DET KONGELIGE
FORSVARSDEPARTEMENT

Prop. 153 L

(2016–2017)

Proposisjon til Stortinget (forslag til lovvedtak)

Lov om nasjonal sikkerhet (sikkerhetsloven)

Særskilt vedlegg: NOU 2016: 19 Samhandling for sikkerhet – Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid

Innhold

1	**Proposisjonens hovedinnhold** ..	7
2	**Bakgrunnen for lovforslaget**	10
2.1	Endringer og utviklingstendenser	10
2.2	Sikkerhetsutvalgets mandat	10
2.3	Sikkerhetsutvalgets rapport – NOU 2016: 19 Samhandling for sikkerhet	11
2.4	Høringen	11
3	**Dagens sikkerhetsutfordringer**	15
4	**Rettstilstanden i andre land**	18
4.1	Sverige	18
4.1.1	Sikkerhetslovgivningen i Sverige ..	18
4.1.2	Informasjonssikkerhet og informasjonssystemsikkerhet	18
4.1.3	Personellsikkerhet	18
4.1.4	Objekt- og infrastruktursikkerhet	19
4.2	Danmark	19
4.2.1	Sikkerhetslovgivningen i Danmark	19
4.2.2	Informasjonssikkerhet og informasjonssystemsikkerhet	19
4.2.3	Personellsikkerhet	19
4.2.4	Objekt- og infrastruktursikkerhet	20
4.3	Storbritannia	20
4.3.1	Sikkerhetslovgivningen i Storbritannia	20
4.3.2	Informasjonssikkerhet og informasjonssystemsikkerhet	20
4.3.3	Personellsikkerhet	20
4.3.4	Objekt- og infrastruktursikkerhet	20
4.4	NATO	21
4.4.1	Informasjonssikkerhet og informasjonssystemsikkerhet	21
4.4.2	Objekt- og infrastruktursikkerhet	21
4.5	Reguleringen av informasjons-sikkerhet og informasjonssystem-sikkerhet i EU	21
5	**Generelt om lovens oppbygging og innhold**	23
6	**Lovens formål og virkeområde**	24
6.1	Gjeldende rett	24
6.2	Utvalgets forslag	25
6.3	Høringsinstansenes syn	26
6.3.1	Formål og virkeområde	26
6.3.2	Virkeområde	27
6.3.3	Begrepsbruk og definisjoner	30
6.4	Departementets vurdering	31
6.4.1	Generelt	31
6.4.2	Formål	32
6.4.3	Virkeområde	37
7	**Ansvar og myndighet**	40
7.1	Gjeldende rett	40
7.1.1	Departementenes ansvar og myndighet	40
7.1.2	Nasjonal sikkerhetsmyndighet	40
7.1.3	Varslingsplikt og myndighet til å fatte vedtak ved risiko for sikkerhetstruende virksomhet	41
7.1.4	Ansvar og myndighet etter relevant sektorregelverk	41
7.2	Utvalgets forslag	41
7.2.1	Departementenes ansvar og myndighet etter loven	41
7.2.2	Sikkerhetsmyndigheten	43
7.2.3	Informasjon om trussel-vurderinger og risikohåndtering ..	44
7.2.4	Nasjonal responsfunksjon for alvorlige dataangrep	44
7.2.5	Vedtaksmyndighet for Kongen i statsråd	45
7.2.6	Klage- og tvisteløsning og tviste-organ	45
7.3	Høringsinstansenes syn	46
7.3.1	Generelt	46
7.3.2	Tvisteorgan	48
7.4	Departementets vurdering	52
7.4.1	Departementenes ansvar og myndighet etter loven	52
7.4.2	Sikkerhetsmyndighetens ansvar for forebyggende sikkerhetsarbeid	53
7.4.3	Utveksling av trusselvurderinger og annen sikkerhetsinformasjon ..	53
7.4.4	Nasjonal responsfunksjon for alvorlige digitale angrep	54
7.4.5	Vedtak ved risiko for skade-virkninger for nasjonale sikkerhetsinteresser	54
7.4.6	Klage- og tvisteløsning og tviste-organ	54
8	**Tilsyn**	56
8.1	Gjeldende rett	56
8.2	Utvalgets forslag	56
8.3	Høringsinstansenes syn	58
8.3.1	Tilsyn med virksomheter	59
8.3.2	Sikkerhetsmyndighetens samarbeid med sektor-myndigheter	60
8.3.3	Generelle prinsipper for tilsyn	62

8.3.4 Stedlige tilsyn 63
8.3.5 Tilsynsmyndighetens behandling av personopplysninger 63
8.3.6 Pålegg 64
8.4 Departementets vurdering 64
8.4.1 Generelt 64
8.4.2 Tilsyn med virksomheter 65
8.4.3 Sikkerhetsmyndighetens samarbeid med sektor-myndigheter 67
8.4.4 Generelle prinsipper for tilsyn 68
8.4.5 Stedlige tilsyn 69
8.4.6 Tilsynsmyndighetens behandling av personopplysninger 69
8.4.7 Pålegg 69

9 Generelle krav til forebyggende sikkerhetsarbeid 71
9.1 Gjeldende rett 71
9.2 Utvalgets forslag 71
9.3 Høringsinstansenes syn 74
9.3.1 Plikt til å gjennomføre sikkerhets-tiltak 74
9.3.2 Sikkerhetsstyring 76
9.3.3 Vurdering av risiko 76
9.3.4 Krav til dokumentasjon og øvelser 77
9.3.5 Varsling 77
9.4 Departementets vurdering 78

10 Informasjonssikkerhet og informasjonssystemsikkerhet .. 83
10.1 Innledning 83
10.2 Gjeldende rett 85
10.2.1 Informasjon som skal beskyttes etter sikkerhetsloven 85
10.2.2 Beskyttelse av skjermingsverdig informasjon 85
10.2.3 Informasjonssystemsikkerhet 85
10.3 Utvalgets forslag 88
10.3.1 Informasjon som skal beskyttes etter sikkerhetsloven 88
10.3.2 Beskyttelse av skjermingsverdig informasjon 89
10.3.3 Informasjonssystemsikkerhet 90
10.4 Høringsinstansenes syn 91
10.4.1 Informasjon som skal beskyttes etter sikkerhetsloven 91
10.4.2 Beskyttelse av skjermingsverdig informasjon 92
10.4.3 Informasjonssystemsikkerhet 94
10.5 Departementets vurdering 95
10.5.1 Informasjon som skal beskyttes etter sikkerhetsloven 95
10.5.2 Beskyttelse av skjermingsverdig informasjon 97
10.5.3 Informasjonssystemsikkerhet 99

11 Objekt- og infrastruktur-sikkerhet 104
11.1 Gjeldende rett 104
11.2 Utvalgets forslag 105
11.3 Høringsinstansenes syn 106
11.4 Departementets vurdering 111

12 Personellsikkerhet 114
12.1 Innledning 114
12.2 Gjeldende rett 114
12.2.1 Innledning 114
12.2.2 Personellklarering og autorisasjon m.m. 114
12.2.3 Saksbehandlingsregler 116
12.2.4 Tilgang til skjermingsverdige objekter 117
12.2.5 Sektorregelverket 117
12.3 Utvalgets forslag 118
12.3.1 Innledning 118
12.3.2 Tilpasninger og strukturelle endringer 118
12.3.3 Klarering av personer som ikke er norske statsborgere og tilknytning til andre nasjoner 119
12.3.4 Hjemmel for adgangsklarering 119
12.3.5 Mangelfull personhistorikk 120
12.3.6 Digitalisert overføring av register-opplysninger 120
12.3.7 Fornyet personkontroll 120
12.3.8 Utlevering av informasjon til Politiets sikkerhetstjeneste 121
12.4 Høringsinstansenes syn 121
12.4.1 Generelt 121
12.4.2 Bruk av vilkår og klarering for stilling 122
12.4.3 Utenlandske statsborgere og tilknytning til andre stater 123
12.4.4 Adgangsklarering 123
12.4.5 Mangelfull personhistorikk 125
12.4.6 Digitalisert overføring av register-opplysninger 127
12.4.7 Fornyet personkontroll 127
12.4.8 Utlevering av informasjon til Politiets sikkerhetstjeneste 127
12.4.9 Sikkerhetssamtale 130
12.5 Departementets vurdering 131
12.5.1 Tilpasninger og strukturelle endringer 131
12.5.2 Utenlandske statsborgere og tilknytning til andre stater 132
12.5.3 Adgangsklarering 132
12.5.4 Bruk av vilkår og klarering for stilling 133

12.5.5 Mangelfull personhistorikk 133
12.5.6 Egen hjemmel for varslingsplikt ... 133
12.5.7 Digitalisert overføring av register-opplysninger 134
12.5.8 Fornyet personkontroll 134
12.5.9 Utlevering av informasjon til Politiets sikkerhetstjeneste og konsekvenser for autorisasjons-ansvarliges plikter 134
12.5.10 Sikkerhetssamtale 135

13 Sikkerhetsgraderte anskaffelser 136
13.1 Gjeldende rett 136
13.2 Utvalgets forslag 137
13.3 Høringsinstansenes syn 138
13.4 Departementets vurdering 141
13.4.1 Generelt 141
13.4.2 Virkeområde for reglene om sikkerhetsgraderte anskaffelser ... 141
13.4.3 Sikkerhetsavtale 142
13.4.4 Leverandørklarering 143
13.4.5 Varslingsplikt ved anskaffelser til skjermingsverdige objekter, informasjonssystemer og infra-struktur 143
13.4.6 Forholdet til annet regelverk 144

14 Eierskapskontroll 145
14.1 Gjeldende rett 145
14.2 Utvalgets forslag 146
14.3 Høringsinstansenes syn 148
14.4 Departementets vurdering 150

15 Kontroll- og tilsynsordninger ... 153
15.1 Gjeldende rett 153
15.2 Utvalgets forslag 153
15.3 Høringsuttalelser 154
15.4 Departementets vurdering 155

16 Ikrafttredelse 156

17 Kompensatoriske ordninger ... 157
17.1 Gjeldende rett 157
17.2 Utvalgets forslag 157
17.3 Høringsinstansenes syn 157
17.4 Departementets vurdering 158

18 Økonomiske og administrative konsekvenser 159
18.1 Utvidelsen av virkeområdet 159
18.2 Informasjonssikkerhet, informasjonssystemsikkerhet og objekt- og infrastruktursikkerhet .. 160
18.3 Personellsikkerhet 160
18.4 Eierskapskontroll 161
18.5 Sikkerhetsmyndigheten 161

19 Merknader til de enkelte bestemmelsene 163
19.1 Kapittel 1 Formål og virkeområde 163
19.2 Kapittel 2 Ansvar og myndighet for forebyggende sikkerhets-arbeid 166
19.3 Kapittel 3 Tilsyn 169
19.4 Kapittel 4 Generelle krav til forebyggende sikkerhetsarbeid ... 172
19.5 Kapittel 5 Informasjonssikkerhet .. 175
19.6 Kapittel 6 Informasjonssystem-sikkerhet 177
19.7 Kapittel 7 Objekt- og infrastruktur-sikkerhet 180
19.8 Kapittel 8 Personellsikkerhet 183
19.9 Kapittel 9 Sikkerhetsgraderte anskaffelser mv. 189
19.10 Kapittel 10 Eierskapskontroll 192
19.11 Kapittel 11 Særskilte kontroll- og tilsynsordninger. Tvangsmulkt, overtredelsesgebyr og straff 193
19.12 Kapittel 12 Ikrafttredelse og endringer i andre lover 194

Forslag til lov om nasjonal sikkerhet (sikkerhetsloven) 195

DET KONGELIGE
FORSVARSDEPARTEMENT

Prop. 153 L

(2016–2017)

Proposisjon til Stortinget (forslag til lovvedtak)

Lov om nasjonal sikkerhet (sikkerhetsloven)

Tilråding fra Forsvarsdepartementet 16. juni 2017,
godkjent i statsråd samme dag.
(Regjeringen Solberg)

1 Proposisjonens hovedinnhold

Forsvarsdepartementet foreslår i denne proposisjonen en ny lov om nasjonal sikkerhet (sikkerhetsloven). Forslaget er en modernisering av lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven). En ny lov om nasjonal sikkerhet er et av regjeringens prioriterte tiltak for å styrke sikkerhetsarbeidet i Norge. Departementet foreslår en dynamisk og fleksibel rammelov som skal bidra til å trygge våre overordnede nasjonale sikkerhetsinteresser. Den vil sette myndigheter og virksomheter bedre i stand til å sikre disse sentrale nasjonale interessene mot et trussel- og risikobilde i stadig og rask endring. Forslaget vil styrke samhandlingen mellom myndigheter og virksomheter slik at det forebyggende sikkerhetsarbeidet mot terror, sabotasje og spionasje kan gjennomføres på en mer effektiv og forsvarlig måte, på tvers av alle samfunnssektorene. Samtidig skal loven sikre at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn. Særlig viktig er det at nødvendige personvernhensyn blir ivaretatt.

Dagens sikkerhetslov var ment å kunne tilpasses samfunnsmessige endringer, men særlig den raske teknologiske utviklingen har gjort det nødvendig å revidere og modernisere loven. Forsvarsdepartementets arbeid med å utforme en ny og moderne sikkerhetslov bygger på Sikkerhetsutvalgets rapport NOU 2016: 19 *Samhandling for sikkerhet – Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*.

Formålet med den nye sikkerhetsloven er i likhet med dagens sikkerhetslov å trygge nasjonale sikkerhetsinteresser, og særlig landets *suverenitet, territorielle integritet og demokratiske styreform*. I tråd med Sikkerhetsutvalgets anbefalinger er den nye sikkerhetsloven innrettet med sikte på å beskytte viktige samfunnsfunksjoner som understøtter disse interessene. Disse funksjonene er kalt *grunnleggende nasjonale funksjoner*. Med dette menes *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*. Sammenlignet med gjeldende sikkerhetslov vil forslaget til ny sikkerhetslov få et noe videre virkeområde.

Departementet foreslår at loven, i likhet med dagens lov, skal gjelde for alle statlige, fylkeskom-

munale og kommunale organer. Virksomheter som råder over informasjon, informasjonssystemer, objekter eller infrastruktur eller driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner, skal omfattes av loven. Det er i tillegg presisert at virksomheter som behandler sikkerhetsgradert informasjon, må være underlagt loven. Lovforslaget viderefører samtidig utvalgets systematikk med at de enkelte departementene innenfor sine myndighetsområder skal utpeke virksomheter som loven skal gjelde for. De enkelte departementene vil fortsatt ha det overordnede ansvaret for forebyggende sikkerhetsarbeid innenfor sitt myndighetsområde. Sett i sammenheng med et utvidet virkeområde vil dette føre til at flere virksomheter enn i dag vil bli underlagt sikkerhetsloven.

I tråd med NOU 2016: 19 foreslår departementet at sikkerhetsmyndigheten (dvs. Nasjonal sikkerhetsmyndighet) skal ha det sektorovergripende ansvaret for å følge opp at forebyggende sikkerhetsarbeid i virksomhetene skjer i samsvar med loven. Dette er langt på vei en videreføring av gjeldende rett, men lovforslaget tydeliggjør sikkerhetsmyndighetens rolle og ansvar. I tillegg legges det opp til utvidet samarbeid mellom ulike myndigheter og en plikt for sikkerhetsmyndigheten til å gi råd og veiledning. Sikkerhetsmyndigheten skal også legge til rette for informasjonsdeling mellom myndigheter og virksomheter.

Departementet foreslår å videreføre tilsynsmodellen som Sikkerhetsutvalget har anbefalt. Sikkerhetsmyndigheten skal som utgangspunkt føre tilsyn etter loven, men i sektorer der det finnes kompetente sektormyndigheter som fører tilsyn med beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur, kan ansvarlig departement bestemme at sektormyndigheten skal ha tilsynsansvaret.

Utvalgets forslag til et tvisteorgan for å behandle klager fra private virksomheter som underlegges loven og uenigheter mellom departementene, videreføres ikke i departementets lovforslag. Isteden videreføres og klargjøres dagens klageordning etter forvaltningsloven.

I lovforslagets kapittel 4 om generelle krav til forebyggende sikkerhetsarbeid foreslår departementet å lovfeste at det først og fremst er den enkelte virksomhet som har ansvar for sikkerheten. I tråd med utvalgets anbefaling foreslås det at det gjennomgående stilles funksjonelle krav til sikkerhetstiltak. Dette vil både kunne legge til rette for sektorspesifikke tilpasninger og kostnadseffektive løsninger. Det stilles krav til at alle virksomheter som er underlagt loven, skal foreta en vurdering av risiko. Denne skal danne grunnlaget for å iverksette tiltak som sørger for et forsvarlig sikkerhetsnivå i virksomheten. Virksomhetene ilegges også en plikt til å varsle om sikkerhetstruende virksomhet. Begrepet *sikkerhetstruende virksomhet* utvides sammenliknet med dagens sikkerhetslov.

Den tiltakende digitaliseringen av samfunnet har ført til behov for å gjøre enkelte endringer i dagens regler om informasjonssikkerhet. Departementet foreslår å videreføre den særlige beskyttelsen av sikkerhetsgradert informasjon. Konfidensialitet, det å skjerme gradert informasjon for uvedkommende, er imidlertid ikke alltid tilstrekkelig. Det er i mange tilfeller også helt avgjørende at informasjonen er tilgjengelig for de som trenger den, og at den er korrekt. Departementet foreslår derfor en plikt til også å beskytte informasjon som er særlig viktig av hensyn til informasjonens tilgjengelighet og integritet, i tillegg til beskyttelse av hensyn til konfidensialitet.

Departementet støtter utvalgets forslag om å utvide lovens beskyttelse av informasjonssystemer. Beskyttelse av informasjonssystemer som behandler sikkerhetsgradert informasjon, skal fortsatt omfattes av sikkerhetsloven. I tillegg foreslås det i lovforslagets kapittel 6 at informasjonssystemer som i seg selv er av avgjørende betydning for grunnleggende nasjonale funksjoner, skal beskyttes etter loven.

I lovforslagets kapittel 7 foreslår departementet et økt systemfokus i det forebyggende sikkerhetsarbeidet. Både objekter – slik som i dag – og infrastruktur som er av avgjørende betydning for grunnleggende nasjonale funksjoner, skal beskyttes etter loven. Dette skal bidra til en mer helhetlig tilnærming til sikkerhetsarbeidet. Ordningen med klassifisering av objekter foreslås videreført.

I tråd med utvalget foreslår departementet å videreføre hovedelementene i dagens regler om personellsikkerhet. Departementet støtter dessuten utvalgets forslag om fornyet personkontroll. De forhold som kan ha betydning for en sikkerhetsklarering, kan endre seg over tid. Det vil derfor kunne oppstå behov for en fornyet personkontroll. Personvernhensyn skal ivaretas, og det skal derfor kun gjennomføres slik fornyet kontroll når klareringsmyndigheten anser at det er behov for det. Videre foreslår departementet å gi hjemmel for å foreta adgangsklarering for tilgang til skjermingsverdige objekter og infrastrukturer, samt en hjemmel for å kunne dele informasjon fra klareringssaker med Politiets sikkerhetstjeneste.

En stadig mer globalisert verden har ført til at norske virksomheter i større utstrekning enn tidli-

gere benytter seg av utenlandsk arbeidskraft. Departementet foreslår derfor moderniserte og bedre tilpassede bestemmelser om sikkerhetsklarering av personer med utenlandsk statsborgerskap.

Reglene om sikkerhetsgraderte anskaffelser foreslås i all hovedsak videreført. Virksomheter som er underlagt loven, har en plikt til å vurdere risikoen når en leverandør kan få tilgang til sikkerhetsgradert informasjon eller skjermingsverdig objekt eller infrastruktur. Det må i slike tilfeller inngås en sikkerhetsavtale med leverandøren, og det må vurderes om leverandøren skal klareres.

Utvalget foreslår å innføre regler om kontroll med eierskap i virksomheter som er underlagt loven. Departementet er enig med utvalget i at det eksisterende regelverket ikke er tilstrekkelig for å hindre at nasjonal sikkerhet blir skadelidende ved at slike virksomheter blir kjøpt opp av utenlandske aktører. Departementet foreslår derfor en lovhjemmel for Kongen i statsråd til å stanse oppkjøp av virksomheter som er underlagt sikkerhetsloven. Hjemmelen antas benyttet kun i helt særskilte tilfeller.

2 Bakgrunnen for lovforslaget

2.1 Endringer og utviklingstendenser

Gjeldende sikkerhetslov trådte i kraft 1. juli 2001. Bortsett fra de endringene som ble gjort med ikrafttredelse 1. januar 2017, har loven i hovedsak bare vært endret to ganger, i 2005 i forbindelse med bestemmelsene om personellsikkerhet og i 2008 om objektsikkerhet. Endringene har således vært på avgrensede områder. Det samme gjelder langt på vei også endringsloven av 12. august 2016 med ikrafttredelse 1. januar 2017. De mest sentrale endringene her var en reduksjon av antall klareringsmyndigheter, med én sentral klareringsmyndighet i sivil sektor og én tilsvarende i forsvarssektoren, nye bestemmelser om varsling og myndighet til å fatte vedtak ved risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført og ved anskaffelser til kritisk infrastruktur, dersom en slik anskaffelse kan innebære en risiko som nevnt foran. Videre ble bestemmelsen om leverandørklarering i forbindelse med sikkerhetsgraderte anskaffelser endret fra oppdragsbasert til tidsbasert.

Samlet sett er det over årene gjort en del endringer i sikkerhetsloven, men det er ikke før nå blitt foretatt en helhetlig lovrevisjon.

Samfunnet og virkelighetsbildet innenfor sikkerhetsområdet har gjennomgått store endringer siden 2001. Markante enkelthendelser av terror og andre anslag, og mer overordnede tendenser, har påvirket den virkeligheten som loven skal forholde seg til. Risiko- og trusselbildet er mer sammensatt enn tidligere, med store teknologiske, demografiske og sikkerhetsmessige endringer. Begrepet samfunnssikkerhet er derfor tatt i bruk og har de siste årene fått stadig større fokus i samfunnsplanleggingen. Samfunnssikkerhet må ses i nær sammenheng med statssikkerhetsbegrepet. Dette har gitt behov for en helhetlig vurdering og nytenkning med hensyn til lovregulering av forebyggende nasjonalt sikkerhetsarbeid.

Samfunnets og borgernes sikkerhet er den viktigste av statens kjerneoppgaver. Et av regjeringens satsingsområder er derfor trygghet i hverdagen og styrket beredskap. Forslaget til ny sikkerhetslov skal legge rammene for at vi har de virkemidlene som er nødvendige for å ivareta nasjonale sikkerhetsinteresser og forebygge mot sikkerhetstruende virksomhet.

Ny teknologi har effektivisert samfunnet på mange områder, også innenfor Forsvaret og viktige samfunnsområder som forsvarssektoren er avhengig av. Teknologiutviklingen fører imidlertid også til økte sårbarheter, noe som er nærmere utredet i NOU 2015: 13 *Digital sårbarhet – sikkert samfunn.* Utredningen er av regjeringen fulgt opp i Meld. St. 38 (2016–2017) *IKT-sikkerhet – Et felles ansvar*. Samfunnssikkerhetsmeldingen peker også på verdien av og utfordringer med å dele og utveksle informasjon i en digital verden, jf. Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn*. Arbeidet med ny sikkerhetslov må derfor ses i sammenheng med regjeringens øvrige politikk for samfunnssikkerhet og statssikkerhet. Departementet viser i denne sammenheng også til Prop. 151 S (2015–2016) *Kampkraft og bærekraft. Langtidsplanen for forsvarssektoren.* Her redegjøres det i kapittel 2.3.3 på side 34 for digitaliseringen av samfunnet og utviklingen av digitale trusler.

Det foreliggende lovforslaget bygger på NOU 2016: 19 *Samhandling for sikkerhet*, utarbeidet av det regjeringsoppnevnte Sikkerhetsutvalget, ledet av ambassadør Kim Traavik. Utvalget hadde som mandat å utarbeide et nytt lovgrunnlag for forebyggende nasjonal sikkerhet. Utvalgets rapport har vært på alminnelig høring fra 17. oktober 2016 til 20. januar 2017.

2.2 Sikkerhetsutvalgets mandat

Noe av bakgrunnen for Sikkerhetsutvalgets arbeid er beskrevet slik i mandatet (NOU 2016: 19 kapittel 1.2, side 11):

> «Erfaringer fra hendelser de senere år illustrerer bredden og kompleksiteten i samfunnssikkerhetsarbeidet, og det har blitt vanskeligere å holde oversikt over de avhengigheter som gjør seg gjeldende på tvers av sektorer, virksomheter og infrastrukturer. Den teknologiske utviklingen utfordrer sikkerhetsarbeidet blant

annet gjennom nye måter å produsere, dele og lagre samfunnsviktig informasjon på. Den økte risikoen ved, og vår avhengighet av, IKT-baserte informasjonssystemer, stiller krav om tidsriktige og dynamiske verktøy for beskyttelse mot trusler i det digitale rom. I tillegg gjør utviklingen det mulig å installere elektroniske innretninger eller utøve frittstående høyteknologisk virksomhet som kan være en trussel mot grunnleggende nasjonale sikkerhetsinteresser.»

Utvalget ble bedt om å vurdere hva som bør reguleres i lov for å sikre nasjonal sikkerhet (kapittel 1.2, side 11):

> «Formålet med nytt lovgrunnlag skal være å beskytte kritisk infrastruktur, kritiske samfunnsfunksjoner og sensitiv informasjon mot tilsiktede, uønskede hendelser. Utvalget skal sikre et helhetlig forebyggende lovgrunnlag innen både den militære og sivile sektoren som er relevant og robust med hensyn til dagens og fremtidens risiko- og trusselbilde. Forslaget skal sikre en kostnadseffektiv regulering, som sikrer balanse mellom akseptabel restrisiko, og kostnaden for sikkerhetsnivået. Samfunnsøkonomisk lønnsomhet skal være en grunnleggende forutsetning, dvs. at aktuelle sikringstiltak må ha en samfunnsmessig nytte som samlet overstiger kostnadene.»

Sikkerhetsutvalget skulle særskilt vurdere
1. struktur, virkeområde og ansvarsforholdet for loven
2. kritisk infrastruktur og kritiske samfunnsfunksjoner
3. informasjonssikkerhet
4. tilsyn og
5. kontroll med selskaper.

Personvern og den enkeltes rettssikkerhet har også inngått som en del av utvalgets vurderinger.

2.3 Sikkerhetsutvalgets rapport – NOU 2016: 19 Samhandling for sikkerhet

Sikkerhetsutvalget avga sin rapport, innen gitt tidsramme, den 12. oktober 2016. Rapporten er enstemmig. Kort oppsummert anbefaler utvalget (NOU 2016: 19, side 17–18):

- «Lovens formål bør være å beskytte grunnleggende samfunnsfunksjoner. Det er disse funksjonene en trusselaktør vil forsøke å ta ut ved anslag som rammer Norges mest grunnleggende interesser.
- Lovens virkeområde bør utvides og samtidig være mer målrettet. Virksomheter som er av kritisk betydning for at grunnleggende samfunnsfunksjoner skal kunne opprettholdes, bør underlegges loven uavhengig av eierskap eller organisasjonsform. En forutsetning for en slik utvidelse er at lovens krav har en funksjonell innretning som kan tilpasses den enkelte samfunnssektor.
- De generelle prinsippene for krisehåndtering og beredskap bør ligge fast, samtidig som behovet for en helhetlig og sektorovergripende tilnærming til forebyggende sikkerhet ivaretas. Dette bør gjenspeiles både i hvordan ansvar og myndighet fordeles, og i hvordan tilsyn med virksomheter som er underlagt loven skal innrettes.
- Loven bør pålegge norske myndigheter en rådgivningsplikt overfor virksomheter som omfattes av loven, og en plikt til å legge til rette for at sikkerhetsrelevant informasjon deles med berørte aktører.
- Alle informasjonssystemer som er av kritisk betydning for grunnleggende samfunnsfunksjoner, bør omfattes av loven. Dette gjelder informasjonssystemer som behandler sikkerhetsgradert informasjon, og andre systemer som er av kritisk betydning for opprettholdelse av samfunnsfunksjonene.
- Loven bør ha et systemfokus som også omfatter beskyttelse av infrastruktur som er av kritisk betydning for samfunnsfunksjonene.
- Loven må legge til rette for effektiv forebygging og avdekking av at utro tjenere får tilgang til informasjon eller områder hvor skadepotensialet er stort.
- Det bør etableres en mekanisme for å kontrollere og i ytterste konsekvens stanse utenlandske oppkjøp av selskaper som er av kritisk betydning for grunnleggende samfunnsfunksjoner.»

2.4 Høringen

Forslaget til ny lov om forebyggende nasjonal sikkerhet (sikkerhetsloven) ble sendt på høring 17. oktober 2016 med høringsfrist 20. januar 2017. Høringsbrevet ble sendt til følgende instanser:

Departementene

Datatilsynet
Departementenes sikkerhets- og serviceorganisasjon (DSS)
Direktoratet for forvaltning og IKT (Difi)
Direktoratet for samfunnssikkerhet og beredskap (DSB)
Finanstilsynet
Forsvarets forskningsinstitutt (FFI)
Forsvarsbygg (FB)
Forsvarsmateriell (FMA)
Forsvarsstaben (FST)
Fylkesmannsembetene
Helsedirektoratet
Jernbaneverket
Klagenemnda for offentlige anskaffelser (KOFA)
Konkurransetilsynet
Kontrollutvalget for kommunikasjonskontroll
Kriminalpolitisentralen (Kripos)
Kystverket
Landbruksdirektoratet
Likestillings- og diskrimineringsombudet
Luftfartstilsynet
Nasjonalt folkehelseinstitutt
Nasjonal kommunikasjonsmyndighet (Nkom)
Nasjonal sikkerhetsmyndighet (NSM)
Norges vassdrags- og energidirektorat (NVE)
Oljedirektoratet
Petroleumstilsynet
Politidirektoratet
Politiets sikkerhetstjeneste (PST)
Norsk romsenter
Norsk Utenrikspolitisk Institutt (NUPI)
Regjeringsadvokaten
Riksadvokaten
Riksarkivet
Sjøfartsdirektoratet
Skattedirektoratet
Statens helsetilsyn
Statens jernbanetilsyn
Statens kartverk
Statens strålevern
Statens vegvesen
Statistisk sentralbyrå (SSB)
Statsbygg

Sysselmannen på Svalbard
Tolldirektoratet
Utdanningsdirektoratet
Utlendingsdirektoratet
Økokrim

Etterretningstjenesten
Forsvarets logistikkorganisasjon (FLO)
Forsvarets sikkerhetsavdeling (FSA)

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

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

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

Bergen kommune
Fylkeskommunene
Longyearbyen lokalstyre
Oslo kommune
Stavanger kommune
Tromsø kommune
Trondheim kommune
Ullensaker kommune
Abelia
Avinor
Den norske kirke
Flytoget
Innovasjon Norge
Kirkerådet
KraftCERT AS
Norsk rikskringkasting (NRK)
Norges Bank
Norges statsbaner (NSB)
Posten AS
Statkraft
Statnett

Statoil
Telenor Norge AS

Aerospace Industrial Maintenance Norway (AIM Norway AS)
Akademikerne
Amnesty International Norge
Antirasistisk senter
Arbeidsgiverforeningen Spekter
Bedriftsforbundet
Befalets fellesorganisasjon
Cargo Net AS
Christian Michelsens Institutt
Den katolske kirke i Norge
Den Norske Advokatforening
Den Norske Atlanterhavskomité
Den Norske Bank (DNB)
Den norske Dataforening
Den norske Dommerforening
Den norske Helsingforskomité
Det norske Menneskerettighetshuset
Det norske Nobelinstitutt
Det norske Veritas
EDB Fellesdata
Energi Norge AS
Fafo
Fagforbundet
Fagpressen
Fellesforbundet
Finans Norge
Finansnæringens hovedorganisasjon
Finansieringsselskapenes forening
Folk og Forsvar
Forskerforbundet
Forsvars- og sikkerhetsindustriens forening (FSi)
Hafslund AS
Hovedorganisasjonen Virke
Human-Etisk Forbund
IKT-Norge
Industri Energi
Innvandrernes Landsorganisasjon
Institutt for fredsforskning (PRIO)
Institutt for journalistikk
Islamsk Råd Norge
Kommunenes Sentralforbund (KS)
Kongsberg Gruppen ASA
Krigsskoleutdannede offiserers forening (KOL)
Landsorganisasjonen i Norge (LO)
Leger uten grenser
Lyse AS
Mediebedriftenes Landsforening
Mnemonic AS
NAMMO AS
Nasjonal støttegruppe etter 22. juli-hendelsene
Nordea
Norges Fredsråd
Norges Juristforbund
Norges Ingeniør- og Teknologorganisasjon (NITO)
Norges Offiserforbund (NOF)
Norges Rederiforbund
Norges Røde Kors
Norsk Folkehjelp
Norsk Hydro ASA
Norsk Journalistlag
Norsk Militærjuridisk Forening
Norsk olje og gass
Norsk Presseforbund
Norsk Redaktørforening
Norsk Tjenestemannslag (NTL)
Næringslivets Hovedorganisasjon (NHO)
Næringslivets sikkerhetsorganisasjon (NSO)
Næringslivets Sikkerhetsråd (NSR)
Organisasjon mot Offentlig Diskriminering
Organisasjon mot politisk overvåking
Politiets Fellesforbund
Samfunnsviterne
Senter for informasjonssikring (NorSIS)
SINTEF IKT
Space Norway AS
Sparebankforeningen i Norge
Statsadvokatenes forening
Statstjenestemannsforbundet
Telia Sonera Norge
Thales Norge AS
TV 2
TVNorge
Unio
Utdanningsforbundet
Utdanningsgruppenes Hovedorganisasjon
Vinghøg AS
Watchcom Security Group
Yrkesorganisasjonenes Sentralforbund (YS)

Følgende høringsinstanser hadde merknader til forslaget:
Arbeids- og sosialdepartementet
Finansdepartementet
Helse- og omsorgsdepartementet
Kommunal- og moderniseringsdepartementet
Olje- og energidepartementet
Samferdselsdepartementet
Utenriksdepartementet

Datatilsynet
Departementenes sikkerhets- og serviceorganisasjon (DSS)
Direktoratet for forvaltning og IKT (Difi)
Direktoratet for e-helse
Direktoratet for nødkommunikasjon

Direktoratet for samfunnssikkerhet og beredskap (DSB)
Finanstilsynet
Forsvarets forskningsinstitutt (FFI)
Forsvarsbygg (FB)
Fylkesmannen i Hordaland
Fylkesmannen i Rogaland
Fylkesmannen i Vestfold
Kystverket
Luftfartstilsynet
Nasjonal kommunikasjonsmyndighet (Nkom)
Nasjonal sikkerhetsmyndighet (NSM)
Norges vassdrags- og energidirektorat (NVE)
Oljedirektoratet
Petroleumstilsynet
Politidirektoratet
Politiets sikkerhetstjeneste (PST)
Riksadvokaten
Skattedirektoratet
Statens jernbanetilsyn
Statens vegvesen
Statistisk sentralbyrå (SSB)
Statens strålevern

Sysselmannen på Svalbard
Tolldirektoratet

Forsvarets sikkerhetsavdeling (FSA)

Domstolsadministrasjonen
Stortingets administrasjon

Politihøgskolen

Universitetet i Stavanger

Bergen kommune
Oslo kommune

Abelia
Avinor
Kirkerådet
Norsk rikskringkasting (NRK)
Norges Bank
Norges statsbaner (NSB)
Statkraft
Statnett
Telenor Norge AS

Arbeidsgiverforeningen Spekter
Energi Norge
Fellesforbundet
Finans Norge
Forsvars- og sikkerhetsindustriens forening (FSi)
Kongsberg Gruppen ASA
Norges Ingeniør- og Teknologorganisasjon (NITO)
Norges Rederiforbund
Norsk olje og gass
Norsk Presseforbund
Norsk senter for informasjonssikring (NorSIS)
Norsk Tjenestemannslag/Utenriksdepartementet
Næringslivets Hovedorganisasjon (NHO)
Næringslivets Sikkerhetsråd (NSR)
Telia Norge AS
Thales Norge AS
Anders Bakke
Bane NOR SF
BDO
Bioteknologirådet
E-CO Energi AS
Generaladvokaten
Kvinners Frivillige Beredskap
Meteorologisk institutt
Nasjonalt ID-senter
NHO Luftfart
Norsk industri
Norsk Sikkerhetsforening
Norsk Vann
Norske Kvinners Sanitetsforening
Oslo politidistrikt
Sandefjord Lufthavn AS
UNINETT AS
UNINETT Norid AS

Følgende instanser har uttalt at de ikke har merknader til forslaget:
Landbruks- og matdepartementet
Fylkesmannen i Sør-Trøndelag
Klagenemnda for offentlige anskaffelser
Statens kartverk
Norsk Helsenett SF
Industri Energi

3 Dagens sikkerhetsutfordringer

Forvaltningen av forebyggende sikkerhetsarbeid har historisk sett hatt en regelbasert tilnærming. Med endringer i rammebetingelsene for sikkerhet har denne tilnærmingen særlig de siste årene blitt utviklet til en mer risikobasert tilnærming. I NOU 2016: 19 kapittel 4.1 beskrives grundig forholdet mellom risikohåndtering og forebyggende nasjonal sikkerhet. Etter departementets vurdering er dette en god og tidsriktig beskrivelse som departementet finner å legge til grunn for det nye lovforslaget. Ettersom forslaget er en såkalt rammelov som forutsettes utfylt med en rekke forskrifter, vil det ikke bli tatt stilling til ulike mulige faglige tilnærminger og metoder for risikovurdering og risikoanalyse. Hvilke tilnærminger og metoder som velges i konkrete tilfeller, vil i stor grad være avhengig av hvilke typer objekter eller systemer som skal vurderes. Systemer som inneholder mye informasjonsteknologi, vil eksempelvis ofte kreve andre tilnærminger enn rene fysiske objekter og systemer.

Utvalget har lagt til grunn den såkalte trefaktormodellen for risiko ved beskrivelsen av dagens sikkerhetsutfordringer (NOU 2016: 19, side 41 flg.). Trefaktormodellen består av faktorene trussel, sårbarhet og verdi. Utvalget gir en grundig drøfting av ulike typer verdier med betydning for nasjonal sikkerhet. Utvalget drøfter også trusler mot nasjonal sikkerhet og nasjonale sårbarheter. Etter departementets vurdering er denne drøftingen godt tilpasset dagens situasjonsbilde. Likevel må det understrekes at trussel- og sårbarhetsbildet vil kunne endres betydelig over tid. Departementet legger derfor opp til at loven i størst mulig grad skal være uavhengig av den videre utviklingen av trussel- og sårbarhetsbildet. Basert på dagens oppfatning følger under en oppsummering av de mest sentrale utfordringene som departementet legger til grunn for loven.

Rammebetingelsene for norsk sikkerhet er endret siden gjeldende sikkerhetslov trådte i kraft i 2001, og den sikkerhetspolitiske situasjonen i Europa og nærliggende områder er i dag mer usikker og uforutsigbar. NOU 2016: 19 beskriver trusselbildet vi står overfor på side 49 og påfølgende sider. I langtidsplanen for forsvarssektoren (Prop. 151 S (2015–2016)) beskrives den sikkerhetspolitiske situasjonen i vår del av verden som mer krevende enn på lenge, og det framheves at store utfordringer tett på NATOs ansvarsområde kan få direkte konsekvenser for norsk og allierte staters sikkerhet. Dette kommer i tillegg til utfordringer i europeiske land og allerede eksisterende sikkerhetsutfordringer knyttet til globale utviklingstrekk. Situasjonen gir ifølge Politiets sikkerhetstjeneste (PST) et spillerom for et bredt spekter av statlige og ikke-statlige aktører (PST Trusselvurdering 2017, side 3). Etterretningstjenesten og PST vurderer at enkeltepisoder som i utgangspunktet er små hendelser, kan få alvorlige og til dels uforutsigbare konsekvenser som ingen av partene i utgangspunktet ønsker eller er tjent med. Nye trusler utvikles raskt.

Nasjonal sikkerhet handler om å verne nasjonens interesser og verdier mot trusler. Nasjonale særegenheter og globale trender setter rammene for Norges sikkerhetssituasjon, men den økende internasjonaliseringen gjør at globale utviklingstrekk har stadig mer å si for det nasjonale trusselbildet. Globalisering og internasjonalisering øker kontakten, sårbarheten og avhengigheten på tvers av landegrenser. Samlet sett har dette ført til en økt sannsynlighet for at nasjonale interesser og verdier blir skadelidende som følge av etterretning, sabotasje og terrorhandlinger. Slike hendelser kan være vanskelig å forutse, og de kan få store konsekvenser for vår sikkerhet. Norge blir også påvirket av andre utviklingstrekk, som digitalisering og økonomisk, demografisk og teknologisk utvikling. Nye verdier skapes, nye sårbarheter etableres og trusselbildet er i stadig endring. Dette stiller store krav til det forebyggende sikkerhetsarbeidet (Prop. 151 S (2015–2016), NSM Risiko 2017, side 7).

For at trusselaktører skal nå sine mål, vil de søke etter sårbarheter som kan utnyttes. Sikkerhetsmessige sårbarheter kan ha organisatoriske, menneskelige eller tekniske årsaker (NSM Risiko 2017, side 23).

I NOU 2016: 19 påpekes det at vi lever i et informasjonssamfunn i rask utvikling. Det er derfor knyttet spenning til hvordan trusler i det digi-

tale rom vil utvikles. Utvalget skriver i NOU 2016: 19 i kapittel 4.3.2.1 på side 56:

> «Den globale teknologiutviklingen er et gode som samtidig fører med seg noen alvorlige og grenseoverskridende utfordringer. Trusselaktører i det digitale rom inkluderer både statlige og ikke-statlige aktører. Metodene som benyttes, blir stadig mer avanserte og målrettede. Den økte avhengigheten på tvers av land og sektorer gjør at nettverksbaserte angrep kan ha omfattende skadevirkninger. Disse utviklingstrekkene har ført til et mer sammensatt og mindre forutsigbart trusselbilde.»

Statlig etterretning er et sentralt virkemiddel for å støtte et lands politiske, økonomiske og sikkerhetspolitiske interesser. Etterretningsvirksomhet mot Norge og norske interesser skjer i stor utstrekning fra statlige aktører. PSTs vurderinger tilsier at fremmed etterretningsvirksomhet som kan ha et stort skadepotensial, vil fortsette i og mot Norge også i tiden framover. Aktiviteten er i stor grad rettet mot politiske beslutningsprosesser, norsk forsvars- og beredskapssektor, nærings- og industriaktører og viktig infrastruktur. Formålet er blant annet å kartlegge sårbarheter i det norske samfunnet, militære kapasiteter og andre sikkerhets- og beredskapsressurser. I tillegg er norske virksomheter som arbeider med høyteknologi særlig utsatt, ifølge PST. Særlig utsatt er også opposisjonelle som lever i eksil i Norge.

Aktørenes mål er å få tilgang til sensitiv og skjermingsverdig informasjon, påvirke politiske, økonomiske og forvaltningsmessige beslutninger og undersøke muligheter for å kunne sabotere viktig infrastruktur ved en eventuell framtidig konfliktsituasjon.

I NOU 2016: 19 pekes det på at aktørers intensjoner om å påføre samfunnet betydelig skade skaper et behov for bevissthet knyttet til spredning av informasjon. Utvalget skriver i kapittel 4.1.2 på side 42:

> «I praksis betyr dette at den eller de som utfører eller planlegger å utføre handlingen vil kunne tilpasse handlingen til de sikkerhets- og beredskapstiltak som de har kjennskap til eller forventer skal finnes. Dette fører til et behov for å ha et bevisst forhold til hvordan informasjon om risikoreduserende tiltak skal distribueres. Behovet for skjerming av slik informasjon er åpenbar.»

Ved en tilspisset sikkerhetspolitisk situasjon forventer PST at Norge vil bli utsatt for et spekter av virkemidler, inkludert etterretningstjenesters involvering i påvirkningskampanjer og spredning av desinformasjon (PST Trusselvurdering 2017, side 10). Hensikten vil trolig være å påvirke den politiske debatten og svekke legitimiteten til politiske beslutningsprosesser.

PST påpeker at fremmede tjenester bruker både datanettverksoperasjoner og tradisjonelle metoder mot norske mål. De arbeider blant annet aktivt for å få tilgang til personer i virksomheter som behandler sensitiv informasjon og teknologi (PST Trusselvurdering 2017, side 9). Nettverksbaserte etterretningsoperasjoner gjennomføres i stort omfang mot Norge og norske interesser.

Flere personer med tilknytning til land som Norge ikke har et sikkerhetsmessig samarbeid med, har stillinger som gir dem tilgang til sensitiv og skjermingsverdig informasjon. Disse kan være særlig utsatt for rekrutteringspress fra hjemlandets etterretningstjenester. Ifølge PST vil en kombinasjon av innsidevirksomhet og datanettverksoperasjoner ha et meget stort skadepotensial.

Etterretningstjenesten peker på at truslene i det digitale rom mot politiske, militære og økonomiske mål i Norge er økende, og at vi kan forvente omfattende etterretningsoperasjoner mot Norge framover (Fokus 2017, side 6). Dette gjelder blant annet operasjoner som tar sikte på å påvirke nasjonale beslutningsprosesser. Det vurderes at digital sabotasje i en spent situasjon kan brukes som virkemiddel for å skape kaos og øve press. NSM vurderer at datanettverksoperasjoner og digital spionasje fra statlige aktører utgjør betydelig risiko for offentlig forvaltning og for virksomheter som forvalter viktig infrastruktur, viktige samfunnsfunksjoner og høyteknologi. Ifølge NSM overvåker trusselaktører de mest attraktive målene kontinuerlig. NSM peker på to trender for IKT-hendelser i Risiko 2017. Den ene er at de mest ressurskrevende sakene fra avanserte aktører øker i omfang. Den andre at de samme aktørene har begynt å angripe mindre norske virksomheter for å utnytte de kompromitterte nettverkene videre, som infrastruktur i angrep mot andre, større mål (Risiko 2017, side 17–18).

Samfunnets økte avhengighet av IKT-baserte informasjonssystemer fører med seg alvorlige sårbarheter mot trusler i det digitale rom. Ved en samfunnsmessig eller sikkerhetspolitisk krise er det avgjørende at IKT-systemene er tilgjengelige og opererer som de skal, skriver NSM i Risiko 2017 side 9. Mange viktige nasjonale funksjoner er avhengige av internett, og bortfall av nettet kan

forsterke eller forverre en krise. Den økte avhengigheten av internett gjør at nettverksbaserte angrep kan ha omfattende skadevirkninger og har potensial til å ramme hele spekteret av norske interesser.

Trusselen fra voldelig ekstremisme har økt. Ifølge Etterretningstjenesten har terrortrusselen fra militante islamister generelt sett blitt mer alvorlig og kompleks. Antallet terrorangrep i Europa har økt, og de fleste av disse kan knyttes til ISIL. Selv om ISIL blir svekket i Irak og Syria og kapasiteten til å gjennomføre sentralstyrte terrorangrep dermed blir redusert, vurderer Etterretningstjenesten at organisasjonens nettverk i Europa vil være en betydelig trussel også den nærmeste tiden (Fokus 2017, side 6). PST vurderer at ekstreme islamister representerer den største terrortrusselen mot Norge (PST Trusselvurdering 2017, side 4).

Departementet legger vekt på sikkerhetsutfordringene som følger av en stadig sterkere globalisering av samfunnet og økende avhengighet av relasjoner med resten av verden. Disse påvirker særlig forholdet til sårbarhet og trussel. En viktig faktor i utviklingen er den sterke utbredelsen av informasjonssystemer og infrastruktur som også i økende grad er globale i utbredelse og funksjon. Sammenholdt med et sammensatt og dynamisk trusselbilde fører dette til komplekse sikkerhetsutfordringer med stor grad av endringer over tid. For å møte disse utfordringene er det etter departementets vurdering behov for en mer dynamisk og fleksibel lov enn tidligere. Som en konsekvens av denne utviklingen foreslår departementet en begrenset utvidelse av lovens virkeområde sammenliknet med dagens lov, der det forventes at flere private virksomheter enn i dag vil bli omfattet av loven. Departementet foreslår en rammelov. Behovet for økt dynamikk og fleksibilitet uttrykkes gjennomgående i de ulike bestemmelsene i lovforslaget.

I NOU 2016: 19 legger Sikkerhetsutvalget etter departementets syn fram en grundig drøfting av ulike virkemidler og tiltak for å oppnå god nasjonal sikkerhet. Denne vil også bli lagt til grunn i det videre arbeidet med forskrifter til loven for å sikre at tiltak er tidsmessige og tilpasset utviklingen.

4 Rettstilstanden i andre land

4.1 Sverige

4.1.1 Sikkerhetslovgivningen i Sverige

Säkerhetsskyddslagen (1996:627) er Sveriges lov som regulerer forebyggende sikkerhet. Det framgår av 1 § at loven gjelder for «staten, kommunerna och landstingen», for «aktiebolag, handelsbolag, föreningar og stiftelser» som myndighetene utøver «ett rättslig bestämmande inflytande» over og for «enskilda, om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism». For riksdagen og underlagte organer gjelder loven i begrenset utstrekning.

I 6 § framgår det at loven skal legge til rette for *säkerhetsskydd* mot «spioneri, sabotage och andra brott som kan hota rikets säkerhet» og mot andre tilfeller som omfattes av hemmelighold etter *offentlighets- och sekretesslagen* og som berører rikets sikkerhet. I tillegg skal loven legge til rette for beskyttelse mot terrorhandlinger, selv om handlingen ikke truer rikets sikkerhet.

Lovens 7 § regulerer at sikkerhetstiltak etter loven skal omfatte informasjonssikkerhet, adgangsbegrensninger og sikkerhetsklarering av personer.

Säkerhetsskyddslagen er for øvrig under revisjon.

4.1.2 Informasjonssikkerhet og informasjonssystemsikkerhet

Säkerhetsskyddslagen og *säkerhetsskyddsförordningen* (1996:633) regulerer informasjonssikkerheten i relasjon til rikets säkerhet. Etter säkerhetsskyddslagen 7 § 1 om skal sikkerhetstiltakene forebygge at opplysninger som er sensitive av hensyn til rikets sikkerhet avsløres, endres eller slettes uten autorisasjon. Hvilke beskyttelsesbehov som oppstår når informasjonen behandles automatisk, skal særlig vurderes ved utforming av regler om informasjonssikkerhet, jf. 9 §. I säkerhetsskyddsförordningen paragrafene 9 til 13 er det fastsatt mer konkrete regler om informasjonssikkerhet. Alle virksomheter som omfattes av loven, må dessuten gjennomføre en *säkerhetsanalys* for å kartlegge hvilke opplysninger i deres virksomhet som må holdes hemmelig av hensyn til rikets sikkerhet, jf. forordningen 5 §. Forordningen regulerer også varsling av sikkerhetsbrudd, nedtegning av såkalte *hemliga handlingar* og forsendelse av dokumenter.

I SOU 2015:25 *En ny säkerhetsskyddslag* foreslås det flere endringer i gjeldende rett. Utredningen viser til at det er utviklingsbehov både på grunn av gjeldende lovs fokus på konfidensialitetsbeskyttelse og av hensyn til ivaretakelse av Sveriges internasjonale forpliktelser. Beskyttelse av sikkerhetsgraderte opplysninger videreføres og det foreslås også å videreføre et system for sikkerhetsgradering som korresponderer med NATOs system.

Det foreslås videre å beskytte informasjon som av andre grunner er av betydning for *säkerhetskänslig verksamhet*. For denne kategorien framheves behovet for å beskytte integritet og tilgjengelighet.

I utredningen foreslås det også en ny *säkerhetsskyddsförordning*, som blant annet inneholder bestemmelser for beskyttelse av IT-systemer. Det stilles krav til beskyttelse av systemer som skal behandle informasjon som er gradert *konfidentiell* eller høyere. Disse systemene skal sikres gjennom blant annet tilgangskontroll, logging av hendelser i systemet som er av betydning for sikkerheten og beskyttelse mot uautorisert avlytting, inntrenging, skadelig kode og forstyrrende signaler. I tillegg følger det av forslaget i kapittel 4 om *informationssäkerhet* 2 § at systemer *«som är av motsvarande betydelse för Sveriges säkerhet»*, skal beskyttes. Det uttales at disse systemene er så ulike at det ikke er hensiktsmessig å fastsette spesifikke sikkerhetstiltak for disse i forordningen.

4.1.3 Personellsikkerhet

Personellsikkerhet reguleres i säkerhetsskyddlagen, særlig i paragrafene 11 til 29.

I Sverige skal det etter 11 § i loven gjøres en *säkerhetsprövning* av personer som deltar i virksomhet som er av betydning for rikets sikkerhet

eller som får tilgang til opplysninger som er viktige for beskyttelse mot terrorisme. Den enkelte virksomhet skal kartlegge hvilke ansettelser som medfører behov for plassering i *säkerhetsklass.* Registerkontroll og særskilt personutredning utføres avhengig av *säkerhetsklass*. Det er også registerkontroll forbundet med sikkerhetsprøvingen for virksomheter som har et særlig behov for beskyttelse mot terrorhandlinger. En sikkerhetsklassifisert stilling i stat, kommune eller landsting kan, med visse unntak, bare innehas av personer med svensk statsborgerskap.

4.1.4 Objekt- og infrastruktursikkerhet

Sverige har også en beskyttelseslov, *skyddslagen* (2010:305), som er relevant for objekt- og infrastruktursikkerhet. Säkerhetsskyddslagen er i stor grad innrettet for å sikre konfidensialitet for informasjon av betydning for *säkerhetskänslig verksamhet*, mens skyddslagen med tilhørende forskrifter og forordninger er innrettet for å beskytte *skyddsobjekter* mot sikkerhetstruende virksomhet. *Skyddsobjekt* kan være bygninger, anlegg og områder, samt militære fartøy og luftfartøy, jf. NOU 2016: 19 kapittel 9.4.4.

4.2 Danmark

4.2.1 Sikkerhetslovgivningen i Danmark

Danmark har ikke en egen sektorovergripende lov som regulerer forebyggende sikkerhetsarbeid. *Cirkulære om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt* (CIS nr 10338 af 17. desember 2014, Sikkerhedscirkulæret), regulerer beskyttelse av sikkerhetsgradert informasjon. I denne beskyttelsen ligger blant annet sikkerhetsklarering av personell og

> «fysiske og proceduremæssige foranstaltninger, der tilsigter, at informationerne beskyttes mod uautoriseret indsigt og ændring samt er til rådighed for autoriserede brugere, når de skal anvendes».

Danmark har heller ikke et sektorovergripende lovverk som omhandler beskyttelse av kritisk infrastruktur.

4.2.2 Informasjonssikkerhet og informasjonssystemsikkerhet

Sikkerhedscirkulæret står sentralt for ivaretakelse av informasjonssikkerhet i Danmark. Sirkulæret forutsettes å gjelde for sentraladministrasjonen, og kan gjøres gjeldende for private etter nærmere avtale.

Sirkulæret regulerer informasjonssikkerhet i vid forstand og regulerer – utover informasjonssikkerhet – både sikkerhetsmyndigheter, personellsikkerhet og fysisk sikkerhet.

Det skal foretas en klassifisering av informasjonen, ut fra en vurdering av det skadepotensialet som uautorisert tilgang til informasjonen vil kunne ha for Danmark, NATO eller EU. Sirkulæret benytter graderingene YDERST HEMMELIGT, HEMMELIGT, FORTROLIGT og TIL TJENESTEBRUG. For sistnevnte gradering forutsettes det ikke et uttrykkelig skadepotensial. Den skal brukes om informasjon som ikke må offentliggjøres eller komme uvedkommende til kjennskap. Sikkerhetstiltakene som fastsettes i sirkulæret er blant annet sikkerhetsklarering av personell, beskyttelse av sikkerhetsgradert informasjon, godkjenning av IKT-systemer, sikkerhetsstyring og fysisk sikring.

I 2015 ble *lov nr. 1567 om net- og informationssikkerhed* vedtatt. Loven setter krav til informasjonssikkerheten for virksomheter som tilbyr offentlige nett- og kommunikasjonstjenester. Dette omfatter både infrastrukturaktører og leverandører av mobiltelefoni, fasttelefoni, bredbånd og lignende. Loven gir dessuten *Center for Cybersikkerhed* relativt vidtgående myndighet for utforming av regelverk om og tilsyn med virksomhetenes informasjonssikkerhet.

4.2.3 Personellsikkerhet

Personellsikkerhet reguleres i *Sikkerhedscirkulæret,* underkapittel A II, *Indsigt i klassificerede informationer*.

Det følger av Sikkerhedscirkulæret § 12 at sikkerhetsgradert informasjon kun må gis til personer som er *sikkerhetsgodkjent* for den aktuelle sikkerhetsgrad. Sikkerhetsgodkjenningen er avgrenset til en konkret stilling. *Politiets Efterretningstjeneste* (PET) gjennomfører en sikkerhetsundersøkelse av den enkelte. Hvilke kilder og registre PET gjennomgår, er avhengig av hvilket klareringsnivå det bes om. Ettersom PET har direkte tilgang til en rekke av de relevante registrene, er saksbehandlingstiden vesentlig kortere enn i Norge.

4.2.4 Objekt- og infrastruktursikkerhet

Sektorprinsippet er styrende for beskyttelse av kritisk infrastruktur i Danmark. Dette innebærer at alle myndigheter har ansvaret for beredskap i egen sektor. Disse myndighetene arbeider systematisk med beredskap. Sikkerhetsutvalget fikk opplyst fra Beredskapsstyrelsen, som er underlagt Forsvarsministeriet, at denne etaten har en generell plikt til å veilede myndighetene om beredskapsplanleggingen, men har ikke et tverrsektorielt ansvar for myndighetenes virkemidler overfor eiere og operatører av kritisk infrastruktur, jf. NOU 2016: 19 kapittel 9.4.3.

4.3 Storbritannia

4.3.1 Sikkerhetslovgivningen i Storbritannia

I Storbritannia utgjør *Security Service Act* fra 1989 lovgrunnlaget for sikkerhetstjenestens virksomhet. I henhold til lovens artikkel 1 skal sikkerhetstjenesten beskytte nasjonal sikkerhet, særlig mot

> «[…] threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.»

Sikkerhetstjenesten skal også beskytte Storbritannias økonomiske velferd og støtte politiets og andre organers arbeid innen forebygging og avdekking av alvorlig kriminalitet.

I NOU 2016: 19 kapittel 6.3.3, side 107, skriver utvalget at

> «[a]rbeidet med beskyttelse av kritisk infrastruktur er etter det utvalget har fått opplyst lovmessig forankret i Security Service Act (1989), og ivaretas av MI5s Centre for the Protection of National Infrastructure (CPNI).»

Government Security Classifications Policy (2014) regulerer beskyttelse av sikkerhetsgradert informasjon. Utvalget påpeker at disse retningslinjene ikke har

> «lovmessig status, men er etablert innenfor rammene av nasjonal britisk lovgivning og inkluderer de krav som følger av Official Secrets Acts (1911 og 1989), Freedom of Information Act (2000) og Data Protection Act (1998).»

4.3.2 Informasjonssikkerhet og informasjonssystemsikkerhet

Systematikken for sikkerhetsgradering av informasjon i Storbritannia følger ikke den samme systematikken som NATO. Det opereres nå med tre sikkerhetsgraderinger, TOP SECRET, SECRET og OFFICIAL. I praksis benyttes to kategorier av sistnevnte, OFFICIAL-SENSITIVE og OFFICIAL. Til grunn for graderingen skal det ligge en vurdering av informasjonens skadepotensial dersom den blir kjent for uvedkommende. Graderingen danner utgangspunkt for hvilke tiltak innenfor personellsikkerhet, fysisk sikkerhet og informasjonssikkerhet som må iverksettes. Kravene omfatter blant annet need-to-know-prinsippet, varsling, merking, sikkerhetsstyring, fysisk håndtering, deling og hvorvidt det er krav om sikkerhetsklarering for tilgang til gradert informasjon.

4.3.3 Personellsikkerhet

I Storbritannia er det fire forskjellige nivåer for personkontroll, avhengig av den enkeltes behov for tilgang til informasjon og lokaliteter. Tre av nivåene omhandler sikkerhetsklarering hvor laveste nivå er *Counter Terrorist Check* (CTC). CTC omfatter personell som skal ha tilgang til personer som vurderes særlig utsatt for terrorhandlinger, tilgang til informasjon eller materiell av verdi for terrorister, eller tilgang til lokaliteter særlig utsatt for terror. Alle de fire nivåene av personkontroll innebærer sjekk av relevante registre og kilder. For det øverste klareringsnivået *Developed Vetting* skal det gjøres en full revisjon av den enkeltes økonomi, samt et detaljert intervju med *Investigating Officer*.

4.3.4 Objekt- og infrastruktursikkerhet

Arbeidet med beskyttelse av kritisk infrastruktur i Storbritannia er forankret i Security Service Act fra 1989 og ivaretas av *Centre for the Protection of National Infrastructure* (CPNI), underlagt MI5. Oppgaven til CPNI er å få implementert det som er vedtatt forebyggende sikkerhetspolicy og sikkerhetsregimer i både offentlig og privat sektor, med målsetting om å minimere risiko og redusere sårbarhet med tanke på tilsiktede handlinger. Dette gjelder fysisk objektsikring, personellsikkerhet og informasjonssikkerhet, inkludert cyber.

Ansvarlig departement utpeker kritisk infrastruktur innenfor sitt område, og CPNI har oppsyn med at definisjonene og klassifikasjonen av

infrastruktur er foretatt etter gjeldende standarder og praksis.

4.4 NATO

4.4.1 Informasjonssikkerhet og informasjonssystemsikkerhet

NATO Security Policy C-M(2002)49 regulerer beskyttelse av NATO-sikkerhetsgradert informasjon. Dokumentet er sammen med flere understøttende direktiver bindende for alle NATOs medlemsland, inkludert Norge. Sikkerhetsavtalen *(C-M(2002)49 Enclosure «A», Security agreement)*, som alle medlemslandene har sluttet seg til, danner det formelle grunnlaget for et relativt omfattende og til dels teknisk regelverk for beskyttelse av NATO-sikkerhetsgradert informasjon. NATOs råd har vedtatt de overordnede rammer og prinsipper for regelverket, mens utfyllende bestemmelser er fastsatt av de fagansvarlige komiteer, henholdsvis *Security Committee* og *C3 Board*. NATOs sikkerhetsregelverk er dels bindende for nasjonene og dels veiledende.

Blant NATOs grunnprinsipper kan nevnes at sikkerhetsgradert informasjon kun skal deles etter need-to-know-prinsippet, at sikkerhetsrisikostyring er obligatorisk for NATO-enheter, men frivillig for medlemslandene, og at sikkerhetstiltakene skal være balansert og bestå av både personell-, fysisk-, informasjons- og IKT-sikkerhet. Videre fastsettes at det etableres en nasjonal sikkerhetsorganisasjon med kompetanse innen og ansvar for ulike sikkerhetsfaglige områder.

Informasjonssikkerhet reguleres særlig i *C-M(2002)49 Enclosure «E»*. Et grunnleggende tiltak er at informasjon skal graderes ut fra den potensielle skaden det kan medføre for NATO eller medlemslandene om den blir kjent for uvedkommende. I NATO benyttes sikkerhetsgradene COSMIC TOP SECRET, NATO SECRET, NATO CONFIDENTIAL og NATO RESTRICTED. Gjennom hele informasjonens livssyklus skal beskyttelsen være på et nivå som er tilpasset sikkerhetsgraderingen. Sikkerhetsgradering skal ikke benyttes i større utstrekning enn nødvendig.

Informasjonssystemsikkerhet, jf. *Enclosure «F»*, omfatter beskyttelse av informasjon som behandles i kommunikasjons-, informasjons- og andre elektroniske systemer mot brudd på konfidensialitet, integritet og tilgjengelighet, både ved utilsiktede og tilsiktede hendelser. Sikkerhetstiltakene skal også beskytte mot brudd på integritet og tilgjengelighet i selve systemet. Dersom en konkret risikovurdering tilsier det, skal det iverksettes ytterligere sikkerhetstiltak. Alle IKT-systemer som behandler gradert informasjon må gjennomgå en sikkerhetsgodkjenningsprosess, som kan fastslå om et relevant sikkerhetsnivå er oppnådd og blir opprettholdt.

4.4.2 Objekt- og infrastruktursikkerhet

NATOs sivile beredskapssystem ble gjennom 1990-tallet gradvis styrket og omstrukturert. Det har vært et økt fokus på internasjonalt samarbeid om beskyttelse av kritisk infrastruktur etter 11. september 2001. Selv om *critical infrastructure protection (CIP)* tradisjonelt ikke er et kjerneområde for NATO, har området fått økt oppmerksomhet.

NATOs arbeid med CIP inkluderer sikring for å ivareta samfunnsfunksjoner og infrastruktur som alliansen er avhengig av for å gjennomføre operasjoner. Det er et formål for alliansen å kunne gjennomføre militære operasjoner uten at det går på bekostning av befolkningens trygghet. Dette innebærer at befolkningens behov er dekket før en eventuell militær operasjon iverksettes. CIP spiller blant annet en nøkkelrolle når det gjelder NATOs energisikkerhet.

4.5 Reguleringen av informasjonssikkerhet og informasjonssystemsikkerhet i EU

Beslutning om regler for beskyttelse av EUs sikkerhetsgraderte informasjon (2013/488/EU) fastsetter prinsipper og minimumsstandarder for beskyttelse av sikkerhetsgradert EU-informasjon (EUCI). Beslutningen gjelder for Rådet og dets sekretariat og skal overholdes av medlemslandene i henhold til nasjonalt regelverk, slik at enhver kan være trygg på at informasjonen beskyttes tilstrekkelig.

Systematikken korresponderer med NATOs systematikk. Informasjon skal sikkerhetsgraderes ut fra en vurdering av skadepotensialet for EU eller en eller flere av medlemsstatenes interesser, dersom informasjonen blir kjent for uvedkommende. I EU benyttes sikkerhetsgradene EU TOP SECRET, EU SECRET, EU CONFIDENTIAL og EU RESTRICTED. Beslutningen inneholder også bestemmelser om merking, risikostyring, personellsikkerhet, fysisk sikkerhet, forvaltning av gradert informasjon og industrisikkerhet.

Det er også egne bestemmelser om IKT-sikkerhet som gjelder for informasjonssystemer som

behandler sikkerhetsgradert informasjon. Systemene må godkjennes, med det for øye å sikre at alle nødvendige sikkerhetstiltak er gjennomført, og at det er oppnådd tilstrekkelig grad av beskyttelse.

5 Generelt om lovens oppbygging og innhold

Sikkerhetsutvalget hadde som mandat å vurdere hva som bør reguleres i lov for å sikre nasjonal sikkerhet. Det heter blant annet i mandatet (NOU 2016: 19, side 11):

> «Formålet med nytt lovgrunnlag skal være å beskytte kritisk infrastruktur, kritiske samfunnsfunksjoner og sensitiv informasjon mot tilsiktede, uønskede hendelser. Utvalget skal sikre et helhetlig forebyggende lovgrunnlag innen både den militære og sivile sektoren som er relevant og robust med hensyn til dagens og framtidens risiko- og trusselbilde.»

Departementet merker seg at utvalgets forslag til lov ikke innebærer noen stor omveltning av gjeldende regelverk innenfor forebyggende sikkerhetsarbeid. Utvalget foreslår at sikkerhetsloven fortsatt skal være en overordnet rammelov, med mer utførlig regelverk i forskrifter og veiledere innenfor fagområder som informasjonssikkerhet, personellsikkerhet og objektsikkerhet. Loven skal være tverrsektoriell og favne både militær og sivil sektor, de ulike samfunnssektorer og deres regelverk skal hensyntas, og Forsvarsdepartementet skal fortsatt være forvaltningsansvarlig for loven. Utvalget har også vektlagt at kravene som stilles til sikkerhetstiltak i forskriftene til loven i så stor utstrekning som mulig skal være funksjonelle.

Som samfunnssikkerhetsmeldingen (Meld. St. 10 (2016–2017)) peker på i kapittel 1.2.3, er sikkerhetsarbeid i stor grad sektorovergripende. Et terroranslag, for eksempel, kan ikke håndteres innenfor én sektor alene, eller på ett enkelt nivå i forvaltningen:

> «Arbeidet krever koordinering og samarbeid på tvers av sektorgrenser og mellom myndigheter på lokalt, regionalt og sentralt nivå».

Blant de områdene som meldingen peker ut til å være av stor betydning i dag, er digitale sårbarheter og IKT-sikkerhet. Dette er også et område som det etter departementets mening er nødvendig at en ny sikkerhetslov bør omfatte. Gjensidige avhengigheter i et totalforsvarsperspektiv bør også være omfattet av en ny sikkerhetslov.

Departementet vil også peke på som viktig at en ny lov skal kunne fungere i et framtidig gjennomdigitalisert samfunn, noe som innebærer at det i lovforslaget er inntatt bestemmelser for å ivareta informasjonssikkerheten og beskytte informasjonssystemer og infrastruktur. Departementet legger i denne forbindelse til grunn at en ny sikkerhetslov skal være en dynamisk lov, som skal kunne tilpasses et samfunn som er i rask teknologisk utvikling.

Departementet har i arbeidet med lovforslaget lagt vekt på å forenkle språkbruken mest mulig, for å tydeliggjøre meningsinnholdet. Som ledd i dette arbeidet har departementet fått bistand fra Språkrådet. Endringen av lovens tittel må ses i lys av arbeidet med språket. Begrepet «forebyggende sikkerhetstjeneste» i dagens lov er i forslaget til ny lov endret til «forebyggende sikkerhetsarbeid». Loven er ment å regulere forebyggende sikkerhetsarbeid av overordnet nasjonal betydning. Av den grunn foreslås det at loven skal hete «lov om nasjonal sikkerhet (sikkerhetsloven)».

6 Lovens formål og virkeområde

6.1 Gjeldende rett

Gjeldende sikkerhetslov ble vedtatt i 1998 og trådte i kraft i 2001. I Ot.prp. nr. 49 (1996–97) sies det om bakgrunnen for proposisjonen på side 3:

> «Forut for og parallelt med Lund-kommisjonens gransking, har spørsmålet om en lovregulering av de «hemmelige tjenester» vært satt på dagsorden. I Ot prp nr 83 (1993–94) uttalte Regjeringen at den vil iverksette arbeid med sikte på å fremme forslag til lovregulering av etterretnings-, overvåkings- og sikkerhetstjenesten (heretter samlet benevnt «EOS-tjenestene»). Justiskomitéen uttalte i Innst O nr 11 (1994–95), som Stortinget sluttet seg til, at den var av den oppfatning at en regulering av overvåkingstjenesten bør innarbeides i politiloven, og at det «bør utarbeides en egen lovgivning for Sikkerhetstjenestens arbeid».

Forsvarsdepartementet viser på side 7 i proposisjonen til Skaugekommisjonen, som anbefalte at det skulle «iverksettes arbeid med sikte på å gi en egen lov om EOS-tjenestene, dvs. om deres organisering, oppgaver og beføyelser». Departementet skriver videre i proposisjonen på side 7:

> «Departementet har funnet det mest hensiktsmessig å fremme forslag om en egen lov om forebyggende sikkerhetstjeneste. Først og fremst skyldes dette at forebyggende sikkerhetstjeneste og den militære etterretningstjeneste har lite til felles. Regulering av Etterretningstjenestens virksomhet bør eventuelt skje gjennom separat lovgivning.»

Formålet med dagens sikkerhetslov framgår av § 1 i loven. Formålet er for det første å «legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser» (bokstav a). For det andre er formålet å «ivareta den enkeltes rettssikkerhet» (bokstav b). I tillegg skal loven legge til rette for å «trygge tilliten til og forenkle grunnlaget for kontroll med forebyggende sikkerhetstjeneste» (bokstav c).

Formålet er kort utdypet i forarbeidene (Ot. prp. nr. 49 (1996–97), side 64):

> «Med «rikets…sikkerhet» siktes både til rikets indre og ytre sikkerhet. Begrepet er for øvrig en utpreget rettslig standard som kan forandre seg med samfunnsutviklingen. Departementet ser ikke i lovforslaget her grunn til å søke å presisere begrepet utover det som allerede er antatt på bakgrunn av andre rettskilder (juridisk teori, domstolspraksis, forarbeider til andre lover, forvaltningspraksis, mv.).
>
> Som et samlebegrep skal forebyggende sikkerhetstjeneste motvirke trusler mot «vitale nasjonale sikkerhetsinteresser». Det anses imperativt at en på denne måten dekker samtlige felter innenfor rikets totale sikkerhetsbehov. Begrepet må derfor til enhver tid vurderes og defineres av overordnede politiske myndigheter. Terskelen for i medhold av denne loven å anse noe for å true slike interesser, vil være høy. Begrepet er nærmere omtalt under pkt 7.2.2 ovenfor. Det må understrekes at begrepet kan endres i pakt med samfunnsutviklingen og de sikkerhetsmessige utfordringer som Norge til enhver tid står overfor.»

På side 33 presiseres det at:

> «For det første må fremheves at opplysningene må være knyttet til rikets sikkerhetsmessige interesser. I ordet «vitale» ligger videre en forutsetning om at det må dreie seg om helt essensielle og samfunnsviktige sikkerhetsinteresser.»

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

Sikkerhetsloven har et såkalt *security*-perspektiv (i motsetning til *safety*); den oppstiller kun regler til beskyttelse mot de tilsiktede (viljestyrte) handlingene spionasje, sabotasje og terror. Sikkerhetsloven oppstiller således ikke krav til HMS-tiltak og omhandler ikke beskyttelse mot naturkatastrofer eller liknende, som for en rekke interesser utgjør den største trusselen. Mens det på safety-området i utgangspunktet foretas risikovurderinger hvor sannsynligheten for at en uønsket hendelse inntreffer står sentralt, vurderer man gjerne på security-feltet risiko som et forhold mellom verdien man ønsker å beskytte, trusler mot verdien og sårbarheter en trusselaktør kan tenkes å utnytte.

Sikkerhetsloven danner en minimumsstandard. Det er derfor ikke tale om et enten/eller-valg i forholdet mellom aktuelt sektorregelverk og sikkerhetsloven. I tråd med sektorprinsippet er det de enkelte sektordepartementene, sammen med sine respektive fag- og bransjemiljøer, som har ansvaret for å vurdere sikkerhetsbehovet i egen sektor, kvaliteten av eget sektorregelverk, og i hvilken utstrekning sikkerhetsloven kommer utfyllende til anvendelse. Sikkerhetsloven eksisterer i flere sektorer side om side med sektorregelverk som har bestemmelser om sikkerhet og beredskap. Sikkerhetsloven med forskrifter inneholder fleksible bestemmelser for særtilpasning til den enkelte sektor for å sikre at kravene som oppstilles, ikke blir unødvendig tyngende.

Praksis har imidlertid vist at sikkerhetsloven med forskrifter ikke oppfattes som tilstrekkelig fleksibel, men at regelverket tvert om oppfattes som tyngende både økonomisk og administrativt blant flere samfunnsaktører. Departementets arbeid med revisjon av sikkerhetsloven for å tilpasse den til de sikkerhetsutfordringene som dagens og morgendagens trusselbilde representerer, har avdekket grunnleggende utfordringer om hva sikkerhetsloven bør regulere, deriblant forholdet mellom sikkerhetsloven og annet sikkerhetsrelatert regelverk. Innenfor objektsikkerhetsområdet er det også avdekket uenighet mellom ulike sektorer om hva reglene skal ta sikte på å beskytte mot, og på hvilken måte, jf. omtalen i Prop. 97 L (2015–2016) *Endringer i sikkerhetsloven* (reduksjon av antall klareringsmyndigheter mv.), side 6.

6.2 Utvalgets forslag

Utvalget mener at sikkerhetsloven bør ha som formål å trygge Norges suverenitet, territorielle integritet og demokratiske styreform ved å motvirke tilsiktede uønskede hendelser mot grunnleggende samfunnsfunksjoner. Disse funksjonene er avgjørende for at staten skal kunne ivareta de verdiene loven skal beskytte og er de funksjonene en trusselaktør vil forsøke å ramme for å skade landets grunnleggende interesser.

I NOU 2016: 19 viser utvalget i kapittel 6.7.1 på side 113 til den usikkerhet som eksisterer når det gjelder hvordan dagens begrepsapparat skal forstås og praktiseres. Med en videreføring av dagens begrepsapparat risikerer man etter utvalgets oppfatning å videreføre denne usikkerheten. Utvalget uttaler også at en slik videreføring vil kunne gjøre virkeområdet til den nye loven for snevert og medføre at den nye loven vil være i utakt med beslektet lovverk for øvrig. Utvalget foreslår derfor at begrepet *grunnleggende nasjonale funksjoner* brukes for å angi lovens virkeområde, for å erstatte gjeldende lovs begrepsapparat og gi loven en funksjonell innretning. Sikkerhetsutvalget legger til grunn en begrenset utvidelse av virkeområdet sammenliknet med gjeldende lov og konkretiserer dette ved å angi fem kategorier knyttet til de grunnleggende nasjonale funksjonene, jf. lovforslaget § 1-2.

Sikkerhetsutvalget uttaler i NOU 2016: 19 kapittel 2 på side 17 at:

> «Statens aller viktigste oppgave er […] å beskytte landets borgere og samfunnet de er en del av. En stat som ikke evner å sikre sin egen og borgernes overlevelse misligholder samfunnskontrakten mellom stat og borger. For å ivareta denne oppgaven og overholde samfunnskontrakten er det helt avgjørende at staten makter å opprettholde samfunnets grunnleggende funksjoner uavhengig av hvilken ekstern påvirkning de utsettes for.»

Fra kapittel 6.7.1 på side 113:

> «[…] en ny lov om forebyggende nasjonal sikkerhet bør ha som formål å beskytte de *funksjonene* som er helt avgjørende for at staten skal kunne ivareta de verdiene sikkerhetsloven skal beskytte.»

Sikkerhetsutvalget uttaler i NOU 2016: 19 kapittel 2.1 om lovens virkeområde på side 18–19:

> «Utvalget anbefaler at forebyggende nasjonal sikkerhet fortsatt reguleres i én lov som gjelder på tvers av sektorer og andre skillelinjer. Felles utfordringer krever felles løsninger, og

én felles lov legger best til rette for tverrsektoriell samhandling og harmonisering av sikkerhetsnivået i samfunnet. Et felles rammeverk gir også de beste forutsetningene for god ledelse, styring, koordinering og ressursutnyttelse.

Utvalget mener at den nye sikkerhetsloven bør ha som formål å beskytte de *funksjonene* som er helt avgjørende for å ivareta de verdiene sikkerhetsloven skal hegne om. I ytterste konsekvens er det nettopp disse funksjonene en trusselaktør vil forsøke å ta ut ved et anslag mot Norge og dets mest grunnleggende interesser og verdier. En slik funksjonstilnærming vil også være i tråd med den øvrige metodikken i arbeidet med samfunnssikkerhet og beredskap. Utvalget har derfor valgt å benytte begrepet *grunnleggende nasjonale funksjoner* for å angi lovens virkeområde.

Selve grunnlaget for å beslutte hva som utgjør *grunnleggende nasjonale funksjoner,* er statens sikkerhetspolitiske ansvar for å ivareta Norges suverenitet, territorielle integritet og demokratiske styreform. En funksjon er å anse som grunnleggende for Norge dersom bortfall av denne får konsekvenser som truer disse overordnede interessene.

Utvalgets lovforslag innebærer en begrenset, men nødvendig utvidelse av virkeområdet sammenliknet med gjeldende sikkerhetslov. Loven vil ikke være en bred samfunnssikkerhetslov, men skal samtidig heller ikke være en ren statssikkerhetslov. Fra utvalgets side er utvidelsen av lovens virkeområde ment å reflektere den generelle samfunnsutviklingen som har funnet sted siden gjeldende sikkerhetslov trådte i kraft for 15 år siden.

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

Den nærmere avgrensningen av hva som vil utgjøre grunnleggende nasjonale funksjoner i medhold av den nye sikkerhetsloven, vil slik utvalget ser det måtte avgjøres konkret basert på en helhetlig vurdering der både sektorovergripende og sektorspesifikke perspektiver ivaretas. For at loven skal få den ønskede effekt vil det være avgjørende å etablere et system for å identifisere grunnleggende nasjonale funksjoner og hvilke virksomheter som er av kritisk betydning for disse.»

6.3 Høringsinstansenes syn

6.3.1 Formål og virkeområde

En hovedvekt av høringsinstansene uttaler seg positivt til beskrivelsene av dagens trussel- og sårbarhetsbilde som gis i NOU 2016: 19. Det er i stor grad også enighet om at dagens sikkerhetslov ikke er tilstrekkelig til å møte de utfordringene som eksisterer i dagens samfunn, og at det derfor er behov for en lov som i større grad enn gjeldende lov fanger opp samfunnssikkerhetsperspektivet i tillegg til statssikkerheten.

Utenriksdepartementet er enig i utvalgets tilnærming og uttaler:

> «Utvalgets tilnærming, hvor det tas utgangspunkt i statens sikkerhetspolitiske ansvar for å ivareta Norges suverenitet, territorielle integritet og demokratiske styreform, og nødvendigheten av å beskytte de nasjonale funksjoner som har avgjørende betydning for statens evne til å ivareta dette ansvaret, synes fornuftig. Utenriksdepartementet støtter som følge av dette utkastets forslag til å heve sikkerhetsloven til å bli en overordnet og sektorovergripende lov som i større grad enn den nåværende loven respekterer den enkelte sektors og den enkelte virksomhets særpreg, men samtidig tar inn over seg betydningen av den økte avhengigheten mellom ulike sektorer.»

Helse- og omsorgsdepartementet mener lovforslaget i hovedsak synes å være en nødvendig oppdatering i tråd med samfunnsutviklingen og intensjonene til den gjeldende loven og uttaler at:

> «Den pågående revisjon av totalforsvarskonseptet som skjer nasjonalt og i regi av NATO, hvor Forsvaret i større grad spesialiseres og baserer seg på støttefunksjoner fra sivil sektor, både offentlig og privat, vil øke betydningen av den sivile delen av totalforsvaret. Samfunnsutviklingen går i retning av mer konkurranseutsetting og «gjensidige avhengigheter» på tvers av sektorer, offentlige aktører og kommersielle aktører. En overgang fra fokus på «statssikkerhet» til også å omfatte «kritisk betydning for grunnleggende samfunnsfunksjoner» og kritisk infrastruktur, kan derfor være formålstjenlig.»

Samferdselsdepartementet er generelt positiv til utvalgets forslag og uttaler:

> «Utredningen synes på en god måte å ta hensyn til de store teknologiske, demografiske og sikkerhetsmessige endringer som har skjedd i tiden som har gått siden gjeldende sikkerhetslov trådte i kraft i 2001. SD deler utvalgets vurdering om at det har vært behov for en bredere tilnærming til lovens virkeområde enn gjeldende sikkerhetslov har.»

Nasjonal sikkerhetsmyndighet (NSM) støtter i utgangspunktet innretningen på forslaget:

> «Utvalgets lovforslag representerer en utvidelse av gjeldende sikkerhetslovs saklige virkeområde. Dagens sikkerhetslov gir tverrsektorielle bestemmelser om beskyttelse av sikkerhetsgradert informasjon og skjermingsverdige objekter. Lovforslaget omfatter i tillegg informasjonssystemer som er av kritisk betydning for grunnleggende nasjonale funksjoner, men som ikke behandler sikkerhetsgradert informasjon, samt infrastruktur av kritisk betydning for grunnleggende nasjonale funksjoner.
>
> Utkast til ny sikkerhetslov inneholder mange gode elementer, og er langt bedre tilpasset dagens samfunnsutvikling enn eksisterende sikkerhetslov. NSM støtter i hovedsak innretningen på forslaget, og mener at dette vil legge til rette for en bedring av sikkerhetstilstanden og en god utvikling av denne. Behovet for sektorovergripende reguleringer er imidlertid mer omfattende enn utvalgets lovforslag.»

Politiets sikkerhetstjeneste (PST) mener at utvidelsen og innretningen på lovforslaget er hensiktsmessig og mer i takt med tiden og den rådende trusselsituasjonen og uttaler at:

> «Samfunnets sårbarhet er ikke lenger bare knyttet til at rikets sikkerhet er tilfredsstillende ivaretatt, som et moderne samfunn er vi også avhengig av en rekke funksjoner for at Norge skal fungere tilfredsstillende.
>
> PST støtter derfor forslaget om at lovens formål utvides til beskyttelse av grunnleggende samfunnsfunksjoner, herunder beskyttelse av informasjonssystemer og infrastruktur som er av kritisk betydning for disse. Likeledes støttes forslaget om at lovens virkeområde utvides til å omfatte virksomheter som er av kritisk betydning for at grunnleggende samfunnsfunksjoner opprettholdes.»

Konsulentselskapet *BDOs* hovedinntrykk av NOU 2016: 19 er:

> «BDO mener forslaget redegjør for historikk, utfordringer, behov og mulige reguleringsløsninger for beskyttelse av nasjonale grunnleggende funksjoner på en meget god måte. BDO er også i det alt vesentlige enig i utvalgets forslag til konkrete bestemmelser i en ny lov på området.»

6.3.2 Virkeområde

Flere høringsinstanser, deriblant *Avinor, BDO, Datatilsynet*, *Departementenes service- og sikkerhetsorganisasjon (DSS), Finans Norge, Forsvars- og sikkerhetsindustriens forening, Fylkesmannen i Rogaland, Fylkesmannen i Vestfold, Norges Bank, Norges Ingeniør- og Teknologorganisasjon (NITO), Norsk senter for informasjonssikring (NorSIS), Statens vegvesen, Telenor, Telia,* og *Thales* stiller seg positive til utvidelsen av lovens virkeområde.

Norges Bank uttaler:

> «Norges Bank ser positivt på den modernisering av loven som foretas gjennom utvidelse av lovens virkeområde. Overgangen til å vurdere «grunnleggende nasjonale funksjoner» er i bankens vurdering mer relevant for å redusere den sikringsrisiko loven omhandler enn tilnærmingen som legges til grunn i eksisterende lov.»

Datatilsynet uttaler:

> «Vi viser til rapportens punkt 6.7.1 om at utvalgets forslag til innretning av lovens formål og virkeområde sannsynligvis vil medføre at flere virksomheter vil bli underlagt den nye loven, og til punkt 7.7.1 om at utvalget foreslår en systematikk for å identifisere virksomheter som bør omfattes av loven for å sikre grunnleggende nasjonale funksjoner. Vi mener dette er positivt og vi har en forventning til å se mer av sikkerhetsloven i den sivile sektor.»

Telenor Norge AS uttaler:

> «Telenor oppfatter lovforslaget som et steg i riktig retning for å styrke nasjonal sikkerhet, herunder også samfunnssikkerhet. Vi anser utvidelsen av virkeområde[t] som naturlig og riktig sett i lys av at Norge i stor grad er avhengig av private virksomheter for å opprettholde grunnleggende samfunnsfunksjoner. Det er

viktig for utviklingen av vår nasjonale forsvarsevne at vi har en sektorovergripende tilnærming, og samtidig at lovkravene er funksjonelt innrettet. Med lovforslaget legges det godt til rette for at Norge kan få en felles innretning på sikkerhetsarbeid på tvers av og innad i sektorene.

[…] I NOUen er det godt belyst at Norge i stor grad er avhengig av private virksomheter/rettssubjekter for å opprettholde nasjonale grunnleggende funksjoner. I lovforslaget bør dette tydeliggjøres, dvs. at man under lovens formål bør beskrive at begrepet virksomhet både omfatter offentlige og private virksomheter.»

Telia Norge AS er enig i utvalgets beskrivelse av de sikkerhetsutfordringene både aktører og myndigheter står overfor i dagens samfunn og støtter utvidelsen av virkeområdet. *Telia* uttaler:

«Som det fremgår på side 18 har en økende grad av digitalisering resultert i økte gjensidige avhengigheter på tvers av tradisjonelle skillelinjer mellom samfunnssektorer, mellom privat og offentlig virksomhet, og mellom sivile samfunnssektorer og landets militære forsvar og forsvarssektoren for øvrig. Utviklingen til et nettverksbasert samfunn er i det store og hele positiv. Det åpner for å løse store utfordringer på en fleksibel og ressurseffektiv måte. Samtidig har digitaliseringen skapt nye sårbarheter. Dette er særlig tydelig i ekomsektoren.

[…]

Vi mener en funksjonell tilnærming tilpasset den enkelte samfunnssektor vil gi bedre sikkerhet sett fra samfunnets ståsted. Dessuten innebærer dette en mer rasjonell fordeling av byrder og kostnader ved at ansvaret for å gjennomføre tiltakene pålegges den aktøren som er best plassert til å begrense risikoen for uønskede handlinger – uavhengig av eierskap eller organisasjonsform. Som utvalget selv fremhever er en slik funksjonstilnærming også i tråd med den øvrige metodikken i arbeidet med samfunnssikkerhet og beredskap.»

BDO mener utvidelsen «vil gi en mer moderne og helhetlig tilnærming til det som er viktigst å beskytte i samfunnet.»

Imidlertid har en rekke høringsinstanser, mange av dem i utgangspunktet positive til lovforslaget, særlig pekt på som et problem at rekkevidden til lovens virkeområde synes uklart. *Norges vassdrags- og energidirektorat (NVE)* uttaler i sin høringsuttalelse at virkeområdet er for vidt og skjønnsmessig:

«Utvalget har ment å foreslå en begrenset utvidelse av dagens sikkerhetslov. NVE mener eksempelbruken og uttalelser fra utvalgets side ikke støtter opp under dette og at forslaget har et for vidt virkeområde.

Bestemmelsen om virkeområdet i § 1-2 er den viktigste bestemmelsen for å definere hvem sikkerhetsloven skal gjelde for. Vi ser det som viktig at virkeområdet angis presist og inneholder minst mulig bruk av skjønnsmessige begreper. Dette er vesentlig for å sikre forutsigbarhet for de som blir underlagt plikter etter loven og avgrense mot annet regelverk.»

Kommunal- og moderniseringsdepartementet, Forsvarets forskningsinstitutt (FFI), Norsk Presseforbund, Petroleumstilsynet og *UNINETT* er blant dem som savner en mer konkret beskrivelse av lovens virkeområde og hvilke virksomheter som skal omfattes av loven.

Kommunal- og moderniseringsdepartementet uttaler:

«Med bakgrunn i utvalgets mandat, og utvalgets vurderinger i denne sammenheng, mener KMD at enkelte punkter i rapporten burde vært mer presisert. Dette gjelder spesielt lovens virkeområde – og hvilke virksomheter som skal omfattes av denne.

[…]

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

Universitetet i Stavanger uttaler at «utvalget har fremmet et forslag til endringer av virkeområdet for loven som det ikke er mulig å overskue omfanget av, og lovens innhold er heller ikke risikovurdert.»

Olje- og energidepartementet understreker at utvalgets forslag innebærer en «forsiktig utvidelse» og at «[d]ette legger føringer for vurderingen av hva som omfattes av loven.»

Direktoratet for forvaltning og IKT (Difi) uttaler om lovens virkeområde:

> «For IKT-sikkerhet vil loven legge sterke føringer. Det bør utredes om den vil føre til at det legges uforholdsmessig stor vekt på risiko som skyldes tilsiktede handlinger når virksomheters risikostyring krever en helhetlig tilnærming med god balanse mellom alle kategorier av uønskede hendelser.»

NSM uttaler seg blant annet slik om lovforslagets virkeområde:

> «Utvalget legger til grunn at de virksomheter som allerede i dag er omfattet av sikkerhetsloven, enten i kraft av å være forvaltningsorgan eller ved enkeltvedtak i medhold av gjeldende lov, også vil være omfattet av den nye loven. NSM slutter seg til disse betraktningene, men kan ikke se at dette er reflektert godt nok i lovforslaget. Lovforslaget legger til grunn at det også skal foretas individuelle vurderinger hva gjelder forvaltningsorganer. NSM mener at alle forvaltningsorganer i utgangspunktet bør være underlagt sikkerhetsloven. De fleste forvaltningsorganer vil kunne komme i en situasjon hvor de må behandle eller tilvirke sikkerhetsgradert informasjon. Dette vil særlig gjelde planlegning for og håndtering av krise og beredskapssituasjoner. Man må ikke komme i en situasjon hvor et forvaltningsorgan ved behov ikke har rettslig grunnlag for å behandle sikkerhetsgradert informasjon.»

NorSIS støtter at «lovens virkeområde endres slik utvalget beskriver», men mener samtidig at «det er en fare for at virkeområdet blir for snevert i forhold til det som NorSIS oppfatter som nasjonale utfordringer.» *Fellesforbundet* og *Kongsberg Gruppen* er opptatt av at lovens virkeområde også burde utvides til å gjelde strategisk teknologi.

E-CO Energi er på sin side «bekymret for at forslaget til et bredt [virkeområde] i § 1-2 vil medføre at unødig mange virksomheter vil omfattes av loven», mens *Næringslivets Hovedorganisasjon* legger til grunn at utvalgets forslag innebærer en «vesentlig utvidelse» av lovens formålsbestemmelse.

Flere høringsinstanser, deriblant *NSM, NVE* og *Energi Norge*, har reagert på at forvaltningsorganer ikke eksplisitt er omfattet av forslaget til virkeområdebestemmelse i § 1-2. *Statistisk sentralbyrå* uttaler i den forbindelse at

> «forholdet mellom bestemmelsen om lovens virkeområde, § 1-2 og departementenes ansvar og myndighet etter loven, § 2-1c, bør tydeliggjøres og formuleres slik at det ikke er noen tvil om statlige forvaltningsorganer faller inn under loven.»

Direktoratet for samfunnssikkerhet og beredskap (DSB) mener at en lov i tråd med forslaget «vil ha sterk innvirkning på det generelle samfunnssikkerhets- og beredskapsarbeidet». *DSB* uttaler om dette:

> «DSB har i innspill til prosessen sagt seg enig i at det er behov for en ny lovregulering av sikkerhetsarbeidet i virksomheter med ansvar for kritiske samfunnsfunksjoner, men har pekt på at et slikt lovgrunnlag må legge et bredt risikoperspektiv («all hazards approach») til grunn. Samfunnet som helhet, sektormyndigheter og den enkelte virksomhet skal gjøre samlede vurderinger av hvordan ulike trusler og farer kan møtes. Bare på denne måten kan man oppnå en effektiv og helhetlig risikostyring med god forankring på alle nivåer.
>
> Lovforslagets perspektiv er i utgangspunktet vesentlig smalere enn dette. Formålet er å «...motvirke tilsiktede uønskede hendelser som kan skade grunnleggende nasjonale interesser» (§1-1). Dette er også i samsvar med mandatet utvalget har hatt.
>
> På objektsikkerhetsområdet utvides loven fra bare å gjelde utvalgte objekter til også å gjelde infrastruktur. Dette sammen med den funksjonsbaserte tilnærmingen loven legger opp til, vil imidlertid medføre at det ikke vil være mulig å sette klare grenser for lovens nedslagsfelt. Vår oppfatning er derfor at en ny lov i tråd med forslaget i betydelig grad vil influere også på det generelle sikkerhets- og beredskapsarbeidet i de virksomhetene som eventuelt vil bli omfattet av det, uten at dette er drøftet nærmere i rapporten.»

Uttalelser fra enkelte fylkesmannsembeter og fra *Nasjonal kommunikasjonsmyndighet (Nkom)* synes å støtte *DSB* sin tilnærming til et bredt risikoperspektiv. *Fylkesmannen i Vestfold* skriver for eksempel:

> «Innenfor samfunnssikkerhet og beredskap legges det til grunn en «all-hazard approach», dvs. at forebygging og beredskap skal være enhetlig uansett hvilken trussel samfunnet står ove[r]for. Ut fra dette følger behov for at det bør stilles identiske krav til de ulike samfunnsfunksjoner, ettersom hybride trusler kan ramme telekommunikasjon eller økonomi like

mye som det vil ramme forsvarsevnen. Imidlertid har Norge tradisjonelt hatt et totalforsvar hvor sektorene har ivaretatt hele spekteret av trusler gjennom særlovgivning og sektorvis forebygging og beredskap.»

Stortingets administrasjon har i sin høringsuttalelse merket seg at utvalget foreslår i ny lov § 1-3 første ledd at loven skal gjelde for Stortinget og Stortingets organer i den utstrekning Stortinget bestemmer, og uttaler blant annet videre:

«I tillegg til å fastsette i hvilken utstrekning loven skal gjelde, vil vi foreslå at Stortinget også gis en uttrykkelig hjemmel til å fastsette særskilte tilpasninger til loven eller forskrifter vedtatt i medhold av loven. I enkelte tilfeller vil det kunne være aktuelt å la lovens system gjelde, men med særskilte tilpasninger med bakgrunn i de spesielle hensyn som gjør seg gjeldende for Stortinget. Slike tilpasninger kan for eksempel være egne bestemmelser om behandling av klager på vedtak etter loven.»

Stortingets administrasjon foreslår på denne bakgrunn følgende ordlyd i § 1-3 første ledd:

«Loven gjelder for Stortinget og Stortingets organer i den utstrekning *og med de tilpasninger til loven eller forskrifter vedtatt i medhold av loven, som* Stortinget bestemmer.»

6.3.3 Begrepsbruk og definisjoner

Flere høringsinstanser har kommentarer til begrepsbruken i NOU 2016: 19, spesielt knyttet til lovens formål og virkeområde.

BDO mener at formålsbestemmelsen også bør omtale andre grunnleggende nasjonale interesser enn det utvalgets forslag angir:

«I merknaden til lovforslagets § 1-1 vises det til at angivelsen i bestemmelsen av de grunnleggende nasjonale interessene ikke er en uttømmende oppregning av de interessene loven tar sikte på å trygge, men kun en fremheving av avgjørende interesser.

BDO anser det regelteknisk uheldig at ordlyden i bestemmelsen ikke gir noen indikasjoner på at det også kan være *andre* grunnleggende nasjonale interesser som loven tar sikte på å beskytte. I stedet for at ordlyden skal tolkes utvidende i så stor grad, bør det heller tas inn i ordlyden en formulering som viser at oppregningen ikke er uttømmende. En måte å gjøre dette på er å benytte følgende formulering: «*Loven skal bidra til å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale grunnleggende interesser, ved å …*»

NVE er kritisk til innføringen av begrepet «grunnleggende nasjonale funksjoner» og mener at «nasjonale sikkerhetsinteresser» bør vurderes:

«Dagens sikkerhetslov bruker begrepet «vitale nasjonale sikkerhetsinteresser» som et samlebegrep som dekker samtlige felt innenfor rikets totale sikkerhetsbehov. Begrepet skal til enhver tid vurderes og defineres av overordnende politiske myndigheter.

Utvalget mener det er en utfordring med forståelsen og praktisering av begrepet og at en videreføring av dagens begrep risikerer å videreføre usikkerheten. Videre mener utvalget at virkeområdet blir for snevert og at loven ikke vil være i takt med moderniseringen. NVE er ikke enig med utvalget i disse vurderingene.

NVE mener utvalgets forslag om at det er «grunnleggende nasjonale funksjoner» som skal beskyttes gjennom sikkerhetsloven blir vagt og lite treffende. Vi mener dagens begrepsbruk, og særlig begrepet «nasjonale sikkerhetsinteresser» har et innarbeidet og allment kjent meningsinnhold og angir tydelig hva denne loven regulerer.

NVE mener at man kan skjerpe innholdet i dagens begrepet ved å fjerne begrepet «vitale». På denne måten vil man utvide virkeområdet av eksisterende lov, men innenfor en kjent ramme. NVE mener et slikt grep også vil fremheve at sikkerhetsloven skal være verktøy for å sikre Norges suverenitet, territorielle integritet og demokratiske styreform, mens det er andre lover som skal sikre den sivile samfunnssikkerheten. For å unngå dobbeltregulering og tydeliggjøre formålet, mener NVE det er viktig at dette skillet tydeligere kommer frem i lovteksten.

NVE mener derfor at § 1-1 første ledd bør endres slik at *grunnleggende nasjonale funksjoner* erstattes med *nasjonale sikkerhetsinteresser*.»

Norges Rederiforbund ønsker å videreføre gjeldende lovs «vitale nasjonale sikkerhetsinteresser»:

«Rederiforbundet er enig i at det er behov for å foreta moderniseringer og tilpasninger av

eksisterende lovgivning til et nytt og stadig mer komplisert trusselbilde. Vi er imidlertid skeptiske til å innskrenke formålsbestemmelsen i § 1-1 i lovforslaget sammenlignet med gjeldende rett. I sikkerhetsloven benyttes formuleringen «andre vitale nasjonale sikkerhetsinteresser». Vi mener dette er en god uttrykksmåte som er tilpasset situasjoner der trusselbildet endrer seg. Det ligger altså et dynamisk element i loven som gir ønskelig fleksibilitet med hensyn til sikkerhetsrelaterte tiltak med hjemmel i loven. Det nye forslaget fremstår i større grad som funksjonsrettet, der grunnleggende nasjonale funksjoner blir den rettslige standarden. Vår bekymring er knyttet til om den nye loven vil frata myndighetene nødvendig handlefrihet til å definere samfunnets vitale interesser når verden rundt oss endrer seg.»

NSM uttaler om begrepet «grunnleggende nasjonale funksjoner»:

«Lovforslagets virkeområde defineres ut fra begrepet «grunnleggende nasjonale funksjoner». NSM forstår det slik at begrepet […] vil konsumere gjeldende lovs begreper som omfatter «rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser» og straffelovens, og utlendingslovens begrep «grunnleggende nasjonale interesser». Forslaget representerer derfor en utvidelse i forhold til dagens sikkerhetslov. NSM støtter en slik utvidelse.

Utvalget peker på at begrepet «andre vitale nasjonale sikkerhetsinteresser» i dagens sikkerhetslov aldri gjennomgikk den dynamiske utviklingen som lovgiver forutsatte da den ble vedtatt. NSM ser det derfor som positivt at det i det nye lovforslaget er inntatt en nærmere presisering av begrepets innhold gjennom fem tydelige kategorier. Erfaring med dagens lov har imidlertid vist at rettslige standarder i liten grad blir praktisert på en dynamisk måte. En proaktiv holdning for kontinuerlig å utvikle begrepets innhold vil derfor være helt nødvendig for å sikre en harmonisert tverrsektoriell utvikling.»

NITO uttaler blant annet:

«NITO slutter seg til at den nye sikkerhetslovens formål er å beskytte grunnleggende nasjonale funksjoner som er avgjørende for å ivareta verdiene sikkerhetsloven hegner om. Likevel er begrepet funksjon mer komplisert, ettersom den impliserer flere ikke-statiske deler. Det kan være vanskelig nok for aktører i samfunnet å ta inn over seg at deres virke utgjør kritisk infrastruktur. Det blir ikke lettere når aktørenes virke blir trukket inn som en kritisk funksjon i det norske samfunnet. NITO deler likevel definisjonen av en funksjon til å være grunnleggende for Norge dersom bortfall av denne får konsekvenser som truer overordnede interesser.»

Flere høringsinstanser, deriblant *DSS*, *NSM*, *Oslo politidistrikt*, *Politidirektoratet*, *PST* og *Riksadvokaten* har etterlyst legaldefinisjoner av sentrale begreper i loven.

6.4 Departementets vurdering

6.4.1 Generelt

Departementet har merket seg at det i høringsuttalelsene ikke har kommet mange innvendinger når det gjelder forslaget til overordnet rammeverk. Mange høringsinstanser er enige i at det er et behov for en utvidelse av sikkerhetsloven til i noen grad å omfatte samfunnssikkerhet i tillegg til tradisjonell statssikkerhet. Dette gjelder blant andre *Utenriksdepartementet*, *Helse- og omsorgsdepartementet*, *PST*, *NSM*, *Datatilsynet* og *Norges Bank*. På den andre siden uttrykker flere høringsinstanser, deriblant *DSB* og *NVE*, at det må skilles tydeligere mellom statssikkerhet og sivil samfunnssikkerhet, for å unngå dobbeltregulering og tydeliggjøre sikkerhetslovens formål. Departementet registrerer også at mange av høringsuttalelsene, som *NVE*, *Kommunal- og moderniseringsdepartementets* og *Difis* uttalelser, gir uttrykk for tvil om rekkevidden av lovforslagets virkeområde. Noen legger til grunn en beskjeden utvidelse, mens andre oppfatter dette som en betydelig utvidelse, eller bare at beskrivelsen av virkeområdet er for vag og upresis.

Sikkerhetsutvalgets foreslåtte endringer sett opp mot dagens sikkerhetslov er størst innenfor virkeområdet til loven, hvordan tilsyn skal gjennomføres i samhandling og samvirke mellom sektortilsyn og sikkerhetsmyndigheten, om eierskapskontroll og når det gjelder opprettelsen av et tvisteorgan. I tillegg innfører utvalget begrepet infrastruktur i NOU 2016: 19 kapittel 9.5.1 om objekt- og infrastruktursikkerhet for å «skape tydeligere skille mellom enkeltstående objekter og infrastruktur som del av et system som understøtter grunnleggende nasjonale funksjoner».

Gjeldende sikkerhetslov har vært oppfattet og praktisert som et regelverk som omhandler statssikkerhet, primært knyttet til rikets selvstendighet og sikkerhet. Siden sikkerhetsloven trådte i kraft i 2001, har endringer i samfunnet gjort det stadig vanskeligere å trekke en klar grense mellom statssikkerhet og samfunnssikkerhet. Dette skyldes flere forhold:

- For det første har vi i dag et mer komplekst og uforutsigbart trusselbilde å forholde oss til. Et nærliggende eksempel er her de såkalte hybride truslene. Hybride trusler kjennetegnes ved at det benyttes et bredt spekter av konvensjonelle og ukonvensjonelle virkemidler, og av at det er vanskelig å spore og dokumentere hvilke aktører som står bak et angrep. Dette vanskeliggjør også vurderingen av om man befinner seg i statssikkerhets- eller samfunnssikkerhetsdomenet.
- For det andre medfører de økte gjensidige avhengighetene – på tvers av samfunnssektorer, mellom offentlig og privat virksomhet, og mellom militær og sivil virksomhet – at grenselinjene mellom stats- og samfunnssikkerhet viskes ut. Dette må også ses i sammenheng med den raske teknologiske utviklingen i de senere år. Revitaliseringen av totalforsvarskonseptet, hvor Forsvaret i økende grad baserer seg på understøttelse fra det sivile samfunnet og det private næringslivet, er et illustrerende eksempel på avhengighetene mellom militær og sivil sektor.

Som en konsekvens av disse forholdene er det etter departementets vurdering nødvendig å tilpasse lovens nedslagsfelt til den virkeligheten vi befinner oss i. I lovproposisjonen foreslås det derfor at lovens formål bør være å trygge *nasjonale sikkerhetsinteresser*. Dette vil i praksis innebære en utvidelse av lovens formål til å gjelde mer enn bare statssikkerhet i snever forstand. Samtidig vil departementet understreke at loven ikke skal være en bred samfunnssikkerhetslov. De nasjonale sikkerhetsinteressene er delt inn i fem underkategorier, som igjen vil være styrende for hvordan loven skal forstås og praktiseres.

Systemet i utvalgets lovforslag er at hvert enkelt departement er ansvarlig for forebyggende sikkerhetsarbeid innenfor sitt myndighetsområde. Dette innebærer at de enkelte fagdepartementene er ansvarlig for å identifisere og holde oversikt over grunnleggende nasjonale funksjoner og virksomheter som er av vesentlig betydning for disse, og treffe enkeltvedtak om virksomheters underleggelse til loven.

Departementet har forståelse for de høringsinstansene som finner virkeområdet til utvalgets lovforslag uklart. Etter departementets syn har dette hovedsakelig sin årsak i at loven etter forslaget er ment å kunne utøves fleksibelt og dynamisk, og at det derfor ikke vil være formålstjenlig eller mulig å gi en uttømmende beskrivelse av virkeområdet. Departementet mener imidlertid at det er viktig å klarlegge virkeområdet og intensjonen med ny lov så langt som mulig. Det er viktig med forutsigbarhet for virksomhetene som vil omfattes av loven, og departementet foreslår i den forbindelse språklige og strukturelle endringer i formåls- og virkeområdebestemmelsene og i lovens begrepsbruk. Det er etter departementets oppfatning særlig viktig av pedagogiske årsaker å skille tydelig og forklare forholdet mellom de tre ulike nivåene i lovteksten, det vil si de overordnede interessene, funksjonene som understøtter interessene og virksomhetene som igjen understøtter funksjonene. Departementet understreker i denne sammenhengen, i likhet med utvalget, at de foreslåtte lovendringene innebærer en begrenset utvidelse av lovens virkeområde. Dette vil også legge føringer for tolkningen av lovens virkeområde.

6.4.2 Formål

Når det gjelder lovens formål, er ordlyden i utvalgets forslag til § 1-1 endret fra dagens formålsbestemmelse, først og fremst ved at begrepet «rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser» er byttet ut til fordel for begrepene «Norges suverenitet, territorielle integritet og demokratiske styreform». Disse interessene skal i henhold til utvalgets forslag trygges gjennom å motvirke tilsiktede uønskede hendelser mot «grunnleggende nasjonale funksjoner».

Departementet er enig i utvalgets funksjonstilnærming og vurderinger om at funksjonene er forutsetninger for å ivareta de overordnede interessene og derfor svært viktige å beskytte. Departementet mener at lovens primære formål er å trygge de overordnede nasjonale sikkerhetsinteressene, ved å forebygge, motvirke og avdekke sikkerhetstruende virksomhet, det vil si tilsiktede handlinger der målet er å ramme *interessene* og tilsiktede handlinger som indirekte kan true interessene. I dette ligger det implisitt at beskyttelse av nasjonale sikkerhetsinteresser også omfatter beskyttelse av de grunnleggende nasjonale funksjonene som understøtter dem. Departementet foreslår at begrepet grunnleggende nasjonale funksjoner tas ut av formålsbestemmelsen, men

presiserer at begrepet skal forstås som en ramme for å angi lovens virkeområde. Det går etter departementets vurdering tydelig fram av lovteksten i sin helhet, inkludert av ny legaldefinisjon av grunnleggende nasjonale funksjoner, at å beskytte funksjonene er en forutsetning og et virkemiddel for å trygge interessene. Departementet mener slik sett å beholde utvalgets funksjonstilnærming, men anser at forholdet mellom interessene og funksjonene blir tydeligere ved at § 1-1 angir at lovens formål er å beskytte interessene, mens begrepet grunnleggende nasjonale funksjoner brukes for å angi lovens virkeområde.

I formålsbestemmelsen (§ 1-1 første ledd) foreslår utvalget at loven skal bidra til «å trygge Norges suverenitet, territorielle integritet og demokratiske styreform». Disse utgjør, slik utvalget beskriver dem i merknaden til bestemmelsen og i kapittel 6.7.2, overordnede sikkerhetspolitiske interesser. Utvalget skriver i kapittel 6.7.2 på side 114–115 at disse overordnede interessene kan deles inn i følgende underkategorier:

a. de øverste statsorganers virksomhet, sikkerhet eller handlefrihet
b. forsvars-, sikkerhets- og beredskapsmessige forhold
c. forholdet til andre stater
d. landets økonomiske velferd og trygghet
e. befolkningens grunnleggende sikkerhet og overlevelse

I utvalgets lovforslag introduseres disse interessene i § 1-2 første ledd, men her som kategorier av interesser *knyttet til* grunnleggende nasjonale funksjoner. Sett i sammenheng med de generelle merknadene framgår det at dette er de overordnede interessene som grunnleggende nasjonale funksjoner skal ivareta. Etter departementets syn er det imidlertid ut fra lovteksten krevende å forstå sammenhengen mellom de overordnede interessene, funksjonene som understøtter interessene og virksomhetene som igjen understøtter funksjonene. Mangelen på legaldefinisjoner av sentrale begreper i utvalgets lovforslag bidrar til å gjøre dette krevende. Slik departementet oppfatter det, mangler det en direkte tekstlig eller logisk binding i utvalgets forslag til lovtekst mellom de tre overordnede sikkerhetspolitiske interessene som oppregnes i § 1-1, underkategoriene som oppregnes i bokstav a til e i § 1-2, og grunnleggende nasjonale funksjoner. Departementet mener at en slik binding er vesentlig for at rekkevidden av lovens formål og virkeområde skal gå tydelig fram av lovteksten.

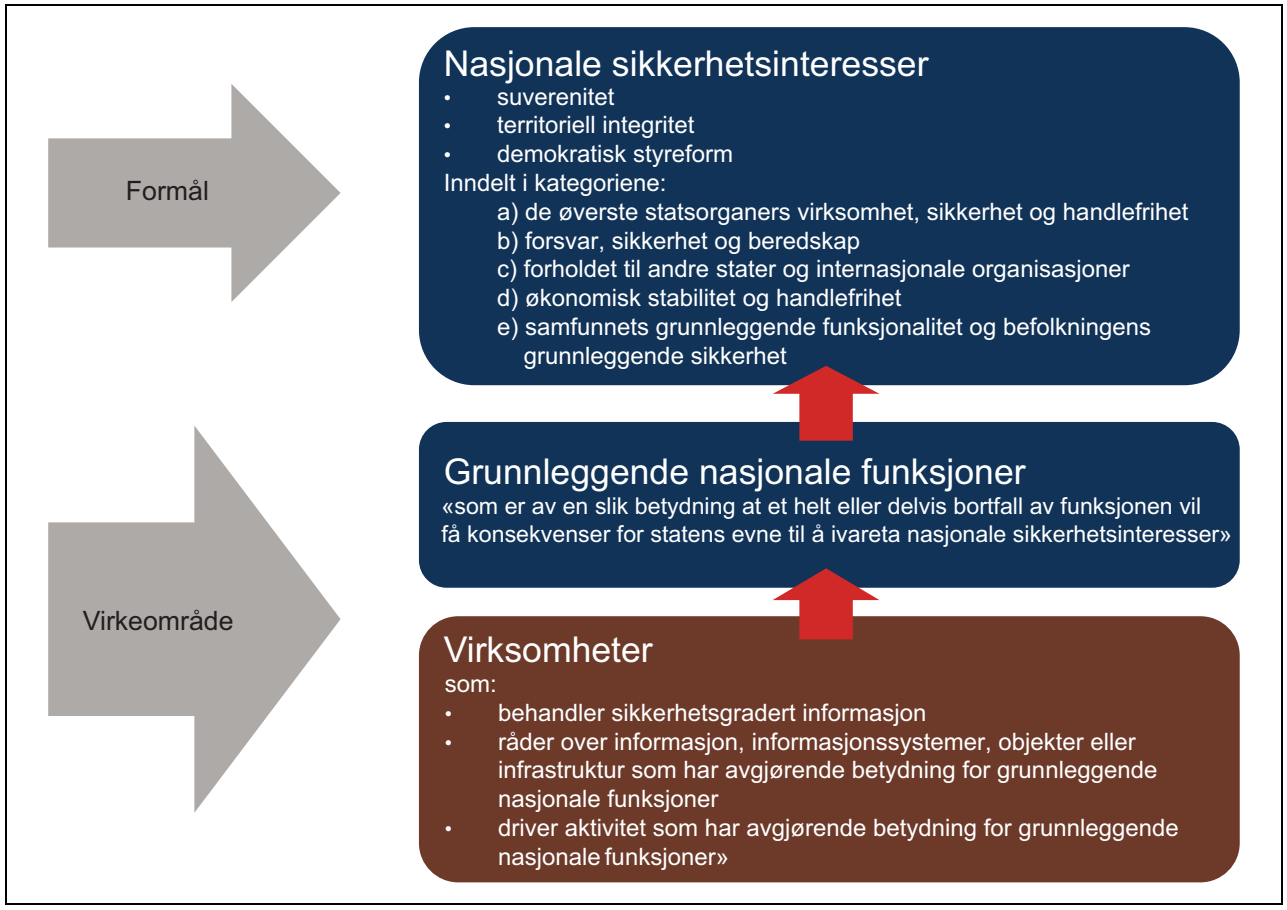
For å klargjøre dette foreslår departementet derfor først at oppregningen med «Norges suverenitet, territorielle integritet og demokratiske styreform» suppleres med «og andre nasjonale sikkerhetsinteresser». Dette grepet vil framheve i lovteksten at kategoriene som oppregnes i bokstav a til e, sammen med de tre overordnede interessene utgjør nasjonale sikkerhetsinteresser. Dette er i tråd med utvalgets beskrivelser i kapittel 6.7.2. *Nasjonale sikkerhetsinteresser* gis videre en legaldefinisjon i lovforslagets § 1-5, som omfatter både de tre overordnede interessene og underkategoriene i bokstav a til e. Dette gir en konkret avgrensning for hvilke interesser loven er ment å skulle beskytte, for å fjerne den usikkerheten som har vært knyttet til det sammenliknbare begrepet *vitale nasjonale sikkerhetsinteresser* i gjeldende sikkerhetslov. Ved å utelate *vitale* i angivelsen av interessene, mener departementet at lovens virkeområde skal tolkes videre enn hva tilfellet er med dagens lov, men innenfor tydelige rammer. Utvalget angir i merknaden til formålsbestemmelsen at de tre overordnede sikkerhetsinteressene ikke utgjør en uttømmende liste. Ved å innføre begrepet *nasjonale sikkerhetsinteresser* mener departementet å gjøre dette tydeligere. Forslaget om å ta inn *nasjonale sikkerhetsinteresser* i formålsbestemmelsen er for øvrig delvis i tråd med *BDOs*, *NVEs* og *Norges Rederiforbunds* høringsinnspill.

Når det gjelder hvordan de enkelte bokstavene i definisjonen av nasjonale sikkerhetsinteresser skal tolkes, er det hensiktsmessig å se til langtidsplanen for forsvarssektoren (Prop. 151 S (2015–2016) *Kampkraft og bærekraft)*, som beskriver sikkerhetsbegrepet slik i kapittel 1.2 på side 17:

> «Utformingen av norsk sikkerhetspolitikk legger til grunn et sikkerhetsbegrep som omfatter statssikkerhet, samfunnssikkerhet og individets sikkerhet. Sikkerhetspolitikkens formål er å ivareta statssikkerheten, som vil si å ivareta statens suverenitet og integritet, samt å sikre politisk handlefrihet. Begrepet inkluderer også Norges bidrag til kollektivt forsvar utløst av NATO-traktatens artikkel 5.»

Sikkerhetsutvalget har valgt å kategorisere de overordnede sikkerhetspolitiske interessene i fem underkategorier. De tre første kategoriene er hentet fra straffeloven (2005) § 121 *Etterretningsvirksomhet mot statshemmeligheter*.

Disse kategoriene (a, b og c) ligger etter departementets syn innenfor statssikkerhetsdefinisjonen.



Figur 6.1 Figuren illustrerer forholdet mellom lovens formål og virkeområde i lovforslaget. Nasjonale sikkerhetsinteresser understøttes av grunnleggende nasjonale funksjoner, som igjen understøttes av virksomheter som har avgjørende betydning for funksjonen.

Departementet mener at bokstav a, *de øverste statorganers virksomhet, sikkerhet eller handlefrihet,* må forstås som regjeringen med departementene i rollen som politisk sekretariat for regjeringen, Stortinget og Høyesterett. Evnen til å opprettholde konstitusjonelle funksjoner og virksomhet i prioriterte deler av forvaltningen er grunnleggende. Det samme er evnen til å opprettholde nasjonal beredskap og håndtere kriser og andre hendelser som kan true nasjonale sikkerhetsinteresser. Departementet understreker at statens råderett over og eksklusive rett til å utøve myndighet i Norge er en del av landets suverenitet, jf. beskrivelsen av begrepet *suverenitet* i lovforslagets særmerknad til § 1-1.

Departementet foreslår å endre bokstav b fra *forsvars-, sikkerhets- og beredskapsmessige forhold* til *forsvar, sikkerhet og beredskap*. Med dette mener departementet Forsvaret og den øvrige forsvarssektoren, med understøttende funksjoner i en totalforsvarssammenheng. Nasjonens evne til å håndtere episoder og sikkerhetspolitiske kriser, og om nødvendig forsvare norsk territorium, er grunnleggende. Totalforsvaret inngår som en grunnleggende faktor i nasjonens evne til militær respons. Gjennom totalforsvaret er Forsvaret direkte avhengig av sivile innsatsfaktorer som elektronisk kommunikasjon (ekom), kraftforsyning, transport, drivstofforsyning, helse og tilførsel av vann og mat. I *sikkerhet* inngår blant annet etterretnings- og sikkerhetstjenestenes virksomhet, altså virksomheten til Politiets sikkerhetstjeneste, Etterretningstjenesten og Nasjonal sikkerhetsmyndighet. *Beredskap* omfatter blant annet systemene for sentral krisehåndtering og beredskap, det vil si Nasjonalt beredskapssystem (NBS), Sivilt beredskapssystem (SBS) og Beredskapssystemet for Forsvaret (BFF).

Når det gjelder bokstav c, *forholdet til andre stater*, foreslår departementet at dette punktet utvides til også å omfatte internasjonale organisasjoner, slik at bokstaven lyder *forholdet til andre stater og internasjonale organisasjoner*. Departementet mener at dette omfatter samarbeidsrelasjoner med andre land innenfor statssikkerhetsområdet og relaterte internasjonale organisasjo-

ner som NATO og EU, og norske forhandlingsposisjoner knyttet til nasjonale sikkerhetsinteresser. Punktet omfatter blant annet bilateralt samarbeid innen sikkerhet og etterretning, og deltakelse i ulike konstellasjoner av internasjonale operasjoner. Punktet omfatter også allierte staters sikkerhet, slik det forstås i gjeldende sikkerhetslov.

Departementet foreslår at ordet «velferd» utelates fra bokstav d, *landets økonomiske trygghet og velferd*, fordi velferdsbegrepet anses utelukkende å ligge innenfor samfunnssikkerhetsbegrepet. Med økonomisk trygghet for landet forstår departementet sikkerhet for politisk handlefrihet på det økonomiske området. Departementet er enig i utvalgets vurdering i NOU 2016: 19 kapittel 6.7.2 på side 115 om at

> «anslag som rammer virksomheter som har en helt sentral rolle for ivaretakelsen av landets økonomiske trygghet og velferd […] [vil] kunne ha en vesentlig negativ innvirkning på nasjonens evne til å opprettholde økonomisk trygghet og velferd».

Utvalget vurderer at petroleumsvirksomheten er en næring som har «sentral betydning for landets økonomiske trygghet». Bokstav d omfatter etter departementets skjønn også stabilitet i økonomien og det finansielle systemet. Dette vil blant annet kunne omfatte en stabil utvikling i makroøkonomiske hovedstørrelser som inflasjon, valutakurs, vekst og sysselsetting, stabile kapitalforhold overfor utlandet, velfungerende systemer for å håndtere offentlige ytelser og inntekter, og stabilitet i den finansielle infrastrukturen og finansmarkedene for øvrig. Departementet foreslår at bokstav d omformuleres til *økonomisk stabilitet og handlefrihet*, for å favne de omtalte aspektene. Departementet vil samtidig understreke at det er opp til det enkelte departementet innenfor sitt myndighetsområde å avgjøre hvilke virksomheter som er av en slik betydning at de skal underlegges loven.

Bokstav e, *befolkningens grunnleggende sikkerhet og overlevelse,* kan oppfattes vidt. Departementet har lagt til grunn at dette alternativet skal forstås som en sikkerhetsventil for blant annet å dekke behovet for beskyttelse mot terrorhandlinger av et visst omfang eller med en viss målrettethet mot grunnleggende nasjonale funksjoner, slik utvalget formulerer det i kapittel 6.7.2 på side 115. Utvalget peker samme sted på at virksomheter som forvalter objekter eller infrastruktur som må anses som særlig utsatt for terrorhandlinger, omfattes, og eksemplifiserer dette blant annet med sentrale knutepunkter for lufttrafikken. Sikkerhetsloven skal trygge nasjonale sikkerhetsinteresser, mens det er andre lover som skal sikre den sivile samfunnssikkerheten. Etter departementets vurdering vil det likevel også være behov for å omfatte infrastruktur og tjenester som anses som avgjørende for at sivilsamfunnet skal kunne fungere på en slik måte at øvrige nasjonale sikkerhetsinteresser kan ivaretas. Særlig vil dette kunne gjelde infrastruktur og tjenester som ikke anses å understøtte Forsvaret direkte, jf. bokstav b, men som likevel er viktig for nasjonens samlede beredskap og forsvarsevne. Departementet foreslår av denne grunn formuleringen *samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet*, slik at bokstav e favner både infrastruktur og objekter som er avgjørende for at sivilsamfunnet skal fungere, og objekter som er særskilt utsatt for sikkerhetstruende virksomhet.

Når det gjelder strukturelle endringer, har departementet valgt å dele opp § 1-1 i tre bokstaver. Dette er gjort av pedagogiske årsaker og for å skjelne mellom lovens primære formål i *bokstav a*, hvilke tiltak loven skal legge til rette for i *bokstav b* for å bidra til dette formålet og i *bokstav c* at tiltak i medhold av loven skal være i samsvar med grunnleggende rettsprinsipper og demokratiske verdier.

Departementet har også vurdert begrepsbruken og språklige aspekter i lovteksten og har i den forbindelse enkelte forslag til endringer. Utvalget bruker verbet *motvirke* (i likhet med gjeldende lov) i formålsbestemmelsen for å beskrive det å hindre «tilsiktede uønskede hendelser». Departementet foreslår å erstatte dette med i § 1-1 bokstav b: *forebygge, avdekke og motvirke*. Forslaget begrunnes med at disse verbene gjensidig forsterker viktigheten av å hindre slike handlinger. De er delvis overlappende, samtidig som de indikerer noen ulike tilnærminger. For eksempel er det naturlig å snakke om å *avdekke* når NSM NorCERT oppdager mulige digitale angrep mot Norge, og det er naturlig at *forebygge* brukes i en lov som regulerer forebyggende sikkerhetsarbeid. *NSM* foreslår også i sitt høringsinnspill å bruke verbet *forebygge*. Bruken av disse tre begrepene er ikke ment å utvide virkeområdets rekkevidde, men snarere å presisere hva slags sikkerhetstiltak loven skal legge til rette for.

Utvalget forklarer begrepet *tilsiktede uønskede hendelser* i kapittel 4.1.2 på side 42 med at «noen har en intensjon om å påføre en eller annen form for skade». I tillegg uttaler utvalget:

> «I forbindelse med nasjonal sikkerhet og samfunnssikkerhet innebærer dette at noen har til

> hensikt å påføre samfunnet betydelig skade. I praksis betyr dette at den eller de som utfører eller planlegger å utføre handlingen vil kunne tilpasse handlingen til de sikkerhets- og beredskapstiltak som de har kjennskap til, eller som de forventer skal finnes.»

Departementet er enig i denne forståelsen, som innebærer at tilnærmingen for å sikre mot tilsiktede handlinger i utgangspunktet er annerledes enn utilsiktede hendelser og som derfor utgjør en viktig avgrensning for sikkerhetslovens virkeområde. Imidlertid mener departementet at begrepet *tilsiktede uønskede hendelser* er en noe unaturlig språklig konstruksjon, ettersom *tilsiktet* innebærer at det ligger en intensjon bak, mens *hendelse* er noe som hender, uavhengig om det ligger en intendert handling eller et uhell bak. I tillegg er det en endring i synsvinkel fra *tilsiktet* til *uønsket*, fordi hendelsen er tilsiktet for den som utfører handlingen, men uønsket for den som rammes. Begrepet *tilsiktede uønskede handlinger* brukes gjerne i sikkerhetsarbeid, eksempelvis i Norsk Standards NS 5830-serie knyttet til risiko for slike handlinger. Det loven skal forebygge, avdekke og motvirke er tilsiktede *handlinger*, men også *hendelser* som oppstår som følge av en slik handling. I *tilsiktet* ligger at en aktør har en intensjon om å forårsake skade, jf. utvalgets definisjon av *tilsiktet uønsket hendelse*. Departementet har vurdert ulike begreper både for å fange opp at loven skal gjelde forsettlige handlinger og hendelsene disse medfører, og for å finne et begrep som kan erstatte *tilsiktede uønskede hendelser* flere steder i lovteksten. Begrepet *sikkerhetstruende virksomhet* er benyttet i gjeldende sikkerhetslov, definert som «forberedelse til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandlinger, samt medvirkning til slik virksomhet», jf. gjeldende lov § 3.

Departementet foreslår å bruke *sikkerhetstruende virksomhet* i § 1-1 bokstav b og enkelte andre steder i lovteksten, men begrepet skal tolkes i en utvidet forstand som reflekterer og tilsvarer utvalgets beskrivelse av *tilsiktede uønskede hendelser*. Med *sikkerhetstruende virksomhet* legger departementet slik til grunn *tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser*. Tilsiktede handlinger som *direkte kan skade* vil si handlinger der intensjonen er å påføre en eller annen form for skade på nasjonale sikkerhetsinteresser, og hendelser forårsaket av slike handlinger. Dette vil blant annet kunne omfatte sabotasje- eller terroraksjoner der målet er å ramme en viktig samfunnsfunksjon, for slik å forsøke å skade myndighetenes styringsevne, jf. figuren over viktige funksjoner og interesser i kapittel 6.4.3. Med tilsiktede handlinger som *indirekte kan skade*, menes handlinger der intensjonen ikke nødvendigvis er å *skade* nasjonale sikkerhetsinteresser, men der konsekvensen eller hendelsen som følger av den tilsiktede handlingen kan skade sikkerhetsinteressene. Dette vil for eksempel kunne innebære etterretningsoperasjoner fra en fremmed stat, der målet ikke nødvendigvis er å *skade* norske interesser, men snarere å fremme egne interesser gjennom å skaffe sensitiv informasjon som kan gi den fremmede staten et fortrinn overfor Norge. Slik etterretningsinformasjon kan i en tilspisset situasjon eller i en forhandlingssituasjon mellom den fremmede staten og Norge potensielt skade norske interesser.

Tiltak etter loven for å forebygge, avdekke og motvirke sikkerhetstruende virksomhet skal redusere risikoen for at nasjonale sikkerhetsinteresser rammes av uønskede hendelser. Sikkerhetstiltakene skal også redusere skadene eller konsekvensene av uønskede hendelser som rammer virksomheten. Interessene og de grunnleggende nasjonale funksjonene som understøtter dem, hviler på de enkelte virksomhetene som er underlagt loven. Det er dermed i stor grad virksomhetenes sikkerhetstiltak som skal forhindre uønskede hendelser som følge av eller knyttet til sikkerhetstruende virksomhet. For en virksomhet som er underlagt loven, vil tiltakene hovedsakelig dreie seg om å forebygge uønskede hendelser, særlig gjennom å redusere virksomhetens egne sårbarheter. Ved å redusere sårbarhetene vil virksomheten også kunne redusere sannsynligheten for og skadevirkningene av å bli rammet av uønskede hendelser knyttet til sikkerhetstruende virksomhet. *Forebyggende* sikkerhetstiltak i en virksomhet som er omfattet av loven, vil for eksempel også kunne innebære tiltak som tar sikte på å forhindre uønskede hendelser som følge av ansattes slurv, uaktsomhet eller manglende risiko- og sikkerhetsforståelse, jf. lovforslaget § 4-1 andre ledd første punktum. Skjødesløs omgang med sikkerhetsgradert informasjon eller uaktsomhet ved bruk av et skjermingsverdig informasjonssystem vil eksempelvis kunne skape sårbarheter som kan utnyttes av en aktør med onde hensikter. Etterretnings- og sikkerhetstjenestenes arbeid vil i tillegg til forebygging dreie seg om å *avdekke* og *motvirke* sikkerhetstruende virksomhet. Se også lovens kapittel 4 og departementets vurdering i kapittel 9.4 knyttet til generelle krav til forebyggende sikkerhetsarbeid.

6.4.3 Virkeområde

Departementet understreker, som nevnt over, at det i likhet med utvalget legger til grunn en begrenset utvidelse av lovens virkeområde. Dette innebærer at begrepet grunnleggende nasjonale funksjoner angir en konkretisering av lovens virkeområde, innenfor rammen av de nasjonale sikkerhetsinteressene som funksjonene skal ivareta.

Utvalget har i NOU 2016: 19 kapittel 6.7.3 sett på sammenhengen mellom grunnleggende nasjonale funksjoner og kritiske samfunnsfunksjoner, og vist til at virkeområdet til loven gis en avgrensning ved innretningen på funksjoner og verdier som er av *nasjonal* betydning (i motsetning til funksjoner av regional og lokal betydning), og til beskyttelse av funksjonene mot tilsiktede uønskede hendelser (med utelukkelse av de utilsiktede hendelsene). Utvalget peker på side 116 på at en rekke av de samfunnsfunksjonene som identifiseres som kritiske i henhold til KIKS-metodikken (om sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner) som DSB benytter, også vil være å anse som grunnleggende nasjonale funksjoner etter den nye loven:

> «Grunnleggende nasjonale funksjoner kan således ses på som en delmengde av kritiske samfunnsfunksjoner i henhold til KIKS-metodikken: Hvilke konkrete funksjoner som vil være å anse som grunnleggende nasjonale funksjoner, vil […] måtte vurderes konkret avhengig av både hvilke verdier som legges til grunn for vurderingen og hvilke kriterier som legges til grunn for kritikalitet.»

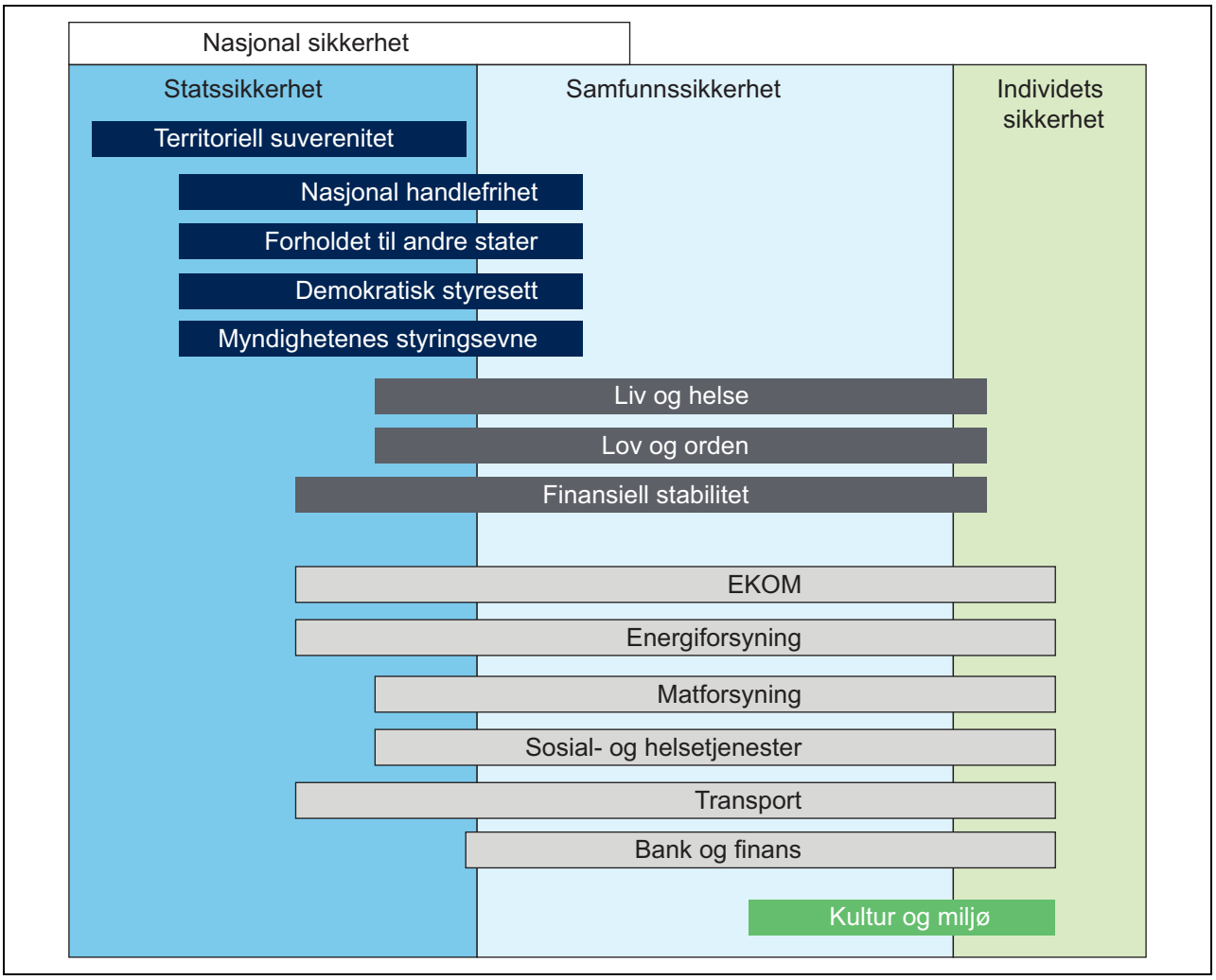
Utvalget peker i NOU 2016: 19 kapittel 6.7.5, side 117 og 118, på hvilke virksomheter som vil omfattes av loven, slik utvalget ser det. Utvalget viser her til beskrivelsen av virkeområdet i NOU 2016: 19 kapittel 6.7.1, der det angis at virksomheter «som har råderett over informasjon, informasjonssystemer, objekter eller infrastruktur, eller som driver aktivitet, som er av kritisk betydning for grunnleggende nasjonale funksjoner, omfattes av loven». Videre angir utvalget følgende typer virksomheter:

1. virksomheter som tilvirker, eller har behov for tilgang til, gradert informasjon
2. virksomheter som eier eller forvalter infrastruktur eller objekter av kritisk (avgjørende) betydning for de grunnleggende nasjonale funksjonene
3. virksomheter som har en rolle i Nasjonalt beredskapssystem (NBS), enten i Sivilt beredskapssystem (SBS) eller Beredskapssystemet for Forsvaret (BFF) («bør vurderes»)
4. aktører med en sentral rolle i totalforsvaret gjennom sin understøttelse av Forsvarets virksomhet («bør vurderes») og
5. virksomheter som har bestemmelsesrett over sivile objekter som er utpekt som nøkkelpunkter av Forsvaret

Departementet er enig i denne tilnærmingen, men presiserer at det for alle fem punktene må foretas en konkret vurdering av om det skal fattes vedtak i medhold av § 1-3 om at virksomheten skal underlegges loven. Punktene 1, 3 og 5 vil i hovedsak angi relativt konkret hvilke typer virksomheter det dreier seg om. For punkt 2 forventer departementet at noen flere virksomheter vil kunne omfattes av ny lov, som følge av introduksjonen av infrastrukturbegrepet. Departementet forventer at det vil knyttes størst grad av usikkerhet til hva punkt 4 om aktører med en sentral rolle i totalforsvaret gjennom sin understøttelse av Forsvarets virksomhet, vil innebære for ulike typer virksomheter. Det vurderes at dette også i stor grad vil dreie seg om private virksomheter som ivaretar oppgaver som er utkontraktert fra Forsvaret.

Totalforsvarskonseptet er av grunnleggende betydning for Forsvarets evne. De senere årene har denne evnen i økende grad blitt avhengig av sivil vare- og tjenesteproduksjon. Denne avhengigheten forsterkes ytterligere av økende direkte og indirekte avhengighet av tjenester fra sivile informasjonsinfrastrukturer. Leveransekjedene mellom sivile virksomheter og Forsvaret har samtidig blitt stadig mer komplekse og utgjør i dag ofte verdikjeder med svært mange ledd. Hvilke virksomheter som vil bli omfattet av loven, vil måtte være gjenstand for konkrete risikobaserte vurderinger. Det må også forventes at det vil skje betydelige endringer i rammebetingelsene for disse vurderingene gjennom hele lovens virketid.

For å gi et bilde av sammenhengen mellom Forsvarets behov og samfunnets funksjoner vises det til skissen under. Denne sammenhengen handler i stor grad om forståelsen av forholdet mellom statssikkerhet og samfunnssikkerhet. I figuren er det gitt en antydning av forholdet mellom statssikkerhet og samfunnssikkerhet sett opp mot en rekke viktige samfunnsinteresser. Dette skillet er imidlertid ikke så tydelig som det kan framstå av figuren. Figuren bør derfor brukes med forsiktighet til å antyde hvordan et begrenset utvidet virkeområde vil slå ut overfor ulike samfunnsfunksjoner. Eksempelvis forventer departe-



Figur 6.2 Figuren viser viktige nasjonale funksjoner og interesser. Plasseringen av de enkelte elementene illustrerer at skillet mellom stats- og samfunnssikkerhet i mange tilfeller er svært krevende å fastsette, og at de fleste funksjonene og interessene vil kunne berøre både stats- og samfunnssikkerheten.

mentet at sivile ekom-tjenester vil ha stor betydning for Forsvaret i framtiden. Det må derfor forventes at en eller flere ekom-tilbydere vil bli omfattet av loven. Det samme gjelder enkelte virksomheter innen transport- og drivstofforsyning. Andre funksjoner som helse, mat og kraftforsyning vil også kunne ha stor betydning, og virksomheter på disse områdene vil dermed kunne bli omfattet av loven. Felles for eksemplene er at det uansett vil måtte legges til grunn konkrete risikobaserte vurderinger for hvilke virksomheter og hvilke funksjoner som blir omfattet av loven, se figur 6.2.

Utvalgets forslag til virkeområdebestemmelse slår fast at «loven gjelder for virksomheter som alene eller sammen med andre råder over informasjon, informasjonssystemer, objekter eller infrastruktur, eller som driver aktivitet, som er av kritisk betydning for grunnleggende nasjonale funksjoner knyttet til [bokstav a til e]». Det framgår deretter i § 2-1 at departementene skal treffe enkeltvedtak om at virksomheter er av slik kritisk betydning for grunnleggende nasjonale funksjoner. Departementet mener at utvalgets forslag er krevende å lese, fordi leseren i praksis må forholde seg til fire nivåer samtidig, det vil si

1. informasjon, informasjonssystemer, objekter eller infrastruktur, i tillegg til aktivitet
2. virksomhetene som råder over disse
3. grunnleggende nasjonale funksjoner og
4. de fem kategoriene av interesser som angis i bokstav a til e

Videre er ikke grunnleggende nasjonale funksjoner definert i lovteksten, men kun gitt en indirekte ramme ved å være «knyttet til» interessene som oppregnes i bokstav a til e.

For å tydeliggjøre og forenkle bestemmelsene om hvem loven skal gjelde for, foreslår departementet enkelte strukturelle og språklige endringer. Det foreslås for det første en bestemmelse om hvilke virksomheter loven i utgangspunktet gjelder for, i § 1-2 *Hvem loven gjelder for*. Enkelte høringsinstanser, som *NSM, NVE* og *Energi Norge*, har reagert på at forvaltningsorganer ikke eksplisitt er omfattet av forslaget til virkeområdebestemmelse i § 1-2, slik tilfellet er i gjeldende lov, og at dette bidrar til å skape usikkerhet om rekkevidden til bestemmelsen. Departementet er enig i dette synspunktet og foreslår at «statlige, fylkeskommunale og kommunale organer» tas inn i første ledd i § 1-2. Dette vil også, slik departementet ser det, bidra til å gjøre lovens virkeområde mer forutsigbart, fordi det dermed ikke er tvil om at statlige, fylkeskommunale og kommunale organer er omfattet av loven. I forskriftshjemmelen som ligger i bestemmelsens fjerde ledd, vil det også ligge en åpning for at bestemte virksomheter, som forvaltningsorganer, helt eller delvis vil kunne unntas fra loven.

Etter departementets mening bør det gå fram av § 1-2 at loven også gjelder for leverandører i forbindelse med sikkerhetsgraderte anskaffelser. Departementet foreslår derfor å flytte bestemmelsen om dette fra utvalgets lovforslag § 1-3 *Særbestemmelser om lovens virkeområde* fjerde ledd, til nytt andre ledd i § 1-2.

I tillegg foreslår departementet å flytte leddet som omtaler lovens virkeområde for virksomheter på Svalbard, Jan Mayen og i bilandene fra lovforslaget § 1-3 femte ledd til nytt tredje ledd i § 1-2. Departementet har gjort lovtekniske endringer fra utvalgets lovforslag, som nevnt over, for å kunne skille ut særbestemmelser for Stortinget, Stortingets organer, regjeringen og domstolene i en egen bestemmelse, § 1-4. Når det gjelder forslaget i høringsuttalelsen fra Stortingets administrasjon om at det i bestemmelsen skal gis en uttrykkelig hjemmel til Stortinget å fastsette særskilte tilpasninger, er departementet av den oppfatning at utvalgets foreslåtte ordlyd om at loven gjelder for «Stortinget og Stortingets organer så langt Stortinget bestemmer det» ivaretar de tilpasningsbehov som Stortinget måtte ha.

Etter departementets vurdering bør det videre gå tydelig fram av virkeområdebestemmelsene at loven gjelder for private virksomheter først etter at et departement innenfor sitt ansvarsområde har truffet enkeltvedtak om dette, slik blant andre *NVE* og *Nkom* også påpeker i sine høringsuttalelser. Departementet foreslår derfor en egen vedtaksbestemmelse, § 1-3 *Vedtak om at loven skal gjelde for andre virksomheter*. I denne bestemmelsen angis vilkårene for hva slags virksomheter et departement skal utpeke i sin sektor. Disse vilkårene er at virksomheten etter bokstav a *behandler sikkerhetsgradert informasjon*, etter bokstav b *råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner* eller etter bokstav c *driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner*. Begrepet *grunnleggende nasjonale funksjoner* forklares i en ny legaldefinisjon i § 1-5 som er ment å være i tråd med utvalgets definisjon og beskrivelse av begrepet.

I legaldefinisjonen knyttes funksjonene direkte opp mot nasjonale sikkerhetsinteresser, ved at det slås fast at 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*.

Etter departementets oppfatning er begrepet *avgjørende* betydning språklig sett bedre enn *kritisk* betydning, som Sikkerhetsutvalget bruker i lovteksten. *Kritisk* er mye brukt i sikkerhetssammenheng, men ordet er sterkt negativt ladet og departementet har i samråd med Språkrådet valgt å unngå det i lovteksten. Unntaket er i objektsikkerhetsregelverket, der KRITISK og MEGET KRITISK, jf. § 7-2, er så innarbeidede klassifiseringsnivåer at det anses uhensiktsmessig å endre dette. Ordet *avgjørende* brukes utstrakt i utvalgets vurderinger, blant annet i merknadene til §§ 1-1 og 1-2, og bør også etter departementets syn brukes gjennomgående i lovteksten. Departementet foreslår å erstatte utvalgets *kritisk* med *avgjørende* blant annet når det gjelder *virksomheter som har avgjørende betydning for grunnleggende nasjonale funksjoner*. Bruken av *avgjørende betydning for* er ment som terskelverdi for hvilke virksomheter som skal omfattes av loven, jf. særmerknaden til § 1-3. Kriteriene for hva som utgjør *avgjørende betydning* er ment å tilsvare *kritisk betydning*, slik utvalget bruker begrepet, noe som framgår blant annet av utvalgets særmerknad til § 1-2 (NOU 2016: 19, side 252). Bruken av *avgjørende betydning* må ikke forveksles med *helt avgjørende skadefølger* i informasjons- og objektsikkerhetsklassifiseringene for STRENGT HEMMELIG og MEGET KRITISK, jf. §§ 5-3 og 7-2.

Enkelte høringsinstanser, som *DSS*, *NSM*, *Politidirektoratet* og *PST*, har etterlyst definisjoner av sentrale begreper i lovforslaget. Departementet er enig i dette og foreslår enkelte sentrale begreper definert i en ny § 1-5.

7 Ansvar og myndighet

7.1 Gjeldende rett

Ansvarsforholdene etter gjeldende sikkerhetslov er regulert i §§ 4 og 5. Det følger av § 4 første ledd at ansvaret for forebyggende sikkerhetstjeneste påhviler «[d]epartementet». Fra lovens ikrafttredelse og fram til 2003 lå dette ansvaret hos Forsvarsdepartementet. Dette var en forlengelse av det overordnede ansvaret som fulgte av Ordningen av den alminnelige sikkerhetstjenesten i statsforvaltningen fra 1965.

I 2003 ble det fastsatt en fordeling av ansvaret mellom justisministeren og forsvarsministeren for henholdsvis sivil og militær sektor, jf. Kronprinsreg. res. 4. juli 2003 med hjemmel i lov av 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven) § 7. Bakgrunnen for delingen var at arbeidet med samfunnssikkerhet ble ansett å være sektorovergripende, og at beredskapsarbeidet skulle styrkes på sentralt, regionalt og lokalt nivå. Samordningen av samfunnssikkerhetsarbeidet skulle forsterkes, og Justisdepartementet fikk et tydeligere samordningsansvar på sivil side. Etter samme resolusjon skal direktoratet Nasjonal sikkerhetsmyndighet på vegne av justisministeren og forsvarsministeren ivareta de utøvende funksjonene for forebyggende sikkerhetstjeneste, jf. også sikkerhetsloven § 4 andre ledd. Forsvarsdepartementet ble gitt det administrative ansvaret for Nasjonal sikkerhetsmyndighet og forvaltningsansvaret for sikkerhetsloven.

7.1.1 Departementenes ansvar og myndighet

Departementenes overordnede ansvar begrenser ikke den enkeltes ansvar og plikter etter bestemmelsene gitt i eller i medhold av sikkerhetsloven, jf. § 4 første ledd andre punktum.

Den enkelte virksomhets plikter følger av sikkerhetsloven § 5. Enhver virksomhet plikter å utøve forebyggende sikkerhetstjeneste i henhold til bestemmelsene gitt i eller i medhold av loven. Begrepet «virksomhet» er i lovens § 3 nr. 6 definert som «et forvaltningsorgan eller annet rettssubjekt som loven gjelder for […]».

Virksomheten plikter å utarbeide en intern instruks for å ivareta sikkerheten, sørge for at virksomhetens ansatte og engasjerte får tilstrekkelig opplæring i sikkerhetsspørsmål, samt regelmessig kontrollere sikkerhetstilstanden i virksomheten, jf. § 5 andre ledd bokstav a til c. Sikkerhetsadministrasjon er den administrative og organisatoriske styringen som ligger til grunn for forebyggende sikkerhetstjeneste. I tillegg er det gitt utfyllende bestemmelser om sikkerhetsadministrasjon i forskrift 29. juni 2001 nr. 723 om sikkerhetsadministrasjon (sikkerhetsadministrasjonsforskriften).

Ansvaret for utøvelse av forebyggende sikkerhetstjeneste påhviler virksomhetens leder, jf. § 5 tredje ledd. Virksomhetens leder kan etter samme bestemmelse delegere utøvende funksjoner internt i virksomheten. Dersom dette gjøres skal det dokumenteres skriftlig.

Det følger videre av fjerde ledd at det påhviler en plikt for enhver ansatt eller engasjert personell til å ivareta sikkerhetsmessige hensyn, og til å bidra til forebyggende sikkerhetstjeneste gjennom sitt arbeid eller oppdrag for virksomheten.

I bestemmelsens femte ledd er fullmakt til å gi nærmere bestemmelser delegert til Nasjonal sikkerhetsmyndighet.

7.1.2 Nasjonal sikkerhetsmyndighet

Sikkerhetsloven kapittel 3 regulerer funksjonen nasjonal sikkerhetsmyndighet. Denne myndigheten (funksjonen) skal koordinere de forebyggende sikkerhetstiltakene, tilby rådgivning og kontrollere sikkerhetstilstanden i virksomheter som er omfattet av loven, samt å være utøvende organ i forholdet til andre land og organisasjoner. Som grunnlag for dette arbeidet skal den nasjonale sikkerhetsmyndigheten blant annet innhente og analysere relevant informasjon, føre tilsyn med sikkerhetstilstanden i virksomheter underlagt sikkerhetsloven, bidra til utvikling av sikkerhetstiltak og drive rådgivningsarbeid.

Den 1. januar 2003 ble myndigheten lagt til et eget direktorat, kalt Nasjonal sikkerhetsmyndighet, under Forsvarsdepartementet. Forsvarets overkommando, inkludert Sikkerhetsstaben (FO/

S), ble nedlagt 1. august 2003, og Forsvarsjefens sikkerhetsavdeling (FSA) ble samtidig opprettet til støtte for forsvarssjefen.

En av Nasjonal sikkerhetsmyndighets viktigste oppgaver er å føre tilsyn og kontroll med sikkerhetsarbeidet og sikkerhetstilstanden i de virksomheter som er underlagt loven. Nasjonal sikkerhetsmyndighets tilsynsoppgave følger i dag av sikkerhetsloven § 9 første ledd bokstav c.

I § 10 hjemles Nasjonal sikkerhetsmyndighets adgangsrett til ethvert skjermingsverdig objekt og områder hvor skjermingsverdig informasjon oppbevares.

Nasjonal sikkerhetsmyndighet driver i dag en nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur (Norwegian Computer Emergency Response Team – NorCERT), og et nasjonalt varslingssystem for digital infrastruktur (VDI). Hensikten med NorCERT og VDI er å innhente, analysere og dele informasjon om digitale angrep mot kritisk infrastruktur. Dette oppnås blant annet gjennom utplassering av sensorer i utvalgte offentlige og private virksomheter som innehar kritisk infrastruktur i tilknytning til deltakernes datanettverk, jf. Prop. 97 L (2015–2016), side 26. Informasjon fra sensorene bidrar til en nasjonal evne til tidlig avdekking og verifikasjon av koordinerte og målrettede angrep.

Nasjonal responsfunksjon og varslingssystemet for digital infrastruktur ble lovfestet som en del av oppgavene til Nasjonal sikkerhetsmyndighet ved endringslov til sikkerhetsloven som trådte i kraft 1. januar 2017 (lov 12. august 2016 nr. 78), jf. Prop. 97 L (2015–2016) og Innst. 352 L (2015–2016), og framgår i dag av sikkerhetsloven § 9 første ledd bokstav e. Det ble samtidig også vedtatt en bestemmelse som nærmere regulerer behandling av personopplysninger knyttet til utførelsen av VDI og NorCERT-funksjonen.

7.1.3 Varslingsplikt og myndighet til å fatte vedtak ved risiko for sikkerhetstruende virksomhet

I endringsloven 12. august 2016 nr. 78 ble det også vedtatt en ny bestemmelse § 5 a, om varslingsplikt og vedtaksmyndighet for Kongen i statsråd.

Bestemmelsen pålegger virksomheter underlagt sikkerhetsloven en varslingsplikt til ansvarlig fagdepartement ved kunnskap om risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført. Bestemmelsen gir også Kongen i statsråd myndighet til å fatte vedtak for å hindre at slik virksomhet blir etablert eller gjennomført, uten hensyn til begrensningene i forvaltningsloven § 35, og uavhengig av om aktiviteten er tillatt etter annen lov eller annet vedtak.

Formålet med bestemmelsen er ifølge forarbeidene primært å etablere en hjemmel i loven for å kunne forebygge mer frittstående høyteknologisk virksomhet som kan innebære en fare for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, som ikke spesifikt er knyttet til sikkerhetsgradert informasjon eller skjermingsverdige objekter. Bestemmelsen omfatter også annen type aktivitet enn det som knytter seg til høyteknologiske innretninger, jf. Prop. 97 L (2015–2016).

7.1.4 Ansvar og myndighet etter relevant sektorregelverk

Det finnes en rekke sektorregelverk som regulerer ulike sikkerhetsspørsmål. Dette gjelder for eksempel innenfor kraftsektoren (energiloven og beredskapsforskriften), med Olje- og energidepartementet som overordnet ansvarlig, petroleumssektoren (petroleumsloven med underliggende forskrifter), med Arbeids- og sosialdepartementet som overordnet ansvarlig for HMS og forebygging av bevisste anslag, innenfor elektronisk kommunikasjon (ekomloven og ekomforskriften), med Samferdselsdepartementet som overordnet ansvarlig, og innenfor luftfartssektoren (luftfartsloven med underliggende forskrifter), med Samferdselsdepartementet som overordnet ansvarlig. Videre kan finanssektoren med blant annet finansforetaksloven og verdipapirhandelloven, med Finansdepartementet som overordnet ansvarlig, og helse- og omsorgssektoren med helseberedskapsloven, og med Helse- og omsorgsdepartementet som overordnet ansvarlig, nevnes.

Det gjeldende sektorregelverket eksisterer sammen med gjeldende sikkerhetslov med underliggende forskrifter.

7.2 Utvalgets forslag

7.2.1 Departementenes ansvar og myndighet etter loven

Sikkerhetsutvalget uttaler i NOU 2016:19 kapittel 7.7 at ansvars- og myndighetsfordelingen for forebyggende sikkerhet etter loven har stått sentralt i utvalgets arbeid. Et utgangspunkt for utvalgets arbeid har vært at de generelle prinsippene for krisehåndtering og beredskap ligger fast, og også bør gjelde for innretningen på en ny sikkerhetslov.

Utvalget anbefaler, i tråd med ansvarsprinsippet, at det primære ansvaret tillegges det enkelte fagdepartement. Utvalget uttaler om dette i kapittel 7.7 på side 137:

> «Det er det enkelte fagdepartement som kjenner sin sektor best, og har de beste forutsetningene for å kunne identifisere grunnleggende nasjonale funksjoner og virksomheter av kritisk betydning for disse, samt gjøre nødvendige samfunnsøkonomiske prioriteringer innad i sektoren.»

Samtidig uttaler utvalget et tydelig behov for at det sektorovergripende perspektivet må ivaretas i tråd med samordningsprinsippet, noe som er helt avgjørende for å kunne ha en helhetlig tilnærming til forebyggende sikkerhet på tvers av sektorene.

Etter utvalgets forslag er det enkelte departement ansvarlig for forebyggende sikkerhet i eget myndighetsområde. Departementene tillegges ansvar for å identifisere og holde oversikt over grunnleggende nasjonale funksjoner innen sitt myndighetsområde. Departementene må identifisere og holde oversikt over både virksomheter som direkte eller indirekte er av vesentlig betydning for grunnleggende nasjonale funksjoner, og de som er av kritisk betydning for grunnleggende nasjonale funksjoner. De virksomhetene som vurderes å være av kritisk betydning, skal det fattes enkeltvedtak overfor, slik at disse underlegges sikkerhetslovens bestemmelser.

Som beskrevet under kapittelet om *formål og virkeområde* er det en forutsetning for lovens virkeområde at de grunnleggende nasjonale funksjonene kartlegges ved at de knyttes til de nærmere angitte kategoriene som framgår av utvalgets forslag til § 1-2 første ledd bokstav a til e.

Sikkerhetsutvalget legger til grunn at det er nødvendig å etablere en systematikk for å kunne identifisere grunnleggende nasjonale funksjoner og identifisere virksomheter som er av kritisk betydning for disse. Utvalget har vurdert det som lite hensiktsmessig å legge denne vurderingen til den enkelte virksomhet. Utvalget mener det er bedre å bygge på etablerte strukturer knyttet til identifisering av kritiske samfunnsfunksjoner etter instruks for departementenes arbeid med samfunnssikkerhet og beredskap. Utvalget uttaler om dette i kapittel 7.7.1 på side 137:

> «Det er i dag allerede etablert et system hvor det enkelte fagdepartement har ansvaret for identifisering av kritiske samfunnsfunksjoner gjennom Instruks for departementenes arbeid med samfunnssikkerhet og beredskap (samordningsresolusjonen). I samordningsresolusjonen stilles det krav om at departementene skal ha oversikt over kritiske samfunnsfunksjoner og kritisk infrastruktur i egen sektor. På bakgrunn [av] disse oversiktene skal departementene blant annet vurdere risiko, sårbarhet og robusthet for de aktuelle kritiske samfunnsfunksjonene. Utvalget mener det vil være hensiktsmessig å bygge på disse etablerte strukturene, også for identifisering av grunnleggende nasjonale funksjoner og virksomheter som vil falle inn under den nye lovens virkeområde. Som nevnt innledningsvis, mener utvalget at de enkelte departementene – i tråd med ansvarsprinsippet – bør ha det primære ansvaret for forebyggende sikkerhet innenfor sitt myndighetsområde. Sektorspesifikk kunnskap og kompetanse er av sentral betydning for å kunne identifisere de funksjoner og virksomheter som er av grunnleggende nasjonal betydning i den enkelte samfunnssektor. En avgjørende forutsetning for at en slik systematikk skal fungere i praksis, er at de enkelte fagdepartementene er sitt ansvar bevisst og følger opp det ansvaret de tillegges gjennom loven. For enkelte departementer innebærer dette behov for kompetanseheving på forebyggende sikkerhet.
>
> Fordi det finnes en etablert systematikk og strukturer for departementenes arbeid med samfunnssikkerhet og beredskap å bygge på, vil systematikken for identifisering og utvelgelse av virksomheter som omfattes av loven sannsynligvis ikke innebære noen vesentlig større ressursbruk hos de enkelte departementene.»

Utvalget mener det er viktig at det sektorovergripende perspektivet ivaretas for å sikre en helhetlig identifisering av gjensidige avhengigheter mellom virksomheter og sektorer. Om dette skriver utvalget i kapittel 7.7.1 på side 138:

> «Dette både for å kunne fange opp sektorovergripende avhengigheter som det enkelte fagdepartement ikke nødvendigvis har forutsetninger for å kunne identifisere, og for å kunne bidra med faglig bistand og kvalitetssikring av det enkelte departements identifisering innen egen sektor.
>
> Også trusselbildet de enkelte virksomhetene står overfor, særlig innenfor cyber-domenet, er i mange tilfeller av sektorovergripende karakter. Både behovet for informasjonsdeling

om slike trusler på tvers av samfunnssektorene, og etablering av sikkerhetstiltak for å forebygge disse truslene, underbygger behovet for å ivareta et helhetlig og sektorovergripende ansvar. I tillegg vil det kunne være selvstendige rettssubjekter som ikke naturlig faller inn under et fagdepartements myndighetsområde. For disse virksomhetene vil det være nødvendig å etablere en mekanisme for identifisering og utvelgelse på lik linje med det enkelte fagdepartements myndighet i egen sektor. Dette er et tiltak som sannsynligvis vil kreve ressursbruk hos den aktøren som skal ivareta et slikt ansvar. Utvalget foreslår at et slik sektorovergripende ansvar tillegges funksjonen Nasjonal sikkerhetsmyndighet.

Funksjonen Nasjonal sikkerhetsmyndighet vil ha en bedre oversikt over sektorovergripende avhengigheter enn de enkelte fagdepartement. Utvalget mener derfor det vil være nødvendig at Nasjonal sikkerhetsmyndighet fremmer begrunnede forslag om virksomheter som bør underlegges sikkerhetsloven til fagdepartementene.

I tillegg mener utvalget at funksjonen Nasjonal sikkerhetsmyndighet burde ha anledning til å påklage tilfeller der den mener at departementenes identifisering og utvelgelse av virksomheter omfattet av loven, er uforsvarlig.»

Videre anbefaler utvalget at det utvikles tverrsektorielle scenarioer som er relevante for sikkerhetslovens virkeområde for å bidra til at grunnleggende nasjonale funksjoner identifiseres. Slike scenarioer vil også bidra til å identifisere virksomheter som er kritiske for disse funksjonene. Utvalget uttaler i kapittel 7.7.2 på side 138:

«Utvalget tror en scenariobasert tilnærming, på linje med det DSB gjør i Nasjonalt risikobilde og Forsvaret gjør for sine interne planprosesser, vil kunne bidra til at en ny sikkerhetslov får et presist nedslagsfelt. Slike scenarier bør derfor legges til grunn både for identifisering av grunnleggende nasjonale funksjoner og for identifisering og utvelgelse av virksomheter som er av kritisk betydning for understøttelsen av disse funksjonene. Utvalget finner det ikke naturlig å foreslå en lovfesting av plikten til å utvikle slike scenarier, men anbefaler en tilnærming for den videre implementeringen av loven.

I tråd med FFIs anbefalinger, mener utvalget at slike scenarier bør utvikles gjennom et samarbeid mellom Justis- og beredskapsdepartementet og Forsvarsdepartementet, i nær kontakt med øvrige berørte departementer. I tillegg mener utvalget at de aktuelle fagmyndighetene bør ha en sentral rolle som premissgivere for slike scenarier.»

Utvalget mener, på bakgrunn av at det eksisterer gjensidige avhengigheter mellom virksomheter, og mellom samfunnssektorer, at det er et behov for at noen ivaretar et helhetlig og sektorovergripende perspektiv. Dette er både for å fange opp sektorovergripende avhengigheter som fagdepartementet nødvendigvis ikke har forutsetninger for å identifisere, og bidra med faglig bistand til identifiseringen. Også trusselbildet, og kunnskap om dette, er sektorovergripende, særlig innen cyberdomenet. Derfor er det behov for (gradert) informasjonsdeling, og dette er en sektorovergripende utfordring. Utvalget mener derfor sikkerhetsmyndigheten må kunne fremme begrunnede forslag om at enkeltvirksomheter underlegges sikkerhetsloven. Dette kommer til uttrykk i § 2-1 fjerde ledd. Utvalget anbefaler videre at det dersom det oppstår uenigheter knyttet til underleggelse av enkelte virksomheter bør det, i ytterste konsekvens, være mulig å få avklart spørsmålet om underleggelse ved å fremme sak om dette til et tvisteorgan.

7.2.2 Sikkerhetsmyndigheten

Utvalget foreslår å videreføre funksjonen nasjonal sikkerhetsmyndighet. Utvalget viser blant annet til at Norge gjennom NATO er forpliktet til å ha en slik nasjonal funksjon. Som et pedagogisk grep har utvalget valgt å omtale funksjonen som *sikkerhetsmyndigheten*.

Utvalget mener det fortsatt vil være naturlig at direktoratet Nasjonal sikkerhetsmyndighet ivaretar de oppgavene som tillegges sikkerhetsmyndigheten i loven.

Utvalget foreslår at sikkerhetsmyndigheten skal ha det sektorovergripende ansvaret for forebyggende sikkerhetsarbeid i medhold av loven. Sikkerhetsmyndighetens ansvar skal ikke gripe inn i de enkelte departementers ansvar innenfor eget myndighetsområde. Det sektorovergripende ansvaret omfatter ansvaret for at forebyggende sikkerhetsarbeid etter loven har en helhetlig tilnærming og ansvaret for å koordinere sikkerhetsarbeidet mellom ulike departementer og ulike relevante sektormyndigheter. En viktig plikt som utvalget foreslår tillagt sikkerhetsmyndigheten, er

å påse at det føres tilsyn med virksomheter som er underlagt loven.

Tilsynsmyndigheter organiseres på ulikt vis i ulike sammenhenger. Enkelte har rendyrkede tilsynsroller, slik som for eksempel Helsetilsynet, mens andre, som eksempelvis Nasjonal kommunikasjonsmyndighet, har en mer integrert tilnærming der tilsyn inngår som en del av en bredere oppgaveportefølje. Nasjonal sikkerhetsmyndighet er også organisert på denne måten.

Utvalget foreslår at sikkerhetsmyndigheten på samme måte som i dag blir organisert etter en tradisjonell integrert modell, hvor flere roller ivaretas innenfor samme organisasjon. Dette begrunnes med at forebyggende sikkerhet mot tilsiktede uønskede hendelser er et snevert fagfelt, hvor tilgangen til kvalifisert kompetanse er begrenset. En oppsplitting av rollene kan medføre at det skapes små og sårbare kompetansemiljøer. For øvrig vises det til utvalgets omtale i NOU 2016: 19, kapittel 7.7.3.

7.2.3 Informasjon om trusselvurderinger og risikohåndtering

Utvalget foreslår at virksomheter som er underlagt loven, skal kunne få tilgang til tidsriktig og relevant informasjon om hvilke trusler de er utsatt for. Dette skal bidra til at virksomhetene skal kunne gjennomføre tilfredsstillende risiko- og sårbarhetsanalyser og dermed iverksette riktige og forsvarlige sikkerhetstiltak. Utvalget begrunner forslaget slik i NOU 2016: 19 kapittel 7.7.5 på side 142:

> «Ettersom relevante trusselvurderinger ofte vil utarbeides av andre myndighetsaktører, herunder Politiets sikkerhetstjeneste og Etterretningstjenesten, vil Sikkerhetsmyndigheten i de fleste tilfeller ikke være eier av den informasjonen som skal deles. Sikkerhetsmyndigheten, bør imidlertid i kraft av sin funksjon ha en generell plikt til å koordinere tilgjengeliggjøring av slik informasjon og påse at det etableres nødvendige arenaer for dette. Slike arenaer bør etableres i tett samarbeid med aktuelle sektormyndigheter i de enkelte samfunnssektorene.
>
> Utvalget mener løsningen vil bidra til å maksimere mulighetene for å kunne dele sikkerhetsrelevant informasjon med virksomheter som har behov for denne. Den vil således være et viktig bidrag til at både private og offentlige virksomheter blir satt i bedre stand til å kunne gjøre gode vurderinger og iverksette forsvarlige tiltak i sitt forebyggende sikkerhetsarbeid.»

7.2.4 Nasjonal responsfunksjon for alvorlige dataangrep

Den nasjonale responsfunksjonen for alvorlige dataangrep mot kritisk infrastruktur (Norwegian Computer Emergency Response Team – NorCERT) og det nasjonale varslingssystemet for digital infrastruktur (VDI) som Nasjonal sikkerhetsmyndighet i dag driver, har som formål å innhente, analysere og dele informasjon om digitale angrep mot kritisk infrastruktur, jf. nærmere omtale i kap. 7.1.2 ovenfor.

Utvalget foreslår å videreføre NorCERT-funksjonen i en egen bestemmelse og begrunner det slik i NOU 2016: 19 kapittel 7.7.6 på side 142:

> «Dette skyldes utelukkende at den nasjonale responsfunksjonen er en operativ funksjon, som ikke naturlig faller inn under de øvrige fagmyndighetsoppgavene som er foreslått tillagt Sikkerhetsmyndigheten. Utvalget har ikke vurdert om responsfunksjonen organisatorisk skal plasseres andre steder enn i dag.»

Om varslingssystemet for digital infrastruktur (VDI) skriver utvalget i kapittel 7.7.6 på side 142:

> «Utvalget har vurdert hvorvidt det burde være en plikt for virksomheter underlagt loven å være tilknyttet varslingssystemet for digital infrastruktur. I likhet med de vurderingene som ble gjort i Prop. 97 L (2015–2016), mener imidlertid utvalget at dagens finansieringsmodell for VDI-samarbeidet gjør det utfordrende å lovfeste en slik plikt. Utvalget støtter derfor regjeringens tilnærming om at en eventuell lovfesting av en slikt plikt, bør ses i sammenheng med den fremtidige finansieringsmodellen for VDI. Utvalget vil i den forbindelse også fremheve viktigheten av at et slikt arbeid igangsettes raskt. […]
>
> Utvalget mener det er viktig at virksomheter som råder over digital infrastruktur av kritisk betydning for grunnleggende nasjonale funksjoner får tilbud om, og anbefales å tilknytte seg dagens VDI-samarbeid. Dette forutsetter at NorCERT/VDI kapasitetsmessig innrettes slik at alle relevante aktører gis anledning til slik tilknytning.»

7.2.5 Vedtaksmyndighet for Kongen i statsråd

Utvalget foreslår å videreføre en hjemmel til å kunne stanse virksomhet som kan ha kritiske skadevirkninger for grunnleggende nasjonale funksjoner, tilsvarende § 5a som trådte i kraft som en endring til gjeldende sikkerhetslov 1. januar 2017. Utvalget begrunner dette blant annet slik i NOU 2016: 19 kapittel 7.7.8 på side 143:

> «Utvalget er enig i at det er behov for en hjemmel for å kunne stanse virksomhet som kan ha kritiske skadevirkninger for grunnleggende nasjonale funksjoner, se kapittel 7.2.3, og foreslår derfor å videreføre den vedtatte § 5a i en form som er tilpasset utvalgets lovforslag.
>
> Slik bestemmelsen er utformet i regjeringens forslag, og omtalt i forarbeidene, vil myndighetene ha et bredt spillerom i forhold til hvilke typer vedtak som kan fattes med hjemmel i den aktuelle bestemmelsen. Formålet med bestemmelsen er å etablere en hjemmel i loven for å kunne stanse, eller nærmere regulere enkelte typer virksomhet som kan innebære en fare for grunnleggende nasjonale funksjoner. Vedtakene må nødvendigvis også være av en slik art og karakter at de forbygger slik aktivitet, noe som vil kunne variere ut fra hvilken type aktivitet det er tale om.
>
> Samtidig mener utvalget at bestemmelsens inngripende karakter gjør det nødvendig å [etablere] ytterligere rettssikkerhetsgarantier enn det som følger av regjeringens forslag.
>
> For det første mener utvalget at myndigheten til Kongen i statsråd bør avgrenses til å gjelde enkeltvedtak, det vil si vedtak som retter seg mot bestemte personer eller virksomheter eller nærmere avgrensede grupper av slike.
>
> For det andre bør det kunne påvises med stor grad av sannsynlighet at den aktuelle aktiviteten vil kunne få slike skadevirkninger at det er tvingende nødvendig å gripe inn. Bevisbyrden for at aktiviteten er av en slik alvorlighetsgrad, vil påligge myndighetene.
>
> For det tredje mener utvalget at det ved avgjørelsen av hvilke vedtak som skal treffes, må påligge myndighetene et uttrykkelig forholdsmessighetskrav. I dette ligger en plikt til å vurdere vedtakets varighet, og forholdsmessigheten mellom vedtaket og den risiko aktiviteten utgjør.
>
> Før vedtak fattes må saken utredes så godt som tiden tillater det. I denne utredningsplikten ligger en plikt til å innhente rådgivende uttalelser fra relevante organer, herunder PST, Etterretningstjenesten og NSM. I den utstrekning det er mulig bør også berørte parter få anledning til å uttale seg. Dersom tidskritiske forhold medfører at ordinære krav til utredning ikke kan følges, bør det gjennomføres en etterfølgende utredning for å sikre at vedtaket er fattet på et korrekt grunnlag.»

7.2.6 Klage- og tvisteløsning og tvisteorgan

Utvalget foreslår å opprette et tvisteorgan som ut fra rettssikkerhetsprinsipper kan ta stilling til klager fra virksomheter som blir underlagt loven ved enkeltvedtak og til klager fra sikkerhetsmyndigheten på departementenes etterlevelse av loven. Utvalget begrunner og beskriver blant annet forslaget slik i NOU 2016: 19 kapittel 7.7.7 på side 142–143:

> «Formålet med tvisteorganets virksomhet er å komme frem til de samfunnsmessig beste løsningene i et helhetsperspektiv.
>
> En grunnleggende utfordring med dagens system for forebyggende sikkerhet etter gjeldende sikkerhetslov er, slik utvalget ser det, at det ikke finnes noen form for mekanisme for å avklare uenigheter mellom sikkerhetsmyndighetene og relevante sektormyndigheter. Justis- og beredskapsdepartementet har det sektorovergripende ansvaret for forebyggende sikkerhet og beredskap for de sivile samfunnssektorene, men er i liten grad gitt myndighet til å kunne instruere de ulike fagdepartementene i deres arbeid.
>
> Etter dagens sikkerhetslov har Nasjonal sikkerhetsmyndighet det utøvende ansvaret på vegne av Forsvarsdepartementet og Justis- og beredskapsdepartementet. Men heller ikke Nasjonal sikkerhetsmyndighet, eller de to departementene NSM har fått delegert sin myndighet fra, har noen instruksjonsmyndighet overfor det øvrige departementsfellesskapet.
>
> Sett hen til dagens organisering av statsforvaltningen, og den strenge praktiseringen av sektorprinsippet, mener utvalget det vil være vanskelig å tillegge et enkelt departement en myndighet til å treffe vedtak overfor det øvrige departementsfellesskapet. Utvalget anbefaler derfor at det etableres et eget kollegialt tvisteorgan som gis myndighet til å treffe vedtak i klagesaker etter loven.
>
> Konkret foreslår utvalget at Kongen gis myndighet til å peke ut et kollegialt organ med

fem medlemmer. Ved oppnevningen av medlemmer foreslår utvalget at det i tillegg til sikkerhetsfaglig kompetanse, skal legges vekt på kompetanse innen personvern og selvstendige rettssubjekters rettssikkerhet, jf. utvalgets forslag til formålsbestemmelse i § 1-1.»

Utvalget foreslår å legge tvisteorganet til eksisterende strukturer, for eksempel Regjeringens sikkerhetsutvalg (RSU). For øvrig vises det til NOU 2016: 19 kapittel 7.7.7 side 142–143.

7.3 Høringsinstansenes syn

7.3.1 Generelt

De fleste høringsinstansene er i all hovedsak enig i utvalgets vurdering av ansvars- og myndighetsfordelingen for det forebyggende sikkerhetsarbeidet.

Samferdselsdepartementet uttaler:

«I tråd med ansvarsprinsippet legger utvalget opp til at det primære ansvaret for forebyggende sikkerhet i de ulike samfunnssektorene bør ligge i det enkelte fagdepartement. Dette er positivt. Vi mener også at det er riktig at Nasjonal sikkerhetsmyndighet (NSM) tilsvarende er gitt det sektorovergripende ansvaret for forbyggende sikkerhetsarbeid etter loven, og skal koordinere sikkerhetsarbeidet mellom ulike departementer og relevante sektormyndigheter.»

Norges Bank uttaler:

«Norges Bank støtter den foreslåtte endringen og presiseringen av ansvars- og myndighetsfordeling for sikkerheten til grunnleggende nasjonale funksjoner. Der endring av ansvars- og myndighetsfordeling synes nødvendig ut fra behovet for en helhetlig tilnærming og oversikt over sikkerhetssituasjonen i Norge, balanseres dette godt med involvering av eksisterende ordninger for sektortilsyn.»

Fylkesmannen i Rogaland uttaler:

«Vi støtter at ansvarsprinsippet legges til grunn for det forebyggende sikkerhetsarbeidet og at fagdepartementene har ansvar innen de ulike samfunnssektorene. Videre at det sektorovergripende ansvaret ivaretas av Nasjonal sikkerhetsmyndighet (NSM). Dette er det samme som i dag. Det er imidlertid nødvendig at det legges til rette for at både fagdepartement og NSM på en bedre måte kan ivareta dette ansvaret. I dag opplever vi at dette ikke gis høy nok prioritet i departementene og at NSM ikke har de ressurser som skal til å gjøre en god nok jobb. Større forventninger må følges opp med nødvendige tiltak for å sikre at oppgavene blir løst på en tilfredsstillende måte.»

Olje- og energidepartementet uttaler:

«Det er som nevnt positivt at det foreslås at de generelle prinsippene for krisehåndtering og beredskap skal ligge fast (sektoransvaret). Departementet er enig i at forebyggende sikkerhet har en sektorovergripende dimensjon, men denne må ikke overskygge behovet for å ivareta sektorenes egenart eller medføre dobbeltregulering.»

Direktoratet for samfunnssikkerhet og beredskap (DSB) uttaler:

«Problemstillingene knyttet til den uklare avgrensingen av lovens virkeområde, blir spesielt tydelig gjennom forslagets beskrivelse av myndigheter etter loven.»

Nasjonal kommunikasjonsmyndighet (Nkom) uttaler:

«Bestemmelsen (§ 2-1) etablerer lovens systematikk for identifisering av hvilke grunnleggende nasjonale funksjoner som omfattes. Bestemmelsens første ledd slår fast at hvert enkelt departement er ansvarlig for forebyggende sikkerhet innen sitt myndighetsområde. Det tillegges deretter sektorene spesifikke oppgaver i et tretrinnssystem i bestemmelsenes første ledd bokstav a, b og c. Nkom mener at bestemmelsen gir en god systematisk tilnærming til ivaretakelse av samfunnssikkerheten i form av å etablere sektorvis myndighet og plikter.

Nkom er positive til etableringen av et tydelig sektoransvar. Bestemmelsen gir en mer detaljert beskrivelse av plikter i forhold til gjeldende sikkerhetslov og videreutvikler departementenes sentrale rolle. Nkom tolker bestemmelsen slik at enhver type virksomhet som sektormyndigheten vurderer som kritisk i egen sektor i henhold til loven § 1-2, vil kunne utpekes av sektormyndigheten uavhengig av sektorregelverket.

Å bli underlagt sikkerhetsloven medfører potensielt økt sikkerhet, men vil også kunne

medføre økte kostnader for den enkelte virksomhet. Nkom mener derfor at det er en viktig rettssikkerhetsgaranti å pålegge sektormyndigheten varslingsplikt og gi de enkelte virksomheter klageretten slik det er foreslått i bestemmelsens andre ledd.

I forhold til å kunne ivareta Sikkerhetsmyndighetens sektorovergripende ansvar etter lovforslaget § 2-2, er Nkom enig i at Sikkerhetsmyndigheten bør ha mulighet til selvstendig vurdering og forslagsrett for utpeking av virksomheter av kritisk betydning slik det foreslås i bestemmelsens fjerde ledd.»

Norges vassdrags- og energidirektorats (NVE) innspill:

«NVE er fornøyd med at hvert enkelt fagdepartement får ansvaret for å følge opp virksomheter innenfor egen sektor, både når det gjelder oversikt, utpeking og tilsyn med at sikkerhetsloven etterleves, jf. § 2-1 første ledd. Dette er i tråd med ansvarsprinsippet og NVE mener det er viktig og positivt at utvalget fastslår at ansvarsprinsippet bør ligge til grunn og være førende for det primære ansvaret for forebyggende sikkerhet i de ulike samfunnssektorene.

NVE mener primært at sikkerhet i energiforsyningen best ivaretas gjennom sektorregelverket. NVE støtter likevel forslaget om at også virksomheter i energiforsyningen som vurderes å være kritiske for nasjonale sikkerhetsinteresser kan underlegges sikkerhetsloven. Forutsetningen er at ansvar for vurdering og utpeking reelt sett ligger hos sektormyndigheten. Det må være vedkommende fagdepartement som avgjør hvilke virksomheter som er vesentlige for nasjonale sikkerhetsinteresser. Vi er derfor positive til det systemet utvalget foreslår i § 2-1 første ledd om at fagdepartementet først skal identifisere og holde oversikt over funksjoner i bokstav a) og virksomheter er av vesentlig betydning for funksjoner i bokstav b). Vi viser også til kommentaren i punkt 2.1 om at det må fremgå eksplisitt at fagdepartementet er ansvarlig for å utpeke virksomheter på bakgrunn av de tidligere trinnene i tretrinns modellen, jf. bokstav c.

[…]

NVE er derimot skeptisk til at sikkerhetsmyndigheten kan overprøve fagdepartementets vurderinger etter § 2-1 fjerde og femte ledd og § 7-1 fjerde ledd. NVE mener at ansvarsprinsippet også må ligge til grunn her, og at sikkerhetsmyndigheten først og fremst skal være et veiledende og rådgivende fagorgan for departementet og tilsynsorganene.»

Norges Ingeniør- og Teknologorganisasjon (NITO) uttaler:

«NITO merker seg at utvalget mener det primære ansvaret for forebyggende sikkerhet i de ulike samfunnssektorene bør ligge i det enkelte fagdepartement. Begrunnelsen er at det er det enkelte departement som kjenner sin sektor best og har de beste forutsetningene for å kunne identifisere grunnleggende nasjonale funksjoner og virksomheter av kritisk betydning for disse. NITO er undrende til om dette er tilstrekkelig, og viser bla til utsetting av IKT-drift i Sykehuspartner.

[…]

Utvalget anbefaler at det lovfestes en systematikk for hvordan de ulike departementene skal identifisere grunnleggende nasjonale funksjoner innenfor eget myndighetsområde, samt de virksomheter som har en kritisk rolle i understøttelsen av slike funksjoner. NITO mener dette er et skritt i riktig retning. NITO vil samtidig understreke behovet for å søke og hensynta faglige råd i slike spørsmål. Utvalget anbefaler at det sektorovergripende ansvaret for sikkerhet fortsatt skal ivaretas av Nasjonal sikkerhetsmyndighet (NSM). NITO slutter seg til dette, men vil understreke at Nasjonal sikkerhetsmyndighet kun kan ivareta dette ansvaret med endrede og utvidede fullmakter.»

Næringslivets Hovedorganisasjons (NHO) innspill:

«Det går frem av lovforslaget at hvert enkelt sektordepartement skal treffe enkeltvedtak om «at virksomheter er av kritisk betydning for grunnleggende nasjonale funksjoner, slik at loven gjelder for dem». Enkeltvedtak skal forhåndsvarsles før vedtak treffes. Selvstendige rettssubjekter kan påklage vedtaket til et tvisteorgan som skal opprettes for å behandle klagesaker.

I dag er 14 private virksomheter pålagt å følge sikkerhetsloven. Det følger av utredningen at det nye regimet vil innebære en betydelig utvidelse, slik at langt flere virksomheter må påregne at loven aktiveres for dem.

NHO legger til grunn at sektormyndighetene i vurderingen også vil legge vekt på bedriftsøkonomiske interesser. Utvidelse av antall bedrifter som omfattes av sikkerhetsloven bør skje gradvis. Terskelen for å aktivere

loven for nye virksomheter må ikke legges for lavt.

NHO forutsetter at eventuelle motforestillinger virksomheter har knyttet til å bli pålagt å følge loven, blir grundig vurdert i saksbehandlingen etter § 2-1 bokstav c.»

Statens strålevern uttaler:

«Den foreslåtte lovfestingen av en systematikk for departementenes identifisering av grunnleggende nasjonale funksjoner, foreslås understøttet ved utarbeidelse av tverrsektorielle scenarier. Strålevernet støtter dette, samt at de aktuelle fagmyndighetene bør ha en sentral rolle som premissgivere for slike scenarier.»

BDO skriver i sin uttalelse:

«Flere steder i utredningen og forslagene om konkrete bestemmelser, legges det opp til at virksomheter som ikke anses å falle innenfor et departements myndighetsområde ved ulike regler om varsling, vedtak osv. skal forholde seg direkte til Sikkerhetsmyndigheten. En del av begrunnelsen er at en del virksomheter ikke tilhører en bestemt sektor, men har oppgaver og funksjoner som i stor grad går på tvers av flere sektorer.

BDO anser det som uheldig at en del virksomheter skal forholde seg direkte til Sikkerhetsmyndigheten, og dermed omgå departementsnivået, med den begrunnelsen at det er uklart hvilken sektor virksomheten skal anses å tilhøre. Sikkerhetsmyndigheten vil da gis en annen og mer operasjonell rolle enn Sikkerhetsmyndigheten for øvrig har og burde ha. Slike avgrensingsutfordringer bør heller løses ved at Justis- og beredskapsdepartementet, som samordnende departement, gis myndighet til å utpeke hvilket departement som skal være hovedansvarlig etter sikkerhetsloven. Alternativt at dersom departementene ikke kommer til enighet på dette punkt, tilfaller ansvaret Justis- og beredskapsdepartementet. Da kan virksomheten forholde seg til det utpekte departementet i saker etter loven, og det utpekte departementet koordinerer med andre berørte departementer. Det vil gi en mer konsekvent og prinsipielt riktig tilnærming til ansvar og roller som loven legger til henholdsvis departementene og Sikkerhetsmyndigheten som direktorat. Gjør også at Sikkerhetsmyndigheten vil måtte fokusere mer faglig og ressursmessig på enkeltvirksomheter fremfor nasjonale og overordnede forhold.»

UNINETT uttaler:

«UNINETT mener det er positivt og sikkerhetsfremmende at lovforslaget tydeliggjør departementenes ansvar for det forebyggende sikkerhetsarbeidet i sine respektive sektorer, samtidig som mekanismer for tverrsektoriell samordning og informasjonsdeling foreslås styrket. […]

UNINETT mener imidlertid at vurderinger av hvilke virksomheter som omfattes av lovforslaget, det vil si hvem som råder over innsatsfaktorer (informasjon, informasjons systemer, objekter eller infrastruktur) eller driver aktivitet som er av kritisk betydning for nærmere angitte nasjonale funksjoner, kan by på vanskelige utfordringer. Det er for eksempel ikke umiddelbart klart for UNINETT hvilke kriterier som departementene skal legge til grunn for vurderinger av om virksomheter er av vesentlig eller kritisk betydning for disse nasjonale funksjonene. Ettersom det kun er virksomheter av kritisk betydning som foreslås omfattet av loven, er det etter UNINETTs syn viktig at det ikke skapes unødig usikkerhet om hvilke virksomheter som kan tenkes å bli omfattet og hvilke momenter som departementene skal legge til grunn for slike vurderinger og vedtak.

UNINETT mener likevel det er positivt at lovforslaget gir departementene en plikt til å identifisere, holde oversikt over og rapportere til Sikkerhetsmyndigheten (NSM) om vesentlige avhengigheter både i egen og mot andre sektorer, og hvilke virksomheter som er ansvarlige for disse, selv om disse virksomhetene i utgangspunktet ikke omfattes av loven. Dette vil, etter UNINETTs oppfatning, bidra til å etablere et forbedret og mer helhetlig forebyggende sikkerhetsarbeid, både internt i sektorene og på tvers av sektorer.»

7.3.2 Tvisteorgan

Når det gjelder utvalgets forslag om opprettelse av et eget tvisteorgan, er det ulike oppfatninger fra høringsinstansene. Flere private virksomheter er positive til forslaget og ser dette som en viktig rettssikkerhetsgaranti i saker som gjelder vedtak om å underlegge virksomheter til sikkerhetsloven. Offentlige myndigheter er i all hovedsak negative til forslaget.

Abelia ser i likhet med utvalget behov for at det opprettes et tvisteorgan slik at det finnes tilstrekkelige rettssikkerhetsgarantier for virksomheter som underlegges loven, som rett til å bli hørt og påklage. Imidlertid savner Abelia tre forhold i drøftelsen om organets plassering og sammensetning:

> «For det første om også underleverandører til *grunnleggende nasjonale funksjoner* vil ha adgang til å klage til tvisteorganet. Igjen mangler vurderinger rundt konsekvenser for næringslivet. For det andre om det samme tvisteorganet skal behandle både militære og sivile saker. Vi mener det bør gjøres en særskilt drøfting av om det er heldig at samme organ vurderer både militære og sivile saker. Et skille mellom militære og sivile saker gjøres på flere andre områder, blant annet når det gjelder sikkerhetsklarering av personell hvilket lovens paragraf 8-4 og 8-5 reflekterer. Og for det tredje, dersom tvisteorganet skal oppfattes som objektivt, og ha en reell rettssikkerhetsgaranti, mener Abelia i likhet med NHO og NSR at minst ett av medlemmene må komme fra det private næringsliv.»

BDO uttaler:

> «I teorien bør tvister mellom departementer kunne løses uten et eget tvisteorgan. Empiri de siste årene har imidlertid vist med all tydelighet at det i praksis dessverre ikke er tilfelle innen objektsikkerhet – selv ikke når toppledelsen ved Statsministerens kontor involveres for å finne løsninger/kompromisser. Å fortsette som før, med sterke og langvarige stridigheter som sprer seg helt ut i ytre etat og virksomheter i sektorer, er ingen tjent med. Det er også slik at det av og til er viktigere å få en avklaring, enn akkurat hvem som får medhold eller ikke i avklaringen, og det vil et slikt tvisteorgan i hvert fall bidra til.»

Direktoratet for e-helse ser et behov for å tydeliggjøre og konkretisere mandatet og funksjonen for klageordningen og tvisteorganet, slik at disse kan være på plass når nytt lovverk trer i kraft.

E-CO Energi AS er skeptisk til ordningen med tvisteorgan, da dette vil kunne undergrave ansvarsprinsippet, og uttaler:

> «Tvister mellom departementer bør kunne løses uten et slikt organ på ordinær måte mellom departementene uten å måtte skyve på og synliggjøre beslutninger til et «kollegialt» Tvisteorgan.»

Energi Norge uttaler:

> «Tverrsektoriell koordinering og informasjonsutveksling er fornuftig, men kan medføre uklare rolle- og ansvarsforhold, økt byråkratisering og manglende kostnadskontroll. Energi Norge vil derfor anbefale at dagens klare rolle- og ansvarsfordeling videreføres. [...]
>
> […]
>
> Energi Norge mener at det endelige ansvaret for sikkerhet og beredskap må ligge hos sektormyndighetene og at NSM/Sikkerhetsmyndigheten ikke bør ha anledning til å overprøve dette. Dermed faller også behovet for et eget tvisteorgan, som skal ta stilling til denne typen uenighet, bort.
>
> For det tilfellet at sektormyndighetenes beslutninger likevel skal kunne overprøves, er det etter Energi Norges oppfatning viktig at det stilles krav om at tvisteorganet settes sammen av medlemmer som også har nødvendig samfunnsøkonomisk kompetanse og relevant sektorkompetanse. […]
>
> Et eventuelt tvisteorgan må under enhver omstendighet være nøytralt og må ha tilstrekkelig kompetanse og øvrige ressurser til å behandle de saker det får seg forelagt på en kompetent og effektiv måte. I forslag til lovtekst fremgår det at tvisteorganets medlemmer skal utpekes av «Kongen». Utvalget foreslår riktignok at tvisteorganet skal ledes fra SMK og at sekretariatsfunksjonen legges til det nye permanente sekretariatet for RSU. Dette er imidlertid ikke bindende, dersom slik myndighet i stedet ønskes delegert til en annen instans/departement. Dette kan i så fall skape utfordringer knyttet til sammensetningen av tvisteorganet og tvisteorganets nøytralitet. […]
>
> [...]
>
> Utvalget har ikke vurdert hvilken faglige kompetanse og ressurser NSM har i dag på de ulike sektorene, og i hvilken grad enheten må styrkes for å ivareta nye oppgaver og funksjoner på tilfredsstillende måte. Et forvaltningsorgan, som ikke ressurs- og kompetansemessig er dimensjonert for oppgaven, kan snarere svekke beredskapen og samfunnssikkerheten enn å styrke den. I tillegg vil det kunne medføre at det går flere saker til tvisteorganet for behandling, noe som vil øke driftskostnadene

for tvisteorganet og forsinke beslutningsprosessene.

[...]

Utvalget har ikke kvantifisert de potensielle kostnadsøkningene som forslaget vil medføre knyttet til etablering og drift av tvisteorganet, økt tilsynsvirksomhet overfor sektormyndighet og virksomheter, nødvendig kompetanse- og ressursoppbygging i NSM, forsinkelser i behandlingsprosessene, konkurransevridende effekter mellom virksomheter, avvikling av virksomheter og tap av arbeidsplasser.»

Forsvarets forskningsinstitutt (FFI) uttaler:

«Det er åpenbart at en sektors vurderinger kan avvike fra NSMs. Dette utfordrer ansvarsprinsippet og NSMs sektorovergripende ansvar. Det vil imidlertid være i strid med ansvarsprinsippet å gi NSM instruksjonsmyndighet overfor andre sektorer, men viktige beslutninger må kunne fattes. Etablering av et tvisteorgan, slik utvalget anbefaler, vil være nødvendig for at sikkerhetsloven skal kunne fylle sin koordinerende funksjon. For at organet skal få tilstrekkelig autoritet, bør det ledes fra Statsministerens kontor.»

Kommunal- og moderniseringsdepartementet uttaler:

«En nærmere presisering av lovens virkeområde vil også bidra til at det blir et mindre behov for å avklare uenigheter mellom sikkerhetsmyndighetene og relevante sektormyndigheter.

[...]

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

Nkom uttaler videre:

«I forhold til å kunne ivareta Sikkerhetsmyndighetens sektorovergripende ansvar etter lovforslaget § 2-2, er Nkom enig i at Sikkerhetsmyndigheten bør ha mulighet til selvstendig vurdering og forslagsrett for utpeking av virksomheter av kritisk betydning slik det foreslås i bestemmelsens fjerde ledd. Nkom mener imidlertid at det er unødvendig og lite formålstjenlig å benytte selvstendig tvisteløsningsorgan som mekanisme ved uenighet mellom Sikkerhetsmyndigheten og ansvarlig departement. Lovforslaget fokuserer gjennomgående på en bred samfunnsmessig tilnærming til sikkerhet med spesiell vekt på samarbeid mellom Sikkerhetsmyndigheten og sektorene, jf. lovforslaget kap 3. Nkom mener uenighet mellom Sikkerhetsmyndigheten og ansvarlig departement når det gjelder utpeking etter § 2-1 bør løses ved drøftelser og regjeringsbehandling som en egnet og allerede etablert metode.

[...]

[…] Nkom mener at det er unødvendig og lite formålstjeneslig å benytte selvstendig tvisteløsningsorgan som mekanisme ved uenighet mellom departementene. Her bør man benytte den ordinære forvaltningsrutinen med drøftelser innad i regjeringsapparatet. Mandatet til tvistorganet bør således begrenses til behandling av konflikter mellom private virksomheter og offentlige myndigheter.»

Nasjonal sikkerhetsmyndighet (NSM) mener sikkerhetsmyndigheten og tvisteorganet må gis en sterk lovforankret autoritet for å kunne styre og beslutte med bindende virkning overfor øvrige aktører. Dette er en nødvendig forutsetning for å sikre en enhetlig implementering av lovforslaget:

«Lovforslaget etablerer et tvisteorgan som skal ta standpunkt til uenighet knyttet til praktisering av enkelte av lovforslagets bestemmelser.

Basert på erfaringer med gjeldende sikkerhetslov ser NSM det som hensiktsmessig at det etableres en mekanisme for å avgjøre saker hvor det er uenighet. En suksessfaktor for forslaget er at Tvisteorganet gis nødvendig beslutte nde myndighet. Med det handlingsrom lovforslaget gir, både til departementene, sektormyndighetene og virksomhetene vil det være av avgjørende betydning for å sikre en harmonisert praksis at de avgjørelser tvisteorganet fatter er bindende for så vel forvaltningen som for private rettssubjekter.»

NITO mener tvisteorganet vil kunne tjene som en rettssikkerhetsgaranti, og at tvisteorganet ved uenighet mellom myndigheter skal sørge for en uavhengig avgjørelse. NITO vil understreke behovet for at tvisteorganet besitter tilstrekkelig kompetanse innenfor fagområdene IKT og sikkerhet. NITO etterlyser derfor en klargjøring av hvilken sammensetning, og hvilke kriterier, tvisteorganet skal styre etter.

Norges Bank mener at forslaget til klage- og tvisteløsninger (jf. forslag til §§ 2-6 og 2-7) er en ordning som kan fungere godt, og både ivareta sektorenes respektive behov og de mer overordnede behov for helhetlig og koordinert sikkerhetsarbeid på tvers av sektorene, og uttaler:

> «Klageordningen fastsatt i § 2-6 retter seg mot vedtak etter loven. Det kan eventuelt vurderes om det i lovens forarbeider bør sies noe om hvem som kan påklage vedtak etter sikkerhetsloven, dvs. hvem som har rettslig klageinteresse.»

NVE er skeptiske til de skisserte mekanismene for å møte en forventet uenighet mellom sikkerhetsmyndigheten og sektormyndighetene om oppfølging av loven. Etter NVEs syn er disse både unødvendige og fremmede i norsk forvaltning:

> «NVE er enig i at enda mer samarbeid, samspill og samhandling er nødvendig for å heve sikkerhetsnivået mot terror og sabotasje totalt sett.
>
> Derfor er vi også skeptiske til de mange skisserte mekanismene for å møte det vi oppfatter som en forventet uenighet om oppfølging av loven i sektorene. Se for eksempel opprettelsen av tvisteorgan § 2-7, avtaleregulering av sektormyndighetens plikter gjennom samarbeidsavtaler (§ 3-2), adgang for sikkerhetsmyndigheten til å gi pålegg til sektormyndigheten (§ 3-6 tredje ledd) og rett for sikkerhetsmyndigheten til å bringe såkalte unnlatelser fra sektormyndigheten inn for Tvisteorganet, jf § 2-1 (utpeking) og § 7-1 (utpeke skjermingsverdig objekt).
>
> Etter vårt syn blir det for mange slike mekanismer. NVE mener at disse er unødvendige og fremmed i norsk forvaltning. De utfordrer også ansvarsprinsippet. Det følger av Grunnloven § 3 at det er Regjeringen med ansvarlig statsråd som har ansvaret. NVE mener dessuten disse mekanismene gir motsatt signaler enn det positive fokuset på tett samhandling og samvirke for sikkerhet som er gjennomgående i NOU'en. Vi tror det samlede sikkerhetsarbeidet er best tjent med at samhandlingen mellom myndigheter skjer på mest mulig «ordinær» måte, og at uenigheter løses enten ved regjeringsbehandling eller ved megling etter modell av innsigelsesinstituttet i plan- og bygningsloven. Private virksomheter som blir underlagt sikkerhetsloven må kunne klage på dette, men også her vil alminnelige klageregler etter forvaltningsloven etter NVEs syn være tilstrekkelig.
>
> Vi foreslår at behovet for denne typen mekanismer for håndtering av uenighet vurderes på nytt. God samhandling mellom sektorene bør fremheves som den bærende tilnærmingen og eventuell uenighet bør løses gjennom eksisterende ordninger.»

Norsk olje og gass uttaler:

> «Det foreslås av Utvalget å opprette et tvisteorgan for overprøving av vedtak etter loven, jf. lovutkastet § 2-6. Ettersom det i lovutkastet er henvist til forvaltningsloven kapittel VI for selvstendige rettssubjekters klageadgang etter loven, legger vi til grunn at tvisteorganet kan overprøve alle sider av vedtaket. Norsk olje og gass foreslår at det bør fremgå av lovforslaget at virksomheten alltid har partsrettigheter i en klagesak for tvisteorganet.
>
> Kongen i statsråd er overordnet det enkelte departement og det fremstår noe underlig at sikkerhetsmyndigheten kan overprøve departementets avgjørelse ved å bringe saken inn for avgjørelse i tvistenemnda jf § 2-1 fjerde ledd. Dersom dette blir løsningen bør virksomheten likefullt ha partsrettigheter også i slike saker.
>
> Det synes fornuftig at tvisteorganet skal sammensettes av medlemmer med sikkerhetsfaglig kompetanse innen personvern, jf. lovutkastet § 2-7. Norsk olje og gass mener at et tvisteorgan i den enkelte sak også bør ha medlemmer som har særskilt kompetanse innenfor den sektor som klagen gjelder.»

NHO ber om at tvisteorganet blir satt med minst en fast representant fra det private næringsliv, slik at private virksomheters interesser i klagesaker blir ivaretatt på en forsvarlig måte.

Næringslivets Sikkerhetsråd (NSR) støtter at det opprettes et tvisteorgan slik at det finnes tilstrekkelige rettssikkerhetsgarantier for virksomheter som underlegges loven, som rett til å bli hørt og påklage. For at tvisteorganet skal oppfattes som objektivt, og ha en reell rettssikkerhetsgaranti, mener NSR at det er avgjørende at minst ett av medlemmene kommer fra det private næringsliv.

Olje- og energidepartementet uttaler om forslaget til tvisteorgan:

> «Utvalget viser til at en utfordring med dagens system er at det ikke finnes noen form for mekanisme for å avklare uenigheter mellom

sikkerhetsmyndighetene og relevante sektormyndigheter. OED viser til at uenighetssaker mellom sektorer normalt skal løftes opp til regjeringsbehandling i siste instans. Dette for å ivareta statsrådenes sektoransvar, og for å sikre at slike beslutninger tas på høyest mulig nivå med alle sider godt belyst. Vi mener dette må være løsningen også i saker under sikkerhetsloven. Et tvisteorgan kan ikke og bør ikke erstatte de etablerte konstitusjonelle mekanismene for regjeringens avgjørelser.»

Samferdselsdepartementet uttaler:

«I dagens sikkerhetslov finnes det ingen form for mekanisme for å avklare uenigheter mellom sikkerhetsmyndigheter og relevante sektormyndigheter. Utvalget anbefaler derfor at det etableres et eget kollegialt tvistorgan som gis myndighet til å treffe vedtak i klagesaker, bestående av fem medlemmer med kompetanse innen sikkerhetsfaget, personvern og rettssikkerhet. SD tror tvisteløsningsfunksjonen kan fungere bra som en form for rettsikkerhetsgaranti for private virksomheter som blir underlagt loven, og at det kan sikre likebehandling på tvers av sektorene. Det bør imidlertid vurderes nærmere om det finnes bedre og allerede etablerte organer for å løse eventuelle tvister mellom myndigheter.»

Statkraft mener det er avgjørende med tydelige ansvarslinjer. Endelig beslutningsmyndighet bør derfor ligge hos sektormyndigheten, ikke hos et tvisteorgan som det ikke er behov for.

UNINETT ser det som positivt at enkeltvedtak som fattes i medhold av loven kan klages inn for et uavhengig tvisteorgan, spesielt mht. hvilke virksomheter som departementene bestemmer skal omfattes av pliktene i den nye sikkerhetsloven.

Utenriksdepartementet ser at det kan være behov for raskt å kunne avklare uenigheter om praktiseringen av loven, men stiller spørsmål ved behovet for å etablere frittstående parallelle strukturer innen statsforvaltningen:

«Sikkerhetsloven er en offentligrettslig lov som skal utøves av de kompetente organer loven utpeker, og det kan stilles spørsmål ved behovet for å etablere særlige organer for å løse tvister. Det stilles også spørsmål ved om det er heldig å knytte et organ med formell beslutningsmyndighet til rene konsultasjonsorganer som RSU eller kriserådet. Dette vil kunne forsterke en allerede utbredt misforståelse innen statsforvaltningen om at disse organene kollektivt har større beslutningskompetanse enn det deltakerne besitter hver for seg.

Uavhengig av organets funksjon er UD skeptisk til benevnelsen «tvisteorgan» da dette kan gi en noe misvisende assosiasjon til et domstolslignende organ.»

7.4 Departementets vurdering

7.4.1 Departementenes ansvar og myndighet etter loven

Departementet er enig i utvalgets forslag når det gjelder fastsettelsen og fordelingen av departementenes myndighet og ansvar etter loven og sikkerhetsmyndighetens ansvar og oppgaver. De ulike rollene er etter departementets syn gjort klarere enn de er etter någjeldende lov. Det er viktig for å tydeliggjøre departementenes ansvar at ansvarsprinsippet eller sektorprinsippet blir mer rendyrket, samtidig som oppgaven med å ivareta helhetlig og sektorovergripende sikkerhet, fortsatt ligger til sikkerhetsmyndigheten som fagmyndighet.

I forslaget til kapittel 2 om ansvar og myndighet fastslås prinsippet om departementenes sektoransvar for forebyggende sikkerhetsarbeid. Det foreslås samtidig at sikkerhetsmyndigheten har det sektorovergripende ansvaret for å holde oversikt over det helhetlige bildet og sørge for at balanserte sikkerhetstiltak på tvers av sektorer iverksettes og vedlikeholdes. En rekke sektorer er gode når det gjelder ivaretakelse av forebyggende sikkerhet. Det er viktig at forholdene legges til rette for at dette kan opprettholdes. For å følge opp det ansvaret departementene får etter loven, vil det imidlertid være behov for kompetanseheving på enkelte områder innenfor forebyggende sikkerhetsarbeid.

Høringsuttalelsene gir i hovedsak uttrykk for enighet om forslaget til fordeling av ansvar og myndighet mellom departementene på den ene siden og sikkerhetsmyndigheten på den andre, jf. eksempelvis uttalelsene gjengitt ovenfor fra *Nkom*, *Norges Bank* og *Fylkesmannen i Rogaland*. En viktig oppgave for departementene er å treffe vedtak om hvilke virksomheter innenfor eget myndighetsområde som sikkerhetsloven skal gjelde for, jf. § 1-3 og omtalen i kapittel 6.4.3.

7.4.2 Sikkerhetsmyndighetens ansvar for forebyggende sikkerhetsarbeid

Sikkerhetsmyndighetens ansvar etter loven framgår av forslaget til § 2-2. Sikkerhetsmyndigheten har det sektorovergripende ansvaret for å se til at gjennomføring av forebyggende sikkerhetsarbeid i virksomhetene skjer i samsvar med loven.

Utfordringen i en slik løsning vil være hvordan og i hvilken grad sikkerhetsmyndighetens faglige vurderinger skal kunne gripe inn og påvirke sektormyndigheter, uten å skape uklarheter eller rokke ved fastlagte ansvarsforhold. Dette er søkt løst gjennom en nærmere beskrivelse av oppgavene til sikkerhetsmyndigheten i § 2-2. Det konstitusjonelle ansvaret vil uansett ligge hos fagdepartementet. Dette gjelder også så langt aktuell sektor har fått delegert tilsynsansvaret i egen sektor.

Det framgår av departementets lovforslag at sikkerhetsmyndigheten skal påse at det føres tilsyn med at virksomheter oppfyller krav til forebyggende sikkerhetsarbeid. Det enkelte fagdepartement kan imidlertid bestemme at sektormyndigheter kan føre tilsyn med virksomheter som er omfattet av loven innenfor sin sektor. Departementet presiserer at det bør legges opp til utstrakt samarbeid mellom sikkerhetsmyndigheten og sektormyndigheter når det gjelder tilsyn etter loven, se for øvrig kapittel 8.

Etter § 2-2 bokstav c i departementets lovforslag skal sikkerhetsmyndigheten innhente og vurdere informasjon som har betydning for forebyggende sikkerhetsarbeid. Departementet understreker at sikkerhetsmyndigheten er avhengig å få tilgang til et bredt informasjonsgrunnlag om trusselbildet og hendelser fra de ulike virksomhetene og sektorene for å kunne vurdere og analysere sikkerhetstilstanden innenfor lovens virkeområde, se for øvrig kapittel 7.4.3.

Videre skal sikkerhetsmyndigheten gi informasjon, råd og veiledning om sikkerhetsfaglige spørsmål, og dessuten utarbeide og gjøre tilgjengelig generell informasjon om loven og praktiseringen av den. For å ha tilstrekkelig oversikt over sikkerhetstilstanden, skal sikkerhetsmyndigheten holde en tverrsektoriell oversikt over departementenes identifisering og enkeltvedtak om å legge virksomheter under sikkerhetsloven. Sikkerhetsmyndigheten skal selv treffe tilsvarende vedtak overfor virksomheter som ikke anses for å falle innenfor et departements myndighetsområde.

Departementet har merket seg at de fleste høringsinstansene har sluttet seg til forslaget til systematikk når det gjelder myndighetsutøvelsen. Særlig gjelder dette klargjøringen av ansvarsprinsippet og at det etableres et tydelig sektoransvar. Imidlertid er enkelte høringsinstanser skeptiske til at sikkerhetsmyndigheten skal ha en sektorovergripende rolle og således kunne overprøve fagdepartementets vurderinger. Disse høringsinstansene mener at ansvarsprinsippet må gjelde fullt ut, og at sikkerhetsmyndigheten først og fremst skal være «et veiledende og rådgivende fagorgan for departementet og tilsynsorganene», jf. *NVEs* høringsuttalelse gjengitt ovenfor.

Departementet er ikke enig i at sikkerhetsmyndigheten skal reduseres til et rådgivende organ. Sikkerhetsmyndigheten skal etter departementets mening fortsatt være et fagorgan og ha myndighet innenfor forebyggende sikkerhetsarbeid. Samtidig skal de enkelte samfunnssektorene respekteres, slik at det skal tas hensyn til sektorspesifikke forhold. For at sikkerhetslovens krav skal kunne ivaretas i de enkelte samfunnssektorene er det for eksempel viktig at sikkerhetsmyndigheten bidrar til å sette de kriterier som er nødvendige for delegering av tilsynsansvar til de enkelte sektorer, og at den kan påse at tilsyn innenfor sikkerhetslovens virkeområde blir gjennomført. Nærmere om oppgaver til sikkerhetsmyndigheten er redegjort for i kapittel 8 om tilsyn og i kapittel 9 om generelle krav til forebyggende sikkerhetsarbeid.

BDO gir i sin høringsuttalelse uttrykk for uenighet til forslaget om at sikkerhetsmyndigheten selv skal kunne treffe vedtak om at sikkerhetsloven skal gjelde for virksomheter som ikke anses for å falle innenfor et departements myndighetsområde. *BDO* foreslår at vedtak for disse virksomhetene legges til et departement, for eksempel til Justis- og beredskapsdepartementet. Departementet vil peke på at sikkerhetsmyndigheten skal ha den nasjonale oversikten over virksomheter under sikkerhetsloven og vil være nærmest til å fange opp hvilke virksomheter som vil være utenfor departementenes myndighetsområder. Det antas å gjelde få virksomheter, og departementet ser ingen prinsipielle motforestillinger til å legge denne vedtakskompetansen til sikkerhetsmyndigheten.

7.4.3 Utveksling av trusselvurderinger og annen sikkerhetsinformasjon

Departementet foreslår å videreføre utvalgets forslag til § 2-3. Bestemmelsen gjelder utveksling av trusselvurderinger og annen sikkerhetsinformasjon, og at sikkerhetsmyndigheten skal legge til

rette for tilgang til slik informasjon. Dette omfatter de virksomheter loven gjelder for, der slik informasjon og vurderinger har betydning for virksomhetenes forebyggende sikkerhetsarbeid. Departementet presiserer at det også ligger et ansvar hos virksomhetene for å dele informasjon om sikkerhetstruende virksomhet eller annen relevant sikkerhetsinformasjon med sektormyndigheter, andre virksomheter og myndigheter som har et tjenstlig behov og sikkerhetsmyndigheten. Dette gjelder også utover det som følger av varslingsplikten etter utvalgets forslag til § 4-6. For å kunne gi virksomhetene et best mulig tverrsektorielt risikobilde innen forebyggende sikkerhetsarbeid, jf. beskrivelsen i kapittel 7.4.2, er for eksempel sikkerhetsmyndigheten avhengig av at virksomhetene er villig til å dele relevant informasjon, særlig når det gjelder IKT-hendelser. Viktigheten av deling og utveksling av informasjon nevnes også i samfunnssikkerhetsmeldingen (Meld. St. 10 (2016–2017)), særlig i forbindelse med nasjonalt rammeverk for håndtering av digitale hendelser i kapittel 6.6.2, side 68, og i stortingsmeldingen om IKT-sikkerhet (Meld. St. 38 (2016–2017)). Departementet viser også til utvalgets vurderinger i NOU 2016: 19 kapittel 2.3, og i særmerknaden til § 5-2 på side 262 i NOU 2016: 19 lovforslag, som omtaler samfunnssikkerhetsprinsippet om samvirke og «responsibility to share».

7.4.4 Nasjonal responsfunksjon for alvorlige digitale angrep

Håndtering av digitale angrep eller avdekking av forsøk på dette er blitt en stadig viktigere del av det forebyggende sikkerhetsarbeidet. I forslaget til § 2-4 gis Kongen hjemmel til å utpeke en myndighet som skal drive en nasjonal responsfunksjon for alvorlige digitale angrep (NorCERT i dag) og det nasjonale varslingssystemet for digital infrastruktur (VDI). Departementet legger til grunn vurderingene som ble gjort i Prop. 97 L (2015–2016) kapittel 6.6, side 28 om plassering og ansvar for responsfunksjonen og VDI-systemet hos Nasjonal sikkerhetsmyndighet.

Bestemmelsen presiserer at myndigheten kan behandle personopplysninger i ulike former *når det er nødvendig for* å drive de to funksjonene. Det vises her til de drøftelsene som er gjort over temaet i Prop. 97 L (2015–2016) kapittel 7.4. Det følger av utvalgets særmerknader til lovforslaget § 2-4 at utvalget mente å videreføre gjeldende rett. Ordlyden i utvalgets forslag kan imidlertid tolkes som en innsnevring ved at den knyttet funksjonenes virkeområde tett til sikkerhetslovens virkeområde. Ettersom både responsfunksjonen og varslingssystemet har virkeområder som går utover sikkerhetsloven, mener departementet at utvalgets forslag til ordlyd blir for snevert. Departementet foreslår derfor en videreføring av gjeldende lov § 9 første ledd bokstav e og § 10 a.

7.4.5 Vedtak ved risiko for skadevirkninger for nasjonale sikkerhetsinteresser

Utvalget har foreslått å videreføre hjemmelen til å fatte vedtak i gjeldende § 5 a om varsling og myndighet til å fatte vedtak ved risiko for sikkerhetstruende virksomhet. Departementet er enig med *Utenriksdepartementet* i at utvalgets forslag til skjerping av kravet til sannsynlighet etter gjeldende § 5 a, kan medføre at bestemmelsen mister sin selvstendige funksjon. Departementet har forståelse for at utvalget ut fra bestemmelsens inngripende karakter ønsker å etablere ytterligere rettssikkerhetsgarantier. Bestemmelsen er imidlertid ment å være en sikkerhetsventil, jf. Prop. 97 L (2015–2016) side 19. Bestemmelsen vil eksempelvis kunne benyttes hvor det ikke foreligger andre rettslige grunnlag for å stanse en aktivitet som innebærer en risiko mot nasjonale sikkerhetsinteresser. At vedtaksmyndigheten er lagt til Kongen i statsråd, og skal baseres på råd fra relevante fagmyndigheter, vil sikre at saken er tilstrekkelig godt opplyst, både hva gjelder den konkrete risikoen og hva gjelder hvilke konsekvenser et eventuelt vedtak vil kunne få. Videre vil det sikre at vedtakene dermed er velbegrunnede og proporsjonale ut fra hensynet til nasjonal sikkerhet. Som det framgår av Prop. 97 L (2015–2016) side 21, vil det også måtte vurderes konkret i hvert enkelt tilfelle hvor bestemmelsen vurderes benyttet, hvorvidt vedtaket vil være i overensstemmelse med Grunnloven, menneskerettighetsloven og Norges internasjonale forpliktelser. Departementet har på denne bakgrunn kommet til at det materielle innholdet i gjeldende § 5 a bør videreføres, med nødvendige tilpasninger til den nye loven. Bestemmelsens natur som sikkerhetsventil tilsier at den i likhet med gjeldende § 5 a skal favne vidt, og bør være anvendelig på alle typer aktiviteter som kan innebære en ikke ubetydelig risiko mot nasjonale sikkerhetsinteresser.

7.4.6 Klage- og tvisteløsning og tvisteorgan

Utvalget har foreslått et tvisteorgan, både for å løse klagesaker fra private aktører og for å løse uenighetssaker mellom offentlige myndigheter. Departementet er enig i at private virksomheter

som blir underlagt loven ved enkeltvedtak skal ha en klageadgang. Videre er det viktig at uenigheter på myndighetsnivå blir løst innen en rimelig tidshorisont. Klagesaker fra private og uenigheter mellom offentlige myndigheter er ikke nødvendigvis sammenlignbare sakstyper. Av høringsinstansene har private virksomheter i stor grad sagt seg enige i forslaget om et tvisteorgan, mens offentlige myndigheter er kritiske til forslaget om at sikkerhetsmyndigheten kan klage ansvarlig departement inn for tvisteorganet. Det bryter med ansvarsprinsippet.

I høringen har *Nkom* foreslått at uenigheter bør løses ved drøftelser og regjeringsbehandling som en egnet og allerede etablert metode. Mandatet til tvisteorganet bør derfor begrenses til behandling av konflikter mellom private virksomheter og offentlige myndigheter. *NVE* foreslår at uenigheter løses ved regjeringsbehandling eller ved megling etter modell av innsigelsesinstituttet i plan- og bygningsloven. *NVE* viser til at innsigelsesinstituttet i plan- og bygningsloven er et av de viktigste styringsvirkemidlene staten og fylker har over kommunenes planlegging. Det medfører at en myndighet som har adgangen til det kan forhindre at planen blir gyldig vedtatt med et innhold som er i strid med det hensynet myndigheten har fremmet. NVE peker på at kommunen med andre ord er avhengig av å bli enig med denne myndigheten, eller få saken avgjort i Klima- og miljødepartementet.

Departementet vil bemerke at private virksomheter i utgangspunktet vil ha klagerett etter forvaltningsloven, slik de også har etter sikkerhetsloven i dag. På noen forvaltningsområder er det opprettet uavhengige klageorganer. Utvalget foreslår en modell der tvisteorganet er tilknyttet regjeringens sikkerhetsutvalg. Det kan da stilles spørsmål ved om tvisteorganet framstår som uavhengig. Departementet anser heller ikke at spørsmål om nasjonal sikkerhet er et område som egner seg til å løftes ut til et uavhengig organ.

Uenighet mellom departementer kan by på utfordringer for enhver regjering, ikke bare i sikkerhetsspørsmål. Uenigheter mellom departementer kan heller ikke løses etter samme prosedyre som ordinære klagesaker etter forvaltningsloven.

Med bakgrunn i en samlet vurdering av innspillene i høringen, samt de prinsipielle sidene ved forslaget, har departementet kommet til at utvalgets forslag om å etablere et særskilt tvisteorgan ikke bør følges opp. Departementet foreslår at dagens klageordning etter forvaltningsloven videreføres. Dette vil sikre rettssikkerheten for private virksomheter. Sikkerhetsmyndighetens vedtak etter § 1-3 fjerde ledd og § 7-1 tredje ledd kan påklages til departementet.

Ved at sikkerhetsmyndigheten gis en lovbestemt rett til å foreslå for alle departementene om virksomheter som bør underleggelses sikkerhetsloven, jf. § 1-3 tredje ledd, og om utpeking av objekter og infrastruktur etter § 7-1 sjette ledd, innebærer dette en mulighet for å få løftet eventuelle saker med motstridende interesser eller uenigheter, for at slike saker ikke blir liggende uløst. Dette fordi det til forslagsretten ligger en rett til å bringe saken inn for endelig avgjørelse til det departement som har det overordnede ansvaret for forebyggende sikkerhetsarbeid i sivil sektor eller det departementet som har det overordnede ansvaret for forebyggende sikkerhetsarbeid i forsvarssektoren, jf. Kronprinsregentens resolusjon av 4. juli 2003. Departementet mener at man på denne måten kan sikre den gode intensjonen til utvalget som lå til grunn for forslaget om et tvisteorgan.

Fordelen med departementets forslag til løsning er at de ordinære og kjente forvaltningsrettslige prinsipper for klagebehandling kan følges, samtidig som det kan etableres mekanismer som gjør at sikkerhetsmyndighetens sektorovergripende rolle kan styrkes.

8 Tilsyn

8.1 Gjeldende rett

Nasjonal sikkerhetsmyndighet (NSM) fører tilsyn med sikkerhetstilstanden i virksomheter som er underlagt sikkerhetsloven, jf. § 9 første ledd bokstav c:

> «[Nasjonal sikkerhetsmyndighet skal] føre tilsyn med sikkerhetstilstanden i virksomheter, herunder kontrollere at den enkeltes plikter i eller i medhold av loven her overholdes, og eventuelt gi pålegg om forbedringer.»

NSM ivaretar rollen som fagmyndighet og tilsynsmyndighet. NSMs rolle er nærmere beskrevet i kapittel 7 ovenfor.

Et hovedmål med NSMs tilsyn, som en viktig del av det forebyggende sikkerhetsarbeidet, er å avdekke sårbarheter og andre behov for forbedring av virksomhetenes forebyggende sikkerhetsarbeid og vurdere den enkelte virksomhets sikkerhetstilstand. NSMs tilsyn gjennomføres i dag som styringssystemrevisjon som understøttes av fagrevisjoner, med utgangspunkt i standarden NS-EN ISO 19011.

Tilsyn er en myndighetsutøvelse og må gjennomføres med nødvendig uavhengighet til sikkerhetsarbeidet som undersøkes. NSM gir derfor ikke råd samtidig som et tilsyn gjennomføres.

Informasjon fra tilsyn benyttes i utgangspunktet som grunnlag for forbedringer av den forebyggende sikkerheten i den enkelte virksomhet, men tilsynserfaringer benyttes også i forbindelse med risikovurderinger for å forbedre sikkerhetstiltak og sikkerhetsarbeid, og for videreutvikling av tilsynsvirksomheten og forbedring av rådgivningsarbeidet.

Som utgangspunkt innehar NSM tilsynsfunksjonen innen alle fagområder knyttet til forebyggende sikkerhetstjeneste etter loven. Innenfor objektsikkerhet er ordningen noe annerledes, se NOU 2016: 19, side 135.

For objektsikkerhet er tilsynsansvaret fordelt mellom NSM og sektortilsyn med ansvar for forebyggende sikkerhet i sin sektor. NSM fører tilsyn med at utvelgelse og klassifisering av skjermingsverdige objekter skjer i henhold til bestemmelser gitt i og i medhold av sikkerhetsloven, jf. forskrift om objektsikkerhet § 4-3 *Tilsyn og påleggskompetanse.*

I de tilfeller hvor det i sektorlovgivning foreligger relevante og tilstrekkelige bestemmelser, og det er etablert et tilsynsorgan, vil det være dette tilsynsorganet som fører tilsyn med at de iverksatte sikkerhetstiltakene hos objekteierne tilfredsstiller de funksjonelle kravene i objektsikkerhetsregelverket.

For andre objekter utpekt som skjermingsverdige, vil NSM ivareta tilsynsfunksjonen.

NSM skal i henhold til forskriften § 4-3 andre ledd siste punktum føre et overordnet tilsyn som «sikrer implementeringen av sektorovergripende harmoniserte sikkerhetstiltak».

8.2 Utvalgets forslag

Sikkerhetsutvalget har vurdert hvordan det skal føres tilsyn med etterlevelsen av ny lovgivning.

Utvalget anbefaler at den ansvarsfordeling som er beskrevet i kapittelet om ansvar og myndighet (NOU 2016: 19 kapittel 2.2, side 19–20) bør etableres også for tilsyn. Utvalget anbefaler en tilsynsmodell som skal ivareta en målsetting om en helhetlig og tverrsektoriell tilnærming til forebyggende sikkerhet, samtidig som den skal ivareta hensynet til den enkelte samfunnssektors særegenheter. Utvalget skriver i NOU 2016: 19, side 19:

> «I samfunnssektorer hvor det eksisterer sektormyndigheter med tilsynsansvar for forebyggende sikkerhetsarbeid, bør disse myndighetene også gjennomføre tilsyn med virksomheter som omfattes av den nye loven. Samtidig må Nasjonal sikkerhetsmyndighet ha en sentral rolle overfor de enkelte sektormyndigheter for å sikre en helhetlig tilnærming til det forebyggende sikkerhetsarbeidet.»

Utvalget har vurdert om det vil være hensiktsmessig å skille mellom tilsynsoppgaver og rollen

som fagmyndighet, og skriver i NOU 2016: 19, side 139:

> «Utvalget foreslår at funksjonen Sikkerhetsmyndigheten på samme måte som i dag blir organisert etter en tradisjonell integrert modell, hvor flere roller ivaretas innenfor samme organisasjon».

Videre skriver utvalget på side 120 at en av utfordringene med dagens sikkerhetslovgivning er

> «knyttet til mangelfull formalisering og/eller praktisering av samhandlingen mellom tilsynsregimet etter sikkerhetsloven og de ulike tilsynsregimene etter annet relevant sektorregelverk. Utvalgets målsetting med reguleringen av ansvars-, myndighets- og tilsynsansvar etter loven er å legge til rette for en god samhandling mellom de sentrale aktørene i forebyggende sikkerhet, på tvers av samfunnssektorene. En slik samhandling er helt avgjørende for at det forebyggende sikkerhetsarbeidet i Norge skal få full effekt, slik utvalget ser det.
>
> [...]
>
> En av de mest sentrale problemstillinger som en regulering skal omfatte, er ansvarsfordelingen mellom ulike aktører. Det er viktig å tydeliggjøre hvilke plikter og rettigheter som følger ulike myndigheter, ulike statlige virksomheter og private aktører. I forbindelse med regulering av forebyggende sikkerhet for grunnleggende nasjonale funksjoner, vil graden av sektorautonomi sett opp mot behovet for en helhetlig nasjonal sikkerhetsstyring stå sentralt.
>
> [...]
>
> En [...] grunnleggende problemstilling er hvordan tilsynsfunksjonen etter loven bør innrettes for å både kunne ivareta den enkelte samfunnssektors særegne behov og samtidig ivareta behovet for en helhetlig og sektoroverg ripende tilnærming til forebyggende sikkerhet. I relasjon til denne [problemstillingen] er også spørsmål om hvilke myndighetsaktører som bør kunne stille krav til, og komme med pålegg overfor, virksomheter underlagt loven. Skal noen, og i så fall hvem, ha myndighet til å påpeke behov for endringer i sikkerhetsnivå, og hvordan skal tiltak på tvers av samfunnssektorer og virksomheter koordineres slik at tiltak blir iverksatt der det er mest samfunnsøkonomisk lønnsomt.»

Utvalget har vurdert ulike alternativer for hvordan tilsynsfunksjonen etter den nye loven bør innrettes. Ett alternativ er å ha en sentral tilsynsmyndighet, med tilsynsansvar for alle virksomheter som omfattes av loven. En slik tilnærming vil i stor grad kunne legge til rette for en helhetlig tilnærming til forebyggende sikkerhet, og sikre et harmonisert sikkerhetsnivå, på tvers av ulike virksomheter og ulike samfunnssektorer.

På den andre siden vil en sentral tilsynsmyndighet i liten grad ha den bransjespesifikke kunnskapen som er nødvendig for å forstå de ulike samfunnssektorenes særegenheter og behov. En annen ulempe vil være at virksomhetene i de ulike samfunnssektorene vil bli utsatt for dupliserende tilsyn fra tilsynsmyndigheter med like, eller lignende, målgrupper og formål.

Et annet alternativ utvalget har vurdert, er hvorvidt tilsynsfunksjonen etter loven bør legges direkte til de enkelte sektortilsynene, og at sikkerhetsmyndigheten gis en rent koordinerende funksjon opp mot de ulike sektortilsynene. En fordel med et slikt delegert tilsyn er at dette vil være i tråd med nærhetsprinsippet og ansvarsprinsippet.

Det vil også kunne bidra til å legge til rette for at tilsynsobjektene ikke utsettes for dupliserende tilsyn.

En delegert tilsynsmyndighet, i tråd med ansvarsprinsippet, innebærer videre at man vil kunne få et helhetlig eierskap til hele sektorens sikkerhetsarbeid, samlet i ett tilsyn. Andre sikkerhetsfaglige organer vil med en slik løsning i liten grad kunne komme inn fra sidelinjen og diktere sektorenes sikkerhetsarbeid med tilsyn og pålegg. Videre vil delegert tilsynsmyndighet være i tråd med nærhetsprinsippet. De som tar avgjørelsene har dermed trolig bedre kjennskap til virksomhetene enn en sentral sikkerhetsmyndighet.

Ulempen med et slikt rendyrket delegert tilsyn, er at det vil kunne bli en rekke ulike tilnærminger og standarder for tilsyn av sikkerhetsarbeidet rettet mot tilsiktede handlinger i de ulike samfunnssektorene. Det vil også kunne vanskeliggjøre den helhetlige tilnærmingen til forebyggende sikkerhet på tvers av samfunnssektorene, som loven for øvrig legger opp til.

Utvalget har kommet til at det beste vil være å etablere en tilsynsmodell som både ivaretar målet om en helhetlig og tverrsektoriell tilnærming til forebyggende sikkerhet, samtidig som samfunnssektorenes særegenheter og behov ivaretas i tilstrekkelig grad.

I samfunnssektorer der det finnes sektormyndigheter med tilsynsfunksjoner som omfatter beskyttelse av informasjon, objekter eller infra-

struktur, bør disse føre tilsyn med virksomheter som omfattes av loven i den aktuelle sektor. Hvorvidt det finnes relevante og tilstrekkelig kompetente sektormyndigheter i den aktuelle sektor, bør etter utvalgets oppfatning avgjøres av det enkelte fagdepartement, i tett samarbeid med sikkerhetsmyndigheten.

I samfunnssektorer der det ikke finnes slike sektormyndigheter, eller de aktuelle sektormyndighetene ikke innehar den kompetansen som er nødvendig for å ivareta tilsynsfunksjonen etter loven, bør tilsynsansvaret legges til sikkerhetsmyndigheten.

For å sikre en helhetlig, samordnet og tverrsektoriell tilnærming til forebyggende sikkerhet foreslår utvalget at sikkerhetsmyndigheten gis myndighet til å føre tilsyn med sektormyndigheter som er tillagt tilsynsansvar etter loven.

For departementsfelleskapet bør sikkerhetsmyndigheten, som i dag, ha ansvaret for å føre tilsyn med departementenes etterlevelse av loven. En slik tilnærming forutsetter et tett og nært samarbeid mellom sikkerhetsmyndigheten og de aktuelle sektormyndighetene. Utvalget foreslår å lovfeste en samhandlingsplikt mellom sikkerhetsmyndigheten og aktuelle sektormyndigheter. Denne samhandlingen foreslås formalisert gjennom en samarbeidsavtale som nærmere fastlegger samhandlingen. Det kan her tenkes løsninger der forholdet mellom sikkerhetsmyndigheten og sektormyndigheten kan variere på ulike fagområder. En slik avtale kan også regulere sektormyndighetenes bruk av kompetanse fra sikkerhetsmyndigheten på enkelte områder, eksempelvis informasjonssikkerhet.

For å ivareta sitt ansvar som sektorovergripende myndighet, bør sikkerhetsmyndigheten gis myndighet til å utarbeide grunnleggende kriterier for hvordan tilsyn etter loven skal innrettes og gjennomføres. Med et delegert tilsynsansvar i enkelte samfunnssektorer vil det være nødvendig med slike grunnleggende kriterier for å sikre en mest mulig enhetlig tilnærming i de ulike sektorene.

Sikkerhetsmyndigheten bør også ha en sentral rolle i opplæringen av tilsynspersonell hos de relevante sektortilsynene, slik at personellet har den nødvendige sikkerhetsfaglige kompetanse for gjennomføring av tilsyn etter loven.

Sikkerhetsmyndighetens ansvar for å ha et sektorovergripende perspektiv, forutsetter tilgang til informasjon om sikkerhetstilstanden i de ulike samfunnssektorene hvor de selv ikke har et direkte tilsynsansvar. Utvalget foreslår derfor en plikt for sektormyndigheter med tilsynsansvar etter loven til å orientere sikkerhetsmyndigheten om hovedfunn fra gjennomførte tilsyn. En slik rapporteringsplikt fra sektormyndighetene til sikkerhetsmyndigheten, vil kunne innebære noe økt ressursbruk. Der det gjøres funn av betydning av sektormyndigheten, vil dette sannsynligvis uansett måtte dokumenteres, og det antas derfor at den økte ressursbruken vil være beskjeden. Dersom virksomhetene ikke oppfyller sine plikter etter loven, bør tilsynsmyndighetene ha adgang til å gi pålegg om gjennomføring av tiltak.

For samfunnssektorer hvor det finnes relevante sektormyndigheter med tilsynsansvar, vil påleggsmyndigheten tilligge den aktuelle sektormyndigheten. Utvalget foreslår også at sikkerhetsmyndigheten gis påleggsmyndighet overfor de sektormyndighetene som har tilsynsansvar etter loven.

Formålet med en slik påleggsmyndighet er å kunne gripe inn overfor en sektormyndighet dersom det skulle vise seg at sikkerhetsnivået i den aktuelle samfunnssektoren utvikler seg på en utilfredsstillende måte.

Slik utvalget ser det, er tilsynsmyndighetens virkemiddelportefølje etter dagens sikkerhetslov ikke tilfredsstillende overfor virksomheter som ikke følger opp kravene etter lov og forskrift. Tilsynsmyndigheten har i medhold av dagens lov § 9 første ledd bokstav c myndighet til å gi pålegg om forbedringer dersom avvik avdekkes. Dersom slike pålegg ikke følges opp av den enkelte virksomhet, er anmeldelse det eneste virkemidlet tilsynsmyndigheten har tilgjengelig. Terskelen for å gå til anmeldelse av en virksomhet vil i de fleste tilfeller være høy. Utvalget mener derfor at tilsynsmyndighetens virkemiddelportefølje bør utvides ved at det gis myndighet til å ilegge tvangsmulkt dersom det avdekkes brudd på regelverket, eller der pålegg ikke følges opp innen en gitt tidsfrist. I nærmere angitte tilfeller, bør tilsynsmyndigheten også kunne ilegge overtredelsesgebyr ved brudd på regelverket. På samme måte som for påleggsmyndigheten, foreslår utvalget at myndigheten til å ilegge tvangsmulkt og overtredelsesgebyr bør legges til den myndigheten som er tildelt tilsynsansvaret. Se nærmere om forslaget til administrative sanksjoner i tillegg til straffebestemmelse i kapittel 15 *Kontroll- og tilsynsordninger.*

8.3 Høringsinstansenes syn

De fleste høringsinstansene er positive til at lovforslaget legger opp til økt samhandling, bedre

arbeidsfordeling, og samordning av tilsyn mellom sikkerhets- og sektormyndigheten.

De fleste er også positive til at det legges opp til økt veiledning og rådgivning fra sikkerhetsmyndigheten, og de ser behovet for og er positive til at sikkerhetsmyndigheten gis et sektorovergripende og koordinerende ansvar.

Enkelte høringsinstanser frykter en dobbeltregulering av sikkerhet i sektorene, og uklarheter knyttet til roller og utøvelse av tilsynsansvaret. Det uttrykkes fra enkelte en skepsis til at sikkerhetsmyndigheten gis kompetanse til å gripe inn i sektormyndighetens ansvar på tilsynsområdet.

Det fremheves at forslaget kan medføre utfordringer knyttet til tilgang på faglig kompetanse, både spesialkompetanse innen sikkerhetsfaget, men også sektorspesifikk kompetanse. Blant annet uttrykker enkelte bekymringer for at man risikerer at det bygges opp dublerende tilsyn og kompetanse, samtidig som det stilles spørsmål ved hvor denne kompetansen skal hentes fra. Enkelte er bekymret for at manglende etterlevelse av lovverket, og ressurs- og kompetanseutfordringer, vil kunne gå ut over oppfølgingen av sikkerhetsarbeidet.

Enkelte høringsinstanser frykter økt byråkratisering og økte administrative kostnader med rapportering fra tilsyn.

8.3.1 Tilsyn med virksomheter

Flere høringsinstanser støtter forslaget om at ansvarlig departement gis myndighet til å bestemme at tilsynsfunksjonen etter loven kan ivaretas av en sektormyndighet med tilsynsfunksjon, som omfatter beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur, jf. forslag til § 3-1 andre ledd.

BDO viser til at det er sektormyndighetene som best kjenner egen sektor, samtidig som utvalgets forslag vil gi sikkerhetsmyndigheten bedre mulighet til å fokusere på sine oppgaver som fagmyndighet innen sikkerhet og tverrsektorielle forhold. *BDO* uttaler også at «[i] tillegg vil en slik fordeling av ansvar og oppgaver i større grad skape eierskap til sikkerhet hos sektormyndigheter som ikke allerede har dette som et ansvar».

Arbeids- og sosialdepartementet er også enige i utvalgets tilnærming, og poengterer i likhet med *BDO* at tilsynet i sektorene best kan ivaretas av en sektormyndighet med inngående kunnskap om sektoren. Arbeids- og sosialdepartementet uttaler videre at

> «[departementet] er enig i utvalgets vurdering av at det er behov for en sterkere sentral koordinering og deling av informasjon og kunnskap om aktuelle trusselbilder og forebygging. Dette vil styrke både sektortilsynene og virksomhetenes forutsetning for å følge opp de plikter som følger av sikkerhetsloven. […]
>
> […]
>
> Vi er også prinsipielt enig i utvalgets vurdering av at det er viktig at tilsynet med sikkerhetsloven primært bør ivaretas av sektortilsyn med inngående bransjekunnskap der dette eksisterer i dag, og at kravene i sikkerhetsloven fortrinnsvis bør kunne inkorporeres gjennom de styringssystemer virksomhetene allerede har etablert for sin hovedaktivitet.»

Nasjonal kommunikasjonsmyndighet (Nkom), *Norges vassdrags- og energidirektorat (NVE)*, *Norsk olje og gass*, *Olje- og energidepartementet, Finanstilsynet* og *Telia* støtter alle utvalgets vurdering om at sektormyndigheter med tilsynsansvar for forebyggende sikkerhetsarbeid bør kunne gjennomføre tilsyn i egen sektor med virksomheter som omfattes av loven. *Finans Norge* kommenterer at det for finansnæringen «vil […] være et sterkt ønske om at tilsyn innenfor sikkerhetsområdet integreres i eksisterende tilsynspraksis i regi av bl.a. Finanstilsynet, Norges Bank og Datatilsynet.»

Enkelte høringsinstanser mener at forslaget vil innebære en risiko for at oppfølgingen av sikkerhetstilstanden i sektorene blir svekket ved at det er departementene som bestemmer hvor tilsynskompetansen skal ligge. Det er en bekymring for om departementene innehar tilstrekkelig kompetanse til å vurdere om egen sektormyndighet er kompetent til å gjennomføre tilsyn. Videre framheves det at det ikke vil være hensiktsmessig ressursbruk at sektormyndigheter gis tilsynsmyndighet for hele bredden av fagområder loven er ment å regulere, da dette vil kreve spesialisert kompetanse som det er liten forekomst av i dag.

NSM mener at hensynet til sektorspesifikk kompetanse har blitt tillagt for stor vekt sammenliknet med det sektorovergripende perspektivet. *NSM* viser til at sektorspesifikk kunnskap må balanseres mot blant annet hensynet til effektiv utnyttelse av tilsynsressursene. *NSM* mener også at et samlet og robust fagmiljø best kan ivareta behovet for en helhetlig og tverrsektoriell tilnærming.

NSM peker på at det er fagområder, som for eksempel beskyttelse av sikkerhetsgradert informasjon, krypto og personellsikkerhet, der sektor-

spesifikk kunnskap i mindre grad er relevant. For slike tilfeller bør det vurderes om sikkerhetsmyndigheten gjennom forskrift kan gis enekompetanse til å føre tilsyn.

Samferdselsdepartementet er positive til utvalgets forslag, men ser utfordringer knyttet til vurderingen av kompetansen hos sektormyndighet og sikkerhetsmyndighet. Departementet uttaler blant annet:

> «Det kan også knyttes usikkerhet til om Sikkerhetsmyndighetene vil inneha tilstrekkelig sektorkompetanse til å overta sektormyndighetens tilsynsrolle.»

Flere høringsinstanser er kritiske til at sikkerhetsmyndigheten skal føre tilsyn med sektormyndigheter som er tillagt tilsynsansvar etter loven, slik det foreslås i § 3-1 tredje ledd. Enkelte mener dette vil kunne medføre uklare rolle- og ansvarsforhold, og representere en potensiell konflikt mellom sektormyndighet med tilsynsansvar og sikkerhetsmyndigheten.

Energi Norge uttaler:

> «En tilnærming slik utvalget foreslår er erfaringsmessig kostnadsdrivende og leder ofte til kompetansestrid mellom de ulike sektormyndighetene (inkl. NSM) om myndighet og kostnadsfordeling. Overlappende kompetanse og ansvarsområder bør derfor i størst mulig grad unngås og ansvaret og ressurser tildeles de som har størst nærhet til og kompetanse om utfordringene (nærhetsprinsippet), uten at dette skal kunne overprøves av etater uten denne nærheten og kompetansen.
>
> Slik lovverket nå er formulert, gis NSM utvidede fullmakter til å gjennomføre kontroller som kan påføre sektoren/selskapene ytterligere tilsyn og kontroll. Energisektoren er i dag gjennomregulert og blir gjennom rapporter og tilsyn kontrollert på et svært detaljert nivå av både NVE og DSB.»

Olje- og energidepartementet uttaler:

> «Samtidig kan andre oppgaver være utfordrende, eksempelvis at sikkerhetsmyndigheten skal utarbeide grunnleggende kriterier for tilsyn, ha en sentral rolle i opplæringen av tilsynspersonell, samt føre tilsyn med sektortilsynene.»

NVE er også negative til en slik ordning og viser til at den «vil bryte med ansvarslinjene i forvaltningen hvis sikkerhetsmyndigheten skal føre tilsyn med sektortilsynene.»

Finanstilsynet mener at det vil være både uheldig og uhensiktsmessig at sikkerhetsmyndigheten skal føre tilsyn med sektortilsyn. Fagdepartementene bør alene kunne gi rammer for sektortilsynenes prioriteringer og vurdere om oppgavene som sektortilsynene er tillagt, er utført i tråd med de føringene som er gitt.

Petroleumstilsynet stiller seg også negativt til dette forslaget, og støtter således Finanstilsynets synspunkter. Etter Petroleumstilsynets syn må sikkerhetsmyndighetens rolle begrenses og heller bruke ressurser på samarbeid og faglig bistand til sektormyndighetene. Petroleumstilsynet viser for øvrig også til at ordningen kan medføre potensielle konstitusjonelle konflikter.

NSM deler ikke denne oppfatningen og mener at sikkerhetsmyndighetens mulighet til å vurdere sektortilsynene bør utvides sammenlignet med utvalgets forslag. Som ledd i tilsyn med sektormyndighetenes oppfyllelse av tilsynsrollen i egen sektor må sikkerhetsmyndigheten ha mulighet til å gjennomføre tilsyn med enkeltvirksomheter i sektoren på stikkprøvebasis. Dette må til for å kunne vurdere kvaliteten på sektortilsynenes gjennomføring av tilsyn i egen sektor. NSM mener det bør lovfestes en rett til å føre tilsyn med enkeltvirksomheter.

8.3.2 Sikkerhetsmyndighetens samarbeid med sektormyndigheter

Høringsuttalelsene er gjennomgående positive til at utvalget foreslår å lovfeste en samarbeids- og samordningsplikt, jf. forslagets § 3-2. Videre er høringsinstansene positive til at sikkerhetsmyndigheten skal utarbeide kriterier for tilsyn og forestå opplæring av tilsynspersonell. Enkelte er negative til at sikkerhetsmyndigheten skal kunne medvirke til sektormyndighetenes tilsyn, og mener dette skaper uklart ansvarsforhold. Det er også enkelte kritiske innspill til forslaget til rapportering til sikkerhetsmyndigheten etter gjennomførte tilsyn i sektorene, og at dette fører til uklare ansvarslinjer og økt byråkratisering.

Arbeids- og sosialdepartementet er positive til det samarbeidet lovforslaget legger opp til, og uttaler:

> «Som et ledd i å sikre en helhetlig, samordnet og tverrsektoriell tilnærming til forebyggende sikkerhet peker utvalget på at det er viktig at det etableres et gjensidig forpliktende samarbeid mellom sektormyndighetene og sikker-

hetsmyndigheten. Vi støtter et slikt utgangspunkt. Vi mener imidlertid at det bør jobbes videre med hvordan det skal sikres at et slikt samarbeid skal kunne fungere og at de ulike myndighetene overholder sine oppgaver. Vi mener at godt samarbeid mellom myndighetene bør tuftes på regler som fremmer samarbeid fremfor et system hvor en myndighet skal kunne kontrollere og gi pålegg til den andre myndigheten. Vi er også opptatt av at myndighetene utad overfor virksomhetene i størst mulig grad fremstår enhetlig og med en stemme, i alle fall når det kommer til virkemiddelbruk.»

NVE uttaler:

«NVE mener det er positivt at sikkerhetsmyndigheten skal utarbeide og vedlikeholde grunnleggende kriterier for tilsyn etter loven med forskrifter og forestå felles opplæring av tilsynspersonell, jf. § 3-2 fjerde ledd.

NVE mener at utvalgets forslag i § 3-2 tredje ledd om at det skal utarbeides en «samarbeidsavtale» mellom myndigheten[e] er unødvendig. Samarbeid mellom sikkerhetsmyndigheten og sektormyndigheten må fungere, og vi ser ikke at en formell avtale mellom myndigheter er et egnet virkemiddel for å få dette til. Sikkerhetsmyndigheten har mange oppgave[r] beskrevet i § 3-2 som bør gi grunnlag for godt samarbeid mellom myndighetene.

NVE forstår § 3-2 femte ledd som en mulighet for sikkerhetsmyndigheten til å få erfaring med hvordan sektormyndighetene utøver sitt tilsyn etter sikkerhetsloven. Vi mener det kan være fornuftig, men forutsetningen må være at sektormyndigheten fortsatt har ansvar for tilsynet.»

NSM uttaler om rapporteringsplikten fra sektormyndighet til sikkerhetsmyndighet:

«Parallell rapportering vil kunne skape uklarheter med hensyn til ansvar og roller, med fare for feil og mangler. En god informasjonsflyt mellom virksomhet, sektormyndighet og sikkerhetsmyndighet som gjenspeiler og forankrer sektormyndighetens ansvar og rolle er derfor viktig. Parallell rapportering bør derfor unngås og rapporteringen i linjen opprettholdes.»

Fylkesmannen i Vestfold uttaler:

«Det fremgår videre at NOU 2016:19 peker på behovet for økte krav til hendelsesrapportering til NSM. Felles situasjonsforståelse er en helt sentral evne for å styrke respons og ledelse, men det er vår erfaring at økte krav til rapportering og situasjonsrapportering like mye medfører en merbelastning for lokale og regionale virksomheter, uten at det påvirker den aktuelle situasjon som er under utvikling. Fylkesmannen i Vestfold mener derfor at det må nøye vurderes behovet for krav til rapportering og at det i slike rapporter utvises en nøkternhet til krav om innhold og hyppighet.»

Luftfartstilsynet er i utgangspunktet positive til at sikkerhetsmyndighetens rolle som koordinerende organ styrkes. Tilsynet peker samtidig på at økt rapportering kan medføre økte administrative konsekvenser uten at sikkerheten bedres.

Nasjonal kommunikasjonsmyndighet (Nkom) uttaler:

«Nkom er generelt positive til at Sikkerhetsmyndigheten, ved utførelse av egen tilsynsaktivitet, har en plikt til å samarbeide aktivt med øvrige relevante tilsynsmyndighetene i den enkelte sektor. Bestemmelsens andre ledd er ment å slå fast et prinsipp om koordinering mellom Sikkerhetsmyndigheten og andre myndigheter som måtte ha parallelle tilsynsaktiviteter innen sikkerhet eller andre områder i den enkelte sektor for å lette den totale belastningen for tilsynsobjektene. Nkom mener ordlyden her er for vagt formulert, og at formålet med å lette den totale belastningen burde nevnes eksplisitt.

Nkom har ingen innsigelser mot at det etableres samarbeidsavtaler mellom Sikkerhetsmyndigheten og sektormyndighetene. I og med at langt flere samfunnsaktører og funksjoner enn i dag vil kunne bli underlagt sikkerhetsloven er Nkom også enig i at også at Sikkerhetsmyndigheten bør ha et overordnet ansvar for å sikre grunnleggende kriterier for tilsyn og opplæring til tilsynspersonell.

I bestemmelsens femte ledd er det foreslått en ordning der Sikkerhetsmyndigheten gis mandat til å være med på forberedelser og faktisk gjennomføring av tilsyn sammen med ansvarlig sektormyndighet. Dette er ment som en «sikkerhetsventil». Lovens øvrige oppbygning er at den utøvende funksjonen som tilsynsmyndighet er lagt til sektorene i tilfellene der det allerede eksisterer kompetent offentlig myndighet. Sikkerhetsmyndigheten skal først

og fremst påse at sektormyndighetene følger opp tilsynsansvaret. Nkom mener forslaget med en slik «sikkerhetsventil» er lite formålstjenlig når det gjelder å etablere klare ansvarsforhold og ansvarliggjøring mellom offentlige myndigheter og uheldig i forhold til å fremstå enhetlig utad overfor den enkelte virksomhet. Dersom det er uklarheter eller oppstår uenighet mellom Sikkerhetsmyndigheten og sektormyndighet vedrørende gjennomføring av tilsyn etter loven, mener Nkom dette må søkes rettet innen ordningen med Sikkerhetsmyndighetens tilsyn med departementene eller annen sektormyndighet i henhold til § 3-1.»

NSM er enig i at den totale belastningen for tilsynsobjektene bør begrenses, og støtter derfor forslaget om en generell koordineringsplikt for tilsyn.

Når det gjelder sektortilsynenes rapporteringsplikt til sikkerhetsmyndigheten, mener NSM denne er for snevert utformet. NSM viser til at de vil ha behov for gjenpart av alle tilsynsrapporter for at de skal kunne få et godt nok situasjonsbilde for å ivareta sine plikter etter den nye loven.

Oslo politidistrikt støtter en koordineringsplikt mellom tilsynsorganene, men framhever at hensynet bak koordinering først og fremst må være å sikre at flest mulig virksomheter blir kontrollert og at de samlede ressursene blir best mulig utnyttet, framfor å vektlegge i for stor grad at tilsynet virker forstyrrende på tilsynsobjektene.

Oslo politidistrikt uttaler:

«Erfaringsmessig har belastningen for et tilsynsobjekt med sikkerhetstilstanden i virksomheten å gjøre. Samtidig vil en virksomhet med gode rutiner og effektiv sikkerhetstjeneste ikke oppleve et tilsyn som belastende, men som kompetansehevende og motiverende siden det anerkjenner og bekrefter nedlagt innsats. En virksomhet med dårlige rutiner og ineffektiv sikkerhetstjeneste vil kunne oppleve eller beskrive et tilsyn som «ødeleggende» eller «forstyrrende» for aktiviteten i lang tid fremover. Den reelle årsaken til denne opplevelsen skyldes det merarbeidet som oppstår på bakgrunn av tilsynet. Dette er oppgaver som skulle vært utført tidligere, men som virksomheten ikke har, eller har hatt evne og eller vilje til å utføre. Manglende kontroll, eller lang tid siden sist kontroll fra overordnet virksomhet eller sikkerhetsmyndighet er også ofte en medvirkende årsak til manglende fokus og prioriteringer.»

8.3.3 Generelle prinsipper for tilsyn

Det har i høringen i det vesentlige framkommet positive tilbakemeldinger på å lovfeste generelle prinsipper for tilsyn. *Nkom* og *Næringslivets Hovedorganisasjon (NHO)* støtter forslaget til utvalget.

NHO uttaler:

«NHO ser positivt på å lovfeste generelle prinsipper for tilsyn. Næringslivet forventer at alle tilsyn etter loven skal følge hovedprinsippet i § 3-3: Tilsyn etter loven skal planlegges og gjennomføres på en slik måte at tilsynet virker minst mulig forstyrrende på tilsynsobjektenes daglige drift.»

Nkom uttaler:

«Nkom er enig i en overordnet bestemmelse med presisering av de generelle prinsippene for gjennomføring av tilsyn etter loven, herunder også henvisning til forvaltningslovens bestemmelser om taushetsplikt. Dette er viktig for å skape [tillit] i kommunikasjonen mellom den enkelte virksomhet og tilsynsmyndighet.»

NSM støtter i utgangspunktet en tilnærming som tilsier at tilsynet skal planlegges og gjennomføres slik at det i minst mulig grad virker forstyrrende på tilsynsobjektets daglige drift. *NSM* legger videre til:

«NSM slutter seg til denne tilnærmingen, men legger til grunn at bestemmelsen ikke kan benyttes av en virksomhet for å nekte tilsyn gjennomført eller for langvarig utsettelse.»

BDO og *NSM* er imidlertid skeptiske til formålsavgrensningen som framgår av bestemmelsens andre ledd.

BDO uttaler:

«Forslaget fastsetter at opplysninger som tilsynsmyndigheten innhenter som ledd i tilsynsvirksomheten bare skal nyttes i direkte forbindelse med tilsyn.

BDO anser en slik formålsavgrensing som for streng. Det er meget viktig at slike opplysninger kan benyttes av tilsynsmyndigheten også til strategiske analyser av aggregerte opplysninger om tilstanden og utfordringer i en sektor som helhet, om et tverrgående sikkerhetsfaglig tema eller summert på nasjonalt nivå.»

NSM uttaler:

> «Det foreslås i bestemmelsens *andre ledd* at «Opplysninger som tilsynsmyndigheten innhenter som ledd i tilsynsvirksomheten skal bare nyttes i direkte forbindelse med tilsynet». Formuleringen er etter NSMs syn for snever. Det må være mulig for tilsynsmyndigheten (sikkerhetsmyndighet eller sektormyndighet) å samle og analysere tilsynserfaringer til bruk i risikovurderinger, for å forbedre sikkerhetstiltak og sikkerhetsarbeid, herunder videreutvikling av tilsynsvirksomheten, revurdering av gitte sikkerhetsmessige godkjenninger av systemer, samt forbedring av rådgivningsarbeidet. Dersom bestemmelsen blir vedtatt med den foreslåtte ordlyden frykter NSM at dette vil svekke både Sikkerhetsmyndighetens mulighet til å ivareta oppgavene i henhold til § 2-2, samt sektormyndighetenes mulighet for å forbedre sikkerheten i egen sektor.

BDO uttaler også:

> «I tillegg kan bestemmelsen tolkes til at tilsynsorganet heller ikke kan rapportere selv alvorlige funn videre til ansvarlig departement. Det vises til at avgrensningen i forslaget til § 4-6 tredje ledd om hvilke hendelser tilsynsorganet skal/kanrapportere til ansvarlig departement, i denne sammenheng antas å måtte tolkes antitetisk. BDO anser det som meget viktig at tilsynsorganer kan bruke opplysninger fra enkelttilsyn til å foreta strategiske analyser og varsle ansvarlig departementet for sektoren om alvorlige funn hos tilsynsobjektet.»

8.3.4 Stedlige tilsyn

Det har i høringen ikke framkommet innvendinger mot bestemmelsene i § 3-4 som hjemler tilsynsmyndigheters adgangsrett og varsling om gjennomføring av tilsyn.

NSM mener imidlertid at bestemmelsen også bør gi tilsynsmyndigheten tilgang til relevant personell. NSM uttaler:

> «Vi foreslår imidlertid eksplisitt også å tilføye tilgang til å gjennomføre samtaler med virksomhetens personell. Eksempler på slikt personell er ledere, sikkerhetspersonell og øvrig relevante medarbeidere. I enkelte tilfeller har det vært en utfordring å få tilgang til relevant personell, noe som har medført at kvaliteten på den informasjon man har fått tilgang til har blitt redusert, og at utbyttet av tilsynet har blitt mindre enn ønskelig.»

NSM stiller også spørsmål ved hensiktsmessigheten av bestemmelsen i andre ledd, som viser til forvaltningslovens § 15. *NSM* uttaler:

> «Henvisningen til denne bestemmelsen synes lite treffende med tanke på hvordan denne type tilsyn gjennomføres. I anerkjente revisjonsstandarder er det nedfelt en rekke prinsipper for god revisjonsskikk. I tillegg vil alltid prinsippene for god forvaltningsskikk ligge til grunn. Det bør derfor vurderes om henvisningen til forvaltningsloven § 15 er nødvendig.»

Oslo politidistrikt mener at det i forskrift bør framkomme en legitimeringsplikt for tilsynsmyndigheten, og uttaler:

> «Som del av forskrift må det gis bestemmelser om hvilke krav som stilles til legitimering av tilsynsmyndighet. Hensikten er å unngå at noen kan skaffe seg adgang til områder eller opplysninger ved å opptre som falsk tilsynsmyndighet. Tiltaket vil også legge forholdene til rette for tillit mellom tilsynsmyndighet og kontrollert virksomhet.»

8.3.5 Tilsynsmyndighetens behandling av personopplysninger

Den foreslåtte bestemmelsen i § 3-5 hjemler behandling av personopplysninger i forbindelse med tilsyn. *NSM* har uttalt om de utfordringer som følger av bestemmelsens tredje ledd:

> «NSM stiller spørsmål ved hensiktsmessigheten av bestemmelsens tredje ledd. En slik bestemmelse vil vesentlig vanskeliggjøre tilsynsvirksomhet. Tilsyn forberedes i dag i NSMs lokaler og som ledd i dette innhentes informasjon fra virksomheten. Tilsyn kan også gjennomføres papirbasert gjennom for eksempel innhenting av en virksomhets saksdokumenter. Innen enkelte fagområder benyttes også virksomhetsovergripende IKT-systemer. Et effektivt tilsyn fordrer at tilsynsmyndigheten kan gå direkte inn og hente informasjon ut fra disse. NSM vil på denne bakgrunn foreslå at tredje ledd strykes.»

8.3.6 Pålegg

Det har kommet flere høringsinnspill til bestemmelsen om pålegg i utvalgets forslag til § 3-6. Innspillene retter seg mot vilkårene for å kunne gi pålegg. Videre stilles det spørsmål ved hva det skal gis pålegg om. Det er dessuten uttrykt motstand fra enkelte til at sikkerhetsmyndigheten skal kunne gi sektormyndighet med tilsynsansvar nødvendige pålegg for å sikre at lovens formål ivaretas.

BDO uttaler om proporsjonalitetsvurderingen:

> «Forslaget fastsetter at pålegg etter loven bare kan gis dersom det er *utvilsomt* (vår utheving) at tiltaket er nødvendig for å ivareta lovens formål og kostnadene som påføres virksomheten står i et rimelig forhold til det som kan oppnås ved tiltaket.
>
> BDO er enig i at det er viktig at pålegg er relevante og proporsjonale, både av samfunnsøkonomiske hensyn, enkeltvirksomheters økonomiske interesser og personverninteresser. Mange av påleggene som typisk er aktuelle å gi, dreier seg imidlertid ikke om konkrete tiltak etter en fri risikovurdering. Ved f. eks. tilsyn er det normalt slik at det gis pålegg om å «lukke avvik», dvs. sørge for at virksomheten kommer i samsvar med lovens krav – hvordan virksomheten velger å gjøre det, er ikke noe tilsynsmyndigheten skal befatte seg med, annet enn å gi veiledning av generell art. Slik bestemmelsen er utformet kan den gi inntrykk av at det ikke kan gis pålegg om å lukke avvik fra kravene, med mindre det er utvilsomt at det er nødvendig og kostnadene er rimelige. I praksis vil mange virksomheter da kunne «risikovurdere seg bort fra» krav i lov og forskrift, fordi det er vanskelig å dokumentere at et nivå utvilsomt er for lavt. Hvis tilsynsmyndigheten på sin sidemå sannsynliggjøre at et pålegg om å lukke et avvik utvilsomt er nødvendig, legges det etter BDOs oppfatning derfor en for stor bevisbyrde på tilsynsorganet. Formuleringen i bestemmelsen bør derfor revurderes.»

NSM uttaler i denne sammenheng at:

> «Utvalgets forslag synes å bygge på et premiss om at tilsyn munner ut i pålegg om gjennomføring av konkrete sikkerhetstiltak. NSMs tilsynsmetodikk har imidlertid en annen tilnærming. Dersom det konstateres manglende samsvar med regelverket, gis det avvik fra de aktuelle bestemmelsene og pålegg om å korrigere avvikene, uten at det er konkretisert hvordan avvikene skal korrigeres. Både ut fra en erkjennelse om at det som regel er den enkelte virksomhet som er nærmest til å finne de de beste løsningene for sin virksomhet, og også for å sikre virksomhetens eierskap til løsningen og prosessene med å gjennomføre tiltakene, vil det da være opp til virksomheten å korrigere slik at forholdene bringes i samsvar med kravene. Med denne metodiske tilnærmingen synes kriteriene som stilles i første ledd mindre treffende.
>
> Det vil være rent unntaksvis at det pålegges gjennomført konkrete tiltak. For de tilfeller tilsynsmyndigheten ser behov for å pålegge konkrete tiltak vil kravet om at det er «utvilsomt at tiltaket er nødvendig» være for strengt. Det bør være tilstrekkelig at tiltaket fremstår som «nødvendig» Første ledd bør på denne bakgrunn reformuleres.»

Energi Norge uttaler:

> «Det er heller ikke vurdert i hvilken grad NSM har kompetanse til å vurdere samfunnsøkonomisk kost-/nytte av ulike tiltak og pålegg de skal gi i de ulike sektorene og om de har tilstrekkelig teknisk og systemmessig forståelse av virksomhetene i de ulike sektorene til å overprøve sektormyndighetene.»

NVE mener om sikkerhetsmyndighetens påleggskompetanse overfor sektormyndigheter at:

> «Videre mener NVE at § 3-6 tredje ledd om at sikkerhetsmyndigheten kan gi sektormyndigheten pålegg for å sikre at lovens formål ivaretas er en uheldig bestemmelse, som ikke er vanlig i forvaltningen. Dersom sektormyndigheten ikke følger opp loven slik sikkerhetsmyndigheten ønsker, må dette løses på andre måter, jf. punkt 3.2 nedenfor. For øvrig er påleggshjemmelen i § 3-6 første ledd unødvendig. Det gjelder et forholdsmessighetsprinsipp i norsk forvaltning og det vil ivareta langt på vei de samme hensynene som første ledd.»

8.4 Departementets vurdering

8.4.1 Generelt

Departementet har merket seg at høringsinstansene er positive til utvalgets forslag om at det etableres en tilsynsmodell som åpner for at departementene kan bestemme at myndigheter med sek-

toransvar kan føre tilsyn etter loven med virksomheter i egen sektor. Departementet har imidlertid også merket seg at flere høringsinstanser mener at den foreslåtte tilsynsmodellen vil medføre uklarheter knyttet til etterlevelsen av regelverket, ved at sikkerhetsmyndigheten skal inneha myndighet til å kontrollere om departementene og sektormyndighetene følger opp ansvaret de er tillagt etter loven.

De fire grunnleggende prinsippene om ansvar, likhet, nærhet og samvirke er styrende for det forebyggende sikkerhetsarbeidet. Den enkelte statsråd har det konstitusjonelle ansvaret på sitt område, innenfor de lover og bevilgninger Stortinget har gitt. Dette innebærer at den enkelte statsråd beholder sitt konstitusjonelle ansvar også i en krisesituasjon. Ansvar for å forberede og iverksette tiltak som er nødvendige for å forebygge og håndtere akutte situasjoner i de enkelte sektorene, er tillagt departementene og deres respektive underlagte etater. Det øverste ansvaret for nasjonal beredskap og krisehåndtering ligger hos regjeringen, herunder det overordnede politiske ansvaret for både styringen og håndteringen av det forebyggende beredskapsarbeidet og kriser som oppstår.

Det er viktig å understreke at etableringen av en ny modell for gjennomføring av tilsyn etter sikkerhetsloven ikke skal endre disse ansvarsforholdene. Departementene skal fortsatt være ansvarlige for det forebyggende sikkerhetsarbeidet innenfor sine myndighetsområder. Den enkelte fagstatsråden vil fremdeles stå til ansvar for sikkerhetstilstanden i sin sektor, selv om det er Nasjonal sikkerhetsmyndighet som gjennomfører tilsyn etter sikkerhetsloven. I dag mottar departementene gjenpart av tilsynsrapporter fra egen sektor. Dette bidrar til ansvarliggjøring, og gir departementene en mulighet til aktivt å følge opp sikkerheten i egen sektor. Departementet presiserer at denne praksisen vil videreføres med ny lov.

Tilsynsmodellen legger opp til at myndigheter med sektoransvar kan føre tilsyn etter loven i sektoren. Dette innebærer blant annet å ha oversikt over og kontrollere sikkerhetstilstanden i egen sektor, og gi nødvendige pålegg om forbedringer til virksomheter i sektoren. Dette, sammen med en tett samhandling mellom sektormyndighet og sikkerhetsmyndigheten, sikrer at statsråden som konstitusjonelt ansvarlig får kontrollert alle sider ved det forebyggende sikkerhetsarbeidet både etter sikkerhetsloven og sektorregelverk.

Departementet mener likevel at sikkerhetsmyndigheten fremdeles skal ha det sektorovergripende ansvaret for forebyggende sikkerhetsarbeid. Sikkerhetsmyndigheten må derfor ha mulighet til å kunne føre et sektorovergripende tilsyn. Justis- og beredskapsministeren har et overordet ansvar i sivil sektor, mens forsvarsministeren har det overordnede ansvaret i militær sektor, jf. Kronprinsregentens resolusjon av 4. juli 2003. I dag er det Nasjonal sikkerhetsmyndighet som i henhold til denne resolusjonen skal ivareta de utøvende funksjonene på vegne av henholdsvis justis- og beredskapsministeren og forsvarsministeren.

Etter dagens praksis orienterer Nasjonal sikkerhetsmyndighet kun sine overordnede departementer om planlagte tilsyn. I hvilken grad man skal orientere om tilsynsplaner, som vil kunne forenkle den praktiske gjennomføringen og tilretteleggingen av tilsyn, må veies opp mot at hastetiltak kan iverksettes dersom tilsynsplanene blir allment kjent. Departementet mener at forslaget til tilsynsmodell ivaretar en god balanse mellom disse hensynene, og gir et godt utgangspunkt for å kunne ivareta målet om en helhetlig og tverrsektoriell tilnærming til forebyggende sikkerhetsarbeid, samtidig som sektorenes særegenheter ivaretas.

Departementet registrerer at utvalget har lagt stor vekt på de utfordringene som har vært i forbindelse med ivaretakelsen av objektsikkerhetsregimet, og sett hen til disse i regulering av de andre områdene loven gjelder for. Departementet mener forslaget gir sektorene tilstrekkelig rom til å gjøre skjønnsmessige vurderinger knyttet til oppfølging og kontroll med forebyggende sikkerhetsarbeid i egen sektor. Dette medfører, etter departementets syn, at det er meget viktig at en sentral myndighet har mulighet til å skaffe seg en oversikt over det forebyggende sikkerhetsarbeidet i sektorene og på denne måten danne seg et bilde av sikkerhetstilstanden på nasjonalt nivå. Departementet mener videre at sikkerhetsmyndigheten må ha tilstrekkelig mulighet til å føre kontroll med hvordan sektormyndighetene gjennomfører sine tilsyn og dersom det anses som nødvendig, ha mulighet til å korrigere manglende ivaretakelse av tilsynsansvaret. Departementet ser likevel behov for å gjøre enkelte endringer i utvalgets forslag for å enda bedre ivareta lovens formål.

8.4.2 Tilsyn med virksomheter

Utvalgets forslag innebærer at det er sikkerhetsmyndigheten som har det overordnede ansvaret for å påse at det gjennomføres tilsyn med virksomheters etterlevelse av loven, jf. utvalgets forslag til

§ 2-2 om sikkerhetsmyndighetens oppgaver. Sikkerhetsmyndighetens ansvar endrer ikke på at de enkelte departementene har ansvar for det forebyggende sikkerhetsarbeidet innenfor eget myndighetsområde. Det enkelte departement kan, dersom visse kriterier er oppfylt, bestemme at myndigheter med sektoransvar skal føre tilsyn etter loven. Dette vil sikre at tilsynsmyndigheten har bransjespesifikk kunnskap om samfunnssektorenes særegenheter, som gjør denne bedre i stand til å ivareta sektorens forebyggende sikkerhetsarbeid. Dersom det ikke er bestemt at en myndighet med sektoransvar skal føre tilsyn i en sektor, vil sikkerhetsmyndigheten føre tilsyn etter loven i den aktuelle sektoren.

Forslaget til tilsynsmodell legger opp til at det er sikkerhetsmyndigheten som har hovedansvar for å føre tilsyn med virksomheter som er omfattet av loven. Departementet ser behov for å presisere dette, og mener derfor at det i § 3-1 første ledd bør framgå at sikkerhetsmyndigheten fører tilsyn med virksomheter underlagt loven. Presiseringen av at sikkerhetsmyndigheten fører tilsyn med departementene flyttes til tredje ledd. Presiseringen er videreført fordi det ikke er intensjonen at en myndighet med tilsynsansvar skal føre tilsyn med eget departement.

Departementet mener at utvalgets forslag til fordeling av tilsynsansvar vil lette gjennomføringen av tilsynene innen flere fagområder, og redusere belastningen på tilsynsobjektene. Departementet er imidlertid enig med *Samferdselsdepartementet* i at det kan være vanskelig alene å vurdere hvorvidt en myndighet med sektoransvar har tilstrekkelig sikkerhetsfaglig kompetanse til å kunne føre tilsyn etter loven. Utvalgets lovforslag oppstiller ingen andre eksplisitte krav enn at en myndighet med sektoransvar må ha tilsynsfunksjoner knyttet til beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur. Utvalget legger imidlertid til grunn at det skal gjøres en helhetsvurdering, hvor det *blant annet* må tas stilling til om den aktuelle sektormyndigheten har den nødvendige sikkerhetsfaglige kompetansen, eller har mulighet til å opparbeide seg kompetanse uten uforholdsmessig høye utgifter, som skal til for å ivareta tilsynsansvaret på en forsvarlig måte. Det har derfor vært en klar forutsetning for utvalget at vurderingen må gjøres i tett samarbeid mellom det enkelte departement og sikkerhetsmyndigheten. Departementet mener at denne forutsetningen bør videreføres i lovforslaget.

Departementet ser derfor behov for at det i forskrift fastsettes ytterligere momenter som skal vurderes før et departement kan bestemme at en myndighet med sektoransvar skal få delegert tilsynsansvaret etter loven. Departementet foreslår at forskriftshjemmelen endres slik at den gir hjemmel for Kongen til å fastsette nærmere kriterier for departementenes tildeling av tilsynsansvar i forskrift. Etter departementets syn vil disse momentene være til stor hjelp når det enkelte departement og sikkerhetsmyndigheten i samarbeid skal vurdere sektormyndighetenes kompetanse på de enkelte fagområdene. Samtidig vil dette bidra til å kartlegge kompetanse og kompetansebehov hos myndigheter med sektoransvar. Departementet mener denne innretningen vil ivareta *NSMs* innspill om at det er viktig at tilstrekkelig sikkerhetsfaglig kompetanse vektlegges i stor nok grad i vurderingen.

Flere høringsinstanser, særlig andre myndigheter med tilsynsoppgaver som *NVE*, *Finanstilsynet* og *Petroleumstilsynet*, er kritiske til at sikkerhetsmyndigheten skal føre tilsyn med sektormyndigheter med tilsynsansvar. Hovedinnvendingen er at det vil utfordre ansvarsprinsippet som ligger til grunn for departementenes forebyggende sikkerhetsarbeid. Flere påpeker at det tverrsektorielle perspektivet, som det forutsettes at sikkerhetsmyndigheten skal ha, best kan ivaretas gjennom nært samarbeid mellom sikkerhetsmyndighet og sektormyndighet, og at sikkerhetsmyndigheten gis tilstrekkelige kontrollfunksjoner gjennom sine tilsyn med departementene. Departementet er enig i at et godt samarbeid, koordinering, og samhandling mellom tilsynsmyndighetene er avgjørende for et best mulig tilsynsregime.

Imidlertid vil det i de tilfellene hvor tilsynsansvaret delegeres, være en risiko for at det vil oppstå ulik tilnærming og standard for tilsyn etter sikkerhetsloven, selv om det utarbeides overordnede kriterier for tilsyn. En vilkårlig og uensartet oppfølging innenfor enkelte fagområder, og i de forskjellige sektorene, vil svekke den helhetlige tilnærmingen til forebyggende sikkerhet som ligger til grunn for lovforslaget. Videre er tilsyn med sektormyndighetene viktig for at sikkerhetsmyndigheten skal kunne ivareta sine pålagte oppgaver etter loven, herunder utvikle kriterier for tilsyn, utvikle sikkerhetstiltak, forestå opplæring av tilsynspersonell mv. Departementet mener derfor det er helt avgjørende å opprettholde utvalgets forslag om at sikkerhetsmyndigheten skal føre tilsyn med sektormyndigheter med tilsynsansvar.

Departementet foreslår videre at sikkerhetsmyndigheten skal kunne gjennomføre tilsyn med virksomheter i sektorer hvor tilsynsmyndigheten i utgangspunktet er delegert til en sektormyndig-

het, når det følger av internasjonale forpliktelser eller når det er *tvingende nødvendig*. Internasjonale forpliktelser kan for eksempel være knyttet til behandling av gradert informasjon gjennom bi- eller multilaterale avtaler med andre stater eller internasjonale organisasjoner, eksempelvis NATO. *Tvingende nødvendig* forutsetter at det foreligger konkrete sikkerhetsinteresser som tilsier at sikkerhetsmyndigheten skal føre tilsyn. Bestemmelsen er ment som en sikkerhetsventil, som kun skal benyttes i spesielle tilfeller. Dersom sikkerhetsmyndigheten ikke har denne muligheten, vil det i ytterste konsekvens kunne medføre utilsiktede og uheldige konsekvenser, særlig sett i lys av at den foreslåtte tilsynsmodellen i utgangspunktet innsnevrer sikkerhetsmyndighetens tilsynskompetanse sammenliknet med dagens sikkerhetslov.

8.4.3 Sikkerhetsmyndighetens samarbeid med sektormyndigheter

Departementet har merket seg at de fleste høringsinstansene er positive til et samarbeid mellom sikkerhetsmyndigheten og myndighetene med tilsynsansvar, jf. § 3-1 andre ledd. Det er imidlertid uenighet knyttet til hvor inngående samarbeidet skal være. Enkelte mener involveringen av sikkerhetsmyndigheten bør avgrenses til råd og veiledning, utarbeiding av overordnede kriterier og overordnet koordinering av tilsyn.

For at tilsynsmodellen skal fungere etter hensikten, er det viktig at det legges opp til utstrakt samarbeid mellom sikkerhetsmyndigheten og den enkelte sektormyndighet, samt en tett koordinering mellom myndigheter som har tilsynsansvar etter loven. Gjennom inngåelse av en avtale skapes en forventning om og en forpliktelse om samarbeid. Departementet har merket seg at flere høringsinstanser mener de allerede har et godt samarbeid med NSM, at en slik regulering synes unødvendig og at en lovpålagt plikt til inngåelse av samarbeidsavtale vil virke mot sin hensikt. Blant annet mener *Arbeids- og sosialdepartementet* at samarbeidet bør være tuftet på regler som fremmer samarbeid, framfor plikt til å samarbeide og etablere kontrollordninger.

Etter departementets syn tyder innspillene i høringen på at det eksisterer forskjellige oppfatninger av hvordan tilsyn etter sikkerhetsloven bør gjennomføres, og at det derfor er, og har vært, enkelte utfordringer knyttet til samarbeid under dagens regime. Departementet mener derfor at en lovfesting av samarbeid og inngåelse av samarbeidsavtale kan være et godt virkemiddel for å sikre at tilsyn gjennomføres koordinert, at ansvar for gjennomføring innenfor særskilte fagområder fastsettes tydelig, og at alle aspekter ved tilsyn ivaretas og blir tatt hensyn til i samarbeidsforholdet.

Departementet mener at utvalgets forslag til § 3-2 fjerde ledd, om utarbeidelse av grunnleggende kriterier for tilsyn, er godt begrunnet. Det er hensiktsmessig at sikkerhetsmyndigheten har mulighet til å påvirke hva det skal føres tilsyn med og hvordan dette gjøres, for at sikkerhetsmyndigheten best mulig skal kunne ivareta sitt sektorovergripende ansvar for det forebyggende sikkerhetsarbeidet. Sikkerhetsmyndigheten har videre oversikten over den totale sikkerhetssituasjonen på tvers av sektorene, og er dermed nærmest, og best egnet, til å utarbeide slike kriterier. Med grunnleggende kriterier for tilsyn menes overordnede føringer som sikrer at lovens formål ivaretas på en forsvarlig måte. De overordnede føringene vil også gjelde der hvor tilsynsansvaret er delegert til aktuelle sektormyndigheter. Sektormyndighetene vil samtidig ha adgang til å supplere de overordnede føringene med spesifikke kriterier tilpasset den enkelte samfunnssektor. Tatt i betraktning at utarbeidelse av kriteriene er en grunnleggende oppgave for sikkerhetsmyndigheten, mener departementet at den bør reguleres sammen med sikkerhetsmyndighetens øvrige plikter. Dette innebærer etter departementets syn ingen realitetsendring fra utvalgets forslag.

Etter departementets syn bør sikkerhetsmyndigheten også ha en sentral rolle i opplæringen av tilsynspersonell, for å sikre at personellet har nødvendig sikkerhetsfaglig kompetanse for å kunne gjennomføre tilsyn etter loven. Det forutsettes at sektortilsynene allerede innehar generell tilsynskompetanse etter anerkjente revisjonsstandarder. Sikkerhetsmyndigheten vil imidlertid legge til rette for opplæring av personellet. NSM har i dag et kurssenter som vil kunne benyttes til opplæringsformål. Det vil være naturlig at det etableres egne program for tilsynspersonell.

Departementet bemerker at lovforslaget legger opp til gjensidig kompetanseoverføring mellom sikkerhetsmyndighet og sektormyndigheter. Sikkerhetsmyndigheten skal bidra med utveksling av sikkerhetsfaglige kompetansen, mens sektormyndigheten skal bidra med sektorspesifikk kompetanse. Departementet mener at det samarbeidet som loven legger opp til, vil bidra til kompetanseheving både hos sikkerhetsmyndigheten og sektormyndigheter, som samlet, og særlig på lengre sikt, vil styrke det nasjonale forebyggende sikkerhetsarbeidet.

Når det gjelder utvalgets forslag i § 3-2 femte ledd om at sikkerhetsmyndigheten, dersom det er nødvendig, kan delta på tilsyn som gjennomføres av et sektortilsyn, er departementet enig med utvalget i at sikkerhetsmyndigheten kan ha behov for å delta på tilsyn som gjennomføres i de ulike sektorene. At sikkerhetsmyndigheten skal kunne kreve å få være med, kan oppfattes som unødvendig, gitt bestemmelsene om samarbeid og samhandling mellom sikkerhetsmyndigheten og sektormyndighetene. Dessuten kan det skape usikkerhet om sikkerhetsmyndigheten skal kunne overta tilsynet på et felt der den ikke har kjernekompetanse. Slik departementet ser det, vil det imidlertid i enkelte tilfeller være nødvendig at sikkerhetsmyndigheten deltar på sektormyndighetenes tilsyn. Det vil i slike tilfeller være sektortilsynet som har ansvaret for tilsynet.

Departementet legger til grunn at hjemmelen for å delta på tilsyn skal brukes unntaksvis og som hovedregel etter forutgående dialog, jf. utvalgets forslag til § 3-2. Dette er også i tråd med utvalgets forutsetninger om at slik deltakelse fortrinnsvis nedfelles i samarbeidsavtalen. Departementet mener at sikkerhetsmyndighetens deltakelse på forberedelse og gjennomføring av tilsyn vil være et kompetansehevende tiltak for både sikkerhetsmyndighet og sektormyndighet.

Departementet mener utvalgets forslag til § 3-2 femte ledd om at sektortilsynene kan be sikkerhetsmyndigheten om bistand i forbindelse med tilsyn er godt, og foreslår derfor å videreføre dette i § 3-2 tredje ledd.

Departementet har videre merket seg at enkelte høringsinstanser, blant annet *NVE, Luftfartstilsynet* og *Fylkesmannen i Vestfold* er negative til at det pålegges en rapporteringsplikt for sektormyndigheter som gjennomfører tilsyn. Det framheves at dette både er ressurskrevende og en unødvendig byråkratisering. Det vises videre til at gevinsten som eventuelt oppveier for ressursbruken bare vil utligne de negative sidene ved en slik rapportering. *NSM* på den andre side bemerker at rapporteringsplikten er helt nødvendig for at sikkerhetsmyndigheten skal kunne ha informasjonsgrunnlaget for å utføre de oppgavene den pålegges i loven. Forebyggende sikkerhetsarbeid er en kontinuerlig prosess hvor tilsyn er et av verktøyene for å avdekke behovet for nye sikkerhetstiltak. Det er derfor av avgjørende betydning at den myndigheten som fastsetter sikkerhetskravene og som skal bidra til å utvikle nye tiltak, blir kjent med resultatene fra tilsynene.

Departementet er enig i innspillet til *NSM*. Departementet mener videre at rapporteringsplikten i all hovedsak ikke vil innebære en omfattende ekstra bruk av ressurser, men ser at de nærmere konsekvensene vil kunne variere noe fra sektor til sektor. Departementet stiller seg imidlertid bak utvalgets og *NSM* sin vurdering av at de positive effektene for sikkerhetsarbeidet, trolig langt overstiger de eventuelle negative konsekvensene for myndigheter med tilsynsansvar.

Departementet mener imidlertid at rapportering av hovedfunn kan utgjøre et for snevert informasjonsgrunnlag for sikkerhetsmyndigheten til å vurdere sikkerhetstilstanden i en sektor hvor sikkerhetsmyndigheten ikke selv fører tilsyn. For sikkerhetsmyndigheten vil en mer detaljert oversikt ofte være nødvendig for å prioritere sin tilsynsvirksomhet inn mot den enkelte sektormyndighet. Departementet mener derfor det bør stilles krav til en nærmere redegjørelse for gjennomførte tilsyn, og at det oversendes informasjon om eventuelle påviste avvik. Redegjørelsen skal gi sikkerhetsmyndigheten informasjon om hvor og når det er gjennomført tilsyn, og om avvik som er påvist. En slik praksis vil etter departementets syn ikke medføre en større belastning på sektortilsynene enn utvalgets forslag, men vil gi en større sikkerhetsmessig gevinst.

Departementet mener videre at sikkerhetsmyndigheten bør ha en oversikt over planlagte tilsyn, for å kunne planlegge eventuell medvirkning til forberedelse og gjennomføring av tilsyn. Departementet foreslår å ta inn i lovteksten at sektormyndigheten orienterer sikkerhetsmyndigheten om planlagte tilsyn. Dette kan for eksempel gjøres i forbindelse med at sektormyndigheten utarbeider sin årlige tilsynsplan.

Departementet bemerker at rapporteringsplikten må konkretiseres på forskriftsnivå. Det er derfor tatt inn en forskriftshjemmel i lovforslaget § 3-2 siste ledd, om samarbeid og informasjonsutveksling mellom sikkerhetsmyndigheten og myndigheter med tilsynsansvar.

8.4.4 Generelle prinsipper for tilsyn

Departementet foreslår, i tråd med utvalgets forslag, at tilsyn ikke skal forstyrre tilsynsobjektenes daglige drift mer enn nødvendig. Dette er et viktig prinsipp som bør stå i loven. Departementet mener imidlertid at hensynet ikke skal kunne benyttes for å unndra seg tilsyn, og at hensynet til virksomheten alene må kunne vike på bekostning av behovet for å gjennomføre tilsyn. Det vil dessuten være for ressurskrevende for tilsynsmyndigheten til enhver tid å unngå å virke forstyrrende på tilsynsobjektets daglige drift.

Departementet er videre enig med *NSM* og *BDO* om at det er en uhensiktsmessig avgrensning, som bryter med dagens praksis, å innføre utvalgets forslag til formålsavgrensning. Departementet mener at tilsynsmyndighetene må kunne benytte opplysningene til å ivareta de krav i loven som stilles til forebyggende sikkerhetsarbeid. Det kan være i forbindelse med vurdering av risiko, utvikling av sikkerhetstiltak eller andre former for analyse. Departementet ser imidlertid at det er gode grunner for å avgrense bruken av opplysningene til det som er nødvendig innenfor lovens formål. Departementet mener også det er hensiktsmessig at der både sikkerhetsmyndighet og sektormyndighet med tilsynsansvar pålegges plikter, omtales disse som *tilsynsmyndigheten*.

8.4.5 Stedlige tilsyn

Utvalget har foreslått en bestemmelse i § 3-4 som regulerer tilsynsmyndighetens uhindrede adgang til informasjon, informasjonssystemer, objekter og infrastruktur som er nødvendig for å gjennomføre tilsyn. Bestemmelsen er en forutsetning for at tilsyn kan gjennomføres, og er en videreføring av den adgangsretten som følger av gjeldende sikkerhetslov § 10. Videre følger det av utvalgets forslag at det normalt skal sendes skriftlig varsel om tilsyn. Dette innebærer at varsling kan fravikes dersom det ikke er mulig eller ønskelig. Departementet foreslår å videreføre bestemmelsen, med noen språklige endringer.

NSM har spilt inn at adgangsretten også bør omfatte adgang til relevant personell. Departementet anser at tilgangen til rett personell ved tilsyn vil bidra til bedre opplyste tilsyn, og lette gjennomføringen i stor grad, og foreslår derfor at det tas inn i bestemmelsen.

Departementet foreslår videre å endre ordlyden i forslaget til § 3-4 andre ledd til «(...) Tilsyn kan likevel gjennomføres uten varsel dersom sikkerhetshensyn gjør det nødvendig».

8.4.6 Tilsynsmyndighetens behandling av personopplysninger

Departementet er videre enig i utvalgets forslag om en egen bestemmelse om tilsynsmyndighetens behandling av personopplysninger i § 3-5. Departementet foreslår at bestemmelsen videreføres med enkelte språklige endringer.

8.4.7 Pålegg

Departementet har merket seg at flere av høringsinstansene har kommentert utvalgets forslag til regulering av pålegg i § 3-6.

Departementet mener, i likhet med utvalget, at påleggskompetansen bør lovreguleres. Det foreslås at tilsynsmyndigheten både skal kunne gi pålegg om gjennomføring av konkrete tiltak og om å korrigere avvik fra lovens krav på egnet måte. Ved sistnevnte type pålegg gjør virksomheten egne vurderinger av hvilke tiltak som er nødvendige for å lukke avviket. Bestemmelsen må ses i sammenheng med virksomhetenes plikt til å ivareta et forsvarlig sikkerhetsnivå, jf. § 4-3. Departementet viser i denne sammenheng til *NSMs* høringsuttalelse:

> «Dersom det konstateres manglende samsvar med regelverket, gis det avvik fra de aktuelle bestemmelsene og pålegg om å korrigere avvikene, uten at det er konkretisert hvordan avvikene skal korrigeres.»

Departementet mener at det er en grunnleggende forutsetning at det å kunne gi pålegg er nødvendig for å ivareta lovens formål. Departement mener videre at pålegg om gjennomføring av konkrete tiltak bare skal kunne gis dersom kostnadene som påføres virksomheten framstår som rimelige sett i forhold til det som kan oppnås ved tiltaket. Departementet viser til *NSMs* høringsuttalelse, hvor det påpekes at pålegg om gjennomføring av konkrete tiltak sjelden gis. Departementet forutsetter derfor at i de tilfellene hvor det gis pålegg, om konkrete tiltak, at tiltaket faktisk er nødvendig. I bestemmelsen forutsettes det at det må gjøres en vurdering av tiltakets kostnad, blant annet om andre rimeligere tiltak kan oppnå samme nytte. Der tilsynsmyndigheten gir en virksomhet pålegg om å lukke et avvik, vil det være opptil virksomheten selv med hvilke tiltak avvik korrigeres. Virksomheten må da selv vurdere tiltakenes kost-nytteverdi innenfor de vurderinger som er gjort etter § 4-3 om virksomhetens forsvarlige sikkerhetsnivå.

Departementet har videre merket seg at flere av høringsinstansene, blant annet *Energi Norge og NVE*, er kritiske til at sikkerhetsmyndigheten skal ha mulighet til å gi pålegg til myndigheter med tilsynsansvar. Departementet mener likevel at sikkerhetsmyndigheten må ha denne sanksjonsmuligheten som virkemiddel, for å sikre at det gjennomføres tilsyn i samsvar med krav fastsatt i eller i medhold av loven i den aktuelle sektoren. Depar-

tementet 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.

9 Generelle krav til forebyggende sikkerhetsarbeid

9.1 Gjeldende rett

De generelle kravene til forebyggende sikkerhet er i dagens sikkerhetslov uttrykt gjennom fastsettelsen av virksomhetsansvaret i § 5.

Den enkelte virksomhet plikter i henhold til bestemmelsen å utøve forebyggende sikkerhetstjeneste i henhold til bestemmelsene gitt i eller i medhold av sikkerhetsloven. Virksomheten plikter å utarbeide en intern instruks for å ivareta sikkerheten, sørge for at virksomhetens ansatte og engasjerte får tilstrekkelig opplæring i sikkerhetsspørsmål, og regelmessig kontrollere sikkerhetstilstanden i virksomheten, jf. § 5 andre ledd bokstav a til c.

Ansvaret for utøvelse av forebyggende sikkerhetstjeneste påhviler virksomhetens leder, jf. § 5 tredje ledd. Virksomhetens leder kan etter samme bestemmelse delegere utøvende funksjoner internt i virksomheten. Dersom dette gjøres, skal det dokumenteres skriftlig.

Det følger videre av fjerde ledd at det påhviler en plikt for enhver ansatt eller personell som er engasjert, til å ivareta sikkerhetsmessige hensyn og til å bidra til forebyggende sikkerhetstjeneste gjennom sitt arbeid eller oppdrag for virksomheten.

I bestemmelsens femte ledd er fullmakt til å gi nærmere bestemmelser delegert til Nasjonal sikkerhetsmyndighet.

Sikkerhetsadministrasjon for forebyggende sikkerhetstjeneste er også regulert i gjeldende sikkerhetslov § 5 om den enkelte virksomhets plikter. Sikkerhetsadministrasjon er den administrative og organisatoriske styring som ligger til grunn for forebyggende sikkerhetstjeneste.

Sikkerhetsadministrasjon omfatter både sikkerhetsledelse, sikkerhetsorganisering, sikkerhetstiltak og prosedyrer, forholdet til andre virksomheter, sikkerhetsoppfølging, sikkerhetsdokumentasjon og risikohåndtering. Styrende for administrasjon av sikkerhetstjenesten er at den utøves slik at den gir grunnlag for allmenn tillit og slik at den er mulig å kontrollere.

I tillegg er det gitt utfyllende bestemmelser om sikkerhetsadministrasjon i forskrift 29. juni 2001 nr. 723. Forskriften gjelder den enkelte virksomhets sikkerhetsadministrasjon innen og på tvers av fagområdene informasjonssikkerhet, personellsikkerhet og sikkerhetsgraderte anskaffelser. Sikkerhetsadministrasjon innbefatter internkontroll ved gjennomføring av systematiske tiltak for å sikre at virksomhetens aktiviteter planlegges, organiseres, utføres og revideres i samsvar med krav fastsatt i og i medhold av sikkerhetsloven, jf. forskrift om sikkerhetsadministrasjon § 1-2 første ledd nr. 1.

Dagens sikkerhetslov inneholder ingen eksplisitt bestemmelse om internkontroll. Det følger imidlertid implisitt av blant annet dagens § 5 andre ledd bokstav a til c.

9.2 Utvalgets forslag

Utvalgets forslag til ny lov er basert på at det skal stilles funksjonelle krav til virksomhetene som omfattes av loven. Den enkelte virksomhet skal, basert på en vurdering av risiko, iverksette de nødvendige sikkerhetstiltakene. Så lenge tiltakene tilfredsstiller grunnleggende krav til sikkerhetsnivå, er det meningen at virksomheten selv kan velge hvilke sikkerhetstiltak som er nødvendige.

Utvalget skriver i NOU 2016: 19, side 144 om generelle krav:

> «Et sentralt forhold i utvalgets arbeid har vært hvilken detaljeringsgrad som er nødvendig for de kravene som oppstilles i loven. På den ene siden tilsier hensynet til den enkelte samfunnssektors særegenheter at kravene bør gjøres relativt overordnede. Et for detaljert sektorovergripende regelverk, vil kunne innebære risiko for at regelverket kommer i konflikt med relevant sektorregelverk på området. Enkelte utvalgsmedlemmer har også uttrykt bekymring for at en for detaljert lov kan skape problemer i form av dobbeltregulering.»

Dette har vært gjenstand for grundig vurdering fra utvalgets side.

Hensynet til virksomhetene, og spesielt de selvstendige rettssubjektenes behov for forutsigbarhet, har vært avgjørende for utvalgets vurderinger og anbefalinger.

En for vag og skjønnsmessig angivelse av hvilke krav som oppstilles etter loven, vil svekke virksomhetens mulighet til å forutberegne sin rettsstilling og til å kunne forstå konsekvensene av de krav som følger av loven. For å ivareta en slik forutberegnelighet er det nødvendig at loven trekker opp de ytre rammene, både for myndighetenes og virksomhetenes skjønnsutøvelse. Utvalget har derfor anbefalt som et generelt og gjennomgående krav at virksomhetene skal iverksette de sikkerhetstiltak som er nødvendige for å oppnå et forsvarlig sikkerhetsnivå. Forholdet til sektorregelverk er nærmere behandlet i NOU 2016: 19 kapittel 7.7.12.

Utvalget beskriver at sikkerhetsnivået skal være *forsvarlig*. Dette er ment å være en rettslig standard som skal trekke opp de ytre rammene for hvilket handlingsrom virksomhetene har for etablering av sikkerhetstiltak.

Om forsvarlighetsstandarden uttales det i NOU 2016: 19, side 144:

> «Hva som vil utgjøre et forsvarlig sikkerhetsnivå for den enkelte virksomhet, og på de enkelte fagfeltene loven dekker, vil måtte vurderes opp mot hva som anses som god faglig praksis på de enkelte fagområdene, herunder informasjons- og informasjonssystemsikkerhet, objekt- og infrastruktursikkerhet og personellsikkerhet. Den nærmere grensedragningen bør, slik utvalget ser det utvikles i samarbeid mellom Sikkerhetsmyndigheten og de aktuelle sektormyndighetene. Dette vil også gi mulighet til å kunne gjøre sektorspesifikke tilpasninger der det er behov.»

Videre vil det være en avgjørende forutsetning for at den enkelte virksomhet skal kunne gjøre en forsvarlig vurdering av risiko, eller risiko- og sårbarhetsanalyse som utvalget legger til grunn, at det gis informasjon slik at virksomhetene forstår det trusselbildet de står overfor. De forslagene utvalget har lagt fram for å gjøre informasjon om trusselbildet og annen sikkerhetsrelevant informasjon tilgjengelig, er et avgjørende virkemiddel for å sette den enkelte virksomhet i stand til å gjøre forsvarlige vurderinger.

Utvalget mener at i vurderingen av hva som utgjør et forsvarlig sikkerhetsnivå, vil sikkerhetsmyndighetens rådgivning være et sentralt bidrag til den enkelte virksomhet, sett hen til den trusselen virksomheten står overfor. En av hovedoppgavene til sikkerhetsmyndigheten, i henhold til utvalgets forslag, vil være å gi informasjon, råd og veiledning til virksomheter underlagt loven. Utvalget skriver om dette i NOU 2016: 19, side 139:

> «Konkret rådgivning overfor de enkelte virksomhetene bør være en helt sentral oppgave for Sikkerhetsmyndigheten innenfor alle de fagområder loven spenner over. Storbritannias *Centre for the Protection of National Infrastructure* (CPNI) sin rolle i det britiske systemet for beskyttelse av kritisk infrastruktur, kan tjene som eksempel på hvordan rådgivningsvirksomheten bør innrettes. CPNI driver utstrakt utadrettet og aktiv rådgivningsvirksomhet mot både offentlige myndigheter og andre virksomheter som råder over kritisk infrastruktur, og har gjennom sin organisatoriske tilknytning og sin fagkompetanse en betydelig tillit og innflytelse overfor de berørte aktørene.»

Et annet element som er framhevet i utvalgets forslag, er at kostnadene ved sikkerhetstiltak etter loven skal stå i et rimelig forhold til det som oppnås ved tiltaket, slik det beskrives i NOU 2016: 19, side 144:

> «Rett og plikt til å gjøre vurderinger av samfunnets samlede nytte ved tiltaket, sett opp mot de kostnader sikkerhetstiltaket fører med seg er, slik utvalget ser det, en nødvendig konsekvens av forslaget om å justere lovens virkeområde. Som utvalget har vært inne på i NOU 2016: 19 kapittel 6 vil justeringen av lovens virkeområde sannsynligvis medføre at flere selvstendige rettssubjekter blir omfattet av loven. Økt sikkerhet vil føre til mange konsekvenser for ulike aktører, inkludert økonomiske. Det er en fare for at dersom virksomheten ikke gis anledning til å gjøre kost-/nyttevurderinger i forhold til hvilke sikkerhetstiltak som bør og skal iverksettes, kan dette medføre at kostnadene ved å etablere sikkerhetstiltak blir uforholdsmessig høye. Spesielt for selvstendige rettssubjekter som blir omfattet av loven, vil det i ytterste konsekvens kunne virke konkurransevridende dersom disse blir pålagt å iverksette uforholdsmessig kostbare sikkerhetstiltak.»

Om virksomhetene etablerer tilfredsstillende og forsvarlige sikkerhetstiltak, vil også måtte være gjenstand for tilsynsmyndighetenes kontroll etter loven. Tilsynsmyndighetene er i loven gitt en rekke virkemidler for å kunne påvirke sikkerhets-

nivået hos den enkelte virksomhet. Utvalget presiserer viktigheten av at såkalt «myke» virkemidler i form av informasjon om trusselnivå, råd og veiledning bør forsøkes først, før tilsynsmyndigheten eventuelt gir konkrete pålegg om iverksettelse av tiltak for å etterleve lovens krav. Utvalget framhever også at tilsynsmyndighetens pålegg overfor virksomhetene som er omfattet av loven, må være basert på en vurdering av samfunnsøkonomisk lønnsomhet. Det må vurderes hvorvidt tiltakenes samlede nytte for samfunnet overstiger kostnadene de fører med seg.

Utvalget påpeker at det ved utarbeidelse og gjennomføring av sikkerhetstiltak er viktig at det tas hensyn til personvernet. Utvalget har redegjort grundig for personvernhensyn i NOU 2016: 19 kapittel 5. Personopplysningsloven gjelder som utgangspunkt for alle typer virksomheter, herunder virksomheter som omfattes av sikkerhetsloven. Utvalget har foreslått å presisere dette ytterligere, ved å innta en lovhjemmel som viser direkte til Europaparlamentets- og rådsforordning (EU) 2016/679 av 27. april 2016, blant annet til de grunnleggende prinsippene for behandling av personopplysninger slik det framgår av personvernforordningen artikkel 5.

Om avveiningen mellom nasjonal sikkerhet og personvernet skriver utvalget i NOU 2016: 19, side 95:

> «Personvern, rettssikkerhet og nasjonal sikkerhet er grunnleggende verdier i et demokratisk samfunn, hvor ingen av natur er mer tungtveiende enn andre. Ivaretakelse av alle disse verdiene er essensielt for å opprettholde demokratiet og rettsstatsprinsippene.»

På bakgrunn av at det ikke utelukkende skal tas personvernhensyn ved utarbeidelse og gjennomføring av sikkerhetstiltak, mener utvalget at loven også skal vise til unntaksbestemmelsen i artikkel 23 i personvernforordningen.

Det vises for øvrig til utvalgets behandling av personvernforordningen i NOU 2016: 19 kapittel 5.3.2, og til avveiningen mellom personvern og nasjonal sikkerhet i NOU 2016: 19 kapittel 5.7.

Utvikling av forsvarlighetsstandarden, kombinert med virksomhetenes og tilsynsmyndighetenes plikt til å gjøre vurderinger av samfunnets nytte sett i forhold til kostnadene, vil også være styrende for graden av risikoaksept etter den nye loven. Utvalget skriver i NOU 2016: 19, side 145:

> «Etter utvalgets vurdering er det ikke mulig, ønskelig eller hensiktsmessig å gjennomføre sikkerhetstiltak som vil eliminere risikoen for at tilsiktede uønskede hendelser inntreffer. Ved å etablere forsvarlige og kostnadseffektive sikkerhetstiltak, vil man imidlertid kunne redusere sannsynligheten for, og konsekvensene av, slike hendelser. I siste omgang vil det være opp til regjering og storting å definere hvilken risiko som er akseptabel for våre grunnleggende nasjonale funksjoner. Utvalget mener at forslaget om å etablere tverrsektorielle scenarioer, som grunnlag for virksomhetenes risiko og sårbarhetsanalyser, og for hvilke sikkerhetstiltak som skal iverksettes, vil være et nyttig bidrag for å avgjøre hva som er akseptabel risiko.»

For at myndighetene skal kunne danne seg et helhetlig bilde av sikkerhetsnivået og trusselbildet for de ulike virksomhetene og samfunnssektorene, mener utvalget det er nødvendig å pålegge virksomheter underlagt loven en plikt til å rapportere hendelser. Utvalget skriver om rapportering i NOU 2016: 19, side 145:

> «Rapporteringslinjene bør i utgangspunktet følge fordelingen av tilsynsansvaret, slik at den enkelte virksomhet plikter å rapportere til den aktør som er tillagt tilsynsansvar etter loven. For å ivareta det sektorovergripende perspektivet, er det imidlertid også nødvendig at sikkerhetsmyndigheten får tilgang til hendelsesrapportering fra alle samfunnssektorer. Utvalget har vurdert hvorvidt det vil være tilstrekkelig at den enkelte sektormyndighet pålegges å videreformidle slike varsler til sikkerhetsmyndigheten, der dette vurderes som relevant. Dette vil imidlertid kunne medføre at de aktuelle sektormyndighetene blir et forsinkende ledd i rapporteringslinjen. I tillegg kan hendelser som blir vurdert som mindre relevante i en samfunnssektor, kunne være viktig informasjon for å forstå det helhetlige trusselbildet – noe sektormyndighetene ikke nødvendigvis har forutsetninger for [å] vurdere.»

Utvalget anbefaler at sikkerhetsmyndigheten skal varsles parallelt der en sektormyndighet er tillagt tilsynsansvar etter loven. Utvalget mener at en slik form for «dobbeltrapportering» vil kunne medføre noe økt ressursbruk hos sikkerhetsmyndigheten, ved at kapasiteten for å motta og behandle varsler må være tilstrekkelig dimensjonert. På den annen side mener utvalget at den sikkerhetsmessige gevinsten ved at sikkerhetsmyndigheten har et mer fullstendig bilde over hendel-

ser av sikkerhetsmessig betydning, vil overstige de kostnadsmessige ulempene en slik varsling eventuelt medfører.

9.3 Høringsinstansenes syn

I høringen har det framkommet for det meste positive tilbakemeldinger på å lovfeste generelle krav til forebyggende sikkerhet i et eget kapittel. Det framheves som positivt at enkelte overordnede prinsipper lovfestes, og at det legges opp til bruk av funksjonelle krav. Flere påpeker imidlertid at en for utstrakt bruk av funksjonelle krav overlater for mye skjønn til de som skal vurdere hvilke sikkerhetstiltak som er nødvendige, og at dette kan skape usikkerhet i møtet mellom virksomheter og tilsynsmyndigheter.

9.3.1 Plikt til å gjennomføre sikkerhetstiltak

Konsulentselskapet *BDO* poengterer viktigheten av klare forskrifter tilpasset de enkelte fagområdene for å unngå dobbelt- eller underregulerte områder og uttaler:

> «Når det gjelder faren for dobbeltregulering og underregulerte områder, er det viktig at Kongen i sin bruk av hjemmel til å gi forskrifter, skaper klarhet i hvilke myndigheter som skal gi forskrifter om hva.»

Departementenes sikkerhets- og serviceorganisasjon (DSS) har kommentert generelt om strukturen i kapittel 4:

> «Det synes som om § 4-1 mer naturlig bør komme etter nåværende § 4-3. Da får man først gitt ansvar, deretter virkemiddel for prioritering, deretter beslutning og gjennomføring, deretter dokumentasjonsplikt.»

Direktoratet for samfunnssikkerhet og beredskap (DSB) bemerker i sin høringsuttalelse at de avveininger som må gjøres knyttet til sikkerhetstiltak har en «all hazards»-tilnærming, til tross for at loven skal være innrettet mot tilsiktede handlinger, og uttaler blant annet:

> «Oppsummert kan man si at lovforslaget, til tross for at det bare skal være innrettet mot tilsiktede handlinger, i prinsippet delvis bygger på en «all hazards»-tilnærming. Årsaken til at dette blir annerledes i lovforslaget enn i gjeldende lov, er primært at lovforslaget legger en funksjons- og systembasert tilnærming til grunn, og at det stilles krav om at sikkerhetsarbeidet skal bygge på en helhetlig risiko- og sårbarhetsanalyse, jf. §§ 4-1 og 4-3.»

Nasjonal kommunikasjonsmyndighet (Nkom) bemerker at loven vil stille store krav til tilsynsmyndighetene knyttet til å se sikringstiltakene i sammenheng, og uttaler:

> «Pliktene er begrenset til sikkerhetstiltak mot tilsiktede uønskede hendelser. Nkom er enig i denne presiseringen i og med at ny sikkerhetslov ikke er ment å være en allmenn overordnet samfunnssikkerhetslov.
>
> Nkom har i likhet med mange andre tilsynsmyndigheter en «all hazards-tilnærming» i det forebyggende sikkerhetsarbeid i egen sektor og i forhold til eget regelverk. Ny sikkerhetslov kan bli gjort gjeldende for virksomheter/objekter som utgjør en viktig komponent i en verdikjede, men som pr. i dag ikke er underlagt sektorregelverkets egne sikkerhetsbestemmelser. Ny sikkerhetslov vil stille store krav til differensiering og tilpasning for sektormyndigheten når det gjelder tilsynsaktivitet og forebyggende sikkerhetsarbeid for tilsynsobjekter etter både eget regelverk og sikkerhetslovens bestemmelser.»

Nasjonal sikkerhetsmyndighet (NSM) mener loven legger opp til omfattende skjønnsmessige vurderinger av hvilke sikringstiltak som er nødvendig, og poengterer at vurderingene som gjøres må være gjenstand for tilsyn, og at sikkerhetsmyndigheten må kunne definere hva som anses som en forsvarlig minimumsstandard. NSM mener det er et behov for ytterligere presisering av hva sikringstiltakene skal bestå av i loven. Mangel på presisering vil etter NSMs syn kunne medføre en vilkårlig og uensartet praksis mellom virksomheter og sektorer.

Norges vassdrags- og energidirektorat (NVE) støtter at det fastsettes generelle krav, men påpeker at de virksomheter som allerede er underlagt strengere krav, ikke også må oppfylle sikkerhetslovens krav og uttaler blant annet:

> «NVE er positiv til de generelle kravene til forebyggende sikkerhet som stilles i kapittel 4. NVE har notert seg at det er foreslått at loven skal ha en struktur med et kapittel med generelle krav til forebyggende sikkerhet. Dette er samme regulering som i beredskapsforskriften kapittel 2. De kravene som er foreslått er i

hovedsak innholdsmessig like de som beredskapsforskriften stiller.

For å unngå dobbeltregulering vil NVE foreslå at virksomheter som allerede er underlagt strengere krav i sektorlovgivning, ikke også må oppfylle sikkerhetskrav etter sikkerhetsloven. NVE peker på at bestemmelsen i § 4-1 tredje ledd presiserer at de tiltakene som iverksettes kan ses i sammenheng med behov for tiltak for å håndtere annen type risiko. Etter beredskapsforskriften § 2-4 skal det gjennomføres ROS-analyser knyttet til «ekstraordinære forhold». For de aktører som er underlagt kravene i beredskapsforskriften er det allerede et strengere krav enn forslagets «forsvarlig sikkerhet».»

Norsk olje og gass tar i sin høringsuttalelse til orde for økt bruk av standarder for best mulig tilpasning til forskjellige objekter og infrastruktur. Organisasjonen peker blant annet på at standarden «forsvarlig sikkerhetsnivå» ikke gir en god nok avgrensing av virksomhetenes ansvar:

«Tiltakskrav vil kunne bli utfylt gjennom henvisning til standarder. Norsk olje og gass vil fremheve at utvikling og etterlevelse av gode standarder er en god og etablert arbeidsmetodikk innen petroleumsnæringen.

Norsk olje og gass vil understreke at det gjør seg gjeldene vidt forskjellige trusselbilder rettet mot objekter og infrastruktur og mot informasjonssystemer. Hva gjelder informasjonssystemer er trusselbildet internasjonalt og tiltakene må langt på vei støttes opp av et internasjonalt samarbeid. Norsk olje og gass vil understreke at henvisninger på dette området utelukkende må vise til internasjonale standarder.

[…]

I den utstrekning private aktører skal bidra, må pliktene ha tydelig lovgrunnlag som også må innebære en avklaring mot myndighetenes ansvar. Vi mener også at loven i større grad bør åpne for at de ulike krav til sikkerhetstiltak tilpasses virksomhetenes art, omfang og øvrige omstendigheter.»

Politidirektoratet og *Oslo politidistrikt* er i sine høringsuttalelser kritiske til en utstrakt funksjonell tilnærming, og mener dette vil skape usikkerhet rundt hva som anses som et tilstrekkelig sikkerhetsnivå, som igjen vil medføre ulik praktisering av regelverket og ulikt sikringsnivå fra virksomhet til virksomhet. De uttaler videre at dette vil gjøre sikkerhetsarbeidet i virksomheten vanskeligere enn det er i dag, da sikkerhetspersonell allerede har utfordringer med å skape forståelse for viktigheten av å gjennomføre sikkerhetstiltak:

Politidirektoratet har uttalt:

«Politidirektoratet oppfatter utredningen slik at det i ny sikkerhetslov er tale om å erstatte eksplisitte, mer detaljerte minimumskrav med mer funksjonelle krav. Politidirektoratet er, i likhet med Oslo politidistrikt, av den oppfatning at en slik overgang vil kunne ha flere uheldige konsekvenser. Oslo politidistrikt fremhever blant annet at varierende risikoforståelse og kunnskap vil medføre at arbeidet knyttet til forebyggende sikkerhet vil vanskeliggjøres uten angivelse av en minimumsstandard i regelverket. Oslo politidistrikt viser videre til arbeidet med etablering av sikkerhetstiltak etter krav i objektsikkerhetsforskriften. Etter deres erfaring har dette arbeidet vist seg å være krevende, nettopp fordi denne forskriften er mindre detaljert. Et mindre detaljert regelverk stiller større krav til kompetanse og erfaring hos sikkerhetspersonellet.»

Politiets sikkerhetstjeneste (PST) er i utgangspunktet positive til en funksjonell tilnærming, men påpeker at det stiller store krav til vurdering hos virksomhetene og oppfølging og veiledning fra tilsynsmyndighetene:

«Forslaget legger opp til at den enkelte virksomhet får et større ansvar for å innføre tilfredsstillende sikring basert på en konkret trusselvurdering. PST støtter en slik risikobasert tilnærming til sikringsspørsmålet. Dette vil imidlertid fordre at den enkelte aktør evner å møte sikkerhetskravene.

Det krever, etter PSTs oppfatning, derfor at forskrifter brukes for å gi virksomhetene retning og rammer for de vurderinger som skal utføres, følgelig må det også utarbeides gode veiledere. Dette er nødvendig for å sikre at virksomhetene innfører relevante og tilstrekkelige sikringstiltak som tar utgangspunkt i informasjonens verdi og det foreliggende trusselbildet. Resultatkrav til sikkerhet vil i den sammenheng være mer hensiktsmessige, og gi et større handlingsrom, fremfor tekniske krav.»

9.3.2 Sikkerhetsstyring

BDO uttaler om begrepsbruk innen sikkerhetsstyring at begrepet «tilstrekkelig opplæring i sikkerhetsspørsmål» ikke er presist nok, og anbefaler at dette endres.

DSS anbefaler at det lovfestes at det skal tas hensyn til standarder, og at ledelsessystem benyttes framfor styringssystem og uttaler:

> «Ansvaret for forebyggende sikkerhet etter loven påhviler leder for virksomheten. Forebyggende sikkerhet skal innarbeides som en del av virksomhetens ledelsessystem. Ledelsessystemet skal ta hensyn til relevante krav som gis av standarder for sikkerhetsområdet fra Norsk Standard og International Organization for Standardization (ISO).»

Nkom er positive til at lederansvaret lovfestes og uttaler:

> «Nkom er enig i at det er viktig med en konkret bestemmelse om plassering av ansvar i forhold til faktisk gjennomføring av sikkerhetslovens krav i den enkelte virksomhet. Dette er spesielt viktig i forhold til utviklingen i ekombransjen og andre bransjer med økt globalisering/outsourcing og samarbeid på tvers av landegrenser, der det kan oppstå fragmentering og uklarheter når det gjelder hvem som har det overordnede ansvaret for sikkerhet innen en virksomhet.»

NSM er positive til at det gis en bestemmelse om sikkerhetsstyring i loven, og poengterer at sikkerhetsstyring er helt sentralt for det systematiske arbeidet med sikkerhet i virksomhetene.

Oslo politidistrikt etterlyser tydelighet om hva som anses som «tilstrekkelig kompetanse» og etterlyser minimumskrav for å unngå store variasjoner i forståelse og praksis innen sikkerhetsarbeidet. De foreslår at slike minimumskrav gis i en forskrift om sikkerhetsstyring.

9.3.3 Vurdering av risiko

BDO uttaler at den oppfølgingen av virksomhetene i form av råd og veiledning som loven legger opp til, er svært omfattende. BDO mener loven ikke burde pålegge myndighetene den omfattende råd- og veiledningsplikten som er foreslått. BDO uttaler om dette:

> «I tillegg mener BDO det er viktig at myndighetsorganer ikke konkurrerer med private leverandører, også på dette området. […] Hvis det ikke er tilstrekkelige oppdrag til at det kan bygges opp gode kompetansemiljøer hos private tjenesteleverandører innen sikkerhet i Norge, som så kan bistå virksomheter som ikke kan få bistand fra offentlige myndigheter, vil det føre til dårligere samfunnssikkerhet. Samme situasjon vil i realiteten oppstå dersom Sikkerhetsmyndigheten, og da uten å måtte forholde seg til oppdraget som en anskaffelse fra kunden, skal gi inngående og konkrete råd til enkeltvirksomheter.
>
> BDO mener ikke med dette at Sikkerhetsmyndighetene ikke skal ha en praktisk tilnærming overfor virksomhetene. Vi mener imidlertid at myndighetene bør fokusere på å oppfylle veiledningsplikten i forvaltningsloven § 11 – dvs. gi veiledning om hvordan regelverket skal forstås og hvilke metoder virksomhetene bør benytte. Sikkerhetsmyndigheten bør derfor i stedet for å gi råd om konkrete tiltak og løsninger til enkeltvirksomheter, heller gi mer konkrete veiledninger, som retter seg til en ubestemt eller stor krets, gjerne i samarbeid med bransjeorganisasjoner.»

NSM mener lovforslaget legger opp til svært utstrakt rådgivningsplikt for sikkerhetsmyndigheten direkte til enkeltvirksomheter, noe som vil fordre en betydelig styrking av sikkerhetsmyndighetens organisasjon sammenliknet med i dag. *NSM* uttaler:

> «NSM mener at en «en-til-mange» tilnærming er mer hensiktsmessig når det gjelder rådgivning, der dette er mulig. I den grad det er ønskelig at NSM skal bedrive rådgivning overfor enkeltvirksomheter må det fremkomme at NSM selv kan prioritere hvem som skal motta slik rådgivning, basert på sin kunnskap om risiko.»

Nkom har uttrykt et behov for at det også gjøres vurderinger av risiko og sårbarhet for hver sektor:

> «I bestemmelsens tredje ledd pålegges sektormyndigheten som er gitt tilsynsansvar etter loven en veiledningsplikt overfor virksomheter for gjennomføring av slike ROS-analyser. Nkom mener at bestemmelsen også burde inneholde en plikt for sektormyndighet med tilsynsansvar til å gjennomføre og vedlikeholde

egne overordnede ROS-analyser for den aktuelle sektoren.»

DSB og *Utenriksdepartementet* mener bruken av ROS-analyse gir inntrykk av at loven har et bredere risikoperspektiv enn det loven er ment å dekke.

Utenriksdepartementet har uttalt om ROS-analyse:

> «I Utenriksdepartementets sikkerhetsarbeid skiller departementet mellom ROS-analyse og risikovurdering. Mens en ROS-analyse er en kartlegging skal virksomhetens leder i en risikovurdering ta standpunkt til hvorvidt den identifiserte risikoen kan aksepteres og/eller håndteres. Departementet foreslår som følge av dette at man i lovteksten legger til grunn begrepsapparatet som fremkommer i Norsk standard NS-ISO 31000:2009 og benytter begrepet risikovurdering fremfor ROS-analyse i lovteksten.
>
> Departementet ser utvalgets behov for å avgrense mot uønskede, ikke villede handlinger som f. eks naturkatastrofer. For virksomheter med et svært differensiert risikobilde som utenrikstjenesten, er det imidlertid viktig å samlet vurdere alle typer hendelser som kan utfordre tjenestens operative evne og dermed true grunnleggende nasjonale funksjoner.»

NSM mener begrepet risikoanalyse bør benyttes og har uttalt:

> «Det er sentralt at virksomhetene har samme metodiske tilnærming til de risikoanalyser som skal gjøres. NSM legger derfor til grunn at man i forskrift vil gi nærmere bestemmelser om hvordan disse analysene skal gjennomføres og hvem som skal etablere det metodiske grunnlaget.»

Oslo politidistrikt har uttalt om skranker knyttet til rådgivningen:

> «I kommentarene til denne bestemmelsen vises det til at rådgiving kan bidra til uheldige situasjoner bl.a. i forhold til regelverk og inhabilitet mv, og at sektormyndigheter må vurdere hvor langt man kan gå. Dette bør muligens også gjenspeiles i lovteksten.»

9.3.4 Krav til dokumentasjon og øvelser

NSM støtter kravet og har uttalt:

> «Bestemmelsen beskriver krav til dokumentasjon som skal foreligge hos virksomhetene. Det er et viktig krav og det er positivt at dette fremkommer klart.»

Oslo politidistrikt har uttalt om formålet med dokumentasjonskravet:

> «Det fremgår at hensikten med bestemmelsen er å legge til rette for tilsyn. Etter vår oppfatning må hensikten med dokumentasjon i en virksomhet må være å skriftliggjøre bestemmelser om organisering, herunder det som er angitt som krav i dagens forskrift om sikkerhetsadministrasjon kapittel 3. Dokumentasjonen brukes for å organisere egen virksomhets sikkerhetsarbeid.»

NSM og Oslo politidistrikt støtter et krav om gjennomføring av øvelser. NSM mener at formålet med øvelsene ikke bare er å gi de ansatte kompetanse og ferdigheter innen håndtering av hendelser, men også å avdekke eventuelle feil og mangler med relevant planverk som virksomheten har utviklet og avdekke mangler ved gjennomførte, eller mangel på gjennomføring av sikkerhetstiltak. Både *NSM* og *Oslo politidistrikt* mener det må gis nærmere konkretiseringer i forskrift.

9.3.5 Varsling

BDO mener bestemmelsen om varsling er for omfattende og har uttalt:

> «Forslaget til § 4-6 fastsetter i første ledd bokstav d at virksomheten omgående skal varsle brudd på sikkerhetskrav i kap.5, 6 og 7, eller forskrifter, til tilsynsmyndigheten. Bestemmelsen gir ingen vilkår eller unntak i så måte, og må således tolkes som at varslingsplikten gjelder alle sikkerhetsbrudd, uavhengig av alvorlighetsgrad. Kongen er i femte ledd riktignok gitt hjemmel til å gi forskrift om varslingsplikten, men BDO antar hjemmelen – slik den er formulert – ikke åpner for at Kongen kan gjøre unntak fra hvilke brudd som skal rapporteres eller med hvilke tidsintervaller.»

NSM mener bestemmelsen bør tydeliggjøre varslingskanalene og har uttalt:

> «Til bestemmelsens tredje ledd bemerkes at det i enkelte tilfeller kan være uklart hvilket departement som er ansvarlig. Dette gjelder for eksempel ved varsler mottatt fra kommunale organer, eller varsler som dreier seg om privat virksomhet uten en klar departementstilknytning, for eksempel datahaller. NSM legger til grunn at varsel i disse tilfellene skal sendes til Justis- og beredskapsdepartementet i kraft av departementets samordningsrolle på sivil side. Det bør imidlertid vurderes om dette skal tydeliggjøres i lovteksten eller eventuelt i forskrift.»

Oslo politidistrikt har uttalt:

> «Slik vi ser det, er det muligens bedre pedagogikk å benytte begrepet «rapportering» fremfor «varsling».»

NVE mener kravet om varsling vil medføre dobbeltvarsling for de virksomheter som allerede er underlagt andre krav om varsling om hendelser og har uttalt:

> «Forslaget § 4-6 annet ledd oppstiller en plikt til dobbeltvarsling både til tilsynsmyndighet etter sektorlovgivning og til sikkerhetsmyndigheten. Vi mener det er positivt at enkelte type hendelser bør varsles til flere enn tilsynsmyndigheten (f.eks. IKT-angrep). NVE er derimot skeptisk til et generelt krav til dobbeltvarsling. Det må være tilsynsmyndighetens ansvar å videreformidle til andre relevante myndigheter, deriblant sikkerhetsmyndigheten og overordnet departementet. NVE foreslår derfor at annet og tredje ledd i § 4-6 blir slått sammen og omskrevet til *nytt § 4-6 annet ledd*.»

Statnett mener i likhet med *NVE* at varslingsbestemmelsen vil medføre unødvendig dobbeltregulering, og at varsling innen energisektoren allerede er tilstrekkelig regulert. Videre stiller *Statnett* spørsmål ved myndighetenes ansvar for oppfølging av mottatte varsler og mener sektormyndighetene bør kunne ivareta varsling til sikkerhetsmyndigheten, og har i denne sammenhengen uttalt:

> «I utvalgets forslag til § 4-6 Varsling, står det blant annet at: «I samfunnssektorer der sektormyndigheter er gitt tilsynsansvar i medhold av § 3-1, skal Sikkerhetsmyndigheten varsles parallelt.» Med bakgrunn i at varsling og dialog under ekstraordinære hendelser allerede er krevende å håndtere, og med bakgrunn i at det allerede er etablerte rutiner for videre varsling ut mot andre sektorer, vurderer Statnett at en utvidet varslingsplikt ikke er hensiktsmessig. Formålet med bestemmelsen (side 260) er å legge til rette for at myndighetene kan ivareta sitt overordnede ansvar. Ved å følge etablerte varslingsrutiner vil formålet med bestemmelsen allerede være ivaretatt. Sikkerhetsmyndigheten vil kunne få en samlet fremstilling for hele sektoren fra NVE, og ikke stykkevis og delt fra den enkelte virksomhet.
>
> Statnett ber derfor om at forslaget om at selskapenes plikt om umiddelbar varsling og rapportering til Sikkerhetsmyndigheten endres til en plikt for sektormyndigheten om å varsle og rapportere. Dette kan gjennomføres uavhengig av om selskaper i energisektoren underlegges sikkerhetsloven eller ikke.»

Finanstilsynet har uttalt at selv om varsling etter sikkerhetsloven for enkelte vil omfatte en dobbeltvarsling, vil dette likevel være formålstjenlig:

> «I forslaget til ny sikkerhetslov stilles krav til rapportering av hendelser til Sikkerhetsmyndigheten i tillegg til sektormyndigheten. Selv om det vil innebære en dobbeltrapportering for foretak omfattet av loven, er det Finanstilsynets vurdering at dette kan være en hensiktsmessig innretning. Det vil uansett være sektormyndigheten som har det primære ansvaret for oppfølging av varsler fra virksomheter i egen sektor.»

9.4 Departementets vurdering

Kapittelet om generelle krav til forebyggende sikkerhet er nytt sammenliknet med gjeldende sikkerhetslov. Kapittelet lovfester enkelte grunnleggende krav som i dag følger av sikkerhetslovens forskrifter. Utvalgets forslag legger i stor grad opp til at det skal utarbeides et underliggende forskriftsverk.

De generelle kravene til forebyggende sikkerhetsarbeid skal sette rammene for det forebyggende sikkerhetsarbeidet i virksomhetene. Dette gjøres ved å lovfeste virksomhetsansvaret, den metodiske tilnærmingen og vurderingene som må gjøres som grunnlag for prioriteringer av sikkerhetstiltak og risikoaksept, samt overordnet definere krav til sikkerhetsadministrasjon i virksomhetene. Videre framgår krav til virksomhetens

involvering av tilsynsmyndighetene som følge av handlinger mot virksomheten.

De generelle kravene er uttrykk for lovens funksjonelle innretning. Bestemmelsene gir i utgangspunktet virksomhetene frihet til å velge de mest hensiktsmessige løsningene tilpasset virksomhetens øvrige rammer. Bestemmelsene legger videre grunnlaget for mer metodiske, spesifikke og detaljerte løsninger i forskrift.

De generelle kravene i kapittel 4 er omtalt i utvalgets utredning i kapittel 7.7.9 og i de særlige merknadene til de enkelte bestemmelsene. Høringsinnspillene gir i det vesentlige uttrykk for støtte til at loven oppstiller generelle krav til forebyggende sikkerhet slik utvalget har foreslått. Enkelte høringsinstanser, blant annet *BDO, Statnett* og *NVE,* har gitt uttrykk for at loven kan medføre en dobbeltregulering av enkelte sektorer. Etter departementets syn vil utformingen av de generelle kravene kunne veie opp for dette, i og med at det langt på vei skal tas hensyn til hvordan tilsvarende krav reguleres i sektorlovgivningen. Andre høringsinstanser gir på den annen side uttrykk for at den manglende detaljeringsgraden gjør det vanskeligere å etterleve lovens krav, da det i for stor grad blir overlatt til virksomhetens skjønn å vurdere hvilke sikkerhetstiltak som er gode nok.

Etter departementets syn oppstiller de funksjonelle kravene en større grad av fleksibilitet, men med en mulighet for tilsynsmyndigheter å påse at virksomhetens vurderinger er gode nok. Tilsynet må også vurdere om valgt løsning «tar hensyn til alle hensyn». Virksomheten får også større behov for faglig informasjon for å finne en løsning som passer i den konkrete situasjonen som vedkommende er i, og tilsynsmyndigheten får en mer veiledende rolle enn detaljkontrollerende. Tilsynsmyndighetens pålegg kan med en slik tilnærming lettere bli gjenstand for diskusjon og faglig tvil.

Departementet har registrert høringsinnspillene fra *Oslo politidistrikt* og *Politidirektoratet* knyttet til bruken av funksjonelle krav, men mener det er gode grunner for den funksjonsbaserte tilnærmingen. Regelverket blir tilstrekkelig dynamisk til å følge utviklingen av de beste løsningene. Virksomhetene får handlefrihet og kan utnytte lokal og situasjonsspesifikk kunnskap til å finne egnede løsninger innenfor regelverkets rammer. Funksjonsregelverk ansvarliggjør i større grad virksomhetene for egen drift og de konkrete løsningene de velger. Funksjonsbaserte regler kan også i større grad bidra til at hensikten med reglene oppnås, og at virksomhetene også kan strekke seg lenger enn til fastsatte minimumskrav.

Departementet mener dette er en hensiktsmessig tilnærming på lovs nivå. Utvalget påpeker også at dersom lovens tilnærming er funksjonsbasert, bør også forskriftene så langt som mulig være det. Departementet er enig i dette, og viser til at for eksempel objektsikkerhet er et område hvor kravene bør være funksjonsbaserte. Samtidig ser departementet også at hensynet til forutberegnelighet og en helhetlig tilnærming til det forebyggende sikkerhetsarbeidet på tvers av sektorene oppstiller et behov for at det innen andre fagområder må være en større andel detaljkrav.

Departementet mener innholdet i utvalgets forslag til bestemmelser bør opprettholdes, men foreslår å gjøre noen endringer som departementet mener forenkler enkelte bestemmelser. Departementet foreslår å gjøre om på rekkefølgen av bestemmelsene for å få mer pedagogisk systematikk i kapittelet, slik *DSS* har påpekt i sin høringsuttalelse. Departementet mener det er mer hensiktsmessig at ansvar fastslås i kapittelets første bestemmelse, slik at utvalgets forslag til § 4-2 kommer først. Deretter følger metode for identifisering av behov og prioriteringer, slik at utvalgets forslag til § 4-3 blir ny § 4-2, og etter dette følger plikten til å iverksette tiltakene, som etter utvalgets forslag stod først i kapittelet.

I departementets forslag til § 4-1 fastslås lederansvaret. Det er virksomhetens leder som formelt bestemmer og fastsetter hvordan sikkerhetsarbeidet skal gjennomføres og organiseres. I hvor stor grad lederen selv er direkte involvert, avhenger av hvordan virksomheten beslutter å organisere sikkerhetsarbeidet. Selv der lederen ikke er direkte involvert i det daglige sikkerhetsarbeidet, er det fremdeles lederen som er ansvarlig. Myndighet og oppgaver kan delegeres, mens ansvaret for forebyggende sikkerhetsarbeid alltid vil tilligge virksomhetens leder.

Ansvaret innebærer å motivere ansatte til å være tilstrekkelig sikkerhetsbevisste i hverdagen, samt legge til rette for kontinuerlig forbedring og læring. Virksomhetens leder skal bidra til å skape et miljø der ansatte har lav terskel for å rapportere om avvik og sikkerhetstruende hendelser.

Virksomhetens leder er også ansvarlig for at sikkerheten i underlagte virksomheter og hos leverandører, kontrolleres. Ansvaret innebærer blant annet å etterspørre informasjon om sikkerhetstilstanden, herunder resultater fra eksterne tilsyn, interne sikkerhetsrevisjoner og leders jevnlige evaluering av sikkerhetstilstanden.

Det følger av utvalgets forslag at forebyggende sikkerhet skal innarbeides som en del av virksomhetens styringssystem, som departementet foreslår som ny § 4-1. Departementet mener dette er et viktig prinsipp som bør lovfestes. Dette er også støttet av flere av høringsinstanser blant andre *NSM* og *Nkom*. Sikkerhetsstyring er helt sentralt for det systematiske arbeidet med sikkerhet. Departementet anser det ikke som nødvendig å presisere nærmere i lovtekst hvordan dette skal gjøres, da dette bedre kan beskrives i forskrift.

Videre er det krav til at virksomhetens ansatte, leverandører og oppdragstakere skal ha tilstrekkelig opplæring i sikkerhetsspørsmål. Dette kravet framkommer i dag av forskrift om sikkerhetsadministrasjon § 3-2. Departementet er enig med utvalget i at dette bør lovfestes, men mener i likhet med *BDO* at begrepet «sikkerhetsspørsmål» er upresist. Departementet foreslår derfor å endre ordlyden til «tilstrekkelig risiko- og sikkerhetsforståelse». Vurderingen er skjønnsmessig, og må ses opp mot nærmere kompetansekrav som kan presiseres i forskrift. Det legges til grunn at virksomheten har et sterkere ansvar for oppfølging av egne ansatte enn de øvrige kategoriene, men virksomheten har også et ansvar for å følge opp at leverandører og oppdragstakere har en tilstrekkelig risiko- og sikkerhetsforståelse.

Utvalget har foreslått en plikt til å gjennomføre risiko- og sårbarhetsanalyse i lovforslaget § 4-3. Etter departementets forslag blir denne bestemmelsen til ny § 4-2.

Bestemmelsen har i høringen vært gjenstand for tilbakemeldinger knyttet til begrepet risiko- og sårbarhetsanalyse (ROS-analyse). Blant andre *DSS*, *Utenriksdepartementet* og *NSM* mener det bør benyttes et annet begrep enn ROS-analyse. *DSB* påpeker også at begrepet ROS-analyse tilsier at loven har et videre nedslagsfelt enn det som er intensjonen.

Departementet er enig i dette og mener at ROS-analyse er en analyse med et bredere risikoperspektiv enn lovens nedslagsfelt, og således kan framstå misvisende. Det har i høringen framkommet andre forslag til begrep, blant annet risikoanalyse og risikovurdering. Det har også kommet forslag om å angi bruken av en anerkjent standard i loven. For å unngå å knytte vurderingen opp mot et spesifikt begrep, hvor meningsinnholdet kan endres over tid, og for ikke å knytte vurderingen til en spesifikk standard, foreslår departementet kun å fastslå at det skal gjennomføres en «vurdering av risiko». På denne måten kan nærmere bestemmelser om gjennomføring av vurderingen gis i forskrift, og således være noe mer dynamisk og fleksibel.

Videre framkommer det av utvalgets forslag, et krav om at virksomhetene som en del av denne vurderingen må kartlegge hvilke andre virksomheter den er avhengig av for å opprettholde sin funksjonalitet. Begrunnelsen for dette er at vurderingen av risiko ikke må ses isolert i den enkelte virksomhet, men omfatte avhengighetsforholdene til andre virksomheter. Departementet støtter denne tilnærmingen. Departementet viser til at virksomheten likevel har et selvstendig ansvar for å redusere sin egen sårbarhet, for eksempel gjennom tiltak knyttet til egenberedskap for bortfall av strøm.

Et avgjørende moment for å gjøre en tilstrekkelig vurdering av risiko er tilgangen på oppdatert og relevant trussel- og sårbarhetsinformasjon. Denne bestemmelsen må derfor ses opp mot sikkerhetsmyndighetens råd og veiledningsplikt, samt plikt til tilrettelegging av deling av denne typen informasjon etter forslagets § 2-3. Departementet anerkjenner at virksomhetene har et visst råds- og veiledningsbehov knyttet til vurderingen av risiko. Virksomhetene må kunne etterspørre råd og veiledning fra både sikkerhetsmyndighet og sin sektormyndighet med tilsynsansvar. Hvordan ansvaret skal utøves i den enkelte sektor kan være gjenstand for regulering i samarbeidsavtale mellom sikkerhetsmyndigheten og sektormyndighet, der dette anses som nødvendig, eksempelvis der en sektormyndighet som gjennomfører tilsyn som følge av annet regelverk, er avskåret fra å gi konkret rådgivning. Departementet mener dette ikke er nødvendig å reflektere i loven.

Departementet har forståelse for utvalgets forslag om at sikkerhetsmyndigheten bør drive konkret rådgivning overfor de virksomheter som omfattes av loven. Rådgivningen bør i hovedsak omfatte overordnede råd, veiledninger og oppdatert trussel- og sårbarhetsinformasjon. Den foreslåtte mekanismen for deling av sikkerhetsrelevant informasjon vil være et nyttig bidrag i så måte. Departementet er enig med *BDO* og *NSM* i at det er viktig å unngå omfattende en-til-en veiledning overfor virksomheter fra myndighetssiden. Dersom virksomheten har behov for inngående støtte til å gjennomføre denne vurderingen for sin virksomhet, utover det som følger av myndighetenes veiledning og nærmere bestemmelser i forskrift, finnes det flere private aktører for dette formålet, slik også *BDO* har anført.

Utvalgets forslag til en bestemmelse om plikt til å gjennomføre sikkerhetstiltak foreslås plassert som § 4-3, framfor § 4-1, som var utvalgets forslag.

Gjennomføringen av sikkerhetstiltak må skje på bakgrunn av virksomhetens vurdering av risiko. Bestemmelsen angir et visst grad av skjønn for virksomhetene. Tiltakene skal til sammen danne et forsvarlig sikkerhetsnivå, og redusere risikoen for handlinger som kan skade virksomheten, samt redusere skadevirkningene dersom noe inntreffer. Videre skal også kostnadene ved sikkerhetstiltakene stå i rimelig forhold til det som oppnås ved tiltaket. Tiltakene skal ses i sammenheng med andre forebyggende tiltak som virksomheten har iverksatt.

Enkelte høringsinstanser, blant andre *NVE*, *Norsk olje og gass* og *BDO*, har kommentert at det er en fare for at sikkerhetslovens krav kommer i konflikt med sektorregelverk. Departementet mener at den overordnede og funksjonelle innretningen loven har, og samhandlingen mellom myndighetene for øvrig, langt på vei reduserer risikoen for kolliderende kravstilling og oppfølging, jf. også utvalgets omtale av dette i NOU 2016: 19 kapittel 7.7.12. Når det gjelder objektsikkerhet viser departementet til at dagens objektsikkerhetsforskrift har en bestemmelse som innebærer at sektorregelverket går foran forskriftens krav, så framt sektorregelverket har relevante og tilstrekkelige bestemmelser og det er etablert tilsynsorgan. Det er imidlertid ikke til å unngå en viss grad av overlappende regelverk. Dette er ikke noe særegent knyttet til forebyggende sikkerhetsarbeid. Departementet mener sikkerhetsmyndigheten og sektormyndighetene, sammen med virksomhetene, i den videre operasjonaliseringen av kravene, vil måtte ta hensyn til alle regelverk som stiller krav til sikkerhet.

Enkelte høringsinstanser, som *Oslo politidistrikt* og *Norsk olje og gass*, påpeker at bestemmelsen er for overordnet og generell, og at kravet om forsvarlig sikkerhetsnivå er for diffust og vanskelig å forholde seg til.

Departementet vil påpeke at forsvarlighetsstandarden er en rettslig standard som kun skal trekke opp de ytre rammene virksomhetene må forholde seg til, og gi virksomhetene mulighet til å se det totale omfanget av sikkerhetstiltak i sammenheng, også tiltak som ikke følger av sikkerhetsloven. Den nærmere grensedragning av hva som anses som forsvarlig, vil måtte utvikles i samarbeid mellom sikkerhetsmyndighet og sektormyndigheter. Videre vil de underliggende forskriftene gi nærmere føringer for hva som kan anses som forsvarlig innen de forskjellige fagområdene. Her kan det tenkes at forskriftene vil variere i detaljgrad, alt ettersom hvilket fagområde det er tale om. Videre vil forsvarlighetsnormen avhenge av hva som er god praksis innen fagområdene og veiledninger og anbefalinger fra sikkerhetsmyndigheten. Departementet forutsetter også, som blant annet *NSM* har påpekt, at forsvarlighetsvurderingen, og kostnadsvurderingen som skal gjøres, blir gjenstand for ettersyn og vurdering fra tilsynsmyndighetene.

Departementet mener at kravet om å gjennomføre øvelser er et godt sikkerhetstiltak, og viser til utvalgets vurderinger av kravet. Departementet mener imidlertid at formålet med øvelsene er mer enn det utvalget har foreslått og beskrevet i bestemmelsen. Det er vel så viktig å verifisere, eller avdekke, om tiltakene som er iverksatt virker som forutsatt, som å sikre at kompetansen til å forebygge og håndtere hendelser vedlikeholdes og utvikles. Departementet foreslår at kravet framgår av § 4-3 som et nytt tredje ledd og at nærmere bestemmelser om øvelser gis i forskrift med hjemmel i samme bestemmelse.

Utvalgets bestemmelse om krav til dokumentasjon foreslås som ny § 4-4, uten materielle endringer. Departementet vil presisere at nærmere krav til dokumentasjon vil måtte framgå av forskrift.

Utvalgets forslag til bestemmelse om varsling framgår nå av § 4-5 og regulerer virksomhetenes varslingsplikt knyttet til hendelser, eller handlinger, som anses å utgjøre en sikkerhetsrisiko. En varslingsplikt er en forutsetning for at myndighetene skal kunne ivareta sitt overordnede ansvar. Tidlig varsling om en hendelse er avgjørende for rask respons fra sektormyndighet og sikkerhetsmyndighet. At virksomhetene pålegges denne varslingsplikten er hovedsakelig av hensyn til at myndighetene skal kunne se hendelser i sammenheng, både på sektornivå og på nasjonalt nivå. En hendelse som rammer en virksomhet i én sektor, kan også ha rammet en virksomhet i en annen sektor, eller det kan være en fare for at det vil ramme andre virksomheter i andre sektorer. For at sikkerhetsmyndigheten skal kunne ivareta sitt sektorovergripende ansvar, er det ekstra viktig at denne kan motta varsler fra alle sektorer, også de sektorene der sikkerhetsmyndigheten ikke har et tilsynsansvar.

Statnett, *BDO*, *NVE* og *Finanstilsynet* har bemerket at varlingsbestemmelsen er detaljert, og samtidig medfører en parallellvarsling der sektorregelverket også har krav om varsling ved hendelser. *Finanstilsynet* og *NVE* bemerker imidlertid at en slik varslingsbestemmelse kan være hensiktsmessig, gitt sikkerhetsmyndighetens tverrsektorielle ansvar, men en forutsetning er at varsel følges opp av sektormyndigheten.

Departementet mener det må foreligge en plikt til varsling for virksomheter som blir utsatt for, eller det er grunn til å mistenke at den blir utsatt for, en handling som har til formål å skade informasjon, informasjonssystemer, infrastruktur eller objekter. Departementet mener denne bestemmelsen er viktig, uavhengig av sektorregelverket. Sikkerhetsloven er sektorovergripende og retter seg mot tilsiktede handlinger som kan skade nasjonale sikkerhetsinteresser. Det er derfor helt sentralt at et varsel kommer fram til den myndigheten som har den totale tverrsektorielle oversikten, slik at varslene kan ses i sammenheng. Videre er det avgjørende for å kunne fatte de nødvendige vedtak for å hindre aktivitet som kan innebære en ikke ubetydelig risiko mot nasjonale sikkerhetsinteresser, at myndighetene mottar varsel om slik aktivitet.

Departementet ser at det kan være vanskelig for en virksomhet å vurdere hvorvidt en hendelse den er utsatt for, skyldes en tilsiktet handling eller ikke. Også derfor er det viktig at det varsles til sikkerhets- og sektormyndighet, slik at hendelsen kan vurderes opp mot andre eventuelle hendelser i sektoren og nasjonalt. Det vil imidlertid være sektormyndighetene med tilsynsansvar etter § 3-1 som har det primære ansvaret for å følge opp de varsler som kommer fra virksomheter i egen sektor.

Bestemmelsene om varsling er til dels en videreføring av gjeldende bestemmelser i dagens sikkerhetslov og forskrift om sikkerhetsadministrasjon. I dagens lov framgår varsling om aktivitet som kan innebære en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført, av sikkerhetsloven § 5 a. Denne bestemmelsen foreslås videreført, hvor varslingsplikten om slik aktivitet fastslås i § 4-5, mens vedtakskompetansen til Kongen i statsråd for å stanse slik aktivitet, skal framgå av § 2-5. For nærmere omtale vises til kapittel 7.

Av forskrift om sikkerhetsadministrasjon kapittel 5 framgår bestemmelser om reaksjon ved sikkerhetstruende hendelser. Blant annet framgår krav om rapportering til Nasjonal sikkerhetsmyndighet for alle virksomheter som blir utsatt for en sikkerhetstruende hendelse, og reaksjoner ved sikkerhetsbrudd.

Bestemmelsen forutsetter at det etableres tydelige varslingsrutiner, og at det etableres tilstrekkelige mekanismer hos sikkerhetsmyndigheten og hos sektormyndigheter til å motta og respondere på varslene. Varslingslinjene bør fastsettes i et nærmere rammeverk for varsling mellom virksomheter og myndighetene.

Departementet er enig med høringsinstansene i at bestemmelsen er for omfattende når det gjelder varsling av ethvert sikkerhetsbrudd. Det anses som unødvendig og krevende å lovfeste at virksomheten omgående skal varsle om *alle* sikkerhetsbrudd, slik *BDO* påpeker i sin høringsuttalelse. Departementet foreslår derfor at det kun varsles om alvorlige brudd på sikkerhetskrav som følger av kapitlene 5, 6 og 7, og det forutsettes at nærmere rutiner for varsling fastsettes i forskrift, slik som i dagens regelverk. Departementet foreslår at utvalgets forslag til § 4-7 *Behandling av personopplysninger,* strykes. Departementet mener det ikke er nødvendig med en slik referanse i loven. Personvernforordningen vil bli implementert i norsk rett og sikkerhetsloven må være i samsvar med forordningen. Virksomheter som er underlagt dagens sikkerhetslov, er også underlagt personopplysningsloven. Departementet mener derfor bestemmelsen kan virke forvirrende. For øvrig er det gitt nærmere bestemmelser om behandling av personopplysninger i de bestemmelsene der dette er særskilt viktig.

10 Informasjonssikkerhet og informasjonssystemsikkerhet

10.1 Innledning

Sikkerhetsloven skal inngå som et viktig virkemiddel for sikkerhet i et samfunn i svært rask utvikling, der særlig informasjons- og kommunikasjonsteknologi utgjør en stadig viktigere faktor. På området informasjonssikkerhet og informasjonssystemsikkerhet har det kommet tydelige høringsinnspill som er uenige i utvalgets lovforslag og mener at det er nødvendig med endringer. Det har videre i løpet av lovarbeidet kommet råd fra Forsvaret og forsvarssektoren som dels utfyller disse høringsinnspillene og som også understreker Forsvarets framtidige behov. Basert på dette er det etter departementets vurdering tre forhold som er av sentral betydning for lovforslaget. Det første er den raske utviklingen og utbredelsen av informasjons- og nettverksteknologi. Det andre forholdet er at samfunnet og forsvarssektoren direkte og indirekte blir stadig mer avhengig av informasjonsteknologi, mens det tredje dreier seg om at lovens virkeområde utvides noe sammenlignet med tidligere lov.

Svært rask utvikling og utbredelse av avansert informasjons- og nettverksteknologi medvirker til at forsvarssektoren og samfunnet for øvrig tilbys stadig mer avanserte tjenester, med mål om å effektivisere samfunnsfunksjoner og sikre velstandsutviklingen. Utviklingen fører også til at teknologien ikke lenger bare er forbeholdt land vi gjerne sammenligner oss med, men nå også er tilgjengelig i et globalt marked. Imidlertid fører også teknologiutviklingen til økte sårbarheter både for forsvarssektoren og samfunnet for øvrig. Norges digitale sårbarheter er grundig utredet i NOU 2015: 13 *Digital sårbarhet – sikkert samfunn*. Dette er sårbarheter som det vil være nødvendig å forholde seg til både i en statssikkerhetskontekst og en samfunnssikkerhetskontekst. Disse sårbarhetene er imidlertid ikke statiske og vil over tid utvikles i både form og innretning, i nær sammenheng med teknologiutviklingen. For å møte denne utviklingen er det av stor betydning at loven har innebygd nødvendig fleksibilitet, og at loven kan tilpasses teknologiutviklingen over tid.

Forsvarssektoren og samfunnet for øvrig blir stadig mer avhengig av teknologi i nær sagt alle sammenhenger. Forsvaret bruker i stadig større grad teknologi til å utvikle militær evne og til å effektivisere militære operasjoner, i nært samarbeid med militære og sivile samarbeidspartnere. Samfunnet for øvrig bruker på samme måte teknologi til å effektivisere samfunnets virksomhet til beste for innbyggerne. I dag brukes informasjonsteknologi blant annet til å automatisere sentrale samfunnsfunksjoner som kraftforsyning, kommunikasjonstjenester og transporttjenester. Teknologi brukes også til å støtte effektiv produksjon og distribusjon av alle typer varer i det moderne samfunnet, som for eksempel mat og andre livsviktige forsyninger. Det vises i denne forbindelse til Meld. St. 27 (2015–2016) Digital agenda, hvor det er en omfattende gjennomgang av Norges digitale tilstand. Det pekes der blant annet på at IKT er vesentlig for innovasjon og produktivitet, at det er behov for styrket digital kompetanse og deltakelse og at personvern og informasjonssikkerhet skal være en integrert del av utviklingen og bruken av IKT.

Teknologien gir muligheter til å behandle og bruke informasjon på helt nye måter sammenlignet med tidligere. Mye av denne informasjonen vil kunne være skjermingsverdig. Nasjonale sivile og militære beredskapsplaner er eksempler på informasjon det vil være nødvendig å skjerme også i framtiden. Det samme gjelder løpende informasjon om konkrete situasjoner og tilstander innhentet fra etterretningskilder og sensorer som for eksempel radarer. Ulike tekniske informasjonstyper utgjør i dag en grunnleggende faktor for produksjon og styring av så godt som alle samfunnets grunnleggende tjenester, som for eksempel kraftforsyning, helse, ekom, transport og finans. Slik informasjon vil også til en viss grad kunne vurderes som skjermingsverdig, men vil samtidig kreve andre former for beskyttelse enn tidligere. Offentlig informasjon til befolkningen i forbindelse med hendelser er av sentral betydning for sivil og militær krisehåndtering. Tidligere hadde myndighetene god kontroll med at informasjonen som ble presentert gjennom tradisjonelle medier som

kringkasting og aviser, både var hensiktsmessig og korrekt. Nye teknologier har gitt samfunnet nye internettbaserte kommunikasjonskanaler som for eksempel sosiale medier. Slike kanaler kan også utgjøre betydelige sårbarheter dersom de blir misbrukt. Felles for alle disse eksemplene er at anvendelsen av teknologi samlet og enkeltvis utgjør en økende potensiell sårbarhet for samfunnet. Mangfoldet av typer informasjon det vil være nødvendig å skjerme er langt mer sammensatt enn tidligere, og vil også kreve en langt mer fleksibel tilnærming i en helhetlig risikobasert kontekst.

Forslaget til ny sikkerhetslov vil favne bredere enn nåværende sikkerhetslov og vil sannsynligvis omfatte flere private virksomheter enn tidligere. Samtidig er Forsvaret gjennom totalforsvaret blitt stadig mer avhengig av tilførsel av sivile varer og tjenester, også direkte i militære operasjoner. Informasjonsteknologi inngår nå som en tett integrert del av både militær og sivil virksomhet, der samhandling er en grunnleggende forutsetning. Et grunnleggende dilemma i sikkerhetslovens praktisering blir å etablere mekanismer som er balansert mellom det sivile samfunns behov for fleksibilitet og raske endringer, og behovet for å ivareta overordnede nasjonale sikkerhetsbehov. Sikkerhetsloven må derfor på den ene siden sørge for å ta høyde for et tilstrekkelig sikkerhetsnivå i et svært dynamisk samfunn, og samtidig må loven ta hensyn til de spillereglene som gjelder i et globalt konkurransemarked. Dette er en særlig stor utfordring på områdene informasjonssikkerhet og informasjonssystemsikkerhet, der endringene i og bruken av teknologi skjer svært raskt.

Informasjonssystemene som brukes for å behandle informasjon, har også endret karakter. Fra å være enkle fysiske redskaper som skrivemaskiner, teleksmaskiner og fysiske arkiv er dagens informasjonssystemer ofte komplekse datasystemer koblet i store og til dels globale nettverk. Økende kompleksitet sett sammen med systemenes økende betydning for mange viktige samfunnsfunksjoner gjør at også forvaltningen av loven blir vesentlig mer kompleks. Dette må tillegges særlig vekt i det videre arbeidet med forskrifter til loven.

Etter departementets vurdering har utvalget ikke i tilstrekkelig grad tatt inn over seg betydningen av utviklingen beskrevet ovenfor. Mange av utviklingstrekkene er godt beskrevet i NOU 2016: 19, men er likevel ikke i tilstrekkelig grad reflektert i lovforslaget. Departementet har derfor funnet det nødvendig å foreta enkelte endringer i utvalgets lovforslag for å gjøre loven mer tilpasset departementets vurdering av teknologi- og samfunnsutviklingen. Det er i disse endringene også tatt hensyn til Forsvarets behov. Det understrekes at dette er et krevende tema som videre må følges opp og videreutvikles i forskriftsarbeidet. Denne oppfølgingen må også knyttes opp mot oppfølgingen av Lysne I- og Lysne II-utvalget og stortingsmelding om IKT-sikkerhet (Meld. St. 38 (2016–2017)).

Sammenlignet med dagens sikkerhetslov foreslår utvalget særlig ett viktig grep innen informasjonssikkerhet. Forslaget går ut på at den nye sikkerhetsloven skal gi beskyttelse til informasjonssystemer som har viktige roller ved produksjon eller leveranse av grunnleggende nasjonale funksjoner. Departementet støtter dette forslaget.

Imidlertid mener departementet at det bør gjøres ytterligere grep for å ta høyde for den digitale utviklingen. Dette gjøres det nærmere rede for i det følgende. Det er ikke lenger tilstrekkelig å tenke hemmelighold når vi tenker på informasjonssikkerhet. Når man skal vurdere hvilken informasjon som må gis ekstra god beskyttelse, må det i større grad enn tidligere anerkjennes at informasjonens integritet og tilgjengelighet er verdifulle egenskaper. Denne utvidede tankegangen må man bringe med seg når man skal vurdere beskyttelsestiltak. Idet man anerkjenner at informasjonens integritet og tilgjengelighet også trenger beskyttelse, får man samtidig behov for en mer fleksibel tilnærming til hvordan informasjonen skal beskyttes. Utvalget foreslo en slik tilnærming for sikkerhetsgradert informasjon. Etter departementets syn må tilnærmingen gjelde for all informasjon som etter lovforslaget er skjermingsverdig. Det må dessuten aksepteres at det kan være behov for individuelle tilpasninger, noe loven må legge til rette for.

Flere høringsinstanser har pekt på utfordringer med praktiseringen av instruks 17. mars 1972 nr. 3352 for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen). Departementet har forståelse for disse synspunktene. Siden utvalget ikke har funnet det hensiktsmessig å vurdere beskyttelsesinstruksen, se NOU 2016: 19 kapittel 8.6.7, har departementet ikke funnet det hensiktsmessig å gå nærmere inn på dette regelverket i forbindelse med arbeidet med en ny sikkerhetslov.

10.2 Gjeldende rett

10.2.1 Informasjon som skal beskyttes etter sikkerhetsloven

Etter sikkerhetsloven § 11 skal en konkret verdivurdering av informasjonen ligge til grunn for om den skal beskyttes etter sikkerhetsloven. Avgjørende for verdivurderingen er i hvilken grad informasjonen kan skade «Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser» dersom informasjonen blir kjent for uvedkommende. Spørsmålet som må stilles, er hva en aktør med onde hensikter kan bruke informasjonen til, som kan skade nasjonale sikkerhetsinteresser. Informasjonens verdi kan beskrives som skadepotensialet ved konfidensialitetsbrudd.

Informasjonens skadepotensial må være på et visst nivå for at den skal falle inn under sikkerhetsloven. Den nedre grensen følger av sikkerhetsloven § 11 bokstav d. Informasjon som, dersom den blir kjent for uvedkommende*, i noen grad kan skade* nasjonale sikkerhetsinteresser, jf. § 11 bokstav d, omfattes dermed av sikkerhetsloven, og skal behandles og beskyttes deretter. Informasjon som har et *større* skadepotensial omfattes også av loven, men må beskyttes bedre. Det er ingen øvre grense. Informasjon som har et *mindre* skadepotensial, som ikke i noen grad kan skade nasjonale sikkerhetsinteresser, omfattes følgelig ikke av sikkerhetsloven. Det kan likevel være at denne informasjonen faller inn under og skal beskyttes i henhold til andre regelverk, for eksempel personopplysningsloven, beredskapsforskriften eller beskyttelsesinstruksen.

Som beskrevet i NOU 2016: 19 kapittel 8.6.1, side 168, sondrer sikkerhetsloven mellom begrepene skjermingsverdig informasjon og sikkerhetsgradert informasjon:

> «Førstnevnte brukes om all informasjon i materiell eller immateriell form som må beskyttes av hensyn til rikets sikkerhet. Skjermingsverdig informasjon oppfyller kriteriene for sikkerhetsgradering. Hvorvidt informasjonen har blitt sikkerhetsgradert etter sikkerhetsloven § 11 har ikke betydning for om informasjonen skal anses som skjermingsverdig. Begrepet sikkerhetsgradert informasjon omfatter skjermingsverdig informasjon som er blitt påført sikkerhetsgradering i henhold til § 11.»

Departementet slutter seg til denne beskrivelsen.

10.2.2 Beskyttelse av skjermingsverdig informasjon

Sikkerhetsloven har flere bestemmelser om tiltak for å beskytte sikkerhetsgradert informasjon. Sikkerhetstiltakene gjenspeiler at loven kun omfatter informasjon som har skjermingsbehov. Det følger likevel av § 12 andre ledd andre punktum en forskriftshjemmel til å legge forholdene til rette for at sikkerhetsgradert informasjon er korrekt, fullstendig og tilgjengelig.

Etter sikkerhetsloven § 11 andre ledd er det «den som utsteder eller på annen måte tilvirker skjermingsverdig informasjon som plikter å sørge for at informasjonen merkes med aktuell sikkerhetsgrad.» Det følger av § 11 første ledd at det skal foretas en konkret verdivurdering av informasjon. Avhengig av informasjonens skadepotensial skal den sikkerhetsgraderes enten BEGRENSET, KONFIDENSIELT, HEMMELIG eller STRENGT HEMMELIG.

§ 12 fastsetter en taushetsplikt for sikkerhetsgradert informasjon og prinsippet om at tilgang til informasjonen kun kan gis til personer som har tjenstlig behov for dette. Videre fastsetter loven krav til informasjonssystemsikkerhet, kryptosikkerhet, tekniske sikkerhetsundersøkelser, monitoring og inntrengingstesting. Mer utfyllende regler om beskyttelsestiltak følger av forskrift 1. juli 2001 nr. 744 om informasjonssikkerhet (informasjonssikkerhetsforskriften). For en nærmere beskrivelse av nevnte sikkerhetstiltak, samt kryptosikkerhet og tekniske sikkerhetsundersøkelser vises det til NOU 2016: 19 kapittel 8.2.1.

10.2.3 Informasjonssystemsikkerhet

I sikkerhetsloven § 3 første ledd nr. 10 defineres *informasjonssystemer* slik:

> «en organisert samling av periferiutrustning, programvare, datamaskiner og kommunikasjonsnett som knytter dem sammen.»

Det følger av gjeldende sikkerhetslov § 13 at informasjonssystemer som skal behandle sikkerhetsgradert informasjon må godkjennes av Nasjonal sikkerhetsmyndighet eller den de bemyndiger før behandlingen starter. Bestemmelsen angir samtidig hvilke informasjonssystemer som skal beskyttes etter sikkerhetsloven, det vil si informasjonssystemer som behandler sikkerhetsgradert informasjon. Slike systemer kalles ofte *graderte systemer.* Med unntak av § 15 første ledd om monitoring omhandler sikkerhetsloven kun graderte

systemer. Systemer som ikke behandler sikkerhetsgradert informasjon, beskyttes dermed ikke av sikkerhetsloven.

De grunnleggende bestemmelsene for beskyttelse av informasjonssystemer følger av informasjonssikkerhetsforskriften kapittel 5. Utvalget har i utredningen kapittel 8.2.1.1 følgende oppsummering av reglene, som departementet stiller seg bak:

> «Det heter i forskriften § 5-1 at sikkerhet i informasjonssystemer skal vurderes opp mot de grunnleggende egenskapene autentisitet, konfidensialitet, integritet og tilgjengelighet til systemets data og tjenester. Videre fremheves brukernes ansvarlighet for egne handlinger og tilliten til at sikkerhetstiltak er korrekt implementerte og ivaretar sikkerheten på en effektiv og hensiktsmessig måte. § 5-2 setter som hovedmål for sikkerheten en sikker plattform, sikker drift, vedlikehold og sikker hendelseshåndtering og gjenoppretting.
>
> I forskriften §§ 5-3 og 5-4 gis det bestemmelser om hva som skal oppnås gjennom sikkerhetstiltak. For eksempel skal tilgjengelighet sikres ved at data beskyttes mot uønsket sletting og tjenester beskyttes mot uønsket reduksjon/stans. Tiltakene skal videre forebygge, detektere, reagere på, kontrollere sikkerhetsbrudd, samt gjenopprette informasjonssystemets sikre tilstand.
>
> Sikkerhetsprinsipper som skal legges til grunn ved utarbeidelse av tiltak, følger av forskriften § 5-5 […]. Videre gis det i forskriften kapittel 5 regler om systemtekniske og administrative sikkerhetskrav, sikkerhetsgodkjenning av informasjonssystemer og sikkerhetsdokumenter.»

Enkelte konkrete sikkerhetstiltak følger imidlertid av loven. § 13 fastsetter som nevnt krav om *forhåndsgodkjenning* av graderte systemer. Det samme følger av forskriften § 5-24. Som utgangspunkt er det virksomhetens leder som godkjenner informasjonssystemet, jf. forskriften § 5-28 andre ledd. Bestemmelsen setter imidlertid begrensninger for hvilke systemer virksomhetens leder kan godkjenne. Informasjonssystemet må være lokalisert i Norge og må ikke ha forbindelse til utlandet, til informasjonssystemer utenfor egen virksomhet eller utenfor kontrollert område.

Etter loven § 15 første ledd og forskriften kapittel 11 kan det foretas *monitoring* av en virksomhets informasjonssystemer. Dette omfatter også informasjonssystemer som ikke behandler sikkerhetsgradert informasjon. Det følger av forarbeidene (Ot.prp. nr. 49 (1996–97) side 6) at monitoring betyr kontroll av «tjenestlig kommunikasjon i og mellom informasjonssystemer, gjennom avlytting av tale eller avlesing av elektroniske saker.» Formålet er å avdekke om det lagres, behandles eller kommuniseres informasjon med høyere sikkerhetsgradering eller skjermingsverdi enn det systemet er godkjent for, jf. informasjonssikkerhetsforskriften § 11-1. Dette innebærer blant annet å kontrollere en virksomhets informasjonssystemer som ikke er ment for behandling av sikkerhetsgradert informasjon, for å se om det likevel behandles gradert informasjon i disse systemene.

Sikkerhetstiltaket monitoring vil ofte innebære behandling av personopplysninger og kan dermed ikke gjennomføres uten videre. I Ot.prp. nr. 49 (1996–97), side 40, ble behovet for monitoring vurdert opp mot tiltakets personvern- og rettssikkerhetskonsekvenser:

> «Det er departementet syn at monitoring er et viktig tiltak for å oppnå god forebyggende informasjonssikkerhet, og at monitoringtjenesten således bør opprettholdes. Sikkerhetsbrudd forekommer fremdeles. Rapporter fra Nasjonal sikkerhetsmyndighet om sikkerhetsbrudd blir tatt alvorlig av avdelinger i Forsvaret, og ordningen må antas å ha en positiv effekt ved å bidra til å hindre at et større antall kompromitteringer forekommer. Ordningen er et supplement, ikke et alternativ, til andre virkemidler for å oppnå respekt for skjermingsverdig informasjon. For øvrig bør nevnes at dagens monitoringstjeneste uansett må opprettholdes som følge av forpliktelser etter NATOs regelverk.
>
> […]
>
> De gjeldende restriktive begrensninger mht gjennomføringen av kontrollen, vil naturligvis bli opprettholdt. Den Norske Advokatforening uttaler om dettte i sin høringsuttalelse at en «... har merket seg at det foreslås lovfestet at monitoring ikke i noe tilfelle skal omfatte privat kommunikasjon som blir formidlet til eller fra andre enn virksomheter og at informasjon som fremkommer ved kontroll skal makuleres når den ikke lenger har betydning for kontrollen. Av personvernhensyn er det viktig at det i forskriftene etableres betryggende kontrollrutiner for å sikre at disse regler blir fulgt.» Departementet slutter seg til uttalelsen, og vil sørge for at betryggende kontrolltiltak iverksettes.»

Om konklusjonen uttaler departementet videre på side 40:

> «Dagens monitoringsvirksomhet har etter departementets oppfatning et aktverdig formål, representerer ikke et uforholdsmessig inngrep og kan ikke ses å ha vesentlige rettssikkerhetsmessige implikasjoner, bl.a tatt i betraktning de begrensninger og retningslinjer for gjennomføring av monitoring som er nedfelt i gjeldende direktiver gitt av Forsvarssjefen. Selv om hjemmelsgrunnlaget anses tilfredsstillende i dag, basert på eierrådighetsbetraktninger og avtale-/samtykkesynspunkter, vil det være naturlig å lovfeste hovedreglene om monitoring i en samlet lov om forebyggende sikkerhetstjeneste.»

Utvalget skriver i NOU 2016: 19 kapittel 8.2.1.3 videre at:

> «Av rettssikkerhets- og personvernhensyn stiller loven flere absolutte krav som må være oppfylt før monitoring kan iverksettes. Den virksomhet som skal kontrolleres må enten selv anmode om eller, dersom NSM har tatt initiativet, samtykke til gjennomføring av kontrollen. Samtykket eller anmodningen skal skje skriftlig, jf. informasjonssikkerhetsforskriften § 11-4 fjerde ledd. Monitoring kan dessuten kun iverksettes i virksomheter som er underlagt sikkerhetsloven og bare tjenestelig kommunikasjon kan kontrolleres. Dersom det i løpet av kontrollen viser seg at nevnte vilkår ikke er oppfylt, skal monitoringen avbrytes umiddelbart, jf. informasjonssikkerhetsforskriften § 11-7.
>
> Det stilles også krav om at alle ansatte og andre direkte berørte må varsles i forkant om at det vil bli gjennomført kontroll, om hensikten med og varigheten av kontrollen, at NSM gjennomfører og på hvilken måte kontrollert informasjon blir behandlet. Det er kun NSM som kan gjennomføre monitoring i henhold til sikkerhetsloven. Etter endt monitoring skal NSM rapportere til virksomheten om resultatet av kontrollen.»

Departementet slutter seg til denne beskrivelsen.

Sikkerhetsloven § 15 andre ledd og forskriften om informasjonssikkerhet kapittel 11 regulerer inntrengingstesting av informasjonssystemer. Dette sikkerhetstiltaket har en del til felles med, men skiller seg også noe fra, monitoring. Det følger av forskriften § 11-2 at formålet med tiltaket er å teste informasjonssystemets motstandsdyktighet for å kontrollere om sikkerhetsgradert informasjon beskyttes i tråd med fastsatte krav. Det handler altså om å forsøke å bryte seg inn i informasjonssystemet. Gjennomføring av inntrengingstesting kan innebære behandling av personopplysninger. Derfor er det krav om blant annet samtykke fra virksomheten og varsling av ansatte. Det er imidlertid ikke krav om å avbryte kontrollen dersom kontrolløren kommer over privat informasjon, slik som ved monitoring.

Sikkerhetsloven § 13 a om sikkerhetsmessig overvåkning trådte i kraft 1. januar 2017 og fastsetter krav om at virksomheten overvåker egne informasjonssystemer for å avdekke ulovlig inntrenging. Det framgår av forarbeidene (Prop. 97 L (2015–2016), side 39) til bestemmelsen at loggingen skal

> «gjøre virksomheten i stand til å foreta en vurdering av omfanget og karakteren av skaden som har oppstått, gjenopprette sikker tilstand, samt sikre sporbarhet og ansvarlighet for utførte handlinger i samsvar med kravene i sikkerhetsloven for øvrig.»

For dette tiltaket vil det også kunne bli aktuelt å behandle personopplysninger. Om ivaretakelsen av personvernet i disse tilfellene uttales det i forarbeidene (Prop. 97 L (2015–2016), side 38):

> «Departementet vil innledningsvis presisere at forslaget er avgrenset til systemer som er godkjent for behandling av sikkerhetsgradert informasjon. Dette er systemer som er klare etterretningsmål, og som derfor må ha et høyt sikkerhetsnivå. Sikkerhetsmessig overvåking av disse systemene slik at angrep på et tidlig tidspunkt kan oppdages, og omfanget kartlegges, framstår derfor etter departementets vurdering som nødvendig.
>
> De systemer som vil være gjenstand for overvåking etter forslagets § 13 er i mindre grad egnet til, eller beregnet for, kommunikasjon av privat karakter, eller annen type privat bruk. Dette er lukkede systemer uten direkte tilknytning til internett. Omfanget av privat kommunikasjon og privat bruk av disse systemene vil derfor være begrenset. Det vil likevel være slik at kommunikasjon av privat karakter vil kunne forekomme, da primært som e-post eller nettprat med videre, mellom brukerne i det lukkede systemet.
>
> […]

> Omfanget av systemer som blir gjenstand for sikkerhetsmessig overvåking etter § 13 a er også av et begrenset omfang. Det er kun et fåtall systemer i offentlig forvaltning som er godkjent for å behandle sikkerhetsgradert informasjon, og som således vil være underlagt kravene til sikkerhetsmessig overvåking i § 13 a.»

For en nærmere beskrivelse av gjeldende rett vises det til NOU 2016: 19 kapittel 8.2. For en oversikt over fremmed rett som dekker kapittel 10.2 til 10.4, se NOU 2016: 19 kapittel 8.4.

10.3 Utvalgets forslag

10.3.1 Informasjon som skal beskyttes etter sikkerhetsloven

Utvalget foreslår å videreføre gjeldende rett. Lovforslaget § 5-1 er likevel ikke helt lik dagens § 11. Endringene består i tilpasninger til lovforslagets øvrige bestemmelser og en forenkling av enkelte elementer.

Utvalget legger en vid forståelse av begrepet informasjon til grunn. Det framgår av utvalgets merknad til § 5-1 i NOU 2016: 19, side 261 at

> «[b]egrepet *informasjon* skal forstås vidt. Måten informasjonen er tilvirket på og hvilken form informasjonen har er ikke relevante momenter i vurderingen av om noe er informasjon. Begrepet omfatter for eksempel informasjon i form av fysiske dokumenter, digitale og maskinlesbare signaler, film, lydopptak og muntlige opplysninger. I vurderingen av om noe skal anses som informasjon skal det legges vekt på om det er egnet til å tilføre en trusselaktør kunnskap som denne direkte eller indirekte kan benytte til å skade grunnleggende nasjonale funksjoner.»

Utvalget drøfter særlig innholdet i verdivurderingen av informasjon og stiller spørsmål om hensynene til informasjonens integritet og tilgjengelighet også burde inngå i vurderingen, i tillegg til konfidensialitetshensynet. NOU 2016: 19 kapittel 8.5.1 gjør rede for noen generelle utgangspunkter for informasjonssikkerhet:

> «For det første må informasjonens verdi angis. Verdivurderingen gir svaret på om informasjonen er beskyttelsesverdig. Informasjonens verdi deles ofte opp i ulike kategorier. De mest brukte er konfidensialitet, integritet og tilgjengelighet. Avhengig av situasjonen benyttes også eksempelvis sporbarhet, ikke-benektbarhet og flere andre. I det videre er det tilstrekkelig å benytte de tre hovedkategoriene.
>
> Med *konfidensialitet* menes at det har en verdi at informasjonen ikke blir kjent for uvedkommende. Et eksempel på informasjon som må beskyttes av konfidensialitetshensyn, er Norges Banks sikkerhetsrutiner.
>
> Med *integritet* menes at det har en verdi at informasjonen er korrekt. Eksempelvis må programkode være korrekt for at dataprogrammet skal virke. Beskyttelse mot tap av integritet innebærer å sørge for at det ikke lar seg gjøre å endre programkoden. I motsetning til beskyttelse av konfidensialitet er det ikke viktig om andre kan lese programkoden.
>
> Med *tilgjengelighet* menes at det har en verdi at informasjonen er tilgjengelig ved behov. Eksempelvis er det fordelaktig å ha bruksanvisningen til badevekten som er tilkoblet hjemmenettverket tilgjengelig den dagen det kommer opp en feilmelding i displayet. Beskyttelse eller ivaretakelse av tilgjengeligheten kan innebære å mangfoldiggjøre informasjonen og oppbevare den på et lett tilgjengelig sted.
>
> Dersom verdivurderingen konkluderer med at informasjonen er beskyttelsesverdig, er neste steg å vurdere informasjonens beskyttelsesbehov. Det må foretas en vurdering av aktuelle sårbarheter og trusler.»

Utvalget legger videre til grunn at verdivurderingen i mange tilfeller vil vise at informasjonen er verdifull med hensyn til alle tre egenskapene.

Utvalget drøfter så disse prinsippene opp mot behovet for beskyttelse i en sikkerhetslovkontekst under kapittel 8.6.1:

> «Som nevnt i kapittel 8.5.1 fokuserer dagens regelverk på lovs nivå særlig på informasjonens konfidensialitet. Utvalget har vurdert om informasjonens integritet og tilgjengelighet bør likestilles med konfidensialiteten. Informasjon kan i mange tilfeller være svært viktig for nasjonens sikkerhet, herunder opprettholdelse av grunnleggende nasjonale funksjoner. Dersom en trusselaktør klarer å endre, slette eller gjøre informasjonen utilgjengelig for de som trenger den, vil dette kunne ha negativ innvirkning på sentrale myndigheters evne til å opprettholde viktige funksjoner. Det er fullt mulig både å endre, slette og gjøre informasjon utilgjengelig uten at en er kjent med informa-

sjonen. Dette vil særlig gjelde for elektronisk lagret informasjon, men også dokumenter må beskyttes mot uønsket påvirkning. Utvalget har ikke funnet grunn til å endre kriteriene for angivelse av hvilken informasjon som skal beskyttes etter sikkerhetsloven. Det bør fortsatt være behovet for å bevare informasjonens konfidensialitet, som er inngangskriteriet for om informasjonen skal sikkerhetsgraderes, og dermed beskyttes etter sikkerhetsloven. Etter utvalgets syn ville det unødig komplisere identifiseringen av informasjon som skal beskyttes, dersom integritet og tilgjengelighet skulle vært ytterligere inngangskriterier. Sett i sammenheng med digitaliseringen og at viktige ugraderte informasjonssystemer skal beskyttes, legger utvalget til grunn at mye viktig ugradert informasjon fanges opp og beskyttes gjennom bestemmelsene om informasjonssystemsikkerhet.»

Utvalget anerkjenner altså behovet for beskyttelse også av informasjonens integritet og tilgjengelighet i en nasjonal sikkerhetskontekst, men mener dette ivaretas godt nok gjennom reglene om informasjonssystemsikkerhet.

Etter gjeldende lov § 11 skal informasjonens skadepotensial vurderes opp mot nasjonale sikkerhetsinteresser. Ettersom utvalget foreslår andre begreper for å angi lovens formål og virkeområde, foreslås det tilsvarende endringer i bestemmelsen om sikkerhetsgradering. Systematikken er likevel den samme. Utvalget skriver om dette i merknaden til lovforslaget § 5-1:

> «Ordlyden i bestemmelsen skiller seg noe fra tidligere lov. Endringen innebærer at man ved skadevurderingen må ta hensyn til skadepotensialet for hele lovens virkeområde, se nærmere i merknad til § 1-2. Tidligere lov nevnte eksplisitt hensynene til vitale sikkerhetsinteresser og alliertes sikkerhet. Slike hensyn er fortsatt relevante, jf. § 1-2.»

Utvalget foreslår å fjerne sondringen mellom skjermingsverdig informasjon og sikkerhetsgradert informasjon. Det framgår følgende av kapittel 8.6.1:

> «Begrepet *sikkerhetsgradert informasjon* foreslås benyttet for all informasjon som trenger beskyttelse av hensyn til grunnleggende nasjonale funksjoner. Begrepet *sikkerhetsgradert informasjon* i den nye loven vil dermed omfatte både *skjermingsverdig* og *sikkerhetsgradert* informasjon etter gjeldende sikkerhetslov, det vil si all informasjon som skal beskyttes etter den nye sikkerhetsloven.»

10.3.2 Beskyttelse av skjermingsverdig informasjon

Utvalget foreslår med ett unntak å videreføre alle dagens bestemmelser om tiltak for å beskytte informasjon. Det er likevel foreslått enkelte justeringer og en ny generell bestemmelse om beskyttelse av informasjon i § 5-2.

Utvalget mener det ikke er behov for å regulere kryptosikkerhet på lovs nivå og viser til at det er tale om et spesifikt sikkerhetstiltak som ikke må reguleres i lov. Utvalget foreslår derfor å fjerne bestemmelsen om kryptosikkerhet fra loven og heller regulere dette i forskrift. Utvalget påpeker at det fortsatt er behov for en tilsvarende regulering som i dag og at det er mest naturlig at Nasjonal sikkerhetsmyndighet fortsetter å forvalte kryptosikkerheten.

I lovforslaget § 5-2 foreslår utvalget en ny generell bestemmelse om beskyttelse av sikkerhetsgradert informasjon. Bakgrunnen for forslaget framgår av NOU 2016: 19 kapittel 8.5.1. Utvalgets vurdering framgår av NOU 2016: 19 kapittel 8.6.1:

> «Informasjon som er blitt sikkerhetsgradert skal så beskyttes både av hensyn til konfidensialitet, integritet og tilgjengelighet. At de to sistnevnte hensynene ikke fremgår av dagens lov, betyr antakelig ikke at de anses irrelevante. Blant annet nevnes alle hensynene som relevante for informasjonssystemsikkerhet, jf. informasjonssikkerhetsforskriften kapittel 5. Utvalget mener i alle tilfelle at plikten til å ivareta alle tre hensynene bør komme tydelig frem i loven. I denne sammenheng må det understrekes at et forsvarlig sikkerhetsnivå forutsetter en god verdivurdering.»

Utvalget foreslår at informasjonssystemsikkerhet bør reguleres i et eget kapittel i loven.

Utvalget foreslår for øvrig enkelte endringer for å ivareta personvernet bedre og ellers endringer av språklig og redaksjonell karakter.

10.3.3 Informasjonssystemsikkerhet

10.3.3.1 Informasjonssystemer som skal beskyttes etter sikkerhetsloven

Utvalget foreslår flere endringer innen informasjonssystemsikkerhet for å sikre et dynamisk og tidsriktig regelverk som er i tråd med digitaliseringen av samfunnet. Utvalget legger til grunn at det finnes en rekke informasjonssystemer som er av avgjørende betydning for om en virksomhet evner å opprettholde sine kritiske tjenester. Utvalget skriver om dette under kapittel 8.6.2:

> «I kategorien ugraderte IKT-systemer befinner det seg både tradisjonelle informasjons- og kommunikasjonssystemer, og såkalte kontroll- og styringssystemer. Nærmere bestemt er dette datasystemer som styrer, og eller kontrollerer, industrielle prosesser og tjenesteleveranser, eksempelvis innenfor telekom og strømproduksjon. Utvalget mener at denne typen systemer, i den grad de er kritiske for grunnleggende nasjonale funksjoner, må beskyttes mot uønskede tilsiktede hendelser. Konfidensialiteten er ikke nødvendigvis like viktig for disse systemene, men den kan heller ikke avskrives. Her som ellers må det foretas en konkret vurdering av det enkelte systems skjermingsbehov. Først etter en slik vurdering blir det klart om informasjonens konfidensialitet må beskyttes.
>
> De ugraderte IKT-systemer som skal beskyttes etter den nye loven, har det til felles at dersom systemet faller ut vil det svekke virksomhetens evne til å understøtte eller opprettholde den grunnleggende nasjonale funksjonen som gjør at de omfattes av sikkerhetsloven. Et grunnleggende spørsmål ved vurderingen er: hva må beskyttes for at den grunnleggende nasjonale funksjonen skal opprettholdes?»

Utvalget foreslår altså at sikkerhetsloven skal omfatte ugraderte informasjonssystemer som er av kritisk betydning for grunnleggende nasjonale funksjoner. Utvalget foreslår også å videreføre beskyttelse av dagens såkalte *godkjente informasjonssystemer.* Som samlebegrep for alle informasjonssystemer som skal beskyttes etter loven, foreslår utvalget å benytte *skjermingsverdige informasjonssystemer.* Se nærmere om dette i lovforslaget § 6-1 og tilhørende merknader.

10.3.3.2 Beskyttelse av skjermingsverdige informasjonssystemer

Utvalget foreslår å videreføre alle dagens sikkerhetstiltak som gjelder informasjonssystemer. Selv om tiltakene videreføres, foreslår utvalget en del mindre endringer. Det var særlig behov for tilpasninger til det øvrige lovforslaget og for bedre å ivareta personvernet.

Utvalget foreslår å ta inn i loven en ny og generell bestemmelse om beskyttelse av skjermingsverdige informasjonssystemer. Det følger av merknadene til lovforslaget § 6-2:

> «Bestemmelsen fastsetter en plikt for virksomheten til å beskytte virksomhetens skjermingsverdige informasjonssystemer. Virksomhetens ROS-analyse, jf. § 4-3, vil danne grunnlaget for å angi hvilke informasjonssystemer som skal beskyttes etter sikkerhetsloven.
>
> Virksomheten plikter å oppnå et forsvarlig sikkerhetsnivå for informasjonssystemene. *Bokstav a og b* konkretiserer hva som ligger i begrepet ved å angi hovedmålene for sikkerhetstiltakene. Ivaretakelse av *a og b* må ses i sammenheng. Eksempelvis er det ikke tilstrekkelig å bare se på sikkerhetsgraderingsnivået for et sikkerhetsgradert informasjonssystem, se kapittel 8.6.2. ROS-analysen vil danne grunnlaget for iverksettelse av de sikkerhetstiltak som er mest hensiktsmessige for det enkelte system. Det vil kunne variere fra system til system hva som skal til for å oppnå et forsvarlig sikkerhetsnivå.»

Om *sikkerhetsmessig godkjenning* av informasjonssystemer uttaler utvalget under kapittel 8.6.4:

> «Utvalget mener at *sikkerhetsmessig godkjenning av informasjonssystemer* er et viktig sikkerhetstiltak som bør videreføres. Utvalget har vurdert om også ugraderte informasjonssystemer som omfattes av loven, bør underlegges et slikt godkjenningssystem. En godkjenningsplikt vil kunne bidra til at både anskaffelse og anvendelse av så vidt viktige informasjonssystemer holder et forsvarlig sikkerhetsnivå. Når det gjelder informasjonssystemer som skal behandle sikkerhetsgradert informasjon, anbefaler utvalget at dagens krav til forhåndsgodkjenning videreføres. Det kan imidlertid stille seg annerledes for ugraderte informasjonssystemer. Det kan også for slike systemer være riktig å kreve forhåndsgodkjenning. Utvalget mener likevel at det for

disse systemene ikke skal være en lovbestemt plikt til forhåndsgodkjenning. Dette vil dessuten gjøre overgangen fra gjeldende til ny sikkerhetslov enklere. Utvalget anbefaler at det overlates til Kongen å utforme nærmere bestemmelser om godkjenningsprosessen, herunder om det er behov for ulike løsninger i ulike sektorer eller for ulike typer informasjonssystemer, hvor omfattende prosessene skal være, og hvem som skal gis myndighet til å kunne godkjenne slike systemer.»

Utvalget foreslår å videreføre *monitoring* som sikkerhetstiltak, men foreslår å erstatte begrepet monitoring med *kommunikasjons- og innholdskontroll av informasjonssystemer*. Utvalget setter en klar premiss for videreføringen i kapittel 8.6.4:

«Når utvalget foreslår en videreføring må det understrekes at det er en absolutt forutsetning med en videreføring også av forbudet mot kontroll av privat kommunikasjon og kommunikasjon med virksomheter som ikke er underlagt sikkerhetsloven.»

Kommunikasjons- og innholdskontroll skal etter lovforslaget § 6-5 kunne gjennomføres i alle virksomhetens skjermingsverdige informasjonssystemer.

Utvalget vurderte om det burde være en lovfestet plikt til å gjennomføre *inntrengingstesting*. Utvalget viste til de mange ulike typene systemer som bestemmelsen omfatter, og ville ikke utelukke at tiltaket i noen tilfeller kunne være direkte uhensiktsmessig. Det ble derfor konkludert med at det ikke var behov for en plikt. Utvalget uttaler videre under kapittel 8.6.4:

«Inntrengningstesting vil dessuten kunne innebære behandling av personopplysninger. Utvalget antar at det vil kunne virke mindre inngripende at den enkelte virksomhet må ta initiativ til gjennomføring av tiltaket, fremfor at det foreligger en rettslig plikt.»

Av personvernhensyn mener utvalget det burde gjøres enkelte endringer i bestemmelsen.

Utvalget mener at *sikkerhetsmessig overvåking* er et «helt nødvendig tiltak for å beskytte skjermingsverdige informasjonssystemer i tilstrekkelig grad». I motsetning til kommunikasjons- og innholdskontroll og inntrengingstesting mener utvalget at virksomhetene må ha en plikt til å gjennomføre sikkerhetsmessig overvåking av sine informasjonssystemer. Utvalget foreslår også her enkelte endringer sammenlignet med dagens bestemmelse. Blant annet at et absolutt krav om en viss mengde lagring for noen vil kunne være svært byrdefullt. Utvalget foreslår også en mer generell angivelse av hvilken informasjon som kan lagres og registreres. I forslaget ligger også en tydeliggjøring av personvernhensyn.

10.4 Høringsinstansenes syn

10.4.1 Informasjon som skal beskyttes etter sikkerhetsloven

Direktoratet for forvaltning og IKT (Difi) viser til forslaget om å videreføre konfidensialitet som eneste inngangsverdi for beskyttelse etter loven, og bemerker at

«det vil være uheldig om en utvidelse av sikkerhetslovens virkeområde påvirker virksomheters vurdering av hensiktsmessig balanse mellom konfidensialitet, integritet og tilgjengelighet.»

Difi skriver også at dagens bruk av informasjonssikkerhet omfatter både konfidensialitet, integritet og tilgjengelighet.

Etter *Forsvarets forskningsinstitutts (FFI)* syn er Forsvarets framtidige behov i for liten grad ivaretatt, for eksempel på områdene kommando- og kontroll i framtidige operasjoner, militær etterretning og operasjonssikkerhet. Forsvarets behov for sikkerhet er for tiden inne i en dramatisk endring uten at *FFI* ser at dette i nødvendig grad er reflektert i lovforslaget. Det er for eksempel svært viktig å utdype forholdet mellom de grunnleggende sikkerhetsfaktorene tilgjengelighet, konfidensialitet og integritet, og hvordan disse skal behandles i den framtidige loven.

Kommunal- og moderniseringsdepartementet viser til digitaliseringen av samfunnet og uttaler at utvalget burde hatt en mer balansert tilnærming til hvordan informasjonen skal beskyttes etter sikkerhetsloven. Balansen mellom de tre sikkerhetsaspektene (konfidensialitet, tilgjengelighet og integritet) må ivaretas på en slik måte at beskyttelsen av de funksjonene som behandler informasjonen, er så god som mulig. Dette er helt avgjørende for å ivareta de verdiene som sikkerhetsloven skal hegne om.

Nasjonal kommunikasjonsmyndighet (Nkom) mener i korte trekk at sikkerhetsloven også bør beskytte informasjon som ikke har sterke konfidensialitetsbehov. Det innebærer at også integritet og tilgjengelighet bør være kriterier som infor-

masjonen må vurderes etter. Dette er ikke tilstrekkelig ivaretatt gjennom bestemmelsene om beskyttelse av ugraderte systemer.

Oslo politidistrikt uttaler at begrepet skjermingsverdig informasjon bør videreføres, blant annet fordi det er et innarbeidet begrep. Når det gjelder beskyttelse av sikkerhetsgradert informasjon, mener *Oslo politidistrikt* at bruken av minimumskrav bør videreføres. *Politidirektoratet* støtter *Oslo politidistrikts* synspunkter.

Skattedirektoratet viser til at forslaget innebærer en videreføring av at det utelukkende skal være konfidensialitet som er driver for om informasjon skal beskyttes etter sikkerhetsloven. *Skattedirektoratet* mener dette kan bidra til at loven unnlater å omfatte viktige sikkerhetsområder som kan omfatte tilsiktede uønskede hendelser. Dette kan blant annet være informasjon som er åpen og ugradert, men som i seg selv er svært viktig å beskytte av integritetshensyn. Noen eksempler på dette kan være informasjon til befolkningen som gjøres tilgjengelig på troverdige nettsteder som for eksempel www.regjeringen.no og www.nrk.no, i det daglige og spesielt i forbindelse med krise eller konflikt. Falske nyheter kan bidra til destabilisering. Slike informasjonskanaler er av vital betydning for nasjonen og bør kunne underlegges sikkerhetsloven basert på behovet for beskyttelse med hensyn til integritet alene.

NSM bemerker at kapitteloverskriften Informasjonssikkerhet gir et misvisende inntrykk fordi det kun er sikkerhetsgradert informasjon som omhandles.

Telenor er av den oppfatning at innføringen av et nytt samlebegrep *sikkerhetsgradert informasjon* ikke nødvendigvis fører til en klargjøring. Det er heller ikke tydeliggjort hvordan skjermingsverdig informasjon i ugraderte systemer blir behandlet i NOU 2016: 19 og lovforslaget. Dersom det er slik at det nye begrepet sikkerhetsgradert informasjon ikke omfatter skjermingsverdig informasjon i ugraderte systemer, anser *Telenor* dette som en mangel i lovforslaget. Dersom informasjon om nasjonal samfunnskritisk infrastruktur/samfunnskritiske funksjoner blir kjent og misbrukt av uvedkommende, vil det kunne ha store nasjonale konsekvenser. Denne type informasjon bør graderes etter sikkerhetsloven, selv om informasjonen ikke kan behandles i graderte systemer. Denne type informasjon lagres og behandles i dag i systemer som benyttes til å sikre levering av blant annet telekommunikasjonstjenester, og som aldri vil tilfredsstille kravene til behandling av sikkerhetsgradert informasjon slik det framstilles i lovforslaget. Denne type «skjermingsverdig informasjon» kan *Telenor* ikke se er hensyntatt og oppfatter at dette vil medføre at informasjonen ikke blir beskyttet på rett nivå. Informasjonssikkerhetsforskriften er i dag gjeldende kun for graderte systemer.

10.4.2 Beskyttelse av skjermingsverdig informasjon

NSM slutter seg til de overordnede prinsipper som defineres for beskyttelse av sikkerhetsgradert informasjon. Det er nødvendig med tverrsektorielle minstestandarder både for å ivareta hensyn til sektorvise særegenheter og internasjonale forpliktelser. *NSM* støtter derfor forslaget om forskriftshjemmelen for dette formålet. *NSM* uttaler videre at de minstekrav som hjemles i § 5-2 andre ledd må omfatte alle relevante fagområder for beskyttelse av sikkerhetsgradert informasjon. Dette omfatter også krav til informasjonssystemer som behandler slik informasjon (herunder bruk av krypto), jf. lovforslagets kapittel 6, til personell som skal ha tilgang til slik informasjon, jf. lovforslagets kapittel 8, og til leverandører i forbindelse med sikkerhetsgraderte anskaffelser, jf. lovforslagets kapittel 9. Det må også kunne stilles minstekrav til virksomheters sikkerhetsorganisasjon og sikkerhetsstyring jf. lovforslagets kapittel 4. På denne bakgrunn bør det vurderes om denne forskriftshjemmelen mer naturlig hører hjemme i kapittel 4.

Norges Rederiforbund skriver at for at kravene til informasjonssikkerhet skal kunne ivaretas bør loven beskrive hvordan en godkjent infrastruktur skal etableres og driftes. Etter *Rederiforbundets* syn vil myndighetene måtte levere både arkitekturen og rammevilkårene for slik kommunikasjon. Dersom løsningen på problematikken ikke i større utstrekning beskrives i loven, vanskeliggjøres en tidsmessig relevant implementering med påfølgende forskriftsmessig forvaltning og bruk av selve systemene.

Direktoratet for samfunnssikkerhet og beredskap (DSB) påpeker utfordringer med sikkerhetsgraderingsregimet. De uttaler blant annet at

> «gradering av informasjon gjør det vanskeligere å gjøre helhetlige vurderinger av risiko og risikoreduserende tiltak, og at forankring av sikkerhetsmessige utfordringer og problemstillinger i ledelsen og organisasjonen blir vanskeligere å få til.»

Statnett mener det er viktig at et nasjonalt regelverk for sikkerhet og beredskap ses i sammen-

heng med det kommende europeiske regelverket som forutsetter og pålegger til dels betydelig utveksling av sensitiv informasjon, for å ivareta hensynet til et felles energimarked med god forsyningssikkerhet for alle. Beredskapsforskriftens kapittel 6 har egne bestemmelser om hva som er sensitiv informasjon i energiforsyningen (kraftsensitiv informasjon), og hvordan denne skal beskyttes. Med sensitiv informasjon menes spesifikke og inngående opplysninger om energiforsyningen som kan brukes til å skade anlegg eller påvirke funksjoner som har betydning for energiforsyningen. Hensikten med bestemmelsen er overlappende med både dagens sikkerhetslov og forslaget til ny sikkerhetslov.

Informasjon som kan misbrukes av ondsinnede aktører, skal beskyttes. Det store skillet i denne sammenheng er styrken i barrierene, og at beredskapsforskriften ikke har flere graderinger av sensitiv informasjon. Der hvor sikkerhetsloven har sin styrke med høy grad av teknisk og organisatorisk konfidensialitet, legger beredskapsforskriften i større grad til rette for en balanse mellom konfidensialitet, integritet og tilgjengelighet.

Deling av informasjon med entreprenører, leverandører og faste ansatte over hele landet er en forutsetning for å ivareta forsvarlig drift av kraftsystemet, og en forutsetning for å gjøre nødvendige investeringer for framtidens kraftsystem. Økt deling av informasjon med europeiske transmisjonsselskaper og markeder er videre en utvikling drevet av endringer i EUs energilovgivning. Selv mindre endringer i verdivurderingen av informasjon for det som i dag faller inn under taushetsbestemmelsene i beredskapsforskriften, vil kunne føre til at Statnett må etablere et nytt landsdekkende gradert samband med tilhørende behov for et stort antall sikkerhetsklareringer. Det må legges til at Statnetts landsdekkende nett anses å ha høy grad av konfidensialitet, integritet og tilgjengelighet. En endring av verdivurdering av informasjon i dette informasjons- og kommunikasjonssystemet vil etter *Statnetts* syn kunne utfordre nødvendig tilgjengelighet, og bremse tiltak knyttet til sikkerhet og beredskap. Eksempelvis behandles ROS-analyser og beredskapsplaner på anlegg og administrative kontorer rundt om i landet, og en gradering etter sikkerhetsloven av disse dokumentene vil måtte føre til ombygging og godkjenning av flere hundre sambandspunkter for å ivareta behovet for å behandle disse etter sikkerhetslovens krav. Det reises også spørsmål om dette vil medføre behov for etablering av et stort antall rom over hele landet som er godkjent for å behandle sikkerhetsgradert informasjon. En eventuell endring av verdivurdering fra energiloven til sikkerhetsloven vil også kunne gjøre Statnetts og Norges deltagelse i utviklingen av det europeiske energimarkedet svært krevende. Usikkerhet vil kunne oppstå ved verdivurdering av sensitiv informasjon. For de første hos den som utarbeider og produserer informasjon i det enkelte selskap som er underlagt to lovverk med samme formål. For det andre mellom to ulike myndigheter som forvalter hvert sitt lovverk med samme formål. For å skape et tydelig og forutsigbart skille, og dermed en tydelig og forutsigbar forvaltning av informasjon i energiforsyningen, må informasjon om kraftforsyningsanlegg med tilhørende systemer reguleres etter energiloven. Dette vil også gi nødvendig fleksibilitet med hensyn til nødvendig deling av informasjon med norske og utenlandske leverandører og samarbeidsparter.

Direktoratet for e-helse viser til at Norm for informasjonssikkerhet i helse- og omsorgstjenesten (Normen) er etablert som et viktig regulatorisk instrument i sektoren. Direktoratet ber om at det tas spesielt hensyn til denne normen ved utforming av nytt regelverk om informasjonssikkerhet.

Telenor støtter utvalget i at plikten til å ivareta alle tre hensynene til informasjonssikkerhet (konfidensialitet, integritet og tilgjengelighet) innarbeides i ny lov. Dette forsterker at det innen informasjonssikkerhet er mange hensyn som skal ivaretas, herunder tilgjengelighet til kritisk funksjonalitet, tjenester og infrastruktur. *Telenor* peker videre på at det innen deres sektor behandles informasjon som burde vært gradert etter sikkerhetsloven. Imidlertid må denne informasjonen behandles i ugraderte systemer som ikke vil kunne tilfredsstille kravene til behandling av sikkerhetsgradert informasjon.

Thales viser til at loven utvides til også å gjelde informasjon og informasjonssystemer for kritiske samfunnsfunksjoner, og foreslår å definere en ny kritikalitetsgradering for informasjonssikkerhet i kapittel 5, med fokus på integritet og tilgjengelighet. Det anbefales å benytte samme eller lignende kategorier som i «§ 7-2 Klassifisering» (MEGET KRITISK, KRITISK, VIKTIG). Om det er informasjonen, informasjonssystemet eller begge som skal kritikalitetsgraderes, så plasserer man definisjonen der det er mest hensiktsmessig, enten i kapittel 5 om informasjonssikkerhet eller i kapittel 6 om informasjonssystemsikkerhet.

10.4.3 Informasjonssystemsikkerhet

Flere av høringsinstansene understreker viktigheten av styring av informasjonssikkerhet og informasjonssystemsikkerhet i en tid der disse temaene har fått økende betydning for sikkerheten i et gjennomdigitalisert samfunn. Høringsinstansene vektlegger imidlertid til dels ulike sider ved informasjonssystemsikkerheten i sine mer detaljerte kommentarer. Flere av høringsinstansene forventer at antallet informasjonssystemer som kan bli omfattet av loven, vil øke og at de selv vil kunne bli omfattet av loven. Mange av høringsinstansene mener at det er hensiktsmessig. Likevel uttrykkes det blant annet fra *Samferdselsdepartementet* en usikkerhet om hvilke krav som vil stilles til sikkerhetsnivå for i utgangspunktet åpne eller ugraderte informasjonssystemer. For noen skaper dette også usikkerhet om dette kan medføre uforutsette kostnader for virksomhetene i framtiden.

Telenor anbefaler blant annet at det etableres vurderingskriterier og prosesser som sikrer at det blir sammenheng mellom utpeking av kritiske systemer innad i en sektor og på tvers av sektorer.

Departementenes sikkerhets- og serviceorganisasjon (DSS) anbefaler at det i lovteksten eksplisitt tas inn at det må tas hensyn til internasjonale standarder.

Noen etater fremmer synspunkter om at det allerede finnes sektorkrav som delvis samsvarer eller overlapper med lovforslagets bestemmelser. *Finans Norge* peker i den sammenheng på at bankene ikke bør påføres økte eller parallelle byrder. *Statnett* og *Norges vassdrags- og energidirektorat (NVE)* peker på at det bør legges opp til at sektorvise særbehov blir ivaretatt. *Statnett* peker også på at det er uklart hva som ligger i forslaget om å åpne for å etablere flere ulike godkjenningsprosesser og godkjenningsmyndigheter, jf. utvalgets merknad til § 6-3 i NOU 2016: 19, side 263. *Statnett* uttrykker behov for at loven vil møte behovet for at ulike virksomheter innen kraftbransjen både innenlands og utenlands også i framtiden kan knyttes sammen i digitale grensesnitt.

Kommunal- og moderniseringsdepartementet mener det må være en forutsetning at sikkerhetsmyndigheten blir tilført tilstrekkelig med ressurser til å ta på seg den store oppgaven som de gis i lovforslaget. *Kommunal- og moderniseringsdepartementet* mener i den sammenheng at det bør vurderes å øke bruken av sikkerhetsgodkjente aktører for å avlaste sikkerhetsmyndigheten.

Det framgår av høringsinnspillene at det er ulike oppfatninger av sammenhengen mellom hva som oppfattes å inngå i bestemmelsene om informasjonssystemsikkerhet og hva som inngår i bestemmelsene om objekt- og infrastruktursikkerhet. *NSM* peker i den sammenheng på at det ligger en utfordring i grensedragningen mellom informasjonssystemene og systemer som vil omfattes av lovens kapittel om skjermingsverdige objekter og infrastruktur.

NSM påpeker videre at de overordnede prinsippene om informasjonssystemsikkerhet bør suppleres med at tiltakene skal sikre ivaretagelse av «autentisitet, ansvarlighet og tillit». Det må dessuten kunne stilles krav til minimumstiltak.

NSM savner en logikk i at systemer som behandler sikkerhetsgradert informasjon skal forhåndsgodkjennes, mens andre skjermingsverdige informasjonssystemer også skal godkjennes, men uten at det er krav om slik godkjenning før de tas i bruk. *NSM* foreslår at også systemer som behandler informasjon av kritisk betydning for nasjonale funksjoner skal forhåndsgodkjennes. *NSM* uttaler dessuten:

> «Det er viktig med sentral oversikt over alle godkjente systemer. Dette er også nødvendig for å kunne ivareta våre forpliktelser overfor NATO. Det må derfor være en tydelig hjemmel for at Sikkerhetsmyndigheten skal kunne ha oversikt over alle godkjente systemer. Det må vurderes nærmere om det er tilstrekkelig at denne hjemmelen etableres i forskrift.»

NVE mener at det ikke bør innføres krav til godkjenning av systemer som ikke skal behandle sikkerhetsgradert informasjon.

NSM peker videre på at lovforslaget ikke synes å gi hjemmel for kommunikasjons- og innholdskontroll av andre systemer enn de som er sikkerhetsgodkjente. Direktoratet argumenterer videre for at det er viktig at slik kontroll også i framtiden skal kunne foretas på ugraderte systemer. *NSM* påpeker også at det bør være mulig for sikkerhetsmyndigheten å samle inn og analysere funn og erfaringer fra kommunikasjons- og innholdskontroll for å utvikle metodikk og som grunnlag for risikovurderinger. Etter *NSMs* syn bør virksomheten motta rapport etter endt kontroll.

DSS og *Oslo politidistrikt* uttrykker at kontroll og test av informasjonssystemer bør legges inn som del av tilsynets virkemidler. *DSB* drøfter også denne problemstillingen i sin uttalelse, der de peker på mellomløsninger der det også er andre enn sikkerhetsmyndigheten som kan foreta slike tester og at det kan foregå på regelmessig basis.

Inntrengingstesting i skjermingsverdige informasjonssystemer er foreslått å være frivillig og samtykkebasert. *NSM* uttrykker imidlertid at det bør vurderes om inntrengingstester også skal kunne benyttes som ledd i sikkerhetsmyndighetens tilsynsaktivitet.

NSM påpeker at forslaget om å avbryte en operasjon med inntrengingstesting med en gang sikkerhetsmyndigheten klarer å trenge inn i informasjonssystemet, vil bryte med dagens praksis og dramatisk kunne redusere verdien av en inntrengingstest. Dette blir blant annet begrunnet med at det ofte vil være mer enn en vei inn i et system, og at en slik begrensing vi redusere muligheten for analyse av svakheter og sårbarheter.

NSM uttaler dessuten:

> «Til femte ledd bemerkes at det også må være mulig for Sikkerhetsmyndigheten å samle og analysere funn og erfaringer fra inntrengningstesting til bruk i risikovurderinger, for å forbedre sikkerhetstiltak, herunder videreutvikling av metodikk for inntrengningstesting, revurdering av gitte sikkerhetsmessige godkjenninger, samt forbedring av rådgivningsarbeidet. En ny lov bør gi tydelig hjemmel for dette.»

NSM påpeker også at dersom det i forskrift legges til rette for at andre enn sikkerhetsmyndigheten kan gjennomføre inntrengingstester av skjermingsverdige informasjonssystemer, må det etableres kriterier og rettslig grunnlag for slik virksomhet.

Datatilsynet har ingen konkrete kommentarer til bestemmelsene som innebærer behandling av personopplysninger, men har en generell merknad:

> «Datatilsynet mener det er positivt at rapporten inneholder et eget kapittel om [forebyggende] sikkerhet og rettssikkerhetsgarantier, hvor personvern er godt beskrevet. Vi ser at det er gjennomgående i rapporten at der det foreslås inngrep eller tiltak som kan påvirke den enkeltes personvern, viser utvalget til vurderinger de har gjort og kommer med anbefalinger for å redusere personvernkonsekvensene, samtidig som man ivaretar sikkerheten. Dette gjenspeiles i stor grad også i lovforslaget.»

10.5 Departementets vurdering

10.5.1 Informasjon som skal beskyttes etter sikkerhetsloven

Temaene informasjonssikkerhet og informasjonssystemsikkerhet er i høringsinnspillene i begrenset grad blitt gjenstand for detaljerte kommentarer og innspill. Likevel peker mange av høringsinstansene på viktigheten av at bestemmelsene om informasjonssikkerhet blir gitt god og tidsmessig behandling i lovarbeidet. Dette blir etter departementets oppfatning også viktig gitt en begrenset utvidelse av lovens virkeområde, der det blant annet forventes at flere virksomheter i sivil sektor vil bli omfattet av loven enn i dag. Dette er virksomheter som gjennom lang tid har utviklet egendefinerte løsninger med IKT-systemer og sikkerhet basert på egen sektors særlige behov. Det er etter departementets syn nødvendig med en hensiktsmessig tilpasning også til disse virksomhetenes behov basert på et helhetlig risikobasert og kostnadseffektivt regime. Dette begrunnes med behovet for at virksomheten i størst mulig grad skal kunne utvikle sin kommersielle virksomhet.

Selv om en ny sikkerhetslov vil få større betydning for sivile aktører enn dagens lov, er det etter departementets syn svært viktig også å ivareta forsvarssektorens behov ved utarbeidelse av nytt regelverk. Dette aspektet ble i liten grad vurdert av utvalget. Slik departementet oppfatter det, er det også for militære aktiviteter et klart behov for endringer i eksisterende sikkerhetslov. Særlig kan forholdet mellom skjerming og deling av informasjon trekkes fram som viktige faktorer for å oppnå effektivitet og slagkraft i framtidens digitaliserte forsvar. Sett fra et militært perspektiv bør en ny sikkerhetslov legge grunnlaget for mer effektive og målrettede materiellanskaffelser tilpasset den løpende utviklingen av teknologi og trusselbilde, enn det dagens sikkerhetslov legger opp til. Det bør også vurderes om en ny sikkerhetslov vil utgjøre et grunnlag for hensiktsmessig operativ sikkerhet i militære operasjoner og digitale operasjoner innenlands og utenlands.

Utvalget hadde i sitt arbeid en grunnleggende oppfatning av at informasjonssikkerhet i utgangspunktet var tilfredsstillende dekket med tilnærmingen i gjeldende sikkerhetslov. Etter utvalgets syn var hensynet til graderingsregimet i NATO et viktig argument for ikke å gjøre større endringer på området informasjonssikkerhet. Ut fra en forståelse av utviklingen innen informasjonsteknologi innen sivil sektor fant utvalget det likevel nødvendig å gjøre visse utvidelser og presiseringer i

forhold til gjeldende sikkerhetslov, for å ta inn over seg endringer i behovet for sikkerhet i IKT-baserte tjenester. Dette gjelder særlig behovet for beskyttelse av informasjonssystemer.

Etter departementets syn er dette likevel ikke tilstrekkelig for å oppnå tilfredsstillende tidsmessighet i bestemmelsene. Høringsinnspill fra både offentlige og private aktører, sett i sammenheng med Forsvarets behov, viser at det bør tas inn en prinsippbestemmelse om informasjonssikkerhet i lovteksten. Denne vil tydeliggjøre at alle de tre grunnleggende sikkerhetsegenskapene konfidensialitet, integritet og tilgjengelighet er viktige, og at de må ses i sammenheng. Departementet foreslår å benytte *skjermingsverdig informasjon* som samlebegrep for all informasjon som skal beskyttes etter sikkerhetsloven.

Skjermingsverdig informasjon skal altså i denne lovproposisjonen omfatte både informasjon som etter dagens sikkerhetslov er sikkerhetsgradert, og informasjon som må beskyttes av integritets- og tilgjengelighetshensyn. Begrepet *sikkerhetsgradert informasjon* videreføres fra gjeldende rett og brukes om den informasjonen som ut fra en verdivurdering pekes ut som skjermingsverdig ut fra en ren konfidensialitetsvurdering, se figur 10.1. Årsaken til videreføringen er blant annet at begrepet er godt innarbeidet i forvaltningen og fremdeles har en sentral plass i andre bestemmelser i loven.

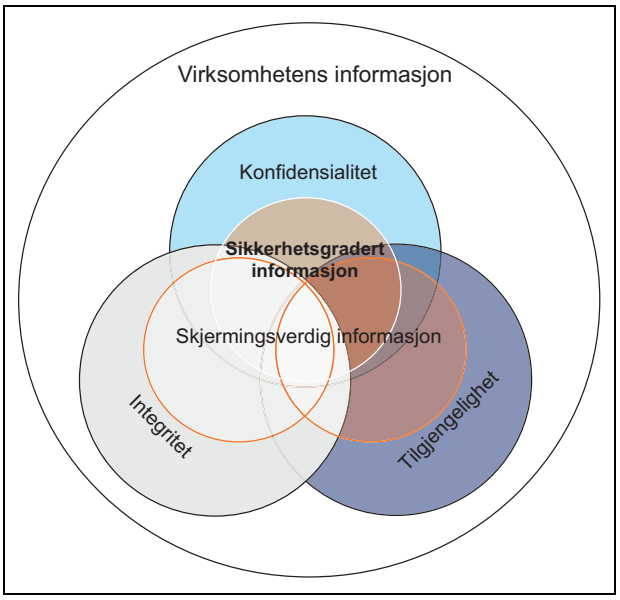
I dagens sikkerhetslov er det i hovedsak samsvar mellom bruken av begrepene skjermingsverdig informasjon og sikkerhetsgradert informasjon. I NOU 2016: 19 foreslås det kun å videreføre begrepet sikkerhetsgradert informasjon som en forenkling av bestemmelsene. Etter dagens lov blir kun informasjon som er verdivurdert som skjermingsverdig på grunn av konfidensialitetshensyn, sikkerhetsgradert.

Behovet for integritetsbeskyttelse har blitt tydeligere med tiden. I praksis har prosessen rundt konfidensialitetsbeskyttelse også i stor grad gitt nytte for å sikre informasjon som krever integritetsbeskyttelse. Ulempen med denne tilnærmingen er at den stadig oftere kommer i direkte konflikt med behovet for å dele informasjon i virksomheter og mellom virksomheter. Dette gjelder blant annet i mange tilfeller der informasjon inngår som viktig virkemiddel i prosesser og funksjoner, både i militær og sivil kontekst.

Manglende mulighet til å dele informasjon kan ha store konsekvenser for operativ evne i militære operasjoner og en virksomhets evne til å produsere varer og tjenester. Eksempler på dette er styringssystemer for vann og kraft og signalsystemer for togframføring. Disse styringssystemene vil kunne inneholde svært mye informasjon som ikke har særlig behov for konfidensialitetsbeskyttelse. Mye av denne informasjonen vil være behandlet i mange ulike prosesser i til dels store systemer, og vil kunne være foredlet i samarbeid med mange eksterne kilder. En svært liten del av informasjon brukes imidlertid også til selve styringsfunksjonen av den fysiske infrastrukturen i vannverk, kraftforsyningsnett og signalene til togene. Dette vil være informasjon som vil kunne vurderes å være skjermingsverdig etter den nye lovens systematikk, fordi det er så viktig at informasjonen er korrekt og tilgjengelig. Konsekvensen av integritetsbrudd vil kunne være at deler av landet blir mørklagt, at vannforsyningen ikke har tilstrekkelig kvalitet eller at militært materiell ikke kan fraktes på jernbane i en sikkerhetspolitisk situasjon.

Det samme gjelder militære operasjoner på stridsteknisk nivå eller spesialstyrkeoperasjoner. Her vil det kunne være behov for ulike typer informasjon som enten er ugradert eller lavt gradert med kort levetid. I en slik sammenheng vil korrekt situasjonsoversikt og korrekt formidling av gitte ordre kunne være langt mer verdifullt enn formelt sikkerhetsgradert informasjon. I ytterste konsekvens vil en feil tilnærming til helhetlig sikkerhet kunne føre til at liv går tapt liv eller at kampen vil tapes. Etter departementets vurdering er det derfor nødvendig at loven også gir eksplisitt beskyttelse av informasjon som må beskyttes først og fremst av hensyn til integritet og tilgjengelighet. Dette vil legge grunnlaget for en modernisert tilnærming til informasjonssikkerhet også innenfor sikkerhetslovens område.

Dagens sikkerhetslov anerkjenner at sikkerhetsgradert informasjon kan ha andre beskyttelsesbehov enn konfidensialitet. Lovens ordning er likevel at det kun er konfidensialitetshensyn som inngår i vurderingen av om informasjonen skal beskyttes etter loven. Utvalget foreslår å videreføre denne ordningen. I takt med at informasjonsteknologi brukes til stadig mer avanserte funksjoner som er tidskritiske, er tilgjengelighetsaspektet blitt stadig viktigere for helhetlig informasjonssikkerhet. Det blir derfor etter departementets vurdering uheldig å videreføre en praksis som ikke fullt ut anerkjenner tilgjengelighet som en sentral sikkerhetsegenskap. Mange funksjoner effektiviseres med utstrakt bruk av informasjonsteknologi både av ressurshensyn og for å samle for eksempel krisehåndteringskompetanse. I en krisesituasjon vil tilgang til situasjonsoversikt fra radarer og andre sensorer kunne være svært viktig for krisehåndteringsevne på både sivil og mili-



Figur 10.1

Illustrasjonen viser forholdet mellom skjermingsverdig og sikkerhetsgradert informasjon og hvilke sikkerhetsbehov virksomhetens informasjon kan ha.

tær side. Det vil både på politisk nivå og i forvaltningen være viktig at slik informasjon både er tilgjengelig til rett tid og med korrekt innhold. Dette er dermed også et eksempel på en situasjon der både tilgjengelighet og integritet kan være viktigere enn konfidensialitetshensyn. Tilsvarende er det viktig at den sentraliserte styringen av kraftnettet eller togtrafikken i Norge både er tilgjengelig til rett tid og innehar tilstrekkelig integritetsbeskyttelse.

Til grunn for å avgjøre hvilken informasjon som faller inn under begrepet *skjermingsverdig informasjon* skal det, som etter gjeldende rett, ligge en verdivurdering. Tema for vurderingen er hvilke konsekvenser det kan få for nasjonal sikkerhet dersom verdien av informasjonen går tapt. For konfidensialitet blir spørsmålet hvilke konsekvenser det kan få for nasjonal sikkerhet dersom informasjonen blir kjent for uvedkommende. For integritet blir spørsmålet hvilke konsekvenser det kan få for nasjonal sikkerhet dersom informasjonen ikke er korrekt. For tilgjengelighet blir spørsmålet hvilke konsekvenser det kan få for nasjonal sikkerhet dersom informasjonen ikke er tilgjengelig. Se for øvrig lovforslaget og merknadene til § 5-1.

Departementet har vurdert om andre egenskaper for informasjonssikkerhet, som for eksempel autentisitet og ikke-benektbarhet, også bør tas inn i loven. Departementet erkjenner at også disse egenskapene tidvis er meget viktige å ta hensyn til for å oppnå tilstrekkelig informasjonssikkerhet. Utvalgets forslag til en egen lovbestemmelse om sikkerhetsmessig overvåking (som departementet foreslår videreført, se nærmere kapittel 10.5.3) ivaretar for eksempel særlig behovet for at aktivitet i et informasjonssystem skal være sporbart. Departementet er imidlertid av den oppfatning at det er tilstrekkelig eksplisitt å nevne de tre hovedhensynene i lovteksten. For det første kan øvrige hensyn utledes av de tre hovedhensynene. For det andre vil det bli utfordrende å sette grensen for hvilke hensyn som skal inkluderes i lovteksten. Og for det tredje vil det unødig komplisere lovteksten.

Det er etter departementets syn viktig å ta inn over seg det store spennet av ulike aktiviteter og tilhørende informasjonssystemer som loven skal omfatte. For eksempel gjelder dette offentlige saksbehandlingssystemer, militære kampsystemer, kontorstøttesystemer og industrielle kontroll- og styringssystemer. Det er videre etter departementets syn viktig å ta hensyn til at lovens bestemmelser vil dekke et område der faktorer som teknologiutvikling, trusselutvikling og anvendelse er i svært rask endring, både militært og sivilt. Fortsatt økt digitalisering er en ønsket og ventet utvikling både for Forsvaret og for det sivile samfunn. Loven må legge til grunn prinsipper som understøtter denne utviklingen, der det samtidig legges til grunn et tidsriktig, helhetlig og balansert risikoregime innen sikkerhet. Dette innebærer forhold med høy iboende kompleksitet som gjør det lite hensiktsmessig med detaljerte bestemmelser i loven. Departementet vil derfor foreslå at nærmere detaljerte bestemmelser gis i forskrift.

10.5.2 Beskyttelse av skjermingsverdig informasjon

10.5.2.1 Beskyttelse av skjermingsverdig informasjon

Beskyttelse av informasjon handler om ivaretakelse av informasjonens verdi. Informasjon består av ulike verdier som tidvis er i konflikt med hverandre. Beskyttelsestiltakene må derfor tilpasses konkret til ulike typer informasjon. For å oppnå god informasjonsbeskyttelse må det ligge til grunn en konkret og grundig verdivurdering av informasjonen.

En slik tilnærming ble også lagt til grunn av utvalget, som nevnt under kapittel 10.3.1. Departementet mener forslaget er godt og ivaretar behovet for en helhetlig og balansert tilnærming til beskyttelse av informasjon. Imidlertid må denne

bestemmelsen om beskyttelse justeres i tråd med departements forslag om at verdivurderingen av informasjon også skal omfatte integritet og tilgjengelighet. Departementet foreslår derfor at begrepet *sikkerhetsgradert* informasjon i første ledd erstattes av samlebegrepet *skjermingsverdig* informasjon.

Departementet mener videre at det bør gå klart fram av bestemmelsen at den enkelte virksomhet plikter å iverksette tiltak slik at det oppnås et *forsvarlig sikkerhetsnivå*. Denne rettslige standarden er nærmere omtalt i NOU 2016: 19 kapittel 7.7.9, side 144. Forskriftshjemmelen i andre ledd bør også justeres slik at den omfatter all *skjermingsverdig* informasjon og slik at den ikke begrenser seg til minimumskrav.

10.5.2.2 Sikkerhetsgradert informasjon

Etter departementets syn bør dagens lovbestemmelser for sikkerhetsgradering og beskyttelse av informasjonens konfidensialitet videreføres, slik som utvalget har foreslått. *Sikkerhetsgradert* informasjon vil dermed bli en delmengde av den *skjermingsverdige* informasjonen. *NSM* påpeker i sitt høringssvar at dette er informasjon som har det samme beskyttelsesbehovet uavhengig av i hvilken sektor eller virksomhet informasjonen håndteres. Dette fordi skadefølgene ikke bare rammer virksomheten, men også bredere nasjonale interesser. Departementet er enig i denne vurderingen. Informasjon som skal sikkerhetsgraderes, vil fortsatt stå i en særstilling og vil måtte underlegges særlige nasjonale tverrsektorielle sikkerhetskrav fastsatt av sikkerhetsmyndigheten slik som i dag. Sikkerhetsgradert informasjon må beskyttes enhetlig og helhetlig på tvers av alle sektorer.

Det må også legges vekt på at denne formen for verdivurdering har betydelige implikasjoner for andre bestemmelser i loven, og at denne lovbestemmelsen på kort sikt sikrer interoperabilitet med NATOs og andre nasjoners graderingsregime. Som utgangspunkt er det derfor grunn til å videreføre dagens regime for beskyttelse av denne type informasjon. En eventuell endring av disse reglene vil kreve en grundig utredning.

Samtidig er trussel- og utfordringsbildet blitt mer komplekst enn tidligere. Dette er godt beskrevet i utredningen. I både militær og sivil sektor har det skjedd og er i ferd med å skje en betydelig utvikling som setter dagens regime på prøve. Blant annet er det i mange tilfeller vanskelig å vurdere behovet for skjerming opp mot behovet for informasjonsdeling. Et eksempel er trusselinformasjon, som kan være svært sensitiv og derfor må skjermes. Samtidig har mange aktører innen forebyggende sikkerhetsarbeid behov for å kjenne til trusselinformasjonen for å kunne iverksette treffende mottiltak. Andre utfordringer oppstår når samme informasjon defineres innenfor flere ulike sikkerhetsregimer. Et eksempel på dette er informasjon som er definert som kraftsensitiv i henhold til energisektorens beredskapsforskrift.

For å fange opp samfunnsutviklingen ser departementet at det i enkelte tilfeller kan være behov for å gjøre konkrete tilpasninger mellom ulike sikkerhetsregimer. For det første kan slike forhold i særlige tilfeller begrunne anvendelse av lovforslaget § 1-2 der det gis forskriftshjemmel til å gjøre helt eller delvis unntak fra lovens virkeområde, inkludert visse typer informasjon og informasjonssystemer. I andre tilfeller kan det være behov for å åpne i noe større grad for unntak fra beskyttelsestiltak som vil bli fastsatt i forskrift. I så fall må andre kompenserende tiltak være på plass. Lovforslaget §§ 5-2 og 6-2 inneholder forskriftshjemler til å fastsette nærmere sikkerhetskrav. Verken ordlyd eller utredningen for øvrig hindrer etter departementets vurdering at hjemmelen også omfatter mulighet til å fastsette unntak fra sikkerhetskravene i særlige tilfeller. Departementet mener likevel at dette bør gå tydelig fram av lovteksten. Se nærmere lovforslaget §§ 5-2 andre ledd andre punktum og 6-2 andre ledd andre punktum.

Departementet vil understreke at unntak fra sikkerhetskrav om beskyttelse av sikkerhetsgradert informasjon, enten det gjelder dokumentbehandling, informasjonssystembeskyttelse eller annet, kun kan forekomme i helt spesielle tilfeller. For det første må slike unntak være godt begrunnet i hensyn til den aktuelle virksomhetens aktivitet. For det andre må det vurderes kompenserende tiltak. I første omgang bør det være opp til sikkerhetsmyndigheten om slike unntak kan innvilges. Blir det ikke enighet, kan spørsmålet eventuelt løftes til et overordnet nivå. De nærmere reglene om når det kan gjøres unntak og av hvem bør vurderes grundig og fastsettes i forskrift.

Departementet er enig med utvalget i at gjeldende rett om taushetsplikt for sikkerhetsgradert informasjon må videreføres. Departementet støtter utvalgets forslag om å regulere tilgjengeliggjøring av og taushetsplikt om sikkerhetsgradert informasjon i en egen bestemmelse. Det vises for øvrig til utredningens merknader til bestemmelsen.

Sikkerhetstiltaket *tekniske sikkerhetsundersøkelser* (TSU) bør videreføres, som foreslått av utvalget. Departementet støtter dessuten *NSMs* forslag om at kontrolløren skal rapportere om resultatet av kontrollen til virksomheten. Departementet er videre enig med *NSM* i at nærmere regler om bemyndigelse av andre virksomheter som TSU-kontrollører må utarbeides i forskrift.

Etter gjeldende lov § 16 åpnes det for at sikkerhetsmyndigheten kan bemyndige andre til å gjennomføre den tekniske sikkerhetsundersøkelsen. Departementet mener at den nye loven også bør åpne for at andre enn sikkerhetsmyndigheten gjennomfører slike kontroller. Imidlertid bør myndigheten til å peke ut andre kontrollører legges til Kongen. Dette samsvarer bedre med lovforslagets øvrige systematikk om delegering av myndighet.

Gjeldende rett om *kryptosikkerhet*, se sikkerhetsloven § 14, må etter departementets oppfatning videreføres i den nye sikkerhetsloven. Kryptosikkerhet er en viktig del av nasjonalt forebyggende sikkerhetsarbeid. I motsetning til utvalget mener departementet derfor at de mest grunnleggende reglene om kryptosikkerhet fortsatt bør gå klart fram av loven. Det er viktig at det på lovs nivå gjøres klart hvordan kryptosikkerheten skal forvaltes og at det stilles særlige krav ved bruk av krypto for å beskytte sikkerhetsgradert informasjon.

Departementet vil bemerke at denne bestemmelsen ikke kommer i konflikt med regjeringens generelle holdning om at bruk av kryptografi verken bør forbys eller reguleres. Bestemmelsen i sikkerhetsloven handler bare om at når krypto skal brukes for å beskytte sikkerhetsgradert informasjon, må det stilles krav om at kryptoen er av en viss kvalitet. Dette legger ikke bånd på bruken av kryptografi for øvrig i samfunnet.

10.5.3 Informasjonssystemsikkerhet

Informasjonssystemsikkerhet utgjør etter departementets vurdering en sentral del av informasjonssikkerheten ved at den beskriver innretning og tiltak for hvordan informasjonssikkerheten skal ivaretas i de systemene der informasjonen behandles og brukes. Høringsinnspillene støtter i hovedsak opp under denne vurderingen. Likevel foreligger det innspill som det er hensiktsmessig å behandle spesielt.

Sikkerhetsloven er en rammelov som skal ha sin funksjon gjennom en relativt lang tidsperiode. Samfunnets anvendelse av informasjonsteknologi og de sikkerhetsutfordringer som følger av denne anvendelsen, må forventes å endres raskt i løpet av den samme tidsperioden. En utfordring vil være at loven kan oppfattes som utydelig innenfor særlig sammensatte områder som informasjonssystemsikkerhet. Dette er en utydelighet som etter departementets syn er uunngåelig, samtidig som at dette også er hensiktsmessig for å gi rom for å møte den framtidige utviklingen. Konkretiseringen av hvilke konsekvenser loven får, vil skje gjennom forskriftsutvikling og praktisering av regelverket.

10.5.3.1 Informasjonssystemer som skal beskyttes etter sikkerhetsloven

Departementet støtter utvalgets drøftelser og forslag om hvilke informasjonssystemer sikkerhetsloven skal beskytte, se nærmere NOU 2016: 19 kapittel 8.5.2 og 8.6.2. En rekke høringsinstanser gir støtte til dette forslaget. En ny sikkerhetslov må, i tillegg til å beskytte informasjonssystemer som behandler sikkerhetsgradert informasjon, også beskytte informasjonssystemer som på grunn av sin funksjonalitet er viktig for nasjonal sikkerhet. Som en naturlig konsekvens av drøftelsene under kapittel 10.5.1 om hvilken informasjon loven skal beskytte, følger det at loven også må beskytte informasjonssystemer som behandler *skjermingsverdig informasjon,* og ikke bare sikkerhetsgradert informasjon. Se nærmere i lovforslaget § 6-1 om hvilke informasjonssystemer loven skal gjelde for.

Utvalget legger til grunn en vid forståelse av begrepet *informasjonssystem,* jf. merknaden til utvalgets lovforslag § 6-1 i NOU 2016: 19, side 262:

> «Med begrepet *informasjonssystem* menes systemer som anvendes for å løse en oppgave eller utføre en funksjon i en organisasjon. Det omfatter menneskelige, organisatoriske og tekniske ressurser, metoder og teknikker.
>
> *Informasjonssystem* skal i sikkerhetsloven forstand forstås vidt. Begrepet omfatter både manuelle og digitale informasjonssystemer, og favner alt fra saksbehandlingssystemer, kontorstøttesystemer og rene kommunikasjonssystemer til kontroll- og styringssystemer.»

Departementet stiller seg bak denne tilnærmingen og mener at beskrivelsen er dekkende for begrepet *informasjonssystem*.

Departementet er videre enig i utvalgets forslag om å bruke begrepet *skjermingsverdige informasjonssystemer* som samlebegrep for alle informasjonssystemer som skal beskyttes etter sikkerhetsloven.

10.5.3.2 Beskyttelse av informasjonssystemer

Informasjonssystemer må gis en konkret og helhetlig beskyttelse basert på en vurdering av risiko for det enkelte informasjonssystemet. Departementet stiller seg bak utvalgets generelle drøftelser i kapittel 8.6.2 og merknaden til utvalgets lovforslag § 6-2. Departementet støtter dermed i hovedsak utvalgets forslag til bestemmelser om informasjonssystemsikkerhet. Det er likevel behov for å gjøre enkelte justeringer. Blant annet mener departementet at utvalget ikke går tilstrekkelig langt i å ta høyde for den raske samfunnsutviklingen på dette feltet.

Det blir i høringsuttalelsene uttrykt at det i virksomheter som må kunne forventes å komme inn under sikkerhetslovens virkeområde, allerede foregår utstrakt informasjonsdeling mellom ulike informasjonssystemer både innenlands og utenlands. Det uttrykkes behov for tiltak som tilpasses denne virkeligheten. Disse informasjonssystemene vil til dels også kunne behandle både sikkerhetsgradert informasjon og informasjon som ikke er sikkerhetsgradert, men som fortsatt er skjermingsverdig.

Et tema som er særlig aktuelt for Forsvaret, er behovet for fleksible risikobaserte løsninger for forhåndsgodkjenning av systemer, særlig til mer kortvarig bruk i feltsammenheng og øvelser.

Flere av høringsinstansene har videre tatt opp behovet for sikker tilgjengelighet som del av informasjonssystemsikkerheten. Kommunikasjonsinfrastrukturer som omfatter både sivile og militære systemer, blir stadig viktigere for militær evne og overlevelse, uten at det oppfattes at dagens sikkerhetsregime tar inn over seg denne utfordringen. Utviklingen mot bruk av stadig flere sivile tjenester blir framhevet som klare utfordringer i slik tilgjengelighetssammenheng.

Loven vil etter departementets vurdering i stor grad møte behovene i både militær og sivil sektor. Dette gjøres i hovedsak ved i større grad enn tidligere å legge til grunn risikobaserte vurderinger for de konkrete løsningene som velges. Det skal også gjøres en konkret vurdering av kostnadene som løsningene kan medføre. Kostnadene skal stå i et rimelig forhold til nytteverdien av det som faktisk oppnås ved tiltaket. Likevel er det viktig også å ta hensyn til begrensninger Norge er pålagt gjennom samarbeid med blant annet NATO og deres sikkerhetsbestemmelser.

På samme måte som for beskyttelse av informasjon mener departementet at det for informasjonssystemer i særtilfeller må være mulig å gjøre spesielle tilpasninger av sikkerhetstiltakene. Dette vil antakelig være særlig aktuelt for informasjonssystemer som behandler både sikkerhetsgradert informasjon og informasjon som ikke skal sikkerhetsgraderes. Departementet foreslår derfor en generell hjemmel for Kongen til å fastsette nærmere regler om unntak fra beskyttelsestiltakene i forskrift. Forskriften bør blant annet fastsette vilkår for hva som skal anses som særlige tilfeller og hvem som skal foreta denne vurderingen. Departementet vil her understreke at det ikke er meningen å lempe på sikkerhetskravene, men å gjøre det mulig gjennom en risikobasert tilnærming å få til tilpassede løsninger som ivaretar hensyn til både sikkerheten og virksomhetens aktivitet. På denne måten tas det også høyde for mulige behov for tilpasning til sektorregelverk. Det vises for øvrig til kapittel 10.5.2 om dette. Samlet skal unntaksbestemmelsene i lovforslaget §§ 1-2, 5-2 og 6-2 gjøre loven tilstrekkelig dynamisk til å møte en fortsatt rask digital utvikling på alle samfunnsområder.

Utvalget foreslår å videreføre dagens regler om at informasjonssystemer som skal behandle sikkerhetsgradert informasjon, må *forhåndsgodkjennes* før de tas i bruk. I utvalgets lovforslag legges det videre til grunn ulik behandling av henholdsvis sikkerhetsgradert informasjon og ugradert, men skjermingsverdig informasjon. Etter departementets syn er det hensiktsmessig å følge lovforslaget der systemer som behandler sikkerhetsgradert informasjon, i utgangspunktet skal forhåndsgodkjennes. Det er også etter departementets syn nødvendig å følge lovforslaget og åpne opp for ulik praksis med sikkerhetsgodkjenning av skjermingsverdige systemer som ikke behandler sikkerhetsgradert informasjon. Dette begrunnes i at en utvidelse av lovens virkeområde vil kunne omfatte systemer som inngår i kommersiell virksomhet. Det vil etter departementets syn være risiko for at et krav om forhåndsgodkjenning utilsiktet vil kunne påvirke kommersiell virksomhet på en uhensiktsmessig måte.

Departementet foreslår å videreføre utvalgets forslag til regulering av *overvåking av informasjonssystemer*, jf. utvalgets lovforslag § 6-4. Som utvalget uttaler er dette et nødvendig sikkerhetstiltak som må gjennomføres for alle virksomhetens skjermingsverdige informasjonssystemer. Ingen høringsinstanser har hatt særlige merknader til denne bestemmelsen. Departementet støtter utvalgets vurderinger og viser til disse i sin helhet i NOU 2016: 19, kapittel 8.6.4 og merknaden til utvalgets lovforslag § 6-4 på side 263–264. Departementet har gjennomført enkelte språklige

endringer, se nærmere lovforslaget og tilhørende merknader.

Enkelte høringsinnspill peker på at *inntrengingstesting* bør kunne inngå som del av sikkerhetsmyndighetens tilsynsaktivitet. *NSM* ber om at det vurderes. Utvalget drøftet spørsmålet i utredningen kapittel 8.6.4, side 171:

> «Av hensyn til de forskjelligartede informasjonssystemer som omfattes av bestemmelsen, kunne beskrivelsen av plikten vanskelig blitt veldig konkret. Utvalget vil dessuten ikke utelukke at tiltaket i enkelte tilfeller er direkte uhensiktsmessig. Inntrengningstesting vil dessuten kunne innebære behandling av personopplysninger. Utvalget antar at det vil kunne virke mindre inngripende at den enkelte virksomhet må ta initiativ til gjennomføring av tiltaket, fremfor at det foreligger en rettslig plikt.»

Lysne-utvalget drøfter også problemstillingen i NOU 2015: 13 kapittel 21.11.3, side 276:

> «NSM anbefaler i sikkerhetsfaglig råd at Sikkerhetsutvalget bør vurdere om «NSM bør gis hjemmel til å gjennomføre inntrengingstesting uten forutgående samtykke fra virksomheten». Utvalget er prinsipielt uenig i at man bør tillate å gjennomføre inntrengingstesting uten samtykke fra virksomheter. Dette begrunnes med at det kan undergrave tillit, samt sektorenes og virksomhetenes selvstendige ansvar.»

Departementet støtter disse vurderingene og mener det vil være et uforholdsmessig stort inngrep å gjøre inntrengingstesting til et virkemiddel i sikkerhetsmyndighetens tilsynsaktivitet uten at det blir gitt samtykke til dette fra systemeier.

Departementet mener at det ikke er hensiktsmessig å følge utvalgets lovforslag om å avbryte en inntrengingstest med en gang sikkerhetsmyndigheten klarer å trenge inn i systemet. *NSM* gir i sin høringsuttalelse en god og konsistent begrunnelse for dette. Hensynet til personvernet er godt ivaretatt i bestemmelsens andre ledd.

Det er i lovforslaget lagt til rette for at andre enn sikkerhetsmyndigheten kan utføre inntrengingstesting. Flere av høringsinnspillene peker også på at dette er et behov. Etter departementets syn er dette hensiktsmessig særlig i lys av et utvidet virkeområde i forhold til dagens lovgivning. *NSM* uttaler i sitt høringssvar at det i så fall må etableres kriterier og rettslig grunnlag for slik virksomhet. Departementet er enig i denne vurderingen. Det rettslige grunnlaget for slik aktivitet følger av lovforslaget § 6-5 første ledd og de nærmere kriteriene vil måtte følge av forskrift, jf. femte ledd.

Bestemmelsen åpner etter ordlyden for at andre enn sikkerhetsmyndigheten utfører testing av alle typer systemer. Departementet legger imidlertid til grunn at det i praksis fortsatt vil være sikkerhetsmyndigheten som skal stå for testing av informasjonssystemer som behandler sikkerhetsgradert informasjon, og andre særlig sensitive systemer. Flere gode grunner taler for å videreføre dagens ordning, jf. forskrift om informasjonssikkerhet § 11-5. Etter denne bestemmelsen kan slik testing gjennomføres kun av personell tilhørende Nasjonal sikkerhetsmyndighet eller som står under ledelse av Nasjonal sikkerhetsmyndighet. Om det skal åpnes for at andre enn sikkerhetsmyndigheten skal foreta inntrengingstesting i de tilfellene som her er nevnt, må vurderes grundig når det skal utarbeides forskrifter.

NSM har i sitt høringssvar påpekt at det er viktig at sikkerhetsmyndigheten har hjemmel til å samle inn og bruke funn og erfaringer fra kontrolltiltakene de gjennomfører. Dette vil være viktig for å videreutvikle metodikk og sikkerhetstiltak og som grunnlag for risikovurderinger. Departementet støtter denne vurderingen og mener det i loven bør gis hjemmel for dette. Muligheten for å kunne nyttiggjøre seg lærdom fra gjennomførte kontroller er viktig for at sikkerhetsmyndigheten skal kunne utvikle seg og holde et faglig høyt nivå. Som det framgår av lovforslaget, er det lagt til hjemmel for viderebruk av informasjon i §§ 5-5, 6-5 og 6-6. Departementet foreslår at de nærmere bestemmelsene for videre bruk av informasjon tilegnet gjennom kontrolltiltak fastsettes i forskrift. Hensynet til personvern må vurderes nøye.

Et særlig spørsmål er forholdet mellom sikkerhetsmyndigheten og andre virksomheter som eventuelt vil kunne utføre inntrengingstesting eller andre kontroller i medhold av sikkerhetsloven. Gode grunner taler i mange tilfeller for at kontrolløren bør dele sine erfaringer og funn fra kontrollene med sikkerhetsmyndigheten. Departementet mener imidlertid at det ikke bør settes krav til slik informasjonsdeling i loven, da hensiktsmessigheten av en slik ordning kan være forskjellig fra tiltak til tiltak. Problemstillingen må vurderes nærmere ved utforming av forskrifter om de ulike kontrolltiltakene.

Departementet støtter utvalgets forslag om å videreføre dagens bestemmelse om *kommunikasjons- og innholdskontroll*. Det er videre departe-

mentets vurdering at det i loven bør gis hjemmel for kommunikasjons- og innholdskontroll i alle virksomhetens ugraderte systemer, og ikke bare de som er skjermingsverdige. Dette er en videreføring av dagens praksis. Som *NSM* uttrykker, bør dette gå tydeligere fram av lovteksten, og departementet foreslår derfor justering i tråd med dette. Departementet slutter seg for øvrig til utvalgets vurderinger i utredningen kapittel 8.6.4 om dette temaet.

Departementet har vurdert om andre enn sikkerhetsmyndigheten bør kunne utføre denne typen kontroller. En slik arbeidsfordeling vil i så fall være i tråd med ordningen for tekniske sikkerhetsundersøkelser og inntrengingstesting. Det kan være grunn til å begrense muligheten for andre fordi det her dreier seg om sikkerhetsgradert informasjon. Imidlertid gjelder også tekniske sikkerhetsundersøkelser som oftest sikkerhetsgradert informasjon. Som nevnt over gir gjeldende sikkerhetslov § 16 åpning for at andre enn sikkerhetsmyndigheten kan gjennomføre tekniske sikkerhetsundersøkelser. Etter departementets syn bør loven åpne for muligheten for en avlastning av sikkerhetsmyndigheten også på dette området. Etter departementets syn må kontrolltjenestene være av en viss kvalitet. Det må derfor settes klare kriterier for hva som skal til for at andre virksomheter, om det er sektormyndigheter eller private selskaper, skal kunne tilby slike kontrolltjenester etter sikkerhetsloven. Dette gjelder for både tekniske sikkerhetsundersøkelser, kommunikasjons- og innholdskontroll og inntrengingstesting. De nærmere kriteriene må utarbeides gjennom forskrift.

NSM påpeker i sitt høringssvar at det bør framgå av lovbestemmelsen at virksomheten etter endt kontroll skal få rapport om kontrollen, slik at virksomheten skal kunne foreta eventuelle utbedringstiltak. Departementet støtter denne vurderingen og foreslår å ta inn et nytt ledd som foreslått av NSM og som tilsvarer utvalgets forslag til § 6-6 femte ledd. Dette vil gjelde for alle kontrolltiltakene.

10.5.3.3 Særlig om sikkerhetsgradering med kort levetid

I dagens sikkerhetslov er informasjonens verdi knyttet til graderingsnivåene for sikkerhetsgradert informasjon. Historisk sett hadde sikkerhetsgradert informasjon lang levetid, det vil si fem år eller mer. Imidlertid behandler informasjonssystemene i dag informasjon som, avhengig av hvilken sammenheng den brukes i, vil kunne ha svært kort levetid. Dette kan for eksempel være teknisk informasjon i et drifts- og styringssystem for en viktig samfunnsfunksjon eller informasjon som brukes i en militær operasjon. Muligheten til å dele visse typer informasjon i nettverk vil være en viktig forutsetning for både militære operasjoner og andre viktige funksjoner i samfunnet. Det er med den bakgrunnen uttrykt ønske om at det blir lagt til rette for en mer fleksibel tilnærming til muligheten for deling av enkelte typer sikkerhetsgradert informasjon, der det tas hensyn til informasjonens levetid i en helhetlig risikobasert sammenheng. Det har imidlertid ikke vært mulig å innarbeide dette hensynet i den nye loven. Det vurderes likevel som viktig å gjøre vurderinger og foreta avklaringer på dette området i det videre forskriftsarbeidet.

10.5.3.4 Særlig om informasjonssystemsikkerhet og objekt- og infrastruktursikkerhet

Etter departementets vurdering utgjør tilgjengelighet og sammenhengen mellom informasjonssystemsikkerhet og objekt- og infrastruktursikkerhet en stadig viktigere del av helhetlig sikkerhet både i militære og sivile informasjonssystemer. Det søkes så langt det er mulig å framheve dette forholdet i lovgrunnlaget. Videre behandling av dette sammensatte temaet vil også måtte bli tatt inn i det påfølgende forskriftsarbeidet.

Utvalgets forslag om å utvide objektsikkerhet til også å omfatte infrastruktursikkerhet er i utgangspunktet ment å skulle tilføre en tydeligere systemtilnærming i lovgivningen. Forslaget vil i noen grad også innebære en utvidelse. Det vil imidlertid fortsatt være objekter og infrastruktur med spesielt høy verdi og skjermingsbehov som vil bli omfattet av den nye loven. Mange av systemene i militære og sivile infrastrukturer er i økende grad nettverksbasert. Økende bruk av informasjonsteknologi i drifts- og styringsfunksjoner i mange samfunnsfunksjoner fører til at infrastrukturene blir stadig mer sammensatte, særlig ved at de utgjør kombinasjoner av fysiske og logiske nettverksfunksjoner. For eksempel er kraftnettet i Norge både avhengig av at det fysiske kraftnettet er robust, og at den fysiske og logiske delen av informasjonssystemene som kraftforsyningen bruker for å styre det fysiske kraftnettet, også er robust.

Det blir derfor på den ene siden nødvendig å se alle typer av infrastrukturer i en helhet, der både objekter og de nettstrukturene som knytter det hele sammen, ses på i et helhetlig sikkerhets-

perspektiv. Her vil det imidlertid være et utydelig skille mellom informasjonssystemsikkerhet og infrastruktursikkerhet. Innenfor informasjonssystemsikkerhet skal det legges til grunn at all sikkerhet i skjermingsverdige informasjonssystemer skal håndteres helhetlig med hensyn til tilgjengelighet, integritet og konfidensialitet.

Samtidig må det imidlertid tas hensyn til at informasjonssystemsikkerhet må ses i nær sammenheng med objekt- og infrastruktursikkerhet for å oppnå tilstrekkelig helhetlig sikkerhet, og dermed et forsvarlig sikkerhetsnivå. Hvordan de fysiske og logiske nettverkene er knyttet sammen i infrastrukturene, vil ha stor betydning for tilgjengeligheten i de fleste moderne informasjonssystemer. Sammenhengen mellom informasjonssystemsikkerhet og objekt- og infrastruktursikkerhet er i særlig grad viktig for å sikre tilgjengeligheten i moderne distribuerte informasjonssystemer. Departementet stiller seg for øvrig bak de betraktninger utvalget gjør omkring dette i NOU 2016: 19 kapittel 8.6.3. Det kan i flere tilfeller være aktuelt å peke ut skjermingsverdige informasjonssystemer som skjermingsverdig objekt eller infrastruktur.

11 Objekt- og infrastruktursikkerhet

11.1 Gjeldende rett

Gjeldende bestemmelser om objektsikkerhet står i sikkerhetsloven kapittel 5 *Objektsikkerhet* med tilhørende forskrift. Opprinnelig, ved ikrafttredelse av sikkerhetsloven 1. juli 2001, var kapittelet om objektsikkerhet svært kortfattet, der hovedbestemmelsene oppstilte en plikt for vedkommende virksomhet underlagt loven til å utpeke skjermingsverdige objekter og til å treffe nødvendige forebyggende sikkerhetstiltak for å beskytte skjermingsverdige objekter mot sikkerhetstruende virksomhet. Som Sikkerhetsutvalget peker på i NOU 2016: 19 kapittel 9.2, side 176, har dette sin historiske bakgrunn i at sikkerhetsloven, som ble vedtatt i 1998, bygde på og erstattet den daværende Sikkerhetsinstruksen, som kun omhandlet informasjonssikkerhet. At objektsikkerhet kom inn i regelverket, var således en nyskapning.

I forbindelse med utarbeidelse av forskrift om objektsikkerhet, som først kom i gang etter ikrafttredelse av loven i 2001, kom man etter hvert til at lovbestemmelsene om objektsikkerhet burde bygges mer ut, for å få inn prinsipielle bestemmelser om utpeking og klassifisering av skjermingsverdige objekter, og for å unngå at alle hovedinnretningene i det operasjonelle regelverket skulle stå i forskrift.

De nåværende hovedbestemmelsene i kapittel 5 kom derfor først inn ved lovendring i 2008 (lov 11. april 2008 nr. 9), jf. Ot. prp. nr. 21 (2007–2008) og Innst. O nr. 33 (2007–2008). Her fastslås det at det er hvert enkelt departement som utpeker skjermingsverdige objekter innen sitt myndighetsområde og at klassifiseringsgradene for skjermingsverdige objekter er MEGET KRITISK, KRITISK og VIKTIG, vurdert etter hvilket skadepotensial et anslag vil kunne få, jf. §§ 17 og 17 a. Det blir dessuten fastslått at det er objekteier som plikter å beskytte skjermingsverdige objekt med sikkerhetstiltak, der tiltakene skal bestå av «en kombinasjon av barrierer, deteksjon, verifikasjon og reaksjon», som i sum tilfredsstiller krav tilpasset de aktuelle klassifiseringsgradene, jf. § 17 b.

Forskrift om objektsikkerhet ble fastsatt ved kongelig resolusjon 22. oktober 2010. Her heter det blant annet at der det finnes relevante og tilstrekkelige bestemmelser innenfor sektorlovgivningen, og det er etablert tilsynsorgan, går disse foran bestemmelsene i objektsikkerhetsforskriften, jf. § 1-3. I forbindelse med departementenes oppgave med utpeking av skjermingsverdige objekter innen sitt myndighetsområde, skal den enkelte virksomhet overfor vedkommende fagdepartement levere en dokumentert skadevurdering over hvilke objekter som kan være skjermingsverdige, jf. § 2-1 andre ledd. Der det finnes tilsynsorgan for sektoren, kan disse foreslå overfor departementet skjermingsverdige objekter uavhengig av virksomhetens eller objekteiers forslag, jf. § 2-1 tredje ledd. Videre heter det i forskriften at de enkelte departementene skal føre register over skjermingsverdige objekter og klassifiseringen av disse innen eget myndighetsområde, og deretter melde inn registreringen til Nasjonal sikkerhetsmyndighet (NSM), jf. § 2-4. Formålet med innmeldingen er at NSM som fagmyndighet skal ha en nasjonal og tverrsektoriell oversikt over de aktuelle objektene og deres klassifiseringsgrad. Forskriften har videre generelle bestemmelser om krav til sikkerhetstiltak som grunnsikring og mer spesifikke tiltak for nærmere angitte trusselsituasjoner, jf. §§ 3-1 til 3-5. Etter § 3-5 plikter eier av skjermingsverdig objekt å legge til rette for at sikringsstyrker kan forberede, øve og gjennomføre tiltak på og ved objektet for å beskytte dette.

I forskriften om objektsikkerhet framgår det også at NSM skal føre tilsyn med at utvelgelse og klassifisering av skjermingsverdige objekter skjer i henhold til sikkerhetsloven og forskriften, og at NSM om nødvendig kan gi pålegg om dette, i samsvar med den oppgave som NSM har om å føre tilsyn med sikkerhetstilstanden i de enkelte virksomhetene, jf. sikkerhetsloven § 9 første ledd bokstav c og objektsikkerhetsforskriften § 4-3.

Tilrettelegging for eventuell bruk av *sikringsstyrker,* jf. gjeldende sikkerhetslov § 17 b siste ledd og forskrift om objektsikkerhet av 22. oktober 2010 nr. 1362 § 3-5, er nærmere regulert i instruks om sikring og beskyttelse av objekter ved bruk av sikringsstyrker fra Forsvaret og politiet i fred, krise og krig, fastsatt ved kongelig resolusjon 24.

august 2012. Instruksen har bestemmelser om ansvarsforhold og samarbeid om politiets og Forsvarets objektsikring ved bruk av sikringsstyrker, og er nærmere omtalt av utvalget i kapittel 9.3.4 side 183–184.

11.2 Utvalgets forslag

Sikkerhetsutvalget gir i NOU 2016: 19 kapittel 9.5.1 uttrykk for at objekter og infrastruktur som er av kritisk betydning for grunnleggende nasjonale funksjoner, må beskyttes. Følgende definisjoner legges til grunn:

> «*Skjermingsverdig objekt*; eiendom som må beskyttes mot tilsiktede uønskede hendelser av hensyn til opprettholdelse av grunnleggende nasjonale funksjoner. Eiendom omfatter områder, bygninger, anlegg, transportmidler eller annet materiell, eller deler av slik eiendom.»

Utvalget viser videre til at en rekke instanser har framhevet et behov for å utvikle objektsikkerhetsregelverket slik at det gir bedre fleksibilitet i hvordan og med hvilke typer tiltak et gitt sikkerhetsnivå skal oppnås. Utvalget peker på at det særlig er vektlagt behov for å stimulere til tiltak som øker redundans (tilgang på alternativer) og resiliens (motstandsdyktighet) for kritiske samfunnsfunksjoner. Utvalget har lagt disse synspunktene og argumentene til grunn for sin anbefaling om å innføre begrepet skjermingsverdig infrastruktur. Utvalget ser det også som naturlig å benytte dette begrepet for å skape en klarere sammenheng med systematikken for risikovurdering i *sikkerhet i kritisk infrastruktur og kritisk samfunnsfunksjoner* (KIKS) som brukes av Direktoratet for samfunnssikkerhet og beredskap (DSB), og for å etablere et begrepsapparat som samsvarer bedre med internasjonal begrepsbruk. Infrastruktur og kritisk infrastruktur går igjen som et offisielt begrep i EU, NATO og de fleste landene Norge har et sikkerhetssamarbeid med.

> «*Skjermingsverdig infrastruktur*; anlegg og systemer som må beskyttes mot tilsiktede uønskede hendelser av hensyn til opprettholdelse av grunnleggende nasjonale funksjoner.»

Utvalget oppfatter skjermingsverdig infrastruktur som en delmengde av kritisk infrastruktur, på samme måte som grunnleggende nasjonale funksjoner oppfattes som en delmengde av kritiske samfunnsfunksjoner:

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

Utvalget peker på at de to begrepene *skjermingsverdig objekt* og *skjermingsverdig infrastruktur* er delvis overlappende, men at de hver for seg ikke anses som tilstrekkelig dekkende for det loven skal regulere. I forståelsen av begrepet skjermingsverdig infrastruktur skal det etter utvalgets mening legges vekt på koplingene mellom relevante objekter og systemer som er nødvendige for å understøtte grunnleggende nasjonale funksjoner.

Utvalget er av den oppfatning at det vil være hensiktsmessig å videreføre dagens praksis med hensyn til at det er de enkelte departementene som er ansvarlige for utpeking av objekter, mv. innenfor sine respektive myndighetsområder. I tillegg er det et behov for at departementene har et utvidet og konkretisert ansvar for å holde oversikt over objekter og infrastruktur som har betydning for grunnleggende nasjonale funksjoner, og ansvar for sikkerhetsnivået i egen sektor. Samtidig ser utvalget behov for å styrke sikkerhetsmyndighetens rolle som ansvarlig for å koordinere sikkerhetstiltak på tvers av sektorer. Utvalget peker på at tverrsektoriell koordinering innebærer å sikre et harmonisert sikkerhetsnivå og å sikre at sårbarheter knyttet til tverrsektorielle avhengigheter blir godt ivaretatt.

Utvalget mener det er nødvendig å tydeliggjøre rapporteringsansvar og informasjonsbehov for ulike etater og virksomheter, for at sikkerhetsmyndigheten skal settes i stand til å ivareta sin koordinerende og sektorovergripende rolle.

Utvalget mener videre at det er en svakhet med dagens objektsikkerhetsregelverk at det ikke hviler noen forpliktelse på departementer eller NSM om å holde oversikt over objekter som er av en type som er nødvendig for understøttelse av kritiske samfunnsfunksjoner, men som ikke er kritiske som enkeltobjekt.

Når det gjelder gjennomføringen av sikkerhetstiltak, mener utvalget at det i loven bør stilles funksjonelle krav til sikkerhetstiltak framfor spesifikke krav. Dette innebærer at det vil være opp til sektormyndigheten å avgjøre i hvilken grad det skal spesifiseres hvilke tiltak som skal gjennomføres eller hvorvidt det først og fremst skal pekes på for lavt sikkerhetsnivå på spesifikke områder og la det være opp til virksomheten å velge hvilke tiltak

som skal gjennomføres. Etter utvalgets syn vil dette være den beste løsningen for å bidra til at sikkerhetstiltakene blir på riktig nivå, med en så lav kostnad som mulig. Det vises til prinsippet og forutsetningen om at aktuelle sikkerhetstiltak mot objekter og infrastruktur i sum er samfunnsøkonomisk lønnsomme.

Utvalget peker videre på at virksomheter og myndigheter som skal vurdere ulike sikkerhetstiltak, gjennomføre tiltak eller føre tilsyn med sikkerhetstilstanden, har behov for tilgang til ekspertkunnskap, og at dette vil være nødvendig for å sikre at de tiltak som blir valgt og iverksatt, er effektive og tilpasset dagens trusselbilde. Utvalget mener at det bør legges til en sentralisert funksjon å holde oversikt over fagmiljøer og å bidra til informasjonsutveksling og samarbeid, samt å identifisere kunnskapshull og behov. Disse oppgavene vil naturlig kunne legges til sikkerhetsmyndigheten, sier utvalget.

Utvalget mener det bør påhvile den enkelte virksomhet som har fått utpekt skjermingsverdig infrastruktur eller objekter, og som dermed omfattes av sikkerhetsloven, å gjennomføre sikkerhetstiltak. Virksomhetene må også ta kostnadene av sikkerhetstiltakene, men kostnadene ved slike tiltak bør stå i et rimelig forhold til det som oppnås ved tiltaket. Ut fra samfunnets behov for sikkerhet vil det kunne være nødvendig å pålegge omfattende sikkerhetstiltak for en spesifikk virksomhet eller i en samfunnssektor. Dette vil gagne samfunnet som helhet og ofte også være nyttig for virksomheten som får pålegg. Utvalget peker likevel på at dersom slike pålegg medfører uforholdsmessig stor belastning for den aktuelle virksomhet eller sektor, sett i forhold til den egenverdi tiltakene har for virksomheten eller sektoren, kan det være behov for å vurdere kompensatoriske tiltak.

11.3 Høringsinstansenes syn

Et flertall av høringsinstansene er enig i utvalgets forslag til regulering av objekt- og infrastruktursikkerhet. Flere uttalelser peker på at det kan være utfordrende å finne hensiktsmessige avgrensninger til hvilke systemer og infrastrukturer som loven skal kunne regulere.

Samferdselsdepartementet uttaler:

> «Utvalget foreslår å utvide sikkerhetsloven fra kun å omhandle objekter til også å omfatte skjermingsverdig infrastruktur. SD mener en slik systemtilnærming er grunnleggende fornuftig. Samtidig er vi av den oppfatning at en slik tilnærming fordrer at man tenker nytt med hensyn til hvordan systemer skal sikres. Det er grunn til å tro at hva som er hensiktsmessige sikringstiltak i stor grad vil variere mellom ulike sektorer og ulike typer infrastrukturer og objekter. SD er derfor positive til at man i større grad legger opp til funksjonskrav, og at det i utgangspunktet vil være sektormyndighetene – med utgangspunkt i sin sektorkunnskap – som skal legge føringer for hva som er forsvarlig sikkerhet.»

NSM uttaler blant annet:

Til lovforslaget § 7-1:

> «Det er av vesentlig betydning å holde en samlet nasjonal oversikt over skjermingsverdige objekter og infrastruktur. Det bør derfor fremgå av § 7-1 at klassifiserte objekter og infrastruktur skal meldes til Sikkerhetsmyndigheten.
>
> Bestemmelsens ordlyd er forenklet sammenliknet med dagens § 17. Dagens bestemmelse stiller opp visse kriterier som særlig skal vurderes i utvelgelsesprosessen. NSM tror det er nyttig å ha denne type kriterier til hjelp i utvelgelsesprosessen og mener derfor at kriteriene vurderes videreført enten på lovs nivå eller i forskrift.
>
> Det må også sikres at objekter og infrastruktur som må skjermes på bakgrunn av internasjonale avtaler og overenskomster, slik som bakkeinfrastruktur til satelittnavigasjonssystemet Galileo, kan utpekes som skjermingsverdig objekt eller infrastruktur.»

Til lovforslaget § 7-2:

> «Ordlyden i første ledd bokstav a til c er forenklet slik at det nå utelukkende vises til «*redusert funksjonalitet*». NSM legger til grunn at dette ikke innebærer en realitetsendring men at begrepet også vil favne skadeverk, ødeleggelse eller rettsstridig overtakelse.»

Til lovforslaget § 7-3:

> «Til bestemmelsens andre ledd første punkt, vil NSM bemerke at siste setningsledd ikke har selvstendig betydning. Konsekvens ved bortfall eller reduksjon av kvalitet er allerede vurdert gjennom klassifiseringen. Siste setningsledd kan derfor strykes.
>
> Bestemmelsens tredje ledd gir hjemmel til å treffe vedtak om adgangsklarering for tilgang

til skjermingsverdig objekt eller infrastruktur. I relasjon til begrepet tilgang legger NSM til grunn at dette både omfatter fysisk og logisk tilgang. Det bør vurderes om dette skal synliggjøres i bestemmelsen.»

Til lovforslaget § 7-4:

«NSM gir sin tilslutning til at det etableres en hjemmel for testing av sikkerhetssystemer. Bestemmelsen må legge til rette for en bred virkemiddelbruk, og herunder blant annet omfatte både fysisk og logisk forsering. NSM legger til grunn at man også med hjemmel i denne bestemmelsen kan gjennomføre Tekniske sikkerhetsundersøkelser i «grunnleggende nasjonale funksjoner».

Nasjonal kommunikasjonsmyndighet (Nkom) uttaler:

Til lovforslaget § 7-1:

«Bestemmelsen regulerer departementenes og Sikkerhetsmyndighetens ansvar og myndighet til å utpeke, klassifisere og holde oversikt over skjermingsverdige objekter og infrastruktur, og må ses i sammenheng med departementenes og sikkerhetsmyndighetens myndighet til å treffe enkeltvedtak lovforslagets § 2-1 første ledd bokstav c og § 2-2, første ledd bokstav e.»

Til lovforslaget § 7-3:

«Nkom har en del erfaring med bruk av sikkerhetsklareringsregimet knyttet til objektsikkerhet. Med et aktørbilde i stadig endring er det mange argumenter for en forenkling av bakgrunnssjekken av personell med tilgang til lavere klassifiserte objekter. Lovforslaget, slik vi forstår det, innfører adgangsklarering som et svar på denne utfordringen. Nkom støtter dette for lavere klassifiserte objekter, men ber departementet vurdere å la myndigheten beholde adgangen til å kreve klarering av personell som skal ha adgang til objekter klassifisert KRITISK eller MEGET KRITISK.»

Telenor uttaler:

«Telenor støtter innføringen av et nytt begrep *skjermingsverdig infrastruktur*, hvor anlegg og systemer ses i sammenheng og ikke bare gjelder fysiske skjermingsverdige objekter. At det åpnes opp for å utpeke kontroll- og styringssystemer som skjermingsverdig infrastruktur på forskjellige klassifiseringsnivåer anses positivt.

Lovforslaget legger opp til funksjonelle krav til sikring. Dette er fornuftig og sett fra et virksomhetsperspektiv gir det stort mulighetsrom for å finne hensiktsmessige løsninger. I et nasjonalt perspektiv kan det imidlertid gi økt risiko hvis det ikke er tverrsektoriell koordinering. Det er viktig at lovforslaget tydeliggjør at sektoransvarlige må sikre samsvar innad i sektoren, og at Sikkerhetsmyndigheten har ansvaret for å sikre samsvar på tvers av sektorer med hensyn på bruk av standarder og begreper og hvordan man vurderer risiko.

Telenor har tidligere påpekt behovet for tverrsektoriell koordinering og synes det er positivt at utvalget med sitt lovforslag legger til rette for det. At sikkerhetsmyndighetene ikke bare koordinerer, men også blir en aktiv pådriver for arbeidet fremover anser vi som viktig.»

Statnett uttaler:

«Det er gjennom energilovens beredskapsforskrift utpekt, klassifisert og etablert oversikt over sektorens objekter og infrastruktur. Sikkerhetsloven er således […] langt på vei overlappende med beredskapsforskriften. Samtidig ser Statnett de sikkerhetsmessige gevinstene ved å kunne adgangsklarere personell til kritiske objekter og infrastruktur.[…]

[…]

Anlegg og systemers sikring etableres ut fra sikkerhetsklassen, og er et veletablert system som gir detaljerte krav til fysisk sikring av anlegg, og ikke minst til robustheten i de elektriske og digitale komponentene. Det fremstår derfor som viktig at en ny sikkerhetslov ikke griper inn og overstyrer energiloven.»

Norges vassdrags- og energidirektorat (NVE) uttaler blant annet:

«Utvalget skriver at det er «*verdt å merke seg at det eksisterende sektorregelverket eksisterer sammen med gjeldende sikkerhetslov, og at i den grad objekter er utpekt som skjermingsverdig objekt omfattes de av dette regelverket*». NVE vil bemerke at dette ikke gjelder for energisektoren. Ingen objekter innenfor energiforsyningen er i dag underlagt gjeldende sikkerhetslov. Beredskapsforskriftens virkeområde er videre enn forslaget i ny sikkerhetslov. Det betyr at de objekter i energiforsyningen som eventuelt vil

bli utpekt av departementet allerede har krav til objektsikring. NVE mener det er god grunn til å videreføre denne systematikken.

[…]

NVE støtter forslaget om å utvide loven til å gjelde «objekter og infrastruktur av kritisk betydning for grunnleggende nasjonale funksjoner» Dette er en utvidelse av dagens sikkerhetslovs «skjermingsverdige objekter». Utvalget skriver at det er «behov for å innføre begrepet infrastruktur, for å skape tydeligere skille mellom enkeltstående objekter og infrastruktur som del av et system som understøtter grunnleggende nasjonale funksjoner.» NVE støtter utvalget i at innføring av begrepet skjermingsverdig infrastruktur i seg selv vil kunne bidra til å imøtegå svakheten de fremhever ved dagens regelverk. NVE mener imidlertid, som utvalget også peker på, at objekter og infrastruktur er ulikt regulert innenfor de ulike sektorene. For å motvirke tilsiktede uønskede hendelser på en samfunnsmessig rasjonell måte, må forskriftene være tilpasset den enkelte infrastruktur.

[…]

NVE er enig med utvalget om at det vil være hensiktsmessig å klassifisere skjermingsverdige objekter og infrastruktur. NVE mener at det også bør være med i vurderingen hvor lang tid det vil ta før system er tilbake til normal funksjon ved for eksempel en sabotasjehandling.

[…]

NVE er enig i utvalgets vurdering om at begrunnelsen for klassifiseringen bør følge sektormyndigheters og sikkerhetsmyndighetens oversikt over skjermingsverdige objekter og infrastruktur. Denne informasjonen vil inneholde viktig informasjon for sektormyndigheter i forbindelse med tilsyn og kontroll med sikkerhetsnivå og gjennomførte sikkerhetstiltak.

[…]

Dersom eiere av virksomheter innen energiforsyningen ved enkeltvedtak blir omfattet av sikkerhetsloven, vil eierne av disse objektene måtte forholde seg til krav som til dels dupliserer de krav som allerede gjelder etter sektorlovgivningen. Det vil da oppstå muligheter for motsetninger eller uklarheter mellom de to regelsettene, samt utfordringer knyttet til grenseflatene mellom NVE som tilsynsorgan etter beredskapsforskriften og damsikkerhetsforskriften og sikkerhetsmyndigheten. De områdene som kan bli spesielt problematiske er samordning av nivået for klassifisering, gradering av store informasjonsmengder, sikkerhetsklarering av et stort antall personell, rett tilsynsmyndighet, ulik tilsynsmyndighet etter sikkerhetsloven og sektorlovgivningen, ulikt nivå for klagebehandling med mer.»

Energi Norge uttaler:

«En infrastruktur som det norske kraftsystemet kan ikke sikres fullstendig, noe som utvalget også slår fast. Nytteeffekten av ulike tiltak må vurderes, og avveiningen mellom objektsikring og systemsikring vil være sentral i slike vurderinger.»

Norsk olje og gass uttaler:

«Klassifiseringen av det enkelte skjermingsverdige objekt eller infrastruktur kan få stor betydning for den enkelte virksomhet. Norsk olje og gass foreslår at det inntas en tilsvarende forholdsmessighetsvurdering som i lovutkastet § 4-1 andre ledd ved klassifisering av skjermingsverdige objekter og infrastruktur, jf. lovutkastet § 7-2 andre ledd. Avgjørelse om klassifisering må anses som et enkeltvedtak, som bør kunne påklages av virksomheten som råder over objektet. Dette synes å være i tråd med utvalgets kommentarer til § 7-1 tredje ledd, men i lovforslaget er kun «utpeking» nevnt. Norsk olje og gass vil foreslå at det her presiseres at også klassifiseringen kan påklages.»

Politidirektoratet uttaler:

«Politidirektoratet støtter en utvidelse av nedslagsfeltet til objektsikkerhetsregelverket slik at det også omfatter infrastruktur. At *systemer* omfattes fremfor *objekter* er en forutsetning for å oppnå en helhetlig sikring med fokus på avhengigheter.

Utfordringen for politiet er at flere objekter vil forvente en høyere prioritet på reaksjonsstyrker fra politiet ved en uønsket hendelse, mens politiets ressurser vil være de samme. […] Dette fordrer at politiet må prioritere bruk av sine ressurser ut fra det til enhver tids gjeldende trusselbilde, og ikke ut fra hvilke objekter som har høyeste klassifisering.»

Oslo politidistrikt uttaler:

> «Utvalget har ikke drøftet nøkkelpersonell og beredskapsressurser som en faktor som må beskyttes. Personell som er innsatsfaktorer til grunnleggende nasjonale funksjoner på lik linje med eiendom definert som skjermingsverdig objekt, bør gis tilsvarende beskyttelse. […] Per i dag berører verken lov eller forskrift nøkkelpersonell som verdiobjekter. Det bør derfor stilles krav til at den enkelte virksomhet skal vurdere beskyttelsestiltak for eget personell, herunder informasjon om personellet i egne informasjonssystemer.»

Luftfartstilsynet uttaler blant annet:

> «Luftfartstilsynet støtter en omlegging av strukturen, slik at regelverket om forebyggende sikkerhet for kritisk infrastruktur og objekter går fra dagens til dels fragmenterte karakter, til å bli samlet i sikkerhetsloven. Vi er også enig i forslaget om å utvide sikkerhetsloven til å omfatte skjermingsverdig infrastruktur.
>
> Luftfartstilsynet legger til grunn som et utgangspunkt at norske lufthavner med passasjertrafikk, alle vil falle inn under «objekter og infrastruktur av kritisk betydning for grunnleggende nasjonale funksjoner». Den etablerte interkonnektiviteten mellom disse lufthavnene, som inngår i det europeiske området hvor det er etablert såkalt «one-stop-security», har som konsekvens at de alle faller inn under sikkerhetsloven, jf. utkastets § 7-1, dog med ulike klassifiseringer, jf. utkastets § 7-2.»

NHO Luftfart uttaler på sin side:

> «Skjermingsverdig objekt og infrastruktur defineres i NOUen som eiendom og anlegg og systemer som må beskyttes mot tilsiktede uønskede hendelser av hensyn til opprettholdelse av grunnleggende nasjonale funksjoner. Vi antar at hva som vil være å anse som «skjermingsverdig» må ses i sammenheng med gjeldende objektsikkerhetsregelverk, herunder de krav som fremkommer av objektsikkerhetsforskriften. Skillet mellom «objekter» og «infrastruktur» er slik vi leser det flytende. Vi legger til grunn i den videre drøftelsen at flyplasser, ift. spørsmålet om disse er å kunne anse som skjermingsverdig, faller inn under infrastrukturdefinisjonen. Slik vi forstår det skal det være en høy terskel for å utpeke et objekt/infrastruktur som skjermingsverdig.
>
> […] Vi stiller oss […] tvilende til om det vil være mulig, og ikke minst om det er ønskelig og praktisk, å definere alle Avinors flyplasser som skjermingsverdig ift. de kriterier som skal ligge til grunn for et slikt vedtak, jf. «opprettholdelse av grunnleggende nasjonale funksjoner». Vi stiller i forbindelse med dette spørsmål om det i hele tatt er mulig å definere flyplasser som skjermingsverdig all den tid de er åpne for publikum på landside, samt på sikkerhetskritiske områder for reisende som har vært underlagt en sikkerhetskontroll. Vi mener således det blir feil å knytte adgangsklarering for vår sektor opp mot begrepet «skjermingsverdig» […]».

Avinor uttaler:

> «Avinor vil måtte gjennomføre sikringsrisikovurderinger ved et større antall geografiske lokasjoner for å belyse infrastrukturens samfunnskritikalitet. Dette vil medføre ressursbruk av betydelig omfang.
>
> Myndighet til å klassifisere objekter og infrastruktur tilligger ansvarlig departement eller Sikkerhetsmyndighet. Formålet med klassifisering av objekter og infrastruktur er dels at det er styrende for hvilke sikkerhetstiltak som skal iverksettes, og dels at det gir myndighetene anledning til å kunne prioritere mellom ulike objekt eller infrastruktur avhengig av graden av kritikalitet ved redusert funksjonalitet.
>
> Departementene og Sikkerhetsmyndigheten gis myndighet til å treffe vedtak om krav til adgangsklarering for tilgang til hele eller deler av objekt eller infrastruktur som er utpekt og klassifisert.
>
> Avinor har ingen merknader til dette utover at det per i dag er vanskelig å kvantifisere eller anslå administrative og økonomiske konsekvenser av forslagene før disse er nærmere detaljert i forskrifts form.»

Norges Ingeniør- og Teknologorganisasjon (NITO) uttaler blant annet:

> «NITO vil understreke at gjensidige avhengigheter i og mellom sektorer er noe av nøkkelen for å få etablert en sikkerhetsbevissthet som ivaretar lovens intensjon.
>
> Utvalget foreslår en videreføring av ordningen der ansvarlig departement for den enkelte

samfunnssektor har det primære ansvaret for å utpeke, klassifisere og holde oversikt over skjermingsverdige objekter og infrastruktur. NITO mener ansvaret kan innskjerpes ytterligere, ved at loven pålegger det enkelte fagdepartement å foreta den vurderingen. Etter NITOs syn vil en delegering av ansvaret trolig medføre at underliggende instans foretar en vurdering som ikke ivaretar helhetsinteressene. Da kan andre hensyn, eksempelvis økonomiske, veie tyngre.»

Konsulentselskapet *BDO* kommenterer de enkelte forslag til bestemmelser i kapittelet om objekt- og infrastruktursikkerhet:

«Forslaget til § 7-2 fastsetter at klassifisering av objekter og infrastruktur skal skje på bakgrunn av en «risiko- og sårbarhetsanalyse».

BDO anser at klassifisering av objekter og infrastruktur bør skje på bakgrunn av en *verdivurdering*. I verdivurderingen bør det inngå en vurdering av skadepotensialet ved redusert funksjonalitet. Det er slik tilnærmingen er for gradering av informasjon både i gjeldende sikkerhetslov § 11 og utvalgets lovforslag § 5-1, og det er også tilnærmingen for klassifisering etter gjeldende sikkerhetslov § 17a. BDO mener det er uheldig og lite pedagogisk at det er en annen tilnærming ved klassifisering av objekter og infrastruktur, enn ved gradering av informasjon. I tillegg mener BDO det er fare for at bestemmelsen, slik den er formulert, fører til at objekter og infrastruktur ikke blir klassifisert med den begrunnelse at trusselnivået er lavt eller at sårbarheten er lav. […] BDO anbefaler derfor at uttrykket «risiko- og sårbarhetsanalyse» erstattes med «verdivurdering».

[…]

Utvalgets tilnærming til sikring av objekter og infrastruktur er i utredningen knyttet til det som er av kritisk betydning for grunnleggende nasjonale funksjoner, uttrykt spesielt i §§ 7-1 til 7-3.

BDO er enig i viktigheten av å inkludere infrastruktur og dermed få en mer systemrettet tilnærming til hva som skal sikres og hvordan. Samtidig er vi bekymret for at forslaget ikke tar med objekter som kan utnyttes til å påføre befolkningen og det ytre miljøet meget store eller langvarig skade. Det vises i denne sammenheng til at gjeldende sikkerhetslov § 17 første ledd bokstav d har en slik kategori som grunnlag for utvelgelse av skjermingsverdige objekter. Dette er objekter som ikke behøver å ha en kritisk funksjon for samfunnet, men som ved rettsstridig overtakelse eller tyveri av materiale derfra, kan utnyttes til omfattende skade på andre. Et eksempel er atomreaktorer for forskningsformål eller store giftdeponier. Dersom denne type objekter, slik BDO forstår utvalgets forslag, ikke lenger skal (kunne) omfattes av sikkerhetsloven, må det utredes nærmere hvilke andre sikkerhetsregelverk disse i stedet skal /kan underlegges, og om det vil være en tilstrekkelig regulering ut ifra det skadepotensialet objektene representerer.»

Statens strålevern uttaler:

«Objekter (anlegg) med stort skadepotensiale (f.eks. C, B og/eller RN materiale) vil kunne utgjøre en fare for samfunnskritiske funksjoner og derfor være skjermingsverdige. Det er viktig at tilsynsorgan kan foreslå objekter som skjermingsverdige uavhengig av objekteiers vurdering. Vi er videre enige i FFIs konklusjon om at det er behov for et nasjonalt tverrsektorielt regelverk for utvelgelse av skjermingsverdige objekter. Dette bør inneholde dimensjonerende trusler for de tiltak som skal iverksettes for objektsikkerhet.»

Generaladvokaten uttaler til lovforslaget § 7-5 Adgang til steder og områder:

«Generaladvokaten forstår lovforslaget slik at adgangsforbudet i gjeldende sikkerhetslov § 18a videreføres i ny lovs § 7-5, og at ordlyden i gjeldende bestemmelse i hovedsak videreføres.

Den gjeldende sikkerhetsloven § 18a er i det vesentlige en videreføring av ordlyden i lov om forsvarshemmeligheter § 1, som ble opphevet da ny straffelov trådte i kraft. Det var ikke tilsiktet noen realitetsendring av bestemmelsen.

I lovforslaget til ny sikkerhetslov § 7-5 har gjeldende sikkerhetslov § 18a bokstav a) «forsvarsbygg og -anlegg hvor gjenstander av interesse for rikets forsvar fremstilles, istandsettes eller oppbevares», falt bort. Generaladvokaten støtter imidlertid utvalget sin begrunnelse om at adgangen til å fastsette slike forbud ivaretas av de øvrige delene av lovforslaget. […] Det er informasjonen, funksjonen og verdien innenfor eller der det er adgangsforbud som er av betydning, og dette endres med trusselbildet, tilgjengelige ressurser, beredskapen

og samfunnsutviklingen for øvrig. En nærmere presisering og konkretisering av hvor og hva et forbud skal omfatte, er dessuten den enkelte etat den nærmeste og best kvalifiserte til å vurdere i forskrifts form. Generaladvokaten tar da forbehold om at en forskrift til § 7-5 om forbudt adgang til visse områder av forsvarshensyn, faktisk blir videreført.»

11.4 Departementets vurdering

Som foreslått av utvalget legger departementet til grunn at lovforslaget skal omfatte både objekt- og infrastruktursikkerhet. Det betyr at gjeldende lovs mer ensidige objektfokus utvides til en mer helhetlig systemtilnærming for sikkerhet i funksjoner. Til grunn for denne vurderingen ligger blant annet at nettverkssystemer i stadig økende grad er viktig for helhetlig sikkerhet i samfunnet. Med denne helhetlige tilnærmingen vil strukturene som ofte binder ulike former for objekt og funksjoner sammen i systemer, også bli omfattet av loven.

Lovbestemmelsene om objekt- og infrastruktursikkerhet er i utgangspunktet rettet mot fysiske objekter og fysiske strukturer. Likevel er det innenfor intensjonen til lovforslaget at også logiske strukturer som inngår i ulike former for informasjonssystemer, skal omfattes av loven. Denne typen strukturer er imidlertid i seg selv svært sammensatte. Det er to hovedtyper av informasjonssystemer som har klar sammenheng med og betydning for objekt- og infrastruktursikkerhet. For det første gjelder dette infrastruktur der informasjonssystemene utgjør integrerte strukturer i den fysiske infrastrukturen. Dette gjelder for eksempel styringssystemer i kraftforsyningen og innenfor jernbanen. Den andre systemtypen utgjør en selvstendig infrastruktur og leverer informasjonstjenester som sluttprodukt, for eksempel ekom-tjenester som mobiltelefoni eller internett.

Etter departementets vurdering er disse typene systemer så vidt komplekse at den grunnleggende risikobaserte vurderingen som hovedregel bør inngå under bestemmelsene for informasjonssikkerhet og informasjonssystemsikkerhet. Disse funksjonene er likevel også viktige for objekt- og infrastruktursikkerhet. 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. Dette vil måtte reguleres nærmere i forskrift.

Departementet er enig med utvalget når det gir uttrykk for å videreføre dagens praksis som gir de enkelte departementene ansvar for å utpeke og klassifisere skjermingsverdige objekter og skjermingsverdig infrastruktur. Dette er også det eneste logiske når lovforslaget for øvrig bygger på å legge ansvar og myndighet til hvert enkelt departement til å identifisere og holde oversikt over grunnleggende nasjonale funksjoner innenfor sitt myndighetsområde, og dessuten til å identifisere og holde oversikt over virksomheter som har vesentlig betydning for grunnleggende nasjonale funksjoner, jf. lovforslagets § 2-1. I en slik identifikasjonsprosess må det forventes at også skjermingsverdige objekter og skjermingsverdig infrastruktur vil bli identifisert.

Når det gjelder begrepsbruken, har departementet merket seg at hovedtyngden av høringsinstansene som har uttalt seg til spørsmålet, er enige i at man også innbefatter infrastruktur i tospann med objekt.

Utvalget mener at begrepet objekt, slik det er benyttet i gjeldende sikkerhetslov, også dekker infrastruktur, men ser likevel behov for å innføre begrepet infrastruktur for å skape et tydeligere skille mellom enkeltstående objekter og infrastruktur som del av et system som understøtter grunnleggende nasjonale funksjoner. Departementet viser i denne sammenheng til at begrepet skjermingsverdig objekt i dagens sikkerhetslov er definert som «eiendom som må beskyttes mot sikkerhetstruende virksomhet…» og at begrepet eiendom er definert som «områder, bygninger, anlegg, transportmidler eller annet materiell, eller deler av slik eiendom», jf. § 3 første ledd nr. 12 og 13. Departementet oppfatter likevel at å bruke begrepet infrastruktur i tillegg til objekt, innebærer en viss utvidelse av lovens virkeområde i forhold til dagens lov, og ikke bare en tydeliggjøring. Departementet oppfatter videre den nye begrepsbruken som en modernisering, ved at den er mer systemrettet og innrettet mot funksjonelle krav for å sikre et forsvarlig sikkerhetsnivå, i motsetning til dagens lov med til dels strenge og mer spesifikke «skal-krav» til beskyttelse av objekter. En begrenset utvidelse av sikkerhetslovens virkeområde etter lovforslagets modell trenger derfor ikke nødvendigvis å innebære store økonomiske og administrative konsekvenser sett opp mot dagens lovverk.

Det er likevel grunn til å utvise noe varsomhet i en slik utvelgelsesprosess inn mot systemer. I utgangspunktet skal det være en relativt høy ter-

skel for utpeking av skjermingsverdige objekter og infrastruktur og for den klassifisering som skal foretas.

Det er den enkelte virksomhet som skal iverksette nødvendige sikkerhetstiltak for å opprettholde et forsvarlig sikkerhetsnivå. Sikkerhetstiltakene er eksemplifisert gjennom en beskrivelse av begrepene «barrierer, deteksjon, verifikasjon og reaksjon». Barrierer er i forslaget til § 7-3 beskrevet som «fysiske, elektroniske, menneskelige eller organisatoriske barrierer». Deteksjon er forklart som «systemer som skal oppdage og varsle om aktiviteter eller hendelser». Verifikasjon er forklart som «systemer og rutiner for avklaring vedrørende aktiviteter og hendelser», mens reaksjon er forklart som «oppfølging av uønskede aktiviteter og uønskede hendelser». Til forskjell fra dagens «skal»-bestemmelse, jf. § 17 b andre ledd, foreslås en mer fleksibel bestemmelse i § 7-3, dels ved å presisere at tiltakene kan bestå av en kombinasjon av de nevnte tiltakene og dels ved å åpne for andre typer sikkerhetstiltak, jf. «kan være» i § 7-3 første ledd andre punktum.

Konsulentselskapet *BDO* viser i sin høringsuttalelse blant annet til dagens sikkerhetslov § 17 første ledd bokstav d som gjelder objektets «mulighet for å utgjøre gjøre fare for miljøet eller befolkningens liv og helse» dersom objektet blir påført skade, og uttrykker bekymring for at slike objekter ikke omfattes av lovforslaget. *BDO* viser til at dette er objekter som ikke behøver å ha en kritisk funksjon for samfunnet, men som ved rettstridig overtakelse eller ved tyveri av materiale derfra kan utnyttes til omfattende skade på andre. Etter departementets syn er dette forhold som kan ligge innenfor nasjonale sikkerhetsinteresser, jf. § 1-5 nr. 1 bokstav e, om «samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet».

Når *BDO* i denne sammenheng uttrykker tvil om lovforslaget vil omfatte objekter som atomreaktorer og giftdeponier, vil det være fagdepartementet som vil måtte foreta en konkret vurdering av dette. Departementet har i denne sammenheng merket seg høringsuttalelsen fra *Statens strålevern* om at objekter med stort skadepotensial vil kunne utgjøre en fare for samfunnskritiske funksjoner og derfor være skjermingsverdige, jf. ovenfor i kapittel 11.3.

Skjermingsverdig objekt innbefatter etter departementets forståelse, på samme måte som etter dagens sikkerhetslov § 17 første ledd bokstav c, også objekter med stor nasjonal symbolverdi, og som dermed vil kunne være mulige terrormål. Eksempler på objekter med stor nasjonal symbolverdi kan være Nasjonalbiblioteket, Nidarosdomen, Akershus slott, og andre historiske bygninger som nasjonen knytter sin identitet til.

Departementet har merket seg at *NSM* i sin høringsuttalelse savner kriterier i lovforslaget § 7-1 som særlig skal vurderes i utvelgelsesprosessen av skjermingsverdige objekter og skjermingsverdig infrastruktur, slik man har i gjeldende sikkerhetslov § 17. Ved å lese lovforslaget § 7-1 i sammenheng med forslag til § 1-3 og departementenes ansvar og myndighet for forebyggende sikkerhetsarbeid etter loven, jf. § 2-1, mener departementet at kriterier for utvelgelse foreligger. Utvalget har foreslått at det utarbeides scenarioer som kan være til hjelp både ved identifisering av virksomheter som skal underlegges loven og ved utvelgelse av skjermingsverdige objekter og infrastruktur. Departementet er enig i at slike scenarioer kan være et nyttig hjelpemiddel i så måte. I tillegg vil de eksempler på kriterier for tiltak som foreslås inntatt i § 7-3 første ledd om barrierer mv., være egnet til å klargjøre de prosesser som skal gjennomføres.

På samme måte som § 1-3 tredje ledd, foreslås det en bestemmelse i § 7-1 sjette ledd som gir sikkerhetsmyndigheten adgang til på eget initiativ å fremme forslag overfor departementene om at det bør fattes vedtak om utpeking av skjermingsverdige objekter og infrastruktur i medhold av § 7-1 andre ledd.

Når det gjelder *NSMs* bemerkning til «redusert funksjonalitet» i lovforslaget § 7-2, er departementet enig i at dette også omfatter skadeverk, ødeleggelse og rettsstridig overtakelse. For å tydeliggjøre denne forståelsen foreslår departementet at dette presiseres uttrykkelig i loven, jf. § 7-1 første ledd.

NSM reiser problemstillingen om hvorvidt en adgangsklarering vil omfatte både fysisk tilgang til et objekt eller en infrastruktur og en logisk (digital) tilgang. I utvalgets forslag kan det settes krav til adgangsklarering både for fysisk og logisk tilgang. Departementet er enig i dette, jf. merknad til § 7-3.

Nkom har i sin høringsuttalelse om etablering av en adgangsklarering bedt departementet om å la myndigheten beholde adgangen til å kreve sikkerhetsklarering av personell som skal ha adgang til objekter klassifisert KRITISK eller MEGET KRITISK. En adgangsklarering skal i utgangspunktet ikke erstatte sikkerhetsklareringsordningen, men være et supplement der det ikke anses nødvendig med en «full» sikkerhetsklarering. Det vil derfor ikke være unaturlig med krav til sikkerhetsklarering for tilgang til objekter og infrastruk-

tur med de høyeste klassifiseringsnivåene. Dette vil det imidlertid være opp til det enkelte fagdepartement å beslutte.

Statnett og *NVE* er i sine høringsuttalelser opptatt av at eget sektorregelverk er godt og at sikkerhetsloven vil kunne duplisere sektorregelverket på en uheldig måte, i den grad sikkerhetsloven får anvendelse i kraftsektoren. Departementet er kjent med at sektorregelverket er godt i kraftsektoren. Sikkerhetsloven er ikke ment å skulle «gripe inn og overstyre energiloven». Der sektorregelverket anses å være tilfredsstillende på sikkerhetsområdet, forutsettes dette i utgangspunktet å gå foran sikkerhetslovens bestemmelser. Dette antas i særlig grad å gjøre seg gjeldende innenfor området objekt- og infrastruktursikkerhet. Departementet vil presisere at denne «forrangen» kan aktualiseres når det er tale om sikkerhetstiltakene, ikke i spørsmålet om objektet eller infrastrukturen er skjermingsverdig etter sikkerhetsloven eller ikke. Departementet ser på samme måte som utvalget at det er behov for et tverrsektorielt regelverk som skal ivareta helheten, oversikten og balansen i sikkerhetsarbeidet i de ulike samfunnssektorene. Det er i en slik sammenheng at sikkerhetsloven bør få anvendelse. Med god samhandling mellom sikkerhetsmyndigheten og sektormyndighet vil dette være egnet til å øke det samlede sikkerhetsnivået i samfunnet. Selv om en konkret vurdering skulle resultere i at enkelte objekter eller infrastruktur fra kraftsektoren blir omfattet av sikkerhetsloven, vil ikke dette nødvendigvis innebære store kostnader siden sikkerhetsnivået allerede er godt ivaretatt gjennom sektorregelverket.

Departementet følger opp utvalgets forslag om at en avgjørelse om utpeking av objekt eller infrastruktur som skjermingsverdig kan påklages til overordnet organ, dersom utpekingen berører selvstendige rettssubjekter, jf. forslaget til § 7-1 femte ledd. *Norsk olje og gass* mener at denne klageretten også må omfatte hvilken *klassifisering* som blir gitt det utpekte objekt eller infrastruktur. Departementet finner det ikke naturlig å skille klassifiseringen ut som et eget enkeltvedtak, idet en klassifisering normalt vil bli gitt samtidig med utpekingen. Utpekingen og klassifiseringen hører nøye sammen med den helhetlige vurderingen som det ansvarlige departementet vil måtte foreta.

Når det gjelder eventuell bruk av sikringsstyrker som sikkerhetstiltak for skjermingsverdige objekter og infrastruktur vil departementet understreke at tiltak for å sikre slike objekter og slik infrastruktur i all hovedsak vil være i form av forebyggende grunnsikring som objekteier eller rådighetshaver har ansvar for å foreta i fredstid. Bare rent unntaksvis, og på et fåtall objekter eller infrastruktur, kan det bli aktuelt med bruk av sikringsstyrker, og da normalt i en krisesituasjon. Det nærmere forholdet mellom instruksen om sikring og beskyttelse av objekter ved bruk av sikringsstyrker fra Forsvaret og politiet og objektsikkerhetsregelverket, forutsettes nærmere behandlet i forbindelse med en revisjon av objektsikkerhetsforskriften.

12 Personellsikkerhet

12.1 Innledning

Formålet med personellsikkerhet er å sikre at personell som skal ha tilgang til sikkerhetsgradert informasjon eller skjermingsverdige objekter og infrastruktur, har den nødvendige lojaliteten og påliteligheten slik at man kan ha begrunnet tillit til at personen er sikkerhetsmessig skikket.

Personellsikkerhet er et område hvor myndighetene gis hjemmel til å innhente og behandle til dels meget sensitive personopplysninger om den enkelte. Personellsikkerhet har således klare grenseflater mot enkeltindividets rettssikkerhet og personvern.

12.2 Gjeldende rett

12.2.1 Innledning

Gjeldende bestemmelser om personellsikkerhet står i dag i sikkerhetsloven kapittel 6. Nærmere bestemmelser er gitt i forskrift 29. juni 2001 nr. 722 om personellsikkerhet (forskrift om personellsikkerhet).

Bestemmelsene om personellsikkerhet har vært revidert i 2006, 2011 og 2016. Formålet med disse endringene var å styrke enkeltindividets rettssikkerhet i klareringsprosessen og å etablere mekanismer slik at personer ikke sikkerhetsklareres i større grad enn nødvendig, jf. Ot.prp. nr. 59 (2004–2005) og Ot.prp. nr. 21 (2007–2008). I endringsloven 12. august 2016 nr. 78, som trådte i kraft 1. januar 2017, ble det vedtatt at antall klareringsmyndigheter skulle reduseres til én for den sivile sektoren og én for forsvarssektoren.

12.2.2 Personellklarering og autorisasjon m.m.

I henhold til sikkerhetsloven § 19 skal personkontroll og sikkerhetsklarering gjennomføres før en person gis tilgang til skjermingsverdig informasjon gradert KONFIDENSIELT eller høyere. For tilgang til informasjon gradert BEGRENSET kreves ikke sikkerhetsklarering, men vedkommende må være autorisert. Fjerde ledd angir de nasjonale sikkerhetsgradene og tilsvarende sikkerhetsgrader som gjelder for NATO-klareringer.

Før klareringsmyndigheten kan treffe en avgjørelse om sikkerhetsklarering, må det gjennomføres en personkontroll, jf. sikkerhetsloven § 20. Personkontroll er definert i sikkerhetsloven § 3 første ledd nr. 18 som innhenting av relevante opplysninger til vurdering av sikkerhetsklarering.

Før autorisasjonsansvarlig i en virksomhet igangsetter personellkontroll, må den det gjelder informeres og samtykke til en slik kontroll, jf. sikkerhetsloven § 20 andre ledd.

Dersom en person skal klareres for HEMMELIG/tilsvarende eller høyere, kan personkontrollen også omfatte kontroll av nærstående personer som er knyttet til vedkommende ved familiebånd, jf. tredje ledd. *Nærstående* er definert i forskrift om personellsikkerhet § 1-2 første ledd nr. 5 som

> «ektefelle, partner, samboer, (herunder tidligere ektefelle, partner eller samboer de siste tre år), forelder til felles barn, barn (herunder ste-, adoptiv- eller fosterbarn), foreldre (herunder ste-, adoptiv- eller fosterforeldre) og søsken (herunder ste-, adoptiv-, foster- eller halvsøsken).»

Sikkerhetsloven § 20 regulerer hvem kontrollen kan omfatte og hvor opplysningene kan hentes fra. Kongen kan bestemme hvilke registre som er relevante for personkontroll.

Personopplysninger som behandles i forbindelse med personkontroll skal ikke brukes til andre formål enn å vurdere om en person kan sikkerhetsklareres. Dette framgår av § 20 sjette ledd. Unntaksvis kan opplysningene gis til autorisasjonsansvarlig dersom det er påkrevet av hensyn til den sikkerhetsmessige ledelse og kontroll av vedkommende.

Det følger av gjeldende forskrift om personellsikkerhet § 3-7 at som hovedregel skal det foreligge ti års relevant informasjon om de personer som inngår i personkontrollen. Kravet kan fravikes etter en konkret helhetsvurdering.

Det vises for øvrig til redegjørelsen i NOU 2016: 19 kapittel 10.2.4 om gjennomføring av personkontroll.

Det følger av sikkerhetsloven § 21 at en sikkerhetsklarering bare kan gis eller opprettholdes dersom det ikke foreligger rimelig tvil om en person er sikkerhetsmessig skikket. Videre regulerer bestemmelsen hvilke opplysninger klareringsmyndigheten kan legge vekt på i vurderingen av om en person kan gis sikkerhetsklarering.

Det er et krav etter § 21 tredje ledd at det skal gjennomføres en sikkerhetssamtale der dette ikke anses som åpenbart unødvendig. Ved lovendringen som trådte i kraft 1. januar 2006 ble kravet til sikkerhetssamtale endret. Endringen ble i Ot.prp. nr. 59 (2004–2005) på side 32 begrunnet med en harmonisering med forvaltningsorganers utrednings- og informasjonsplikt i medhold av forvaltningsloven § 17 og innebærer at klareringsmyndigheten bør gjennomføre en slik samtale dersom det er tvil om vedkommende skal gis klarering. Sikkerhetssamtalen er ment som en rettssikkerhetsgaranti og skal ivareta hensynet til kontradiksjon.

Det følger av femte ledd at det i særlige tilfeller kan settes vilkår for sikkerhetsklarering. Denne bestemmelsen trådte i kraft 1. januar 2006, jf. Ot.prp. nr. 59 (2004–2005), side 32.

Det vises for øvrig til redegjørelsen i NOU 2016: 19 kapittel 10.2.5 om vurderingsgrunnlaget for sikkerhetsklarering.

Sikkerhetsloven § 22 regulerer når en utenlandsk statsborger kan gis sikkerhetsklarering. Utenlandske statsborgere kan gis sikkerhetsklarering etter en vurdering av hjemlandets sikkerhetsmessige betydning og personens tilknytning til hjemlandet og Norge, jf. Ot.prp. nr. 59 (2004–2005), side 32. I 2006 ble bestemmelsen endret for å åpne for at utenlandske statsborgere kunne bli sikkerhetsklarert. Før lovendringen i 2006 var hovedregelen at utenlandske statsborgere ikke skulle gis sikkerhetsklarering.

Det vises for øvrig til redegjørelsen i NOU 2016: 19 kapittel 10.2.6 om sikkerhetsklarering av utenlandske statsborgere.

Sikkerhetsloven § 23 første ledd regulerer når en person skal gis autorisasjon og hvem som er autorisasjonsansvarlig. En autorisasjon gis normalt av virksomhetens leder. En autorisasjonssamtale skal avholdes før autorisasjon gis. Autorisasjon skal ikke gis hvis autorisasjonsansvarlig har opplysninger som gjør det tvilsomt om personen er sikkerhetsmessig til å stole på. Autorisasjon skal ikke gis før det foreligger melding om sikkerhetsklarering, med unntak av tilgang til informasjon sikkerhetsgradert BEGRENSET.

Det følger av sikkerhetsloven § 23 andre ledd at det skal være én klareringsmyndighet for forsvarssektoren og én for sivil sektor. I tillegg kan Kongen utpeke andre klareringsmyndigheter. Bestemmelsen ble endret ved lov 12. august 2016 nr. 78 og trådte i kraft 1. januar 2017, jf. Innst. 352 L (2015–2016) til Prop. 97 L (2015–2016). Tidligere var det 42 klareringsmyndigheter.

For forsvarssektoren er det Forsvarets sikkerhetsavdeling (FSA) som er klareringsmyndighet. Nasjonal sikkerhetsmyndighet (NSM) og Etterretningstjenesten klarerer eget personell, jf. forskrift om personellsikkerhet § 4-1 a. I sivil sektor vil Politiets sikkerhetstjeneste (PST) klarere eget personell.

Det er foreløpig ikke opprettet en klareringsmyndighet for sivil sektor, og det er derfor fortsatt det enkelte departement som er klareringsmyndighet for egen sektor, jf. forskrift om personellsikkerhet § 4-1. Justis- og beredskapsdepartementet arbeider med etableringen av den nye sivile klareringsmyndigheten, med sikte på iverksetting fra tidlig i 2018.

Det vises for øvrig til redegjørelsen i NOU 2016: 19 kapittel 10.2.7 om klareringsmyndighet og autorisasjonsansvarlig.

Personer som blir autorisert og sikkerhetsklarert, har en plikt til å orientere om forhold som kan være av betydning for om vedkommende er sikkerhetsmessig skikket, jf. sikkerhetsloven § 24 første ledd. Det vil for eksempel være endringer i forhold som den enkelte har opplyst om i personopplysningsblanketten.

Dersom det framkommer opplysninger som kan reise tvil om en sikkerhetsklarert person er sikkerhetsmessig skikket, skal klareringsmyndigheten vurdere hvorvidt klareringen skal tilbakekalles, nedsettes til et lavere klareringsnivå eller suspenderes, jf. § 24 andre ledd. Klareringsmyndigheten skal i slike situasjoner iverksette nærmere undersøkelser for å avklare forholdet.

Tredje ledd regulerer meldeplikten til NSM og varslingsplikten til autorisasjonsansvarlig.

En autorisasjon vil automatisk falle bort i de tilfellene personen fratrer den stillingen autorisasjonen omfatter, når behovet for autorisasjon av andre grunner ikke lenger er tilstede eller når personen ikke har tilstrekkelig sikkerhetsklarering, jf. § 24 fjerde ledd.

Hvor lenge en sikkerhetsklarering skal være gyldig, reguleres i forskrift om personellsikkerhet § 4-8, jf. sikkerhetsloven § 24 sjette ledd.

Autorisasjonsansvarlig skal også vurdere å tilbakekalle, nedsette eller suspendere klareringen dersom det framkommer opplysninger som gir grunn til tvil om den autoriserte personen er sikkerhetsmessig skikket, jf. § 24 femte ledd. Autorisasjonsansvarlig kan etter denne bestemmelsen igangsette nærmere undersøkelser for å avklare forholdet. En forutsetning er imidlertid at personens klarering vurderes av klareringsmyndigheten uten ugrunnet opphold, jf. Ot.prp. nr. 49 (1996–97), side 70.

Det vises for øvrig til redegjørelsen i NOU 2016: 19 kapittel 10.2.8 om bortfall, tilbakekall, nedsettelse og suspensjon av sikkerhetsklaring og autorisasjon.

Sikkerhetsloven § 26 gir Kongen og NSM hjemmel til å gi forskrifter om personellsikkerhet. Første ledd gir hjemmel til Kongen for å opprette et register for klareringsavgjørelser. Etter andre ledd skal NSM gi utfyllende bestemmelser om personellsikkerhet, herunder om sikkerhetsklarering av bestemte kategorier personell, om arkivering, oppbevaring og forsendelse av dokumenter, og om avholdelse av sikkerhetssamtaler.

12.2.3 Saksbehandlingsregler

Saksbehandlingsreglene for avgjørelser om personellklarering og autorisasjon følger av sikkerhetsloven §§ 25, 25 a, 25 b og 25 c. Ved lovendringen 17. juni 2005 nr. 81 som trådte i kraft 1. januar 2006, ble det innført nye saksbehandlingsregler som skulle bedre den enkeltes rettssikkerhet i klareringsprosessen, jf. Ot.prp. nr. 59 (2004–2005).

Forvaltningsloven kapittel IV og VI gjelder ikke for avgjørelser om sikkerhetsklarering og autorisasjon. Dette følger av sikkerhetsloven § 25 første ledd. Det betyr at sikkerhetslovens saksbehandlingsregler er uttømmende for disse avgjørelsene.

Etter sikkerhetsloven § 25 andre ledd har personer som blir vurdert sikkerhetsklarert, en rett til å bli underrettet om resultatet av klareringen. Dersom avgjørelsen er negativ, skal klareringsmyndigheten på eget initiativ underrette vedkommende om resultatet og opplyse om klageadgangen. En *negativ avgjørelse* omfatter både de tilfellene der klarering nektes og de tilfellene der klarering gis, men på et lavere nivå enn det ble bedt om, jf. Ot.prp. nr. 59 (2004–2005), side 32. En negativ avgjørelse omfatter også de tilfellene der klareringsmyndigheten treffer avgjørelse om tilbakekallelse, nedsettelse og suspensjon av sikkerhetsklarering etter § 24, jf. Ot.prp. nr. 49 (1996–97), side 70.

En avgjørelse om klarering skal begrunnes, men personen som klareringen gjelder for, har ikke krav på en begrunnelse, i den utstrekning begrunnelsen ikke kan gis uten å røpe opplysninger som følger av § 25 tredje ledd bokstav a til d.

I forskrift om personellsikkerhet § 4-4 er det nærmere bestemmelser om underretning om klareringsavgjørelser. Etter § 25 fjerde ledd skal klareringsmyndigheten utarbeide en intern begrunnelse. Begrunnelsen skal vise til «dei reglar og faktiske omstende som avgjerda byggjer på, og på dei omsyna som det har vore lagt vekt på. I den interne grunngjevinga må alle vesentlege omstende takast med, også dei grunngjevingar som eventuelt er unntatt i den eksterne grunngjevinga med heimel i tredje leddet», jf. Ot.prp. nr. 59 (2004–2005).

I § 25 a gis det regler om retten til å få innsyn i sakens dokumenter. Man har først rett på innsyn etter at avgjørelsen er fattet. Innsyn på et tidligere tidspunkt vil kunne påvirke verdien av en sikkerhetssamtale for klareringsmyndigheten, jf. Ot.prp. nr. 59 (2004–2005).

I § 25 a andre ledd første punktum er det gitt unntak fra innsynsretten som samsvarer med § 25 tredje ledd bokstav a til d. I andre punktum følger et unntak for interne dokumenter. Unntaket skal forstås på samme måte som etter forvaltningsloven § 18, jf. Ot.prp. nr. 59 (2004–2005).

For å ivareta rettssikkerheten til de som ikke har rett på begrunnelse etter § 25 tredje ledd og innsyn etter § 25 a andre ledd første punktum, har sikkerhetsloven § 25 b bestemmelser om retten til bistand fra særskilt oppnevnt advokat. Retten til advokat inntrer først når personen avgjørelsen gjelder, har utprøvd klageadgang etter § 25 c andre ledd. Klagefristen må heller ikke være utløpt. Retten til advokat gjelder bare ved førsteinstansbehandlingen, jf. Ot.prp. nr. 59 (2004–2005) side 33. Advokaten har rett på tilgang til sakens faktiske opplysninger og til begrunnelser etter § 25 tredje ledd.

Forsvarsdepartementet oppnevner en gruppe advokater for dette formålet som sikkerhetsklareres på høyeste nivå. Begrunnelsen for at det oppnevnes en særskilt gruppe er at advokatene må sikkerhetsklareres for å få tilgang til opplysninger i klareringssaker.

«Advokaten skal gi vedkommande råd om saken bør påklagast. Ein advokat som blir kopla inn i saka har teieplikt i forhold til den saka gjeld, slik at dei opplysningane advokaten får tilgang til etter tredje leddet ikkje kan gis vidare til den som

skal klarerast. Advokaten vil såleis ikkje kunne representere vedkommande i ei eventuell klagesak», jf. Ot.prp. nr. 59 (2004–2005) side 33.

Det følger av sikkerhetsloven § 25 c at forvaltningsloven kapittel VI om klage på enkeltvedtak i utgangspunktet gjelder for klareringssaker med mindre annet følger av sikkerhetsloven eller forskrift om personellsikkerhet.

Unntak fra forvaltningsloven følger av § 25 c andre til tredje ledd og forskrift om personellsikkerhet § 4-5. Negative avgjørelser kan etter andre ledd påklages av den avgjørelsen retter seg mot. Tredje ledd regulerer hvem som er klageinstans.

Etter tredje ledd skal klagen sendes til den som har fattet avgjørelsen i første omgang. Dette er i samsvar med forvaltningslovens bestemmelser. NSM er klageinstans. Dersom NSM har behandlet saken i første instans, vil Forsvarsdepartementet være klageinstans, jf. tredje ledd tredje punktum. Fjerde ledd har bestemmelser om klagefrist og beregning av fristen.

Dersom en advokat har gjennomgått saken etter § 25 b, løper ny klagefrist fra den dag rådet fra advokaten har kommet fram til vedkommende.

Det vises for øvrig til redegjørelsen i NOU 2016: 19 kapittel 10.2.9 om saksbehandlingsregler.

12.2.4 Tilgang til skjermingsverdige objekter

Sikkerhetsloven § 17 b fjerde ledd gir Kongen hjemmel til å bestemme hvorvidt det skal kreves sikkerhetsklarering etter reglene i loven kapittel 6 for den som skal gis tilgang til skjermingsverdig objekt klassifisert MEGET KRITISK eller KRITISK. Bestemmelsen trådte i kraft 22. oktober 2010.

Det framgår av forarbeidene (Ot.prp. nr. 21 (2007–2008), side 44) til bestemmelsen at

> «[d]ette innebærer en innstramming i forhold til dagens hjemmelsgrunnlag på to områder: For det første at klareringsprosessen først skal igangsettes for person som «skal» gis tilgang til skjermingsverdig objekt. For det andre at sikkerhetsklarering først kan kreves for tilgang til objekt klassifisert MEGET KRITISK eller KRITISK. Klareringskravet og den nærmere utformingen av dette vil bli fastsatt i forskrifts form.»

Krav til sikkerhetsklarering og autorisasjon er nærmere regulert i objektsikkerhetsforskriften § 3-6. Det er det enkelte fagdepartement som bestemmer om det skal stilles krav om sikkerhetsklarering for personell som skal gis permanent adgang til objekter klassifisert KRITISK eller MEGET KRITISK. Sikkerhetsklarering skal ikke foretas der dette ikke anses som et egnet virkemiddel, og objekteier må begrunne behovet for klarering.

Det vises for øvrig til redegjørelsen i NOU 2016: 19 kapittel 10.2.3 om tilgang til skjermingsverdige objekter.

12.2.5 Sektorregelverket

Det er få andre lover som regulerer krav til klarering, vandelsdokumentasjon eller sikkerhetsvurderinger for personer som arbeider med sikring av objekter og anlegg.

Det er gitt særbestemmelser i eller i medhold av lov 11. juni 1993 nr. 101 om luftfart (luftfartsloven), lov 16. februar 2007 nr. 9 om skipssikkerhet (skipssikkerhetsloven) og lov 11. juni 1993 nr. 100 om anlegg og drift av jernbane, herunder sporvei, tunnelbane og forstadsbane m.m. (jernbaneloven).

Forskrift 1. mars 2011 nr. 214 om forebyggelse av anslag mot sikkerheten i luftfarten mv. (forskrift om sikkerheten i luftfarten mv.) regulerer personkontroll i luftfarten. Forskriften er hjemlet i luftfartsloven. Forskriften § 13 regulerer blant annet hvilke persongrupper som må inneha sikkerhetsklarering etter sikkerhetsloven. Forskriften kapittel IV regulerer adgangen til sikkerhetsbegrenset område mv. Her reguleres blant annet krav til ID-kort, bakgrunnssjekk, akkreditering og vandelskontroll. Forskriftens bestemmelser om bakgrunnssjekk er basert på kommisjonsforordning (EU) nr. 185/2010 som er erstattet av 2015/1998/EU.

Regjeringen besluttet i juni 2016 å innføre et midlertidig krav om akkreditering. Etter politiregisterforskriften § 38-5 kan politiet foreta akkreditering av personer som skal ha tilgang til bestemte områder hvor det av sikkerhetsmessige eller tungtveiende ordensmessige grunner er nødvendig med en kontroll av personen. Bestemmelsen benyttes typisk ved arrangementer der sikkerhetshensyn i stor grad gjør seg gjeldende, for eksempel ved statsbesøk. 1. september 2016 ble det vedtatt endringer i forskrift om sikkerhet i luftfarten som innebærer at Luftfartstilsynet kan stille krav om akkreditering av de som skal arbeide på sikkerhetsbegrenset område på lufthavnene, jf. forskriften § 35a.

Etter forskrift 22. juni 2004 nr. 972 om sikkerhet, pirat- og terrorberedskapstiltak og bruk av maktmidler om bord på skip og flyttbare boreinnretninger (sikkerhetsforskriften) § 20 andre ledd kan det stilles krav om personkontroll av vakts-

elskap og vakter, dersom et skip kan ha væpnede vakter om bord. Etter en risikovurdering og konsultasjon med skipsføreren kan et fartøy ta i bruk væpnede vakter for å hindre eller beskytte fartøyet mot terrorhandlinger og piratvirksomhet, jf. sikkerhetsforskriften § 20 første ledd. Bestemmelsen er hjemlet i skipssikkerhetsloven § 15.

Etter jernbaneloven § 3 d kan tilsynsmyndigheten fastsette krav om blant annet vandel for førere av rullende materiell og annet personell som skal utføre oppgaver knyttet til sikkerheten ved jernbane.

Det vises for øvrig til redegjørelsen i NOU 2016: 19 kapittel 10.3 om sektorregelverk.

12.3 Utvalgets forslag

12.3.1 Innledning

Sikkerhetsutvalget beskriver personellsikkerhet som et sentralt virkemiddel for å kunne forebygge, og eventuelt avdekke, at utro tjenere får tilgang til informasjon eller områder hvor skadepotensialet er stort. Samtidig understreker utvalget at det er denne delen av forebyggende sikkerhet som i størst grad gjør inngrep i den enkeltes personvern. Utvalget har videre hatt som gjennomgående prinsipp at forslag som innebærer inngrep i den enkeltes rettssikkerhet og personvern, skal være godt begrunnet, forholdsmessige og ha en sikkerhetsmessig effekt som overstiger personvernulempene.

På generelt grunnlag mener utvalget at dagens regelverk for personellsikkerhet i hovedsak klarer å balansere avveiningen mellom sikkerhetsmessige hensyn og hensynet til den enkeltes rettssikkerhet og personvern. Utvalget viser til at regelverket på lovs nivå har en fleksibel og dynamisk tilnærming, men peker på utfordringer knyttet til praktiseringen av regelverket. Det vises til at enkelte veiledninger og rundskriv på området gir inntrykk av en mer skjematisk tilnærming enn den individuelle og konkrete helhetsvurderingen loven legger opp til.

Personellsikkerhetsregelverket var gjenstand for en grundig revisjon i 2006, hvor hensynet til å sikre den enkeltes rettssikkerhet var førende for revisjonsarbeidet. Utvalgets syn er at saksbehandlingsreglene som er regulert i dagens sikkerhetslov, inneholder de nødvendige rettssikkerhetsgarantiene og ivaretar den enkeltes rettigheter i klareringsprosessen. Utvalget foreslår en videreføring av disse saksbehandlingsreglene uten store endringer. Utvalget har også merket seg at det i mange klareringssaker er svært lang saksbehandlingstid. I den utstrekning utfordringene med lang saksbehandlingstid skyldes regelverket, har utvalget vurdert hvorvidt det er mulig å innrette loven på en måte som understøtter behovet for effektivitet.

Utvalget har sett på hvorvidt personellsikkerhet bør vurderes i en sektorovergripende lov, eller om det vil være en tilstrekkelig regulering at dette fagfeltet også kan overlates til de ulike sektorregelverkene. Det fremgår av NOU 2016: 19 punkt 10.6, side 213 at:

> «Som et generelt utgangspunkt mener utvalget at personellsikkerhet fremdeles bør reguleres i et sektorovergripende regelverk. En slik tilnærming vil bidra til å sikre et enhetlig sikkerhetsnivå på tvers av samfunnssektorene, samtidig som det sikrer likebehandling av ansatte i stillinger som krever klarering – uavhengig av hvilken samfunnssektor de arbeider innenfor. At en klarering etter sikkerhetsloven som utgangpunkt ikke er knyttet til en konkret stilling, at utvalget heller ikke foreslår at dette endres, taler også for å regulere personellsikkerhet i en sektorovergripende lov.»

12.3.2 Tilpasninger og strukturelle endringer

Utvalget har fremmet forslag om endringer for å gjøre lovens kapittel om personellsikkerhet mer oversiktlig. Regler om autorisasjon og autorisasjonsansvarliges plikter samles i egne bestemmelser. Tilsvarende er foreslått for klarering og klareringsmyndighetene.

Utvalget foreslår å fjerne opplistingen av relevante forhold klareringsmyndighetene kan legge vekt på ved vurderingen av den enkeltes sikkerhetsmessige skikkethet. Det vises til gjeldende § 21 første ledd bokstav a til l. Utvalget oppfatter opplistingen som for detaljert i en overordnet lov og mener den bør legges på forskriftsnivå. En forskriftsregulering av slike detaljerte opplistinger vil også gjøre regelverket mer dynamisk og lettere å endre ved behov.

Utvalget foreslår at bestemmelsen om bruk av vilkår for klarering skilles ut i en egen bestemmelse i forslagets § 8-9. Det presiseres av utvalget at dette også gir hjemmel for å kunne klarere en person for en konkret stilling. Forslaget begrunnes med (NOU 2016: 19 kapittel 10.6.1, side 214):

> «Muligheten for bruk av stillingsklarering følger i dag av forarbeidene til sikkerhetsloven. Utvalget mener at bruk av vilkår eller stillingsklarering i gitte tilfeller kan være viktige

sårbarhetsreduserende tiltak, som bør brukes aktivt der alternativet vil være å gi avslag på klareringsanmodningen. Forslaget innebærer således ingen materiell endring av rettstilstanden, men en fremheving av muligheten til å kunne gjøre konkrete tilpasninger ut fra den sikkerhetsmessige situasjonen.»

Det foreslås også at plikten som autorisert og klarert personell har til å varsle om forhold av betydning, skilles ut i en egen bestemmelse, jf. forslaget til § 8-11.

12.3.3 Klarering av personer som ikke er norske statsborgere og tilknytning til andre nasjoner

Utvalget har foreslått en endring i gjeldende sikkerhetslov § 22 som regulerer klarering av utenlandske statsborgere. Utvalget viser til at revisjonen av personellsikkerhetsregelverket i 2006 innebar en viss oppmykning av adgangen til å klarere utenlandske statsborgere. Bakgrunnen for endringen var at Norge har opplevd en større demografisk endring siden lovens ikrafttredelse.

Utvalget viser også til at det har vært en stor demografisk utvikling i Norge etter at sikkerhetsloven trådte i kraft. Globalisering av samfunnet medfører blant annet at norske virksomheter i større grad er avhengig av å hente inn nøkkelkompetanse fra andre land. Utvalget påpeker at dette kan bidra til å skape nye sårbarheter. Det vises også til at utenlandsk etterretning mot norske interesser er, og fortsatt vil være, en reell trussel mot grunnleggende nasjonale funksjoner. Utvalget har derfor hatt som målsetting at det legges til rette for å forebygge og eventuelt avdekke utro tjenere.

Det vises videre til at personell med tilgang til sensitiv informasjon eller sensitive områder vil kunne bli satt under press for å misbruke slike tilganger. Det er også her avgjørende at myndighetene kan forsikre seg om at personell som gis slike tilganger har den nødvendige pålitelighet. Utvalget viser til PSTs trusselvurderinger som framhever utenlandske etterretningstjenesters mål om å få tilgang til sensitiv informasjon, for eksempel informasjon som kan belyse muligheten for å sabotere kritisk infrastruktur ved en eventuell framtidig konflikt. Utvalget anser derfor tilknytningen til en annen stat som et selvsagt og nødvendig vurderingsmoment som videreføres i sikkerhetsloven.

Når det gjelder vurderingsmomentet som omhandler den utenlandske statsborgerens tilknytning til Norge, foreslår utvalget en justering. Det vises til at slik gjeldende bestemmelse har blitt forstått og praktisert, har en form for tilknytning til Norge vært et avgjørende kriterium for å kunne innvilge klarering. Utvalget påpeker at i praksis har dette medført at personer ikke har fått klarering, selv om vurderingen for øvrig ikke gir grunn til å betvile vedkommendes sikkerhetsmessige skikkethet. Utvalget mener at dette har vært en utilsiktet konsekvens av bestemmelsen, og foreslår en justering som åpner for å kunne klarere utenlandske statsborgere som ikke har tilknytning til Norge.

12.3.4 Hjemmel for adgangsklarering

Utvalget anbefaler at det i den nye sikkerhetsloven etableres en hjemmel for adgangsklarering. Adgangsklareringen vil gjelde for personell som skal ha tilgang til objekter eller infrastruktur, eller deler av disse, som er av kritisk betydning for grunnleggende nasjonale funksjoner. Det vises til at en rekke sentrale aktører har påpekt behovet for en tverrsektoriell hjemmel for bakgrunnskontroll, utover det som følger av dagens klareringsinstitutt.

Utvalget har sett på muligheten for at det etableres en hjemmel for personkontroll i relevante sektorregelverk. En fordel med en slik tilnærming vil være at personkontrollen kan begrenses til det som er nødvendig i den aktuelle sektoren. Samtidig erkjenner utvalget at det kan være en risiko forbundet med at regelverket praktiseres ulikt i de ulike samfunnssektorene. Det vises til at det vil være sikkerhetsfaglig uheldig dersom enkelte legger opp til et liberalt regime, mens andre sektorer praktiserer en streng personkontroll. Utvalget mener at dette kan føre til en ubalanse mellom samfunnssektorene, som vil kunne øke sårbarheten.

Utvalget påpeker at det foreligger en hjemmel i gjeldende sikkerhetslov for å kunne kreve sikkerhetsklarering for tilgang til skjermingsverdige objekter klassifisert KRITISK eller MEGET KRITISK. Det anbefales at det på samme måte som etter dagens objektsikkerhetsforskrift gis hjemmel til at det enkelte fagdepartement kan kunne fatte vedtak om krav til adgangsklarering for tilgang til nærmere angitte objekter eller infrastruktur, jf. utvalgets forslag til § 7-3 tredje ledd.

Utvalget har vurdert hvor omfattende en slik adgangsklarering bør gjøres. Det framheves at en uttømmende politiattest ikke synes å være tilstrekkelig ut fra et sikkerhetsmessig perspektiv. Samtidig mener utvalget at en like omfattende

prosess som en ordinær sikkerhetsklarering både vil utgjøre et stort inngrep i den enkeltes personvern og være ressurskrevende å administrere. Utvalget legger derfor til grunn at personkontrollen for adgangsklarering skal gjøres mindre omfattende enn for dagens sikkerhetsklareringsregime.

Utvalget viser til at adgangsklarering bør utformes etter de linjer man har i Storbritannia for en såkalt Counter Terrorist Check. Utvalget beskriver en slik personkontroll som mindre omfattende enn en ordinær sikkerhetsklarering, men med en bredere informasjonstilgang enn en uttømmende politiattest.

Utvalget anbefaler at gjennomføring av adgangsklarering legges til de allerede etablerte strukturene for sikkerhetsklarering. Utvalget erkjenner at det vil medføre økt ressursbruk, da antall klareringssaker vil øke. Ettersom det vil være opp til det enkelte fagdepartementet å avgjøre hvorvidt det skal settes krav til adgangsklarering, er det vanskelig å si noe konkret om behovet for økte ressurser.

Utvalget påpeker at forslaget vil innebære personvernulemper for personell i stillinger hvor det settes krav til adgangsklarering. Klareringsinstituttet er i seg selv av inngripende karakter. Utvalget legger derfor til grunn at det enkelte fagdepartement kun setter krav til adgangsklarering der dette er nødvendig og også har en reell sikkerhetsmessig effekt.

Utvalget mener imidlertid at den sikkerhetsmessige gevinsten ved etablering av en generell regel for adgangsklarering veier tyngre enn ulempene dette vil ha kostnadsmessig og for den enkeltes personvern. Utvalget har for øvrig vurdert hvorvidt forslaget kan være i strid med tilbakevirkningsforbudet i Grunnloven § 97, men finner ikke grunnlag for dette.

12.3.5 Mangelfull personhistorikk

Utvalget mener at regelverket på lov- og forskriftsnivå er tilstrekkelig fleksibelt til å kunne gjøre unntak fra kravet til personhistorikk der gode grunner taler for dette. Utvalget viser imidlertid til at praktiseringen av dette unntaket ikke samsvarer med den fleksibiliteten som regelverket muliggjør. Utvalget mener den nye klareringsmyndighetsstrukturen bør gjenspeiles i de ulike rundskrivene vedrørende personellsikkerhet. Utvalget mener også at den nye klareringsmyndighetsstrukturen vil bidra til økt kompetanse hos disse myndighetene og at de da vil være bedre rustet til konkrete og individuelle helhetsvurderinger (NOU 2016: 19 kapittel 10.6.3, side 215).

12.3.6 Digitalisert overføring av registeropplysninger

Utvalget foreslår å lovfeste en plikt for registereiere til å legge til rette for en digitalisert overføring av registeropplysninger til NSM, jf. utvalgets forslag til § 8-7 femte ledd.

Sikkerhetsloven og forskrift om personellsikkerhet regulerer hvilke registre som er relevante ved gjennomføring av personkontroll. På bakgrunn av utvalgets dialog med NSM har utvalget fått forståelse av at samhandlingen med enkelte registereiere er basert på en manuell prosess. Den aktuelle informasjonen som skal overføres fra registereier til NSM er ikke digitalisert, noe som forsinker prosessen vesentlig. Dette er utslagsgivende for saksbehandlingstiden i klareringssakene.

Utvalget påpeker at det er viktig at forholdene legges til rette for at saksbehandlingen i klareringssaker kan gå så raskt som mulig. Utvalget mener en digitalisert overføring av relevante registeropplysninger vil bidra til å effektivisere klareringsregimet.

En forutsetning for en slik løsning er at det etableres sikre kommunikasjonslinjer mellom NSM og de aktuelle registereierne, som tilfredsstiller kravene for digital behandling av slik informasjon. Utvalget erkjenner at forslaget på kort sikt vil innebære økte investeringskostnader knyttet til etableringen av sikre kommunikasjonslinjer mellom NSM og aktuelle registereiere. Samtidig påpekes det at på lengre sikt vil en løsning kreve mindre ressursbruk knyttet til denne type oppgaver hos NSM og registereier.

12.3.7 Fornyet personkontroll

Utvalget foreslår at det tilføres en hjemmel for ytterligere personkontroll utover den personkontroll som gjennomføres ved førstegangsklarering og reklarering. Utvalget mener det er en svakhet ved dagens regelverk at det ikke foreligger en slik hjemmel. Det vises til at dagens system er lite egnet til å kunne fange opp endringer i klarert personells sikkerhetsmessige skikkethet, utover den enkeltes opplysningsplikt overfor autorisasjonsansvarlig. Hensikten med forslaget er å kunne kontrollere om det er skjedd endringer av betydning for vurderingen av sikkerhetsmessig skikkethet. Ny personkontroll vil kunne gjøres på regelmessig basis og ved mistanke om at det kan

ha skjedd endringer som kan ha betydning for den enkeltes klarering.

Utvalget har kommet til at forslaget ikke har vesentlige negative konsekvenser for den enkeltes personvern. Hjemmel for å innhente slike opplysninger i klareringsprosessen eksisterer allerede i dag og er godt begrunnet. Utvalget viser også til at dersom en slik personkontroll innebærer at det fattes en negativ avgjørelse, vil den enkeltes rettssikkerhet bli ivaretatt i klageomgangen.

12.3.8 Utlevering av informasjon til Politiets sikkerhetstjeneste

Utvalget har foreslått en hjemmel for deling av informasjon mellom sikkerhetsmyndigheten og PST. En slik hjemmel vil innebære et inngrep i den enkeltes personvern. I gjeldende lov er det ikke åpning for en slik informasjonsdeling. Dagens lov hjemler at informasjon om den enkelte ikke skal benyttes til andre formål enn å vurdere den enkeltes sikkerhetsmessige skikkethet knyttet til en konkret anmodning om klarering. Samtidig påpeker utvalget at klareringsinstituttet på visse områder er sammenfallende med de straffebud som PST har som formål å forebygge og etterforske. Det vises til at formålet med klareringsinstituttet er å redusere risikoen for at sikkerhetsgradert informasjon kompromitteres på en måte som kan skade grunnleggende nasjonale funksjoner. Utvalget mener at en hjemmel for informasjonsdeling vil bidra til at PSTs forebyggende arbeid blir mer målrettet og gi en sikkerhetsmessig gevinst.

Av personvernhensyn mener utvalget at en slik informasjonsdeling må avgrenses til det som er strengt nødvendig for at PST skal kunne ivareta sine oppgaver etter politiloven. Det foreslås derfor en begrenset hjemmel til å kunne dele informasjon med PST etter politiloven § 17 b og § 17 c nr. 1.

En generell hjemmel for deling av alle opplysninger som framkommer under en personkontroll, vil utgjøre et uforholdsmessig inngrep i personvernet. En viktig rettssikkerhetsgaranti for den enkelte vil være EOS-utvalgets kontroll med EOS-tjenestene. Utvalget legger derfor til grunn at praktiseringen av en slik informasjonsdeling mellom sikkerhetsmyndigheten og PST vil ha et særlig fokus fra EOS-utvalget.

Utvalget har forstått det slik at det er tre typer opplysninger som er relevante for PST. Det gjelder informasjon om vedkommendes identitet og klareringsstatus, vedkommendes tilknytning til andre nasjoner og vedkommendes arbeidssted. Utvalget forutsetter at det uttrykkelig bør framgå av personopplysningsblanketten at nærmere angitt informasjon vil kunne deles med PST.

Utvalget mener at det er mest hensiktsmessig at PST har ett enkelt kontaktpunkt inn mot klareringsinstituttet. NSM vil være dette kontaktpunktet, og en slik lovhjemmel vil forutsette at NSMs sentrale klareringsregister innrettes på en slik måte at nevnte opplysninger enkelt kan hentes ut. Det forutsetter også at de autorisasjonsansvarlige pålegges en plikt til å innrapportere til NSM hvilket personell som har blitt autorisert i den enkelte virksomhet, slik at endring av tjenestested fanges opp. Det finnes ikke noen oversikt over hvor klarert personell arbeider i dag, og utvalget mener at dette er en svakhet ved dagens system. En slik rapportering, uavhengig av PSTs behov, vil etter utvalgets syn styrke personellsikkerheten i Norge gjennom oppfølging av og kontroll med klarert personells skifte av arbeidssted. Forslaget vil ha noen kostnadsmessige konsekvenser i form av behov for økt saksbehandlingskapasitet hos sikkerhetsmyndigheten og de autorisasjonsansvarlige.

12.4 Høringsinstansenes syn

12.4.1 Generelt

NSM stiller spørsmål ved hensiktsmessigheten av at NATOs graderingsbetegnelser listes opp i § 8-1 femte ledd. Etter deres syn bør det være tilstrekkelig at det følger av den innledende tekst at det også kan gis NATO-sikkerhetsklarering. Videre bemerkes at § 8-4 første ledd andre setning ikke hører naturlig hjemme i denne bestemmelsen, og at ordlyden dessuten er betydningsmessig lik det som følger av § 8-5 første ledd.

NSM bemerker til 8-5 tredje ledd at politisk engasjement og annet lovlig samfunnsengasjement kan ha grenseflater mot kriterier som vil være relevant å vektlegge, særlig etter dagens § 21 bokstav c, i, k og l. For å tydeliggjøre dette mener NSM at bestemmelsen bør presiseres til:

> «Politisk engasjement og annet lovlig samfunnsengasjement, herunder medlemskap i, sympati med eller aktivitet for lovlige politiske organisasjoner, skal *i seg selv* ikke ha betydning for vurderingen av en persons sikkerhetsmessige skikkethet».

NSM har videre innspill til § 8-5 fjerde ledd og bestemmelsen i § 8-7 tredje ledd om vektlegging av opplysninger knyttet til nærstående. Etter ord-

lyden er det kun «negative» opplysninger som kan vektlegges. *NSM* mener dette blir for snevert. Det må være mulig å vektlegge enhver relevant opplysning som kan ha betydning for hovedpersonenes sikkerhetsmessige skikkethet. Begrepet «negative opplysninger» må tolkes som opplysninger som kan være negative for klareringsavgjørelsen, ikke nødvendigvis at det hefter noe negativt ved den nærstående. *NSM* foreslår derfor at ordet «negative» i § 8-5 fjerde ledd tas ut av lovteksten for å unngå misforståelser rundt dette.

NSM foreslår videre at det bør framgå av § 8-7 at anmodninger om personkontroll skal framsendes fra klareringsmyndighetene til sikkerhetsmyndigheten. Dette representerer en kodifisering av etablert praksis, og er også konsistent med bestemmelsen i § 8-8 om fornyet personkontroll.

Videre foreslår *NSM* at det bør tas inn en egen hjemmel til å unnta opplysninger om sikkerhetstjenestens metoder i opplistingen av hvilke forhold som kan unntas fra begrunnelse og innsyn. Innsyn i enkelte av de metoder som klareringsmyndighetene benytter for å opplyse en sak vil kunne skade fremtidige muligheter for å opplyse tilsvarende saker på en sannferdig måte. Inngående kjennskap til enkelte metoder kan etter *NSMs* oppfatning medføre at det blir mulig å lage oppskrifter for hvordan man skal kunne manipulere klareringsmyndigheten til å fatte uriktige avgjørelser. På denne bakgrunn foreslår de en ny bokstav e i bestemmelsens andre ledd som angår sikkerhetstjenestens metoder. *NSM* støtter forslaget om at varslingsplikten i forslagets § 8-11 blir tydeliggjort i en egen paragraf, og at autorisasjonsmyndigheten nå gis en plikt til å varsle klareringsmyndigheten dersom forholdet antas å kunne få betydning for vedkommendes klarering.

NSM foreslår at § 8-14 siste ledd bør harmoniseres med dagens praksis hvor innsyn i opptak og referat fra sikkerhetssamtale kun gis ved gjennomsyn hos klareringsmyndigheten. Dette er begrunnet i sikkerhetsmessige forhold, og praksisen ble forutsatt ved innføringen av retten til innsyn, jf. Ot.prp. nr. 59 (2004–2005), merknad til ny § 25 a. *NSM* foreslår på denne bakgrunn at tredje ledd endres til:

> «Den som har krav på innsyn skal på anmodning gis kopi av dokumentet. Innsyn i opptak og referat fra sikkerhetssamtale gis ved gjennomsyn hos klareringsmyndigheten».

Når det gjelder § 8-15, viser *NSM* til at denne bestemmelsen ble innført ved lovendring i 2005, og var ment å styrke rettssikkerheten til den enkelte. Tidligere var det angitt at det var Forsvarsdepartementet som skulle oppnevne en gruppe advokater for dette formålet. Gitt bruken av begrepet «departementet» og dagens ansvarsdeling er det ikke klart om Forsvarsdepartementet fortsatt skal ha denne rollen. *NSM* mener dette bør tydeliggjøres.

Til 8-16 om klage viser *NSM* til at de som klage- og tilsynsmyndighet har erfart at reguleringen av klagesaksbehandlingen, dels i sikkerhetsloven og dels i forvaltningsloven, har skapt betydelig usikkerhet knyttet til saksbehandlingen. NSM har på denne bakgrunn tidligere fremmet forslag om å samle all regulering av klage innenfor personellsikkerhetsområdet i egne bestemmelser under sikkerhetsloven. *NSM* foreslår at henvisningen til forvaltningsloven erstattes av en bestemmelse som gir hjemmel for å gi utfyllende bestemmelser om klage i forskrifter til ny lov om forebyggende nasjonal sikkerhet.

Anders Bakke har i sin høringsuttalelse, om utvalgets forslag til § 8-5, påpekt at fjerningen av opplistingen av relevante forhold i bokstav a til l kan medføre at vurderingskriteriene blir mindre tilgjengelige. Han mener også at omgjøringsreglene i forskrift om personellsikkerhet bør inngå i ny sikkerhetslov. *Anders Bakke* uttaler også at det kan være vanskelig for den autorisasjonsansvarlige å vite hvilke opplysninger som kan være av interesse for klareringsmyndigheten, og at terskelen for varsling bør være lav i utvalgets forslag til § 8-11.

Nasjonalt ID-senter og *Politidirektoratet* har påpekt at verken dagens sikkerhetslov eller utvalgets forslag til ny sikkerhetslov stiller spesifikke krav til identitetskontroll.

BDO har i sitt høringsinnspill om utvalgets forslag til § 8-7 fjerde ledd vist til at private registre ikke er nevnt. Det vises til at gjeldende lov gir hjemmel til å innhente opplysninger fra private kredittopplysningsregistre.

12.4.2 Bruk av vilkår og klarering for stilling

Telenor er positive til at det åpnes opp for stillingsklarering av utenlandske statsborgere som ikke har tilknytning til Norge. De viser til at det i dag er nærmest umulig å få autorisert en person som ikke er norsk statsborger og/eller har vært bosatt i Norge over lengre tid. Telenor uttaler videre:

> «Tilsvarende utredninger (stillingsklarering av utenlandske statsborgere) bør også vurderes

for autorisasjonsprosessen for BEGRENSET, og i tillegg hvordan dette skal håndteres.

Telenor støtter utvalget når de påpeker viktigheten av å sikre en praksis som ivaretar en helhetsvurdering også for norske statsborgere med tilknytning til andre land, slik at man ikke blir for restriktiv og mister verdifull kompetanse grunnet for streng tolkning av loven.»

Utenriksdepartementet deler utvalgets erkjennelse av effekten av globalisering og det flerkulturelle mangfoldet som i dag kjennetegner det norske samfunnet. Departementet uttaler at:

«Departementet støtter videre utvalgets forslag om å åpne opp for stillings- og adgangsklarering i tillegg til dagens nivåklarering, samt understrekingen av at klareringsavgjørelser skal fattes på bakgrunn av en helhetlig konkret vurdering i hvert enkelt tilfelle. Departementet støtter således også forslaget om at oppstillingen av hvilke forhold som kan tillegges betydning i §21 1. ledd a- l i dagens sikkerhetslov ikke videreføres i utkastet til ny lov».

Anders Bakke uttaler i sin høringsuttalelse at bruk av *stillingsklarering* bør være begrenset til i «særskilte tilfeller» da utbredt bruk kan medføre at klareringssystemet blir mindre fleksibelt, men mer tidkrevende.

12.4.3 Utenlandske statsborgere og tilknytning til andre stater

NSM er kritiske til utvalgets justering av bestemmelsen som regulerer klarering av utenlandske statsborgere og uttaler:

«Et grunnleggende prinsipp når det gjelder sikkerhetsklarering er at den som skal klareres må forutsettes å være lojal mot norske sikkerhetsmessige interesser. En slik lojalitet fordrer etter NSMs oppfatning en viss tilknytning til Norge. Etter sikkerhetslovens § 22 gis i dag klarering av utenlandske statsborgere etter en «vurdering av hjemlandets sikkerhetsmessige betydning og vedkommendes tilknytning til hjemlandet og Norge». Forslaget om å endre ordlyden til «..vedkommendes eventuelle tilknytning til Norge» innebærer en vesentlig oppmyking av adgangen til å klarere utenlandske statsborgere uten at de sikkerhetsmessige konsekvenser kan sees utredet i lovforslaget. NSM mener at det allerede i dag ligger til rette for en skjønnsmessig praktisering av gjeldende bestemmelse, og at graden av tilknytning til Norge og betydningen av denne, også etter gjeldende regelverk undergis en individuell og skjønnsmessig vurdering som forutsettes å ivareta både sikkerheten og rettssikkerheten på en god måte. NSM mener derfor at dagens ordlyd på dette punkt bør videreføres.

I den utstrekning det skal være mulig å klarere en person uten noen form for tilknytning til Norge bør dette bare skje unntaksvis, og basert på en dispensasjon gitt av Sikkerhetsmyndigheten. Det bør i så fall etableres en dispensasjonshjemmel med utgangspunkt i en ordlyd videreført fra dagens § 22.»

NSM foreslår også at bestemmelsen om utenlandske statsborgere knyttes direkte til de kravene som gjelder for alle som skal sikkerhetsklareres:

«For å unngå misforståelse knyttet til klarering av personer som ikke er norske statsborgere bør bestemmelsen knyttes tettere til de generelle krav som gjelder for personer i § 8-5. Dette kan gjøres ved å tilføye som siste setningsledd i første ledd andre setning: (...), jf.§ 8-5.

Videre bør ordlyden endres slik at det fremgår at disse kriteriene kommer i tillegg til kriterier som vil følge av og i medhold av § 8-5. Første ledd tredje setning bør derfor lyde: I vurderingen skal det i tillegg legges vekt på […]»

Anders Bakke uttaler:

«Åpningen for å kunne sikkerhetsklarere utenlandske statsborgere som ikke har tilknytning til Norge, bør revurderes. Det må legges til grunn at beviskravet for å finne en person skikket er høyt, og at slik kravet er utformet, bør undersøkelsene ta sikte på å klarlegge lojalitet og tilknytning til Norge, ikke ta dette for gitt. Det utvalget i punkt 10.6.3 omtaler som en utilsiktet konsekvens er ikke nødvendigvis en uønsket konsekvens, men er i tråd med sikkerhetsfaglige vurderinger og det strenge beviskravet».

12.4.4 Adgangsklarering

Departementenes sikkerhets- og serviceorganisasjon, Direktoratet for nødkommunikasjon, Oljedirektoratet, Norges Bank, Norges vassdrags- og energidirektorat (NVE), Forsvarsbygg, Skattedirektoratet, Statens strålevern, Statnett, Fylkesmannen

i Rogaland og *Fylkesmannen i Vestfold* støtter utvalgets forslag om adgangsklarering.

Samferdselsdepartementet viser til at dagens sikkerhetslov gir hjemmel for å kunne kreve sikkerhetsklarering for skjermingsverdige objekter klassifisert KRITISK eller MEGET KRITISK og uttaler:

> «Så vidt SD kan forstå må behovet for mer omfattende personkontroll dermed være avgrenset til tilgang til infrastruktur og objekter klassifisert som VIKTIG.
>
> SD er positive til etableringen av et forenklet klareringsregime som kan benyttes på lavere klassifiserte infrastrukturer og objekter. Vi støtter derfor forslaget i § 7-3 om å ta inn en hjemmel til å kunne kreve adgangsklarering.»

Samferdselsdepartementet er samtidig svært skeptisk til at det i utkast til § 7-3 ikke foreligger hjemmel til å kreve ordinær sikkerhetshetsklarering for MEGET KRITISKE objekter. Det vises til at:

> «Fysisk og logisk tilgang til objekter vil ikke bare kunne utgjøre en fare for sabotasje o.l., men vil også kunne gi personell inngående informasjon om objektets utforming, sårbarheter, mv. Dette er informasjon, som om den er nedfelt i et dokument, normalt er sikkerhetsgradert. SD stiller i lys av dette spørsmål ved det skillet som utvalget synes å trekke mellom tilgang til *informasjon* på den ene siden, og fysisk og logisk tilgang til *objekter* på den andre. Etter SDs vurdering bør spørsmålet om det skal gjennomføres en sikkerhetsklarering eller en enklere adgangsklarering, være knyttet til *skadepotensialet* ved at personell får tilgang – uavhengig av om tilgangen gjelder informasjon eller objekter.»

Samferdselsdepartementet uttaler også at det kan være behov for å adgangsklarere personellgrupper som ikke nødvendigvis skal ha adgang til skjermingsverdige objekter eller infrastruktur. Det vises til personell som har sikkerhetsrelaterte oppgaver i tilknytning til objekter og områder som er særlig utsatte for terrorhandlinger, eksempelvis sentrale knutepunkter innen luftfarten. Samferdselsdepartementet foreslår at det utformes en lovhjemmel for adgangsklarering av kritiske personellgrupper. Omfanget av antall adgangsklareringer vil øke betydelig og Samferdselsdepartementet uttaler at:

> «Ordningen med adgangsklarering vil kunne få et relativt bredt anvendelsesområde, særlig dersom det legges opp til at adgangsklarering skal erstatte ulike typer bakgrunnssjekker som i dag gjennomføres i de ulike sektorene. Dette vil kunne være ressurskrevende for Klareringsmyndigheten. Eksempelvis gjennomfører Luftfartstilsynet årlig over 10 000 bakgrunnssjekker av personell som skal jobbe i luftfarten. SD mener derfor at det er viktig at ordningen med adgangsklarering innrettes på en slik måte at den vil gi bedre sikkerhet enn dagens bakgrunnssjekk, men at den samtidig ikke blir så omfattende at den ikke blir praktisk gjennomførbar, bl.a. med hensyn til saksbehandlingstid.»

Luftfartstilsynet har også påpekt at det er behov for å adgangsklare andre personellgrupper utover de som skal ha tilgang til sikkerhetsgradert informasjon eller adgang til skjermingsverdige objekter og uttaler:

> «Luftfartstilsynet mener at det er behov for etablering av en hjemmel slik at også andre enn personer som skal ha tilgang til sikkerhetsgradert informasjon, eller adgang til klassifiserte områder innenfor kritiske objekter eller kritisk infrastruktur, kommer inn under regelverket for personellsikkerhet.
>
> Innenfor luftfarten er det behov for adgangsklarering også for andre kritiske personellgrupper som ikke direkte kommer inn under sikkerhetslovens bestemmelser, jf. utkastets § 8-1.»

Norsk vann uttaler:

> «Det er ønskelig for vannverkseier i større grad å kunne foreta kontroll av personell en det er mulighet til i dag. Dette gjelder også de vannverkene som ikke er definert som skjermingsverdige. Dagens system med sikkerhetsklarering er for omfattende, mens vandelsattest oppleves som noe enkelt. I NOU 2016:19 foreslås det adgangsklarering som en mellomløsning. Det bes om at denne typen klarering også kan benyttes av vannforsyningssystemer etter nærmere gitte kriterier basert på risiko».

Avinor mener at det vil stille store krav til klareringsmyndighetens kapasitet og uttaler:

> «Svikt i klareringskapasitet vil ha store implikasjoner for lufthavners evne til å opprettholde

samfunnets grunnleggende behov og funksjoner.»

PST støtter forslaget om innføring av adgangskontroll, men peker på:

> «PST støtter derfor forslaget om å innføre en hjemmel for krav om adgangsklarering for tilgang til klassifiserte områder. PST vil i den forbindelse peke på at utformingen av lovforslaget innebærer at adgangsklaringen kun kan kreves for adgang til den delen av et område/bygning som defineres som skjermingsverdig objekt etter forslaget. Dersom dette skal være et nyttig forebyggende verktøy, legger PST til grunn at for eksempel såkalt rød sone på alle norske flyplasser vil defineres som skjermingsverdige.»

NVE støtter forslaget om innføring av adgangskontroll. NVE argumenter samtidig for at virksomheten med adgangsklarert personell ikke nødvendigvis må underlegges sikkerhetsloven:

> «For NVE er det viktig at personklarering kan gjennomføres for medarbeidere i en virksomhet uten at virksomheten i seg selv er underlagt sikkerhetsloven.
>
> For virksomheter som er av vesentlig betydning for nasjonale sikkerhetsinteresser (jf. §2-1 b), vil det være viktig å kunne adgangsklarere eller sikkerhetsklarere personer som skal ha adgang til ulike typer sensitiv informasjon (f.eks. kraftsensitiv informasjon), informasjonssystemer eller objekter/infrastruktur.
>
> Det er også relevant å kunne adgangs- eller sikkerhetsklarere enkeltpersoner uten at virksomheten de er ansatt i er underlagt sikkerhetsloven. Dette er aktuelt dersom f.eks. konsulenter skal utføre arbeid i områder hvor sikkerhetsklarering er nødvendig, eller når enkeltpersoner i en virksomhet skal motta sikkerhetsgradert informasjon som trusselvurderinger, f.eks. i fylkesberedskapsrådet.»

Politidirektoratet støtter ikke forslaget om å innføre en ny kategori klarering og uttaler:

> «Politidirektoratet er av den oppfatning at dette skillet mellom adgangsklarering og sikkerhetsklarering, og da også skillet mellom fysisk adgang og logisk tilgang, er lite problematisert. Vi stiller spørsmål ved om dette skillet vil være hensiktsmessig og forsvarlig. Etter vårt syn kan det være et stort skadepotensiale også knyttet til personell med kun adgang til anlegg og som da etter forslaget kun skal adgangsklareres. Eksempelvis kan slikt personell sette hele funksjonaliteten ved et anlegg/objekt ut av drift. I praksis vil det også være vanskelig å skille ut personell som kun gis adgang til anlegg, uten å gis tilgang til sikkerhetsgradert eller sensitiv informasjon. Fysisk adgang til et anlegg kan i seg selv innebære at det samtidig gis sikkerhetsgradert eller sensitiv informasjon slik at det ikke vil være mulig å skille ut kun den fysiske adgangen. Årsaken er at plassering og sikringstiltak rundt det skjermingsverdige objektet kan være sikkerhetsgradert informasjon. Med logisk adgang til et skjermingsverdig objekt, eksempelvis styringssystem til datarom/ datahall, vil man kunne utsette objektet for større skadepotesial. Personellet vil også kunne ha behov for fysisk adgang til objektet.»

Norges ingeniør- og teknologorganisasjon (NITO) er kritisk til å innføre et slikt system for adgangsklarering og uttaler:

> «Dersom adgangsklarering innføres mener NITO at kravet til klarering ikke må gis tilbakevirkende kraft. En manglende klarering kan få svært alvorlige konsekvenser for ansatte. I verste fall vil den ansatte kunne få oppsigelse som følge av manglende klarering. Det vil være sterkt urimelig å innføre et krav om klarering med tilbakevirkende kraft. Et krav om klarering kan også være i strid med tilbakevirkningsforbudet i Grunnloven § 97.»

12.4.5 Mangelfull personhistorikk

LO/NTL i Utenriksdepartementet uttaler at regelverket praktiseres for strengt og at dette har stor betydning for deres medlemmer:

> «Personellsikkerhet må i større grad enn i dag tilpasses et globalisert og multikulturelt samfunn. Dagens praksis er, slik utvalget også noterer seg, strengere en loven i utgangspunktet stiller krav om. Dette rammer våre medlemmer uforholdsmessig hardt. Praksis er også betydelig strengere enn andre land vi normalt sammenligner oss med, herunder våre allierte i NATO.
>
> Det stilles i dag krav om sporing av ektefeller til ansatte i utenrikstjenesten for nær sagt alle klareringer. Utenlandsopphold som med-

følgende til tjenestemann omfattes ikke i dag av unntaket i sikkerhetsloven for tjeneste i den norske stat. Dette har i de siste åren medført at en rekke medlemmer ikke har blitt re klarert på grunnlag av ektefellens sporingsstatus. Dette er urimelig og streng fortolkning av loven, og synes å være unikt for Norge i forhold til de fleste andre land vi normalt sammenligner oss med. Særlig når det også medfører at det heller ikke gis klarering til K, evt. K med vilkår, på dette grunnlag, til tross for at lovens bokstav kun sier at det kan gjennomføres personkontroll av nærstående ved klarering til hemmelig eller andre særlige tilfeller. Dagens praksis medfører også at det legges store begrensinger på rekrutteringsmulighetene til departementet, i en situasjon hvor det er stadig større behov for internasjonal erfaring fra flere deler av verden.

Utvalget uttaler også at det anbefaler at tilknytning til andre stater videreføres som et moment i sikkerhetsvurderingen. Det er forståelig. NTL UDs erfaring tilsier imidlertid at dagens praksis ikke er slik at det gjøres en individuell vurdering, men snarere at enhver tilknytning til noen stater automatisk medfører klarering med vilkår/nedsatt klarering eller IK, uten at det gjøres en tilstrekkeligvurdering av i hvilken grad dette vil ha betydning i det konkrete tilfellet. Særlig hva gjelder ektefeller med utenlandsk bakgrunn synes praksis å være svært streng, og i liten grad ta hensyn til familiens totale tilknytning. Det er for eksempel i de seneste år flere tilfeller av at reklarering ikke er gitt til personer som har vært gift med ektefelle med utenlandsk bakgrunn (ikke nødvendigvis statsborgerskap) i lengre tid (over ti år). Dette har tidligere ikke hatt betydning for vedkommendes klarering, og innstrammingen skjer altså uten at det er endringer i de ansattes situasjon. Dette er igjen en praksis som er betydelig strengere enn andre land vi normalt sammenligner oss med, og særlig i forhold til land som USA og Canada, som har lengre erfaring som multikulturelle samfunn, og som legger betydelig begrensinger på statens muligheter til å rekruttere riktig kompetanse.

NTL/UD setter pris på at utvalget har notert seg at praksis i forhold til sporing i dag kan være noe strengere en lovens bokstav tilsier, og uttrykker en forventning om at en sentralisert instans vil ha bedre kompetanse til å gjøre en individuell helhetsvurdering. Erfaringen så langt tyder ikke på dette. NSM, den sentrale instansen som burde ha kompetanse til å gjøre dette i dag har etter det vi erfarer lagt seg på en konsekvent streng praksis. Dette står i motsetning til praksis i andre etater som UD og Forsvaret før innstrammingen NSM har foretatt de siste årene, hvor man i større grad var villig til å gjøre en individuell helhetsvurdering basert på den kunnskap man hadde om personen og tjenesten. Dette er kanskje særlig relevant for en institusjon som UD, som i sin natur er internasjonalt anlagt, og har særlige behov. Dersom en sentralisert aktør med en smalt sikkerhetsfokus skal sette føringene, bør det etter NTL UDs oppfatning sikres en bedre kontroll av om praksis følger loven intensjon, enn dagens EOS-utvalg innebærer. Gjentatte saker i de senere år hvor EOS-utvalget har påpekt kritikkverdig behandling av klareringssaker i NSM synes i liten grad å ha medført endring i praksis, og EOS-utvalget påpeker selv i tidligere årsmeldinger at utvalget ikke har sanksjonsmuligheter.

Dagens praksis innebærer også et rettssikkerhetsproblem. Fordi all erfaring tilsier at NSM har en svært streng praksis, synes både arbeidsgivere og arbeidstagerorganisasjoner i stor grad å anbefale de som er utsatt for nedsatt klarering ikke å klage fordi det er stor risiko for en strengere avgjørelse i NSM. Dette, kombinert med svært lite kunnskap og informasjonstilgang om prosessene gjør det svært vanskelig å ta klareringssaker videre. Det synes også å være svært lite tilgjengelig juridisk kompetanse, samtidig som det er svært mangelfull tilgang på informasjon, og lite kunnskap om muligheten til å få juridisk veiledning etter lovens paragraf 8-16 (25b etter gammel lov). Totalt sett utgjør denne mangelen på åpenhet og kunnskap et betydelig rettssikkerhetsproblem som den nye loven i større grad burde bidra til å rette opp i.»

Politidirektoratet uttaler:

«I utredningens punkt 10.6.3 omtales mangelfull personhistorikk. Utvalget viser til at Utenriksdepartementet og Landsorganisasjonen har påpekt at praksisen med at man i rundskrivene har lagt seg på en restriktiv linje for å kunne gjøre unntak fra kravet til 10 års personhistorikk er problematisk.

Politidirektoratet er imidlertid av den oppfatning at 10 års personhistorikk i utgangspunktet ikke er mye, og at det bør være vanskelig å lempe på kravet til slikt informasjonsgrunnlag. Politiet har behov for å ha tillit til at

sikkerhetsklarering av personell gjøres på et tilstrekkelig informasjonsgrunnlag. Dette fordi personell gis tilgang til svært sensitiv Informasjon og/eller objekt, noe som gjør skadepotensial for samfunnet stort. Politidirektoratet viser også til at behovet for sikkerhetsklarering skyldes nasjonale sikkerhetsmessige hensyn. Vi er derfor av den oppfatning at en mindre restriktiv linje for å kunne gjøre unntak fra kravet til 10 års personhistorikk vil innebære en uthuling av regelverket på et sentralt punkt.»

12.4.6 Digitalisert overføring av registeropplysninger

Datatilsynet uttaler:

«Vi støtter utvalgets vurderinger om at det er viktig at saksbehandlingen skal gå så raskt som mulig, og at en digitalisert overføring av relevante registeropplysninger vil kunne bidra til å effektivisere klareringsregimet.

Våre merknader til dette punktet er at når overføringen skal digitaliseres, må de ulike registereierne sørge for at det ikke overføres mer informasjon enn det som er nødvendig. Dersom kravet om digitalisert overføring innebærer at man må utvikle nye system eller løsninger, bør registereierne følge prinsippene om innebygd personvern, som er et krav i det kommende personvernregelverket.

Vi forutsetter at NSM sørger for, og stiller krav til, at overføringer sikres fra ende til ende.»

12.4.7 Fornyet personkontroll

Datatilsynet har uttalt til forslagets § 8-8 at:

«Vi forstår behovet for en slik hjemmel og utvalgets argumenter om at det vil være i tråd med personopplysningslovens krav om at personopplysninger skal være korrekte og oppdaterte.

Vi ser allikevel at det er negative personkonsekvenser ved at NSM til enhver tid kan innhente opplysninger om personer fra de ulike registrene. Vi mener at en regelmessig innhenting gir bedre personvern enn enkeltvis innhenting som er basert på mistanke, da enkeltvis innhenting vil sende signaler til registereiere om at en person er under mistanke.

Vi forutsetter at det gis informasjon til den registrerte når klareringsprosessen initieres.»

Anders Bakke viser til at utvalgets forslag kan påvirke tillitsforholdet mellom den klarerte og klareringsmyndigheten:

«Slik reglen nå er foreslått vil det foreligge en ubetinget rett for klareringsmyndigheten til å foreta nye personkontroller når som helst på allerede sikkerhetsklarert personell. I dag er klareringsmyndighetens behov for å holde seg oppdatert på relevant informasjon om de undersøkte basert på et en tillitsavtale mellom disse to «partene» jf. § 24 første ledd.»

12.4.8 Utlevering av informasjon til Politiets sikkerhetstjeneste

BDO er kritiske til den foreslåtte oversikten over klarert personells arbeidssted og uttaler:

«BDO mener bestemmelsen er altfor vidtgående. Vi støtter forslaget om at Sikkerhetsmyndigheten skal informere PST om klareringsstatus for personer med tilknytning til andre stater. Vi mener imidlertid at det fremstår uproporsjonalt ut i fra samfunnsøkonomiske hensyn, men også unødvendig, at den enkelte virksomhet skal rapportere om hvem de har autorisert. Dersom Sikkerhetsmyndigheten og PST har behov for å vite hvilken arbeidsgiver personene dette gjelder har, antar vi det vil være langt enklere at Sikkerhetsmyndigheten eller PST selv knytter opplysninger fra Arbeidsgiver- og arbeidstakerregisteret (Aa-registeret) opp mot enten klareringsregisteret eller bare opp mot de opplysningene som PST mottar. Aa-registeret er et register med lav sensitivitet, som mange offentlige virksomheter har tilgang til, og bør være uproblematisk at også Sikkerhetsmyndigheten og PST kan benytte. Dersom en rapportering skal skje slik utvalget foreslår, medfører det en samlet sett meget stor arbeidsmengde for virksomheter eller Sikkerhetsmyndigheten. Alle virksomheter med autorisert personell, som i sum antas å utgjør over 100.000 personer, må da antakeligvis enten gis tilgang til å legge opplysninger direkte inn i klareringsregisteret, eller sende dette manuelt til Sikkerhetsmyndigheten som så legger det inn, med de kostnader det medfører. BDO anbefaler derfor at nevnte bestemmelser revurderes, og da spesielt opp imot alternative måter å oppnå samme målsetning på.»

Datatilsynet er positive til forslaget, men viser til at EOS-utvalget må føre kontroll med informasjonsutvekslingen:

> «Forslaget om informasjonstilgang for Politiets sikkerhetstjeneste (PST) innebærer at opplysninger vil bli brukt til andre formål enn det de opprinnelig var innhentet for. Datatilsynet erkjenner at det kan være behov for at sikkerhetsmyndigheten i noen tilfeller bør kunne utlevere opplysninger til PST for at PST kan utføre sine lovpålagte oppgaver. Vi ser det som positivt at lovbestemmelsen selv oppstiller klare og forutsigbare regler om avgrensning av hvilke type opplysninger som kan utleveres (opplysninger om klareringsstatus, tilknytning til andre stater og tjenestested).
>
> Vi har merket oss at det i rapportens punkt 10.6.7 står at «*for å ytterligere styrke forutsigbarheten for den enkelte, mener utvalget at det uttrykkelig bør fremgå av personopplysningsblanketten den enkelte fyller ut som grunnlag for klareringsprosessen, at nærmere angitt informasjon vil kunne deles med PST*». Vi legger til grunn at denne informasjonsplikten forskriftsfestes.
>
> Som det fremgår av spesialmerknadene til den foreslåtte lovbestemmelsen er det PST som skal vurdere hvorfor det er nødvendig å få utlevert informasjon fra sikkerhetsmyndigheten. I noen tilfeller vil ikke PST kunne dele sin begrunnelse med andre, derfor må sikkerhetsmyndigheten legge til grunn at vilkårene for utlevering av informasjon er oppfylt. I ettertid vil begrunnelsen kunne kontrolleres av EOS-utvalget. Det forutsettes derfor at EOS-utvalget gis de nødvendige ressurser for reelt å kunne oppfylle denne oppgaven.»

Forsvarets sikkerhetsavdeling (FSA) er positive til forslaget, men mener at muligheten til å dele informasjon bør utvides ytterligere:

> «FSA kan vise til en rekke eksempler på klareringssaker hvor det er fremkommet opplysninger som grunnet sin alvorlighetsgrad (blant annet vedrørende organisert kriminalitet) vanskelig kunne ha blitt forsvarlig håndtert kun ved at FSA fattet vedtak om tilbakekall i selve klareringssaken. Sakene ville heller åpenbart ikke ha blitt tilfredsstillende løst kun ved at det ble gitt varsel til autorisasjonsansvarlig om å vurdere autorisasjon og øvrige tilganger, jf. bestemmelsens andre punktum.
>
> FSA har savnet en henvisning til at klareringsmyndighetene unntaksvis, og for å oppfylle sitt samfunnsoppdrag, må kunne benytte personkontrollopplysninger til annet enn vurdering av sikkerhetsklarering. Etter vår vurdering er det nødvendig i saker med stort og sektorovergripende nedslagsfelt å kunne ha en sikkerhetsventil for å kunne bidra til effektiv motvirkning av sikkerhetstruende hendelser også utenfor egen organisasjon, jf. formålsbestemmelsen i sikkerhetsloven § 1. Vi legger til grunn at fremkomne opplysninger om alvorlig og/eller organisert kriminalitet må kunne videreformidles til Kripos/PST.
>
> Videre anser vi at fremkomne opplysninger om alvorlig eller organisert kriminalitet samt mulig spionasje/ etterretningsvirksomhet i Forsvarets avdelinger må kunne videreformidles PST og om nødvendig internt i FSAs egen organisasjon. Det legges til grunn at dette er innenfor sikkerhetstjenestens formål.
>
> FSA er kjent med straffeloven § 196, og den plikt som enhver hver har til å hindre de typer lovbrudd som nevnes i bestemmelsen, uten hindring av annen taushetsplikt. FSA mener likevel at forholdet reguleres i sikkerhetsloven. Dette for å synliggjøre at det finnes visse snevre unntak fra taushetsplikten. Videre ansees det viktig da straffeloven ikke nødvendigvis i et hvert tilfelle vil fange opp de behov som gjør seg gjeldende på sikkerhetslovens område.
>
> FSA etterlyser avslutningsvis presisering i lovteksten av hva som menes med sikkerhetsmessig ledelse, også sett i sammenheng med det ovennevnte. FSA konstaterer at det i NOU 2016:19 punkt 10.5.7 er lagt opp til at det kan foretas informasjonsdeling i visse tilfeller. Dette er ment inntatt ved henvisning til eventuell fremtidig forskrift i ny § 2-3 tredje ledd. Sistnevnte bestemmelse gjelder imidlertid etter sin ordlyd ikke personellsikkerhet direkte.
>
> FSA mener adgang til informasjonsdeling som omfatter personkontrollopplysninger bør lovfestes.
>
> FSA foreslår følgende formulering av sikkerhetsloven § 8-7, sjette ledd:
>
> «Opplysninger som er gitt klareringsmyndigheten i forbindelse med personkontroll, skal ikke benyttes til andre formål enn vurdering av sikkerhetsklarering.
>
> Unntak kan allikevel gjøres dersom det fremkommer opplysninger om alvorlig og/ eller organisert kriminalitet, eller etterretningsvirksomhet, jf. § 8-12.
>
> Autorisasjonsansvarlig kan også meddeles slike opplysninger dersom dette anses hen-

siktsmessig av hensyn til den sikkerhetsmessige ledelse og kontroll av vedkommende.»

FSA mener også at § 8-12 bør utvides slik at klareringsmyndigheten kan dele informasjon internt i FSA og med Etterretningstjenesten. Det pekes særlig på Etterretningstjenestens behov for relevant informasjon i tråd med Instruks om etterretningstjenesten § 5 tredje ledd og behovet for å kunne ivareta tjenestens ansvar i krise og krig.

NSM støtter forslaget, men ønsker også å dele informasjon til PST på eget initiativ. Videre har *NSM* et ønske om at PST informerer tilbake til NSM:

«NSM merker seg at forslaget i Sikkerhetsfaglig råd om å legge til rette for målrettet informasjonstilgang med Politiets Sikkerhetstjeneste (PST) er tatt videre av utvalget. NSM antar at det i denne forbindelse også vil være hensiktsmessig at hjemmelsgrunnlaget også omfatter å gi PST informasjon om vedkommendes autorisasjonsstatus som en pekepinn på hvilket potensielt skadeomfang det kan være snakk om.

Bestemmelsen bygger på det utgangspunkt at informasjon gis etter forespørsel fra PST. Innen de rammer som følger av bestemmelsen bør sikkerhetsmyndigheten også kunne gi denne type informasjon av eget tiltak, av hensyn til at slik informasjon raskt kan komme PST i hende.

Sikkerhetsmyndigheten bør imidlertid i saker hvor det deles informasjon i medhold av § 8-12 orienteres i nødvendig grad om de forebyggende tiltak som PST gjennomfører, slik at den daglige sikkerhetsmessige ledelse av vedkommende ikke kommer i konflikt med disse tiltakene. NSM antar at dette kan løses gjennom forskrift til bestemmelsen.

I forlengelsen av denne problematikken vil NSM påpeke viktigheten av det legges til rette for at PST generelt og fortløpende informerer sikkerhetsmyndigheten om alle nye forhold som er relevante for sikkerhetsklarerte personers sikkerhetsmessige skikkethet. Dette bør vurderes i det videre lovarbeidet.

Det er viktig at man i det videre arbeidet tar hensyn til at sikkerhetsmyndigheten og PST har ulike formål med sin virksomhet og at begges formål blir ivaretatt på en god måte.

[…]

NSM støtter forslaget om at virksomheten skal holde sikkerhetsmyndigheten løpende orientert om hvilke personer som er autorisert. Dette vil imidlertid ha ressursmessige konsekvenser knyttet til teknisk tilrettelegging og løpende drift, både for Sikkerhetsmyndigheten og for den enkelte virksomhet. De sikkerhetsmessige gevinstene ved å ha oversikt over hvem som til enhver tid er autorisert antas imidlertid å oppveie de ressursmessige kostnadene. Det bør reguleres på forskriftsnivå hvordan registreringen skal gjennomføres.

[…]

NSM mener videre at det bør gis en klar hjemmel for Sikkerhetsmyndigheten og klareringsmyndighetene til å benytte opplysningene i den grad det er nødvendig for å ivareta ansvar og oppgaver innen personellsikkerhet, herunder tilsyn, utvikling av personellsikkerhetsfaget og -tiltak, informasjon, råd og veiledning, samt informasjon om trusselvurderinger og risikohåndtering.»

Oslo politidistrikt er kritiske til den løpende orienteringen om autorisasjon til sikkerhetsmyndigheten og uttaler:

«Kravet om å holde sikkerhetsmyndigheten orientert om de som til enhver tid er autorisert synes som et ambisiøst krav. Autorisasjon er en aktivitet som medfører kontinuerlige endringer. Løpende innrapportering antas medføre et betydelig merarbeid for sikkerhetsmyndigheten langt utover den effekten ordningen vil kunne ha. Det må forutsettes at sikkerhetsmyndigheten har tilgang til en effektiv søkefunksjon som også må omfatte at samtlige som autoriseres for BEGRENSET må registreres elektronisk av sikkerhetsmyndigheten. Slik oversikt finnes pr i dag kun hos autoriserende myndighet.

Som et tiltak for å sikre bedre etterlevelse av autorisasjonsregimet i den enkelte virksomhet anses det som mer formålstjenlig å pålegge den enkelte virksomhet å foreta rapportering av autoriserte til nærmeste overordnede virksomhet. Som tilsynsmyndighet har sikkerhetsmyndigheten hjemmel til å pålegge virksomheter å oversende gjeldendeautorisasjonsliste for kontroll.

Manglende oppdateringer av autorisasjonsliste til overordnet myndighet vil gi grunnlag for at nærmeste overordnet virksomhet reagerer overfor underlagt virksomhet. En utfordring i dag er manglende oversikt over hvor personellsikkerhetspapirer til en personsom slutter er oppbevart. Her kan det knyttes krav til at om en sikkerhetsklarert person slutter i

en virksomhet skal dette innrapporteres til klareringsmyndigheten. Tilsvarende innrapportering kan skje når personellsikkerhetspapirer overføres til ny arbeidsgiver. Dette vil gi grunnlag for den samme oversikten, basert på en viss risiko da den ikke uten videre omfatter alle personer autorisert for BEGRENSET. Den vil likevel kunne omfatte utenlandske statsborgere autorisert for BEGRENSET, siden godkjenning av om vedkommende skal kunne autoriseres avgjøres av vedkommende virksomhets klareringsmyndighet. Ved autorisasjon for BEGRENSET er det ikke krav om sikkerhetsklarering, men slik autorisasjon skal ikke gis dersom vedkommende er nektet sikkerhetsklarering. Dersom en person blir nektet sikkerhetsklarering og senere skifter arbeidsgiver, er det mulig at ny arbeidsgiver ikke er kjent med forholdet og autoriserer vedkommende. Det bør derfor være krav om at forut for autorisasjon til BEGRENSET skal autoriserende myndighet kontakte klareringsmyndigheten og forsikre seg om at vedkommende kan autoriseres.»

PST støtter forslaget og uttaler:

«Gjennom forslaget § 8-12 gis PST særskilt tilgang til informasjonen fra klareringsmyndighetene.

Dagens økonomi og samfunnsliv er preget av en utstrakt global samhandling. Kompetanse internasjonaliseres og kritisk viktig kunnskap er tidvis kun tilgjengelig på et globalt marked. En naturlig følge av dette er at personer med tilknytning til land som kan representere en etterretningstrussel får arbeid i Norge som kan gi dem tilgang til sikkerhetsgradert informasjon. Det er alltid en fare for at personer som har tilgang til sensitiv informasjon kan bli utsatt for fremmed etterretning. Dersom man også har tilknytning til et annet land enn Norge, vil dette være mer sannsynlig. Det kan derfor være behov for å iverksette tiltak overfor slike personer for å forebygge rekrutteringsforsøk fra fremmed stat.

Det er viktig å understreke at PST ikke er av den oppfatning at disse personene per se utgjør en trussel mot rikets sikkerhet, men at de derimot er i en posisjon som gjør at de selv er utsatt for press fra fremmed etterretning. Skal PST kunne iverksette de nødvendige forebyggende tiltak, må tjenesten ha kunnskap om hvem disse personene er. En annen utfordring er bruk av såkalte illegalister. Illegalister er etterretningsoffiserer som bosetter seg i utlandet med det siktemål å arbeide seg inn i stillinger som krever sikkerhetsklarering i Norge, ofte skifter de identitet. Det er kjent at blant annet russisk etterretning benytter seg av denne metoden. Også på denne bakgrunn er det viktig for PST å ha kunnskap om landtilknytning til personer som skal klareres.

For å avdekke disse truslene er man avhengig av et tett samarbeid mellom NSM og PST, og PST og de andre klareringsmyndighetene. For å gjennomføre dette arbeidet er PST avhengig av kunnskap om både antall, hvem personer med relevant landtilknytning er og hvor de jobber på tidspunktet klarering gis. PST støtter på denne bakgrunn forslaget til § 8-12.»

12.4.9 Sikkerhetssamtale

FSA og *NSM* mener det bør gjøres endringer i forslaget til § 8-5 andre ledd om når en sikkerhetssamtale skal gjennomføres. *NSM* mener:

«[…] det bør vurderes å gjøre endringer i kravet i andre ledd til at sikkerhetssamtale skal gjennomføres i alle saker, med mindre dette anses som «*åpenbart unødvendig*». En sikkerhetssamtale er ressurskrevende å gjennomføre og kan ofte også representere en belastning for vedkommende person. Kravet slik det i dag er formulert gir klareringsmyndigheten lite handlingsrom. Klareringsmyndigheten har en lovfestet plikt til å opplyse saken. Sett hen til dette mener vi at kravet til når sikkerhetssamtale skal gjennomføres kan modereres, slik at klareringsmyndigheten gis en større fleksibilitet i forhold til hvordan man velger å opplyse saken. Økt profesjonalisering gjennom en betydelig reduksjon av antallet klareringsmyndigheter må antas legge til rette for et slikt forslag.»

FSA uttaler følgende:

«FSA forutsetter for sin videre vurdering at sikkerhetssamtale er et verktøy som kan benyttes for å redusere tvil. Denne tolkningen er imidlertid ikke i tråd med forslaget til lovforslagets henvisning til at samtaler skal gjennomføres «der dette ikke anses som åpenbart unødvendig». Formuleringen tilsier bokstavelig tolket at sikkerhetssamtale som hovedregel skal gjennomføres i enhver klareringssak. FSA finner grunn til å understreke at bestemmelsen ikke har vært tolket slik at en klareringssak aldri vil være tilstrekkelig opplyst før sikker-

hetssamtale er gjennomført. Formuleringen av bestemmelsen er imidlertid egnet til å skape tvil også i dette henseende.

FSA viser for øvrig til formålet med klarering, jf. forslagets § 8-5, tredje ledd, som er å foreta en vurdering av pålitelighet, lojalitet og sunn dømmekraft. Denne type vurdering står etter vårt syn i en særstilling sammenliknet med øvrige forvaltningsorganers vurderinger, som gjerne består i å vurdere om en søker oppfyller gitte objektive vilkår.

I det klareringsmyndigheten skal foreta en vurdering av personers egenskaper og derved egnethet for sikkerhetsklarering, anser FSA det som åpenbart at formålet med en sikkerhetssamtale skal være avgrenset til dette. Vi legger derved til grunn at ren informasjonsinnhenting er ment håndtert som ellers i forvaltningen, gjennom dokumentasjon.

FSA gjennomfører et stort antall sikkerhetssamtaler årlig, og finner det klart at sikkerhetssamtalen som sådan for mange fremstår som inngripende og innenfor intimsfæren. Samtalen kan blant annet dreie seg om mulige pressgrunnlag i form av seksuelle forhold (eksempelvis skjult homofil legning), økonomiske misligheter, straffbare handlinger, psykisk historikk, rusmiddelbruk med videre. Mange innkalte har, til tross for at de etter gjennomført samtale synes det har gått greit, gruet seg og vært urolige i forkant.

Å være innkalt kan oppfattes som stigmatiserende, og en del har derfor ikke ønsket å fortelle overordnede eller kolleger at de skal møte til samtale.

Audiovisuelt opptak av samtalene lagres videre i 25 år, jf. dagens bestemmelse i personellsikkerhetsforskriften § 6-8.

FSA viser til at ordlyden i forslaget fastsetter at sikkerhetssamtale er hovedregelen i klareringssaker. På bakgrunn av dette vil det bli avholdt en rekke samtaler som grunnet objektive vilkår uansett ikke vil medføre at klarering blir gitt (eksempelvis med tanke på manglende personhistorikk). En slik praksis fremstår etter vårt syn som betenkelig, og potensielt i strid med lovgivers intensjon etter § 1-1, annet ledd. FSA har forståelse for at de som har vært innkalt til en samtale som primært er gjennomført for å oppfylle lovens krav, uten reell mulighet til å oppnå klarering, vil anse en slik prosess som formålsløs.

FSA har videre merket seg at man i lovutkastet ikke har valgt å konkretisere hvilke forhold som kan tillegges betydning for vurdering av sikkerhetsmessig skikkethet, slik som i nåværende lov § 21, første ledd bokstav a til l. FSA legger til grunn at momentene i bokstav a til l vil bli videreført i forskrift, slik utvalget legger opp til i NOUens punkt 10.6.1.

FSA foreslår følgende ordlyd i sikkerhetsloven § 8-5, annet ledd, siste punktum:

Sikkerhetssamtale kan benyttes i de tilfeller klareringsmyndigheten anser dette som nødvendig for å fjerne tvil om sikkerhetsmessig skikkethet.

I vurderingen av om samtale anses nødvendig skal det særlig ses hen til hvorvidt en samtale vil bidra til å redusere oppstått tvil om omspurtes personlige egenskaper av betydning for utfallet av klareringssaken.»

12.5 Departementets vurdering

12.5.1 Tilpasninger og strukturelle endringer

Departementet foreslår ytterligere strukturelle endringer i kapittelet om personellsikkerhet. Dette kapittelet vil berøre alle personer som klareres og autoriseres. Det er derfor viktig at strukturen på kapittelet har en pedagogisk oppbygning.

Departementet er enig i utvalgets forslag om å samle bestemmelsene om autorisasjon og autorisasjonsansvarliges plikter i egne bestemmelser, og tilsvarende for klarering og klareringsmyndighetenes plikter. Dette vil tydeliggjøre forskjellen mellom klarering og autorisasjon og gjøre kapittelet mer oversiktlig. Departementet foreslår imidlertid å plassere bestemmelsen om autorisasjon lenger bak i kapitlet. Departementet har også foreslått endringer i enkelte av overskriftene for i større grad å tydeliggjøre innholdet i bestemmelsene. Departementet foreslår også språklige forenklinger i en rekke bestemmelser uten at hensikten er å endre innholdet i bestemmelsene.

Departementet har ikke fulgt opp utvalgets forslag om at opplistingen av relevante forhold i gjeldende sikkerhetslov § 21 første ledd bokstav a til l skal reguleres på forskriftsnivå, jf. utvalgets forslag til § 8-5. Departementet mener blant annet at legalitetshensyn taler for at opplistingen står i loven. Personkontroll er et inngripende tiltak mot den enkelte. Departementet mener at de forholdene som kan vektlegges blir lettere tilgjengelig for personer som skal klareres, ved at de framgår av loven og ikke i forskrift.

12.5.2 Utenlandske statsborgere og tilknytning til andre stater

Departementet støtter utvalgets syn om at det er viktig at loven gjenspeiler at Norge i dag er mangfoldig og at globaliseringen av samfunnet medfører at norske virksomheter i økende grad er avhengig av å hente inn nøkkelkompetanse fra utlandet. Samtidig, og i likhet med utvalget, mener departementet at tilknytning til andre stater kan innebære en økt sikkerhetsmessig sårbarhet. Departementet mener derfor at tilknytningen til andre stater, disse statenes sikkerhetsmessige betydning, og tilknytningen til Norge, skal utgjøre hovedmomentene i det helhetlige vurderingsgrunnlaget i forslaget til ny § 8-7.

Utvalgets forslag til presisering av bestemmelsen omhandler utenlandske statsborgere uten tilknytning til Norge, hvor det påpekes at det i praksis forutsettes en viss tilknytning til Norge for at vedkommende skal kunne klareres, jf. utvalgets forslag til § 8-10. Forslaget klargjør at det er mulig å klarere utenlandske statsborgere uten en tilknytning til Norge. *NSM* er kritisk til en slik endring og viser til at det må foreligge en viss tilknytning til Norge som grunnlag for en lojalitet til norske sikkerhetsinteresser. Departementets vurdering tar utgangspunkt i at klarering av utenlandske statsborgere uten tilknytning til Norge ikke i særlig grad omhandler mangfold og integrering. Dette er som følge av den manglende tilknytningen. Departementet finner det heller ikke unaturlig at en klarering av denne personellgruppen i utgangspunktet krever en viss tilknytningsgrad, da vedkommendes lojalitet til norske sikkerhetsinteresser inngår i det sentrale vurderingsgrunnlaget for sikkerhetsklarering. 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.

Departement har for øvrig foreslått å dele opp utvalgets forslag til første ledd i to ledd og gjort språklige endringer. Departementet foreslår å presisere i første ledd andre punktum at vurderingsmomentene hjemlandets sikkerhetsmessige betydning, personens tilknytning til hjemlandet og tiknytningen til Norge, kommer i tillegg til vurderingstemaene etter § 8-4.

Utvalget har foreslått å erstatte «utenlandske statsborgere» med «personer som ikke er norske statsborgere». Departementet påpeker at en slik endring vil innebære at personer med dobbelt statsborgerskap, et utenlandsk og et norsk, ikke lenger kan vurderes etter denne bestemmelsen. Dette mener departementet er uheldig, da vurderingsgrunnlaget i denne type saker sammenfaller med vurderingsgrunnlaget i bestemmelsen. Departementet foreslår derfor ordlyden *personer med utenlandsk statsborgerskap*.

12.5.3 Adgangsklarering

Departementet støtter utvalgets forslag til hjemmel for adgangsklarering, jf. utvalgets forslag til § 7-3 tredje ledd, men foreslår at bestemmelsen tas inn som en ny bestemmelse i forslaget til § 8-3. Gjeldende sikkerhetslov gir hjemmel for å kunne kreve sikkerhetsklarering for adgang til skjermingsverdige objekter klassifisert KRITISK eller MEGET KRITISK. Samtidig er vurderingsgrunnlaget for sikkerhetsklarering i gjeldende lov relatert til behandling av sikkerhetsgradert informasjon. Departementet finner det derfor naturlig at klarering som omhandler tilgang til skjermingsverdige objekter og infrastruktur tydeliggjøres i loven på samme måte som klarering for tilgang til sikkerhetsgradert informasjon.

Forslaget fra utvalget innebærer at det enkelte sektordepartement kan treffe enkeltvedtak om krav til adgangsklarering for tilgang til hele eller deler av skjermingsverdige objekter eller infrastruktur innen sitt myndighetsområde. Adgangsklarering i ny sikkerhetslov vil gi hjemmel for personkontroll i større omfang enn etter dagens regelverk. Samtidig vil anvendelsen av adgangsklarering avgrenses til klassifiserte objekter og infrastruktur etter sikkerhetsloven. En slik avgrensing vil naturlig nok ikke tilfredsstille de virksomheter som har fremmet et behov for en tverrsektoriell bakgrunnskontroll, men som faller utenfor sikkerhetslovens virkeområde.

Departementet legger til grunn at bruksområdet for adgangsklarering omfatter skjermingsverdige objekter og infrastruktur klassifisert som MEGET KRITISK, KRITISK eller VIKTIG. Utvidelsen i ny lov for *når* man kan kreve klarering etter sikkerhetsloven, omhandler derfor klassifiseringsgraden VIKTIG, samt infrastruktur for alle klassifiseringsgradene.

Departementet har vurdert hvor omfattende adgangsklarering skal være. Utvalget har påpekt

at uttømmende politiattest ikke synes å være tilstrekkelig ut fra et sikkerhetsmessig perspektiv. Samtidig har utvalget lagt til grunn at personkontrollen skal gjøres mindre omfattende enn for ordinær sikkerhetsklarering. Departementet viser til kravet til forholdsmessighet ved utøvelse av forebyggende sikkerhetsarbeid, som det overordnede og styrende prinsipp for omfanget av personkontroll ved adgangsklarering. Departementet legger likevel til grunn at personkontroll for adgang til de lavest klassifiserte objektene og infrastrukturene er mindre omfattende enn ved ordinær sikkerhetsklarering. Samferdselsdepartementet har i sitt høringsinnspill uttrykt skepsis til at forslaget innebærer at det ikke kan kreves ordinær sikkerhetsklarering for objekter klassifisert MEGET KRITISK. Departementet viser til at personkontroll for adgangsklarering for høyt klassifiserte objekter og infrastruktur kan ha et større omfang, eller være tilnærmet lik ordinær sikkerhetsklarering. Regulering av omfang av personkontroll og vurderingsgrunnlag ved adgangsklarering legges på forskriftsnivå.

Forslaget innebærer at adgangsklarering legges til de allerede etablerte strukturene for sikkerhetsklarering. Utvidelsen av bruksområdet til adgangsklarering kan medføre økt ressursbruk, men det er vanskelig å si noe konkret om omfanget. I militær sektor er det i dag normalt krav til sikkerhetsklarering for de fleste stillinger. Her kan man anta at adgangsklarering kan erstatte en del av de ordinære sikkerhetsklareringene. I sivil sektor kan utvidelsen til objekt og infrastruktur klassifisert VIKTIG bety en relativt stor økning i antall klareringssaker. Departementet ser det derfor som viktig at det enkelte fagdepartement kun setter krav til adgangsklarering der dette har en reell sikkerhetsmessig effekt. Forslaget vil innebære personvernulemper for personell i stillinger hvor det settes krav til klarering. Klareringsinstituttet er i seg selv av inngripende karakter, og departementet viser til at en adgangsklarering, i likhet med sikkerhetsklarering, ikke skal foretas der dette ikke anses som et egnet virkemiddel. Andre sikringstiltak skal iverksettes først, dersom de kan kompensere for bruk av adgangsklarering. Nærmere krav til dokumentasjon og begrunnelse ved anmodning om adgangsklarering vil, som ved sikkerhetsklarering, gis i forskrift.

Departementet mener at et eventuelt behov for en tverrsektoriell hjemmel for bakgrunnskontroll utenfor sikkerhetslovens virkeområde, bør utredes som et eget regelverk utenfor sikkerhetslovens ramme.

12.5.4 Bruk av vilkår og klarering for stilling

Departementet støtter utvalgets forslag om å videreføre gjeldende sikkerhetslov § 21 siste ledd om å kunne sette vilkår for sikkerhetsklarering, og at det i denne bestemmelsen presiseres at det også gir hjemmel for å kunne klarere en person for en konkret stilling, jf. utvalgets forslag til § 8-9. En sikkerhetsklarering for en konkret stilling kan eksempelvis benyttes ved klarering av utenlandske statsborgere, eller i saker hvor personen har tilknytning til stater som kan utgjøre en etterretningsmessig trussel. Sikkerhetsklarering for en konkret stilling avgrenser bruksområdet for klareringen og kan derfor være risikoreduserende. I Norge er klareringsinstituttet tuftet på at en sikkerhetsklarering gjelder for et konkret nivå, og klareringen skal normalt legges til grunn for alle stillinger med samme klareringsnivå. Det betyr i praksis at selv om en person kan klareres for en konkret stilling, er det ikke nødvendigvis slik at vedkommende kan klareres for det aktuelle nivået. Ved bruk av stillingsklarering utvides derfor mulighetsrommet for klareringsmyndighetene til å innvilge en sikkerhetsklarering. Departementet foreslår å videreføre utvalgets bestemmelse i forslaget til § 8-6. Det foreslås enkelte språklige endringer for å forenkle bestemmelsen. Stillingsklarering er et eksempel på vilkår som kan brukes. Departementet mener derfor det ikke er naturlig at stillingsklaringen nevnes eksplisitt i overskriften til bestemmelsen.

12.5.5 Mangelfull personhistorikk

En avgjørelse om klarering skal baseres på en helhetsvurdering av om personen kan anses å være sikkerhetsmessig skikket. Departementet støtter utvalgets vurdering i NOU 2016: 19 kapittel 10.6.3 om at gjeldende regelverk på lov- og forskriftsnivå er tilstrekkelig fleksibelt får å kunne gjøre unntak fra kravet til personhistorikk dersom det er nødvendig. Det er åpenbare grunner til at en klareringsavgjørelse må baseres på sikkerhetsmessig relevant informasjon om de personer som inngår i personkontrollen. Det bør samtidig tas høyde for at det i noen tilfeller vil være utfordrende å innhente denne type informasjon i den tidsperioden som normalt vil være aktuell. I dag reguleres dette i forskrift om personellsikkerhet.

12.5.6 Egen hjemmel for varslingsplikt

Departementet støtter utvalgets forslag til § 8-11 om at varslingsplikten for klarert og autorisert

personell tydeliggjøres med en egen hjemmel. Bestemmelsen videreføres i forslaget til ny § 8-11. Andre ledd i utvalgets forslag som framhever autorisasjonsansvarliges plikt til å orientere klareringsmyndigheten hvis forholdet anses å kunne ha betydning for vedkommendes sikkerhetsklarering, er tatt ut. Det vises til at varslingsplikten til autorisasjonsansvarlig overfor klareringsmyndigheten er ivaretatt i forslaget til § 8-10 første ledd andre punktum.

Departementet foreslår en presisering i overskriften av hva varslingsplikten gjelder. I tillegg foreslås enkelte språklige endringer for å forenkle bestemmelsen.

12.5.7 Digitalisert overføring av registeropplysninger

Departementet støtter utvalgets forslag om å lovfeste en plikt for registereiere til å legge til rette for en digitalisert overføring av registeropplysninger til sikkerhetsmyndigheten, jf. utvalgets forslag til § 8-7 femte ledd. Departementet anser dette som en naturlig løsning for å kunne effektivisere og redusere saksbehandlingstiden i klareringssakene. Departementet forutsetter at kommunikasjonslinjene vil være tilstrekkelig sikret og at alle krav til personvern er ivaretatt. Et absolutt krav om digital overføring kan først gjelde fra det tidspunktet de nødvendige systemer er på plass.

Departementet foreslår at utvalgets bestemmelse tas inn i forslaget til § 8-5 niende ledd.

12.5.8 Fornyet personkontroll

Departement støtter utvalgets forslag i § 8-8 om å innføre et tydeligere hjemmelsgrunnlag for å kunne iverksette ny personkontroll opp mot relevante registre når som helst innenfor en klarerings gyldighetstid. Det foreligger i dag ingen hjemmel for klareringsmyndigheten til å foreta regelmessig kontroll av relevante registre i den hensikt å avdekke hvorvidt det har skjedd endringer av betydning for den enkeltes sikkerhetsmessige skikkethet i klareringsperioden.

Det foretas i dag fornyet personkontroll bare når en person skal reklareres og når det er behov for å avklare tvil om en person er sikkerhetsmessig skikket. Forslaget om fornyet personkontroll åpner for at klareringsmyndