må begrunnes og dokumenteres, og det må fremgå hvilken type sikkerhetsgradert informasjon personen skal ha tilgang til.

Utenlandske statsborgere kan bare autoriseres for tilgang til informasjon sikkerhetsgradert av fremmede stater dersom personen er borger av den fremmede staten, eller dersom Nasjonal sikkerhetsmyndighet har innhentet tillatelse fra statens kompetente myndigheter.

Utenlandske statsborgere kan bare autoriseres for tilgang til informasjon sikkerhetsgradert av internasjonal organisasjon dersom staten personen er borger av, er medlem av organisasjonen, eller dersom Nasjonal sikkerhetsmyndighet har innhentet tillatelse fra organisasjonen.

Første til tredje ledd gjelder også for personer som har dobbelt statsborgerskap, er statsløse eller har uavklarte statsborgerskap.

§ 62 Nødautorisasjon

Ved nødrett, jf. straffeloven § 17, kan en person autoriseres uten å ha nødvendig klarering. Virksomheten skal uten ugrunnet opphold varsle klareringsmyndigheten og Nasjonal sikkerhetsmyndighet om hvilke personer som har nødautorisasjon, og på hvilket nivå.

§ 63 Oversikt over personell med autorisasjon

Autorisasjonsansvarlig skal ha oversikt over personell som er autorisert. Oversikten skal inneholde opplysninger om

a) den enkeltes navn, statsborgerskap, tjenestested, saksfelt eller stilling

b) klareringsnivå og autorisasjonsnivå
c) klareringens gyldighetstid
d) eventuelle vilkår knyttet til klareringen
e) dato for autorisasjonssamtale
f) eventuelle nødautorisasjoner.

Autorisasjonsansvarlig skal gjøre klarerings- og autorisasjonsavgjørelser kjent for personell med tjenstlig behov.

§ 64 Dokumentasjon på autorisasjon

Hvis autorisasjonsansvarlig utsteder dokumentasjon på at en person er autorisert, skal dokumentasjonen være tidsbegrenset og vise hvilket graderingsnivå for informasjon, eller hvilket klassifiseringsnivå for objekt eller infrastruktur, som personen er autorisert for å få tilgang til.

§ 65 Nedsettelse, suspensjon og tilbakekallelse av autorisasjon

Dersom autorisasjonsansvarlig vurderer om en autorisasjon skal endres eller tilbakekalles, jf. sikkerhetsloven § 8-10, skal vurderingen og avgjørelsen dokumenteres. Avgjørelsen kan ikke påklages.

Hvis autorisasjonen endres til ulempe for personen, skal autorisasjonsansvarlig uoppfordret gjøre personen kjent med avgjørelsen og informere klareringsmyndigheten etter sikkerhetsloven § 8-10 første ledd. Avgjørelsen skal begrunnes overfor klareringsmyndigheten.

Dersom klareringsmyndigheten, etter å ha blitt informert etter andre ledd, opprettholder klareringen, kan autorisasjonsansvarlig ikke tilbakekalle, nedsette eller suspendere autorisasjonen på grunnlag av de innmeldte opplysningene.

§ 66 Begrunnelse og dokumentasjon ved forespørsel om klarering

Når autorisasjonsansvarlig ber om klarering, jf. sikkerhetsloven § 8-1, skal behovet for klarering begrunnes og dokumenteres. Hvis begrunnelsen for forespørselen er risiko for vilkårlig tilgang, skal autorisasjonsansvarlig bekrefte at andre sikkerhetstiltak for å redusere risikoen ikke er tilstrekkelig til å fjerne behovet for klarering.

Autorisasjonsansvarlig skal sende samtykke til klarering, og egenopplysninger fra personen som vurderes klarert, jf. klareringsforskriften § 7, til klareringsmyndigheten sammen med forespørselen om klarering.

§ 67 Merking av personopplysninger for klarering og autorisasjon

Opplysninger med personopplysninger i saker om autorisasjon, personkontroll eller klarering skal merkes PERSONKONTROLL. Kravet gjelder ikke meldinger om at autorisasjon eller klarering er gitt som forespurt, og meldinger om andre autorisasjons- eller klareringsavgjørelser til personen som avgjørelsen gjelder.

§ 68 Beskyttelse av personopplysninger for klarering og autorisasjon

Autorisasjonsansvarlig skal utpeke hvilket personell i virksomheten som kan få tilgang til opplysninger merket PERSONKONTROLL. Opplysningene skal lagres atskilt fra andre opplysninger i virksomheten, og slik at de bare er tilgjengelige for det utpekte personellet.

Når virksomheter utveksler opplysninger merket PERSONKONTROLL, skal det gjøres på en slik måte at uvedkommende ikke får tilgang til opplysningene.

§ 69 Bevaring og kassasjon av opplysninger i saker om autorisasjon og klarering

Autorisasjonsansvarlig skal uten ugrunnet opphold kassere eller returnere dokumenter med personopplysninger som er innhentet for autorisasjon eller klarering av søkere som ikke blir tilsatt, engasjert eller opptatt på skoler eller kurs.

Autorisasjonsansvarlig skal bevare opplysninger i autorisasjonssaken i 1 år etter at autorisasjonen er utløpt. Dersom den autoriserte er klarert skal autorisasjonsopplysningene bevares i klareringens gyldighetstid. Bevaringsplikten opphører dersom autorisasjonsopplysningene sendes til ny autorisasjonsmyndighet etter § 59 tredje ledd.

Autorisasjonsansvarlig skal bevare taushetserklæring signert av den autoriserte og oversikter over personell som er eller har vært autorisert, jf. § 63, i 25 år.

Når bevaringstiden etter andre og tredje ledd utløper, skal autorisasjonsansvarlig kassere opplysningene.

Autorisasjonsansvarlig skal føre et register over kassasjoner med opplysning om

a) hvem de kasserte opplysningene gjelder
b) hvilken type opplysninger eller dokument som er kassert
c) dato for kassasjonen.

Kapittel 10. Sikkerhetsgraderte anskaffelser

§ 70 Vurdering av graderingsnivået for ulike deler av en sikkerhetsgradert anskaffelse

Oppdragsgiveren skal ta stilling til hvilken sikkerhetsgradert informasjon, eller skjermingsverdig objekt eller infrastruktur, som tilbydere og leverandører kan få tilgang til i de ulike fasene av anskaffelsen.

§ 71 Krav til sikkerhetsavtalen etter sikkerhetsloven § 9-2 når leverandøren skal ha sikkerhetsgradert informasjon eller tilgang til skjermingsverdig objekt eller infrastruktur i eller fra sine egne lokaler

Dersom leverandøren skal ha sikkerhetsgradert informasjon eller tilgang til et skjermingsverdig objekt eller infrastruktur i eller fra sine egne lokaler, skal det fremgå av sikkerhetsavtalen

a) hvilken sikkerhets- eller klassifiseringsgrad informasjonen, objektet eller infrastrukturen har
b) hvem som skal få tilgang til den sikkerhetsgradert informasjonen eller det skjermingsverdig objektet eller infrastrukturen
c) hvordan den sikkerhetsgraderte informasjonen skal formidles mellom avtalepartene
d) hvilket informasjonssystem som skal brukes for å behandle den sikkerhetsgraderte informasjonen, eller for å få tilgang til det skjermingsverdige objektet eller infrastrukturen, og hvem som er ansvarlig for å godkjenne systemet
e) hvilke lokaler den sikkerhetsgraderte informasjonen skal behandles i
f) hvordan det skal varsles om sikkerhetstruende virksomhet og avvik fra sikkerhetskrav
g) om den sikkerhetsgraderte informasjonen skal leveres tilbake eller destrueres når oppdragets er avsluttet.

Avtalevilkårene etter første ledd kan inngå i en egen sikkerhetsavtale eller tas inn i det ordinære avtaledokumentet for anskaffelsen.

§ 72 Unntak fra krav om sikkerhetsavtale etter sikkerhetsloven § 9-2

Det kreves ikke sikkerhetsavtale dersom leverandørens personell bare skal gis tilgang til sikkerhetsgradert informasjon, eller skjermingsverdige objekter eller infrastruktur, under oppsyn av en representant for oppdragsgiveren.

§ 73 Tilbakelevering av sikkerhetsgradert informasjon

En leverandør som ikke tildeles kontrakt, skal levere tilbake sikkerhetsgradert informasjon uten unødig opphold.

Når kontraktsforholdet opphører, skal leverandøren levere tilbake sikkerhetsgradert informasjon. Som del av kontraktsforholdet regnes også eventuell service- og garantitid. Oppdragsgiveren skal melde fra til klareringsmyndigheten om at kontraktsforholdet har opphørt.

Dersom klareringsmyndigheten tilbakekaller leverandørklareringen etter sikkerhetsloven § 9-3 fjerde ledd, skal oppdragsgiveren inndra all sikkerhetsgradert informasjon fra leverandøren.

§ 74 Krav om leverandørklarering

En leverandør i en sikkerhetsgradert anskaffelse skal ha leverandørklarering når det er nødvendig for å oppnå et forsvarlig sikkerhetsnivå under anskaffelsen. Leverandøren skal uansett ha leverandørklarering dersom den skal

a) behandle eller oppbevare informasjon gradert KONFIDENSIELT eller høyere i sine egne informasjonssystemer eller lokaler
b) ha elektronisk tilgang til objekter eller infrastruktur klassifisert KRITISK eller MEGET KRITISK fra sine egne informasjonssystemer eller lokaler
c) råde over objekter eller infrastruktur som tilhører oppdragsgiveren, og som er klassifisert KRITISK eller MEGET KRITISK

§ 75 Leverandører med lokaler utenfor norsk jurisdiksjon og utenlandske leverandører

Dersom leverandøren som skal klareres, jf. § 74:

a) driver sin virksomhet fra en annen stats jurisdiksjon, eller
b) skal behandle eller oppbevare informasjon i lokaler utenfor norsk jurisdiksjon, eller
c) skal ha tilgang fra egne lokaler utenfor norsk jurisdiksjon, eller
d) skal råde over objektet eller infrastrukturen i lokaler utenfor norsk jurisdiksjon

må Norge ha en sikkerhetsavtale med staten som har jurisdiksjon der lokalene ligger eller der virksomheten drives fra.

Sikkerhetsavtalen må minimum bestemme hvem som skal kontrollere at leverandøren oppfyller kravene i sikkerhetsloven og virksomhetsforskriften, eller tilsvarende krav sikkerhetsregelverket til den andre staten, jf. klareringsforskriften § 33. Dersom myndighetene i den andre staten skal kontrollere virksomheten, skal klareringsmyndigheten be myndighetene i staten om å gjennomføre kontrollen.

§ 76 Forespørsel om leverandørklarering

Oppdragsgiveren skal be klareringsmyndigheten om leverandørklarering. Forespørselen skal inneholde informasjon om det høyeste graderingsnivå i anskaffelsen, jf. § 70, og egenopplysninger fra leverandøren, jf. klareringsforskriften § 30.

§ 77 Oversikt over sikkerhetsgraderte anskaffelser

Oppdragsgiveren skal føre en oversikt over sikkerhetsgraderte anskaffelser til sin virksomhet. Oversikten skal inneholde informasjon om

a) hva anskaffelsen gjelder
b) leverandørens navn, adresse, organisasjonsnummer og nasjonalitet
c) den høyeste sikkerhetsgraden til informasjon som leverandøren får tilgang til
d) det høyeste klassifiseringsnivået til objekter eller infrastruktur leverandøren får tilgang til
e) anskaffelsens varighet.

Oversikten skal årlig sendes til klareringsmyndigheten.

§ 78 Prosedyrer for besøk fra utlandet

Før et besøk fra en utenlandsk oppdragsgiver eller utenlandsk leverandør i en sikkerhetsgradert anskaffelse, skal de besøkendes identitet og klarering kontrolleres. Kontrollen skal

skje i samsvar med besøksprosedyrene i eller med hjemmel i avtalen mellom Norge og den andre staten.

Første ledd gjelder også dersom oppdragsgiver er en internasjonal organisasjon.

Kapittel 11. Avsluttende bestemmelser

§ 79 Ikrafttredelse

Forskriften trer i kraft 1. januar 2019.

§ 80 Overgangsregler

Informasjon som er sikkerhetsgradert etter lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste § 11, er sikkerhetsgradert er også etter lov 1. juni 2018 nr. 24 om nasjonal sikkerhet § 5-3.

Objekter som er klassifisert etter lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste § 17 a, er klassifisert også etter lov 1. juni 2018 nr. 24 om nasjonal sikkerhet § 7-2.

Skjermingsverdige informasjonssystemer og kryptosystemer som er godkjent etter forskrift 1. juli 2001 nr. 744 om informasjonssikkerhet §§ 5-24 og 7-2, er godkjent til godkjenningen opphører og systemene krever ny godkjenning.

Destrueringsmetoder og oppbevaringsenheter som er godkjent etter forskrift 1. juli 2001 nr. 744 om informasjonssikkerhet §§ 4-36, 6-11 og 6-12, er godkjent til godkjenningen opphører og destrueringsmetoden eller oppbevaringsenheten krever ny godkjenning.

Et rom som er godkjent etter forskrift 1. juli 2001 nr. 744 om informasjonssikkerhet § 9-1 og som ikke får godkjenningen trukket tilbake, anses å oppfylle kravet til forsvarlig sikkerhetsnivå, jf. § 44.

En klage på klassifisering eller godkjenning etter andre til fjerde ledd avgjøres etter reglene på vedtakstidspunktet.

11 Utkast til forskrift om klarering av leverandører og personell

Kapittel 1. Generelle bestemmelser om sikkerhetsklarering og adgangsklarering

§ 1. *Klareringsmyndighet*

Forsvaret klarerer personell i forsvarssektoren. Sivil klareringsmyndighet klarerer personell i sivil sektor. Nasjonal sikkerhetsmyndighet, Etterretningstjenesten, Politiets sikkerhetstjeneste og Statsministerens kontor klarerer personell i eller tilknyttet egen virksomhet.

Klareringsmyndighetene kan i enkeltsaker avtale hvem av dem som skal være klareringsmyndighet.

Ved tvil om hvem som er rett klareringsmyndighet fastsetter Nasjonal sikkerhetsmyndighet hvilken klareringsmyndighet som skal behandle saken.

Personell som utøver klareringsmyndighet, skal ha klarering for det høyeste klareringsnivået som personellet er gitt myndighet til å fastsette.

§ 2. *Definisjoner*

I denne forskriften menes med

a) nærstående: Personer som er i nær familie eller som har annen nær tilknytning som kan ha betydning for om en person er sikkerhetsmessig skikket.
b) nær familie:
    1. Ektefelle, partner eller samboer
    2. Tidligere ektefelle, partner eller samboer siste tre år
    3. Barn, stebarn, adoptivbarn og fosterbarn
    4. Forelder til felles barn, stebarn, adoptivbarn, fosterbarn
    5. Foreldre, steforeldre, adoptivforeldre, fosterforeldre
    6. Søsken, halvsøsken, stesøsken, adoptivsøsken og fostersøsken.
c) samboere: Personer som lever sammen i et ekteskapslignende forhold.
d) annen nær tilknytning: tilknytning av samme kvalitet som til personer i bokstav b og c. Det vil si personer som vedkommende har et tett personlig forhold til eller regelmessig privat omgang med.
e) personkontrollopplysninger: Personopplysninger innhentet i forbindelse med personkontroll etter sikkerhetsloven § 8-5.

§ 3. *Forholdet mellom adgangsklarering og sikkerhetsklarering*

Personer med sikkerhetsklarering for KONFIDENSIELT eller høyere er også klarert for adgang til skjermingsverdig objekt eller infrastruktur med krav om adgangsklarering.

§ 4. *Hvem som kan be om klarering*

Autorisasjonsansvarlig i virksomheter som er underlagt sikkerhetsloven kan be klareringsmyndigheten om klarering av personell.

For personell hos leverandører er det oppdragsgiver som skal be om klarering.

Kapittel 2. Personkontroll

§ 5. *Kontroll og avvisning av forespørsel om personkontroll*

Før klareringsmyndigheten kan be Nasjonal sikkerhetsmyndighet om å gjennomføre personkontroll, skal den kontrollere at forespørselen om klarering er tilstrekkelig begrunnet og

dokumentert, jf. virksomhetsforskriften § 66. Klareringsmyndigheten skal avvise forespørselen dersom den ikke er tilstrekkelig begrunnet og dokumentert.

§ 6. *Personer som inngår i personkontrollen*

Personkontroll ved sikkerhetsklarering omfatter

a) for KONFIDENSIELT: Den som skal klareres
b) for HEMMELIG: Den som skal klareres og dennes ektefelle, samboer eller partner
c) for STRENGT HEMMELIG: Den som skal klareres og nær familie.

Dersom det foreligger opplysninger som gir grunn til å anta at andre nærstående enn de som er nevnt i første ledd kan påvirke personens pålitelighet, lojalitet eller dømmekraft, kan også disse inngå i personkontrollen.

Personkontroll ved adgangsklarering omfatter den som skal klareres.

Ved utvidet adgangsklarering kan nærstående personer inngå i personkontrollen dersom det skal gis tilgang til MEGET KRITISK objekt, eller foreligger opplysninger som gir grunn til å anta at disse kan påvirke pålitelighet, lojalitet eller dømmekraft til den som skal klareres.

§ 7. *Sikkerhetsklarering – krav til egenopplysninger*

Den som skal sikkerhetsklareres for KONFIDENSIELT, skal på skjema fastsatt av Nasjonal sikkerhetsmyndighet gi sitt samtykke til gjennomføring av personkontroll og opplyse om

a) personalia
b) nåværende og tidligere statsborgerskap, eventuelt pass uten statsborgerskap
c) bostedsadresser og utenlandsopphold utenfor Norge
d) sivil status og familieforhold
e) utdanning og arbeidsforhold
f) man har vært anmeldt, siktet eller tiltalt for straffbare forhold, eller er blitt ilagt strafferettslige og disiplinære reaksjoner, både i Norge og i utlandet
g) eiendom eller andre økonomiske interesser man har eller har hatt i utlandet
h) man selv, eller noen i nær familie som man deler bosted med, sender eller mottar penger eller andre ytelser fra utlandet
i) særlig tilknytning til andre stater som kan ha betydning for klareringsavgjørelsen
j) man har vært i kontakt med personer, organisasjoner eller grupper i Norge eller utlandet som kan ha vært involvert i organisert kriminalitet eller i spionasje-, sabotasje- eller terrorhandlinger
k) forhold som kan føre til at man selv eller nærstående, jf. § 2 bokstav a utsettes for trusler slik at man kan bli presset til å handle i strid med nasjonale sikkerhetsinteresser
l) økonomiske forhold
m) forhold til rus- og dopingmidler
n) helsen og om bruk av medisiner som kan ha betydning for dømmekraften
o) andre forhold som kan gi grunn til å frykte at man selv vil kunne opptre i strid med nasjonale sikkerhetsinteresser
p) referanser
q) kjennskap om forhold angitt i bokstav f til j om nærstående jf. § 2 bokstav a. Ved slik kjennskap skal det også gis opplysninger som nevnt i bokstav a til e om disse personene.

Den som skal sikkerhetsklareres for HEMMELIG, NATO SECRET eller tilsvarende, skal i tillegg gi opplysninger angitt i første ledd bokstav a til c om nåværende ektefelle, partner eller samboere.

Den som skal sikkerhetsklareres for STRENGT HEMMELIG, COSMIC TOP SECRET eller tilsvarende, skal i tillegg gi opplysninger som nevnt i første ledd bokstav a til c om personer angitt i § 2 bokstav b nr. 2 til 6.

§ 8. *Adgangsklarering – krav til egenopplysninger*

Den som skal gis adgangsklarering, skal opplyse om det som kreves etter § 7 første ledd bokstav a og c.

Den som skal gis utvidet adgangsklarering, skal opplyse om det som kreves etter § 7 første ledd bokstav a til d og i til k.

§ 9. *Registre for personkontroll ved sikkerhetsklarering*

For personkontroll ved sikkerhetsklarering kan Nasjonal sikkerhetsmyndighet innhente og videreformidle til klareringsmyndigheten opplysninger fra

a) politiets registre
b) registre hos Politiets sikkerhetstjeneste
c) Skatteetatens registre
d) Nasjonal sikkerhetsmyndighets egne registre
e) Arbeidsgiver- og arbeidstakerregisteret
f) Utlendingsdirektoratets registre
g) namsmyndighetens registre
h) Kartverkets registre
i) Brønnøysundregistrene
j) kommersielle registre med inkasso- og kredittopplysninger.

For personkontroll av nærstående kan Nasjonal sikkerhetsmyndighet innhente og videreformidle til klareringsmyndigheten opplysninger som nevnt i første ledd bokstav a til f.

§ 10. *Registre for personkontroll ved adgangsklarering*

For personkontroll ved adgangsklarering kan Nasjonal sikkerhetsmyndighet innhente og videreformidle til klareringsmyndigheten opplysninger fra

a) politiets registre
b) registre hos Politiets sikkerhetstjeneste
c) Skatteetatens registre
d) Nasjonal sikkerhetsmyndighets egne registre
e) Arbeidsgiver- og arbeidstakerregisteret

For personkontroll ved utvidet adgangsklarering kan Nasjonal sikkerhetsmyndighet, i tillegg til opplysningene i første ledd bokstav a til e, innhente og videreformidle til klareringsmyndigheten opplysninger fra

f) Utlendingsdirektoratets registre
g) namsmyndighetens registre
h) Kartverkets registre.

For personkontroll av nærstående ved utvidet adgangsklarering kan Nasjonal sikkerhetsmyndighet innhente og videreformidle til klareringsmyndigheten opplysninger som nevnt i bokstav a til f.

§ 11. *Innhenting av personkontrollopplysninger fra andre stater*

Nasjonal sikkerhetsmyndighet kan innhente tilsvarende opplysninger som i §§ 9 og 10 fra andre staters myndigheter. Forespørselen om personkontrollopplysninger skal bare inneholde personens navn, fødselsdato, og adresse i den aktuelle staten, eller andre faktiske opplysninger som er nødvendige for å identifisere personen.

§ 12. *Behandlingsansvarliges plikter ved utlevering av opplysninger*

Behandlingsansvarlig skal utlevere personkontrollopplysninger uten ugrunnet opphold. Nasjonal sikkerhetsmyndighet avtaler med den enkelte behandlingsansvarlige hvordan personkontrollopplysningene skal utleveres.

Dersom det er usikkerhet knyttet til personkontrollopplysningenes kvalitet, skal behandlingsansvarlig opplyse Nasjonal sikkerhetsmyndighet om det før opplysningene utleveres.

§ 13. *Bruk av opplysninger fra registre hos politiet og Politiets sikkerhetstjeneste*

Politiet og Politiets sikkerhetstjeneste skal i avtale med Nasjonal sikkerhetsmyndighet fastsette til hva og hvordan opplysninger som innhentes etter § 9 første ledd bokstav a og b, og § 10 første ledd bokstav a og b, skal brukes. Det skal minst fastsettes hvordan hensynet til det opprinnelige formålet med opplysningene skal avveies mot hensynet til at opplysningene kan brukes i vurderingen av om en sikkerhetsklarering kan gis. Ved uenighet skal bruken av opplysningene avgjøres av Justis- og beredskapsdepartementet.

§ 14. *Personhistorikk*

For at en personkontroll for sikkerhetsklarering kan anses å være tilfredsstillende må personkontrollopplysninger for de siste ti årene om alle som inngår i personkontrollen være tilgjengelig for klareringsmyndigheten.

For at en personkontroll for adgangsklarering kan anses å være tilfredsstillende må personkontrollopplysninger for de siste fem årene om alle som inngår i personkontrollen være tilgjengelig for klareringsmyndigheten.

For at en personkontroll av personer som har oppholdt seg i utlandet kan anses å være tilfredsstillende må Norge ha et sikkerhetssamarbeid med staten som gir klareringsmyndigheten tilgang til personkontrollopplysninger fra staten.

Etter en konkret helhetsvurdering kan klarering likevel gis selv om kravet til personhistorikk i første til tredje ledd ikke er oppfylt. I vurderingen skal det blant annet legges vekt på om mangelen på personhistorikk skyldes kortvarig utenlandsopphold, om personen har tatt utdanning i utlandet, om personen har tjenestegjort for den norske stat eller humanitære organisasjoner, har arbeidet for en norsk virksomhet eller om mangelen skyldes andre forhold av liten betydning for om personen er sikkerhetsmessig skikket.

Etter en konkret helhetsvurdering kan en klareringsavgjørelse fra en annen stat eller internasjonal organisasjon som Norge har sikkerhetssamarbeid med kompensere for kravet til personhistorikk i første til tredje ledd.

Kapittel 3. Sikkerhetsklarering og adgangsklarering

§ 15. *Vurderingsgrunnlaget for adgangsklarering*

I vurderingen av adgangsklarering kan klareringsmyndigheten vektlegge forhold som nevnt i sikkerhetsloven § 8-4 fjerde ledd bokstav a, b, d, l og m. I vurderingen av forhold etter bokstav a skal det i hovedsak legges vekt på forhold som er relevant for planlegging, gjennomføring eller forsøk på terror.

I vurderingen av utvidet adgangsklarering kan klareringsmyndigheten i tillegg vektlegge forhold som nevnt i lovens § 8-4 fjerde ledd bokstav k og n. I vurderingen av forhold etter bokstav a skal det i tillegg til terrortrusselen legges vekt på forhold som er relevant for planlegging, gjennomføring eller forsøk på spionasje, sabotasje, attentat eller lignende.

§ 16. *Vurderingsgrunnlaget for tilknytning til andre stater*

I vurderingen av tilknytning til andre stater etter sikkerhetsloven § 8-4 fjerde ledd bokstav n, skal klareringsmyndigheten legge vekt på Nasjonal sikkerhetsmyndighets vurdering av risiko for at den andre staten kan påvirke påliteligheten, lojaliteten og dømmekraften til personer med tilknytning til staten, og hvilken grad av sikkerhetssamarbeid Norge har med den andre staten.

§ 17. *Klareringsintervju*

Med klareringsintervju menes sikkerhetssamtale etter sikkerhetsloven § 8-4 tredje ledd.

Formålet med klareringsintervjuet er å innhente opplysninger om forholdene i § 8-4 fjerde ledd.

Innholdet i et klareringsintervju skal dokumenteres med lydopptak. Dersom klareringsmyndigheten i stedet ønsker å dokumentere klareringsintervjuet med audiovisuelt opptak, kreves samtykke fra den som skal intervjues.

Den som innkalles til klareringsintervju har rett til å stille med bisitter som personlig støtte. Bisitter skal ikke ta del i dialogen under intervjuet. Bisitter kan uttale seg dersom denne anser at intervjuet gjennomføres i strid med sikkerhetsloven eller på en utilbørlig måte.

Hvem bisitteren er skal meldes til klareringsmyndigheten på forhånd. Nærstående til den som vurderes klarert kan ikke stille som bisitter. Klareringsmyndigheten kan avvise en bisitter av sikkerhetsmessige hensyn.

Bisitter skal undertegne en taushetserklæring før intervjuet.

§ 18. *Vurdering av om lavere klareringsnivå kan gis og bruk av vilkår*

Dersom klarering ikke kan gis for det klareringsnivået autorisasjonsansvarlig har bedt om, skal klareringsmyndigheten vurdere om klarering kan gis for et lavere nivå.

Dersom det brukes vilkår etter sikkerhetsloven § 8-6 skal disse være egnet til å redusere risikoen forbundet med å gi personen klarering.

§ 19. *Karantene før ny klareringsvurdering*

Dersom klareringsmyndigheten ikke innvilger klarering i samsvar med det den autorisasjonsansvarlige har bedt om, skal klareringsmyndigheten, så langt det er hensiktsmessig, fastsette en karantene. Personen kan ikke vurderes på nytt før karantenen har utløpt og det foreligger en ny begrunnet og dokumentert forespørsel om klarering. Karantenen kan ikke være lenger enn fem år.

Karantenen er bindende for andre klareringsmyndigheter. Karantenen hindrer likevel ikke at en avgjørelse kan omgjøres etter forvaltningsloven § 35.

§ 20. *Melding om klareringsavgjørelse*

Klareringsmyndigheten skal gi melding om klareringsavgjørelser til autorisasjonsansvarlig og til Nasjonal sikkerhetsmyndighet. Karantene etter § 19 eller vilkår etter sikkerhetslovens § 8-6 skal fremgå av meldingen.

Melding til autorisasjonsansvarlig om helt eller delvis avslag om klarering, skal gis individuelt.

I melding om helt eller delvis avslag til personen som har vært vurdert klarert, skal ikke opplysninger fra Politiets sikkerhetstjeneste eller etterretnings- og arbeidsregistre fra politiet inngå uten tillatelse i hvert enkelt tilfelle, eller i strid med eventuelle vilkår for bruk av opplysningene i avtale etter § 13.

§ 21. *Innsyn i klareringssak*

Klareringsmyndigheten kan ikke gi innsyn i opplysninger fra Politiets sikkerhetstjeneste eller etterretnings- og arbeidsregistre fra politiet uten tillatelse i hvert enkelt tilfelle, eller i strid med eventuelle vilkår for bruk av opplysningene i avtale etter § 13.

Innsyn i lydopptak eller audiovisuelt opptak av eget klareringsintervju gis kun ved oppmøte hos klareringsmyndigheten.

§ 22. *Gyldighetstid for sikkerhetsklarering og adgangsklarering*

En sikkerhetsklarering og adgangsklarering er gyldig i inntil fem år, dersom ikke annet følger av avtale mellom Norge og en annen stat eller internasjonal organisasjon. I særlige tilfeller kan klareringsmyndigheten forlenge gyldighetstiden med inntil ett år dersom den har mottatt forespørsel om ny klarering.

Dersom en ektefelle, partner eller samboer inngår i personkontrollen for en person med klarering, og denne personen inngår nytt ekteskap, partnerskap eller samboerskap, skal klareringsmyndigheten vurdere om klareringen kan opprettholdes.

Dersom en tidligere gitt klarering har blitt vurdert på nytt og opprettholdes, gjelder klareringens opprinnelige gyldighetstid. Dersom det er fattet avgjørelse om ny klarering gjelder gyldighetstiden etter første ledd.

§ 23. *Betydningen av forhold som ble vurdert ved en tidligere klareringsavgjørelse*

Forhold som har vært vurdert ved tidligere klareringsavgjørelser, kan ikke alene danne grunnlag for helt eller delvis å avslå en ny forespørsel, med mindre særlige sikkerhetshensyn taler for det.

§ 24. *Bevaring, kassasjon og avlevering av dokumenter i klareringssaker*

Nasjonal sikkerhetsmyndighet skal fastsette instruks om bevaring, kassasjon og avlevering av dokumenter i saker om personkontroll og klarering, som behandles av klareringsmyndighetene og Nasjonal sikkerhetsmyndighet. Instruksen skal godkjennes av Riksarkivaren.

§ 25. *Dekning av kostnader ved klarering*

Klareringsmyndigheten dekker kostnadene ved klarering, med mindre annet er avtalt med autorisasjonsansvarlig.

Klareringsmyndigheten dekker rimelige og nødvendige utgifter til reise og opphold. Utgifter ved bruk av bisitter under klareringsintervjuet, dekkes ikke.

Klareringsmyndigheten dekker utgifter til bruk av særskilt oppnevnt advokat når det brukes etter sikkerhetsloven § 8-15.

Kapittel 4. Samtykke til å autorisere utenlandske statsborgere for BEGRENSET

§ 26. *Samtykke til å autorisere utenlandske statsborgere for BEGRENSET*

Før en utenlandsk statsborger kan autoriseres for BEGRENSET skal klareringsmyndigheten samtykke til autorisasjonen. Autorisasjonsansvarlig skal be klareringsmyndigheten om samtykke til å autorisere en utenlandsk statsborger for BEGRENSET.

Forespørselen skal inneholde opplysningene som fremgår av § 27, og begrunnelsen for at den utenlandsk statsborgeren skal autoriseres. Dersom forespørselen ikke er tilstrekkelig begrunnet skal klareringsmyndigheten avvise forespørselen.

§ 27. *Egenopplysninger*

Den utenlandske statsborgeren skal opplyse om forhold angitt i § 7 første ledd bokstav a til c og g til j, på skjema fastsatt av Nasjonal sikkerhetsmyndighet.

Dersom den utenlandske personen har kjennskap om forhold angitt i § 7 bokstav g til j om personer i nær familie, jf. § 2 bokstav b, skal den utenlandske statsborgeren opplyse om forholdene, og om opplysninger nevnt i bokstav a til c om disse personene.

§ 28. *Saksbehandling og avgjørelse av forespørsel om samtykke til autorisasjon*

Når klareringsmyndigheten behandler en forespørsel om samtykke til å autorisere en utenlandsk statsborger for BEGRENSET, skal det legges vekt på risikoen ved å gi autorisasjon.

Klareringsmyndigheten skal ta utgangspunkt i Nasjonal sikkerhetsmyndighets vurdering, jf. § 16. Det skal også tas hensyn til omfanget av autorisasjonsbehovet.

Samtykke skal bare gjelde for et nærmere bestemt formål og kun innenfor myndighetsområdet til den autorisasjonsansvarlige som har bedt om tillatelsen.

Klareringsmyndigheten kan sette vilkår om hvordan den utenlandske statsborgeren skal autoriseres skal følges opp av autorisasjonsansvarlig.

Forespørsler og samtykke til autorisasjon av utenlandske statsborgere for BEGRENSET skal dokumenteres. Dokumentasjonen skal være tilgjengelig for Nasjonal sikkerhetsmyndighet.

Kapittel 5. Leverandørklarering

§ 29. *Klareringsmyndighet for leverandørklarering*

Nasjonal sikkerhetsmyndighet klarerer norske leverandører i sikkerhetsgraderte anskaffelser. Utenlandske leverandører klareres av myndighetene i sitt hjemland.

§ 30. *Egenopplysninger fra leverandøren*

Leverandør som skal klareres skal gi samtykke til å bli kontrollert og i skjema fastsatt av Nasjonal sikkerhetsmyndighet gi opplysninger om

a) leverandørens navn, adresse og eierstruktur
b) utenlandske eierinteresser i leverandøren
c) leverandørens eierinteresser i utlandet
d) virksomhetens leders navn, fødselsnummer og statsborgerskap
e) pågående oppdrag for utenlandske oppdragsgivere, med opplysninger om oppdragsgivere og hvilken andel av leverandørens omsetning oppdragene utgjør

Leverandøren skal sammen med skjemaet levere skisser eller tegninger over lokalene som skal brukes til behandling og oppbevaring av sikkerhetsgradert informasjon.

§ 31. *Vurderingsgrunnlaget for leverandørklarering*

Før en leverandørklarering gis må leverandøren oppfylle kravene i sikkerhetsloven og virksomhetsforskriften. I tillegg kan det i vurderingen av om leverandørklareringen skal gis, legges vekt på:

a) økonomiske forhold, også risikoen for insolvens
b) organisasjonsform og eierstruktur
c) om virksomheten er registrert med straffbare forhold
d) om det foreligger andre forhold som kan gi grunn til å tro at leverandøren vil kunne opptre i strid med nasjonale sikkerhetsinteresser.

Før en leverandørklaring kan gis, skal virksomhetens leder og styremedlemmer klareres for det samme nivå som det er bedt om leverandørklarering for.

Leverandørklarering kan likevel gis dersom det styremedlem eller virksomhetens leder som ikke kan klareres, gir avkall på innsynsretten i den sikkerhetsgraderte informasjonen eller tilgangen til objekter eller infrastruktur, som gjør det nødvendig med leverandørklarering, jf. § 74 i virksomhetsforskriften. Dokumentasjon på at det er gitt avkall skal sendes til klareringsmyndigheten.

§ 32. *Kilder for leverandørkontroll*

I tillegg til å innhente opplysninger fra leverandøren etter sikkerhetsloven § 9-3 tredje ledd kan klareringsmyndigheten innhente opplysninger om leverandøren fra

a) politiets registre
b) registre hos Politiets sikkerhetstjeneste
c) skatteetatens registre
d) Brønnøysundregistrene
e) kommersielle registre med leverandøropplysninger
f) kommersielle registre med inkasso- og kredittopplysninger
g) klareringsmyndighetens egne registre.

§ 33. *Kontroll av om leverandøren oppfyller sikkerhetskravene*

Før leverandørklarering kan gis skal klareringsmyndigheten kontrollere at leverandøren oppfyller kravene i sikkerhetsloven og virksomhetsforskriften, jf. § 31. Dersom leverandøren ikke oppfyller kravene til styringssystem eller ikke har gjennomført tilstrekkelig sikkerhetstiltak skal leverandørklarering ikke gis eller gis på vilkår.

Klareringsmyndigheten skal kontrollere leverandøren på nytt dersom det i løpet av klareringens gyldighetstid er nødvendig ut ifra en vurdering av risiko, ved reklarering og hvis leverandøren selv ber om det. Dersom det er gjennomført tilsyn med leverandøren skal klareringsmyndigheten innhente rapport fra tilsynsmyndigheten om tilsynet.

Leverandøren skal motta skriftlig varsel før klareringsmyndigheten gjennomfører en stedlig kontroll. Kontrollen kan likevel gjennomføres uten varsel dersom sikkerhetshensyn gjør det nødvendig. Klareringsmyndigheten skal utarbeide rapport fra kontrollen.

Kontrollen etter første og andre ledd kan gjennomføres av oppdragsgiveren etter avtale med klareringsmyndigheten.

Klareringsmyndigheten skal ikke føre kontroll dersom det følger av sikkerhetsavtale mellom Norge og annen stat eller internasjonal organisasjon at kontrollen skal gjennomføres av andre.

§ 34. *Tilbakekall av leverandørklarering*

Leverandørklareringen kan kalles tilbake dersom leverandøren ikke retter avvik fra kravene i sikkerhetsloven og virksomhetsforskriften innen en fastsatt frist. Foreligger det et vesentlig avvik kan klareringsmyndigheten tilbakekalle leverandørklareringen uten at det settes en frist.

§ 35. *Leverandørklareringens gyldighetstid*

En leverandørklarering kan gis for inntil fem år, med mindre annet følger av avtale mellom Norge og en annen stat eller internasjonal organisasjon.

§ 36. *Registrering av klareringsavgjørelser*

Avgjørelser om leverandørklarering skal registreres i det sentrale registeret over leverandørklareringer, jf. myndighetsforskriften § 9.

Kapittel 6. Særbestemmelser for domstolene

§ 37. *Kapitlets virkeområde*

Bestemmelsene i dette kapitlet gjelder i saker for domstolene hvor det blir gitt opplysninger om sikkerhetsgradert informasjon.

Kapitlet gjelder for dommere og alle andre aktører som kan få tilgang til sikkerhetsgradert informasjon.

§ 38. *Klareringsmyndighet og autorisasjonsansvarlig*

Justitiarius er klareringsmyndighet og autorisasjonsansvarlig for Høyesterett og førstelagmannen i hver av lagmannsrettene, samt klageinstans for klareringsavgjørelser fattet av lavere rettsinstans.

Førstelagmannen er klareringsmyndighet og autorisasjonsansvarlig for lagmannsretten og sorenskriveren i lavere rettsinstans, samt klareringsmyndighet for lavere rettsinstans.

Førstelagmannen og Sivil klareringsmyndighet kan avtale at klareringsmyndighet etter andre ledd utøves av Sivil klareringsmyndighet. I saker der Sivil klareringsmyndighet utøver klareringsmyndighet etter andre ledd, gjelder særbestemmelsene for domstolene i §§ 37 til 41.

Sorenskriveren er autorisasjonsansvarlig for egen rettsinstans.

§ 39. *Forhåndsvalg av domstoler for enkeltstående rettergangsskritt i straffesaker*

Enkeltstående rettergangsskritt i straffesaker hvor det vil bli gitt sikkerhetsgradert informasjon, skal bare foretas ved domstoler høyesterettsjustitiarius utpeker. Før justitiarius fatter sin avgjørelse, skal uttalelse innhentes fra Riksadvokaten.

§ 40. *Sikkerhetsklarering og autorisasjon av meddommere*

Meddommere som skal delta i en sak med sikkerhetsgradert informasjon skal være sikkerhetsklarert og autorisert.

§ 41. *Unntak fra sikkerhetslovens bestemmelser*

Sikkerhetsloven § 3-1, § 3-4 og § 3-6 gjelder ikke for domstolene i saker om autorisasjon og klarering.

Kapittel 7. Avsluttende bestemmelser

§ 42. *Ikrafttredelse*

Forskriften trer i kraft 1. januar 2019.

§ 43. *Overgangsregler*

Den som er sikkerhetsklarert etter lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste § 19, er sikkerhetsklarert frem til klareringen opphører.

En klage i sak om sikkerhetsklarering avgjøres etter reglene på vedtakstidspunktet.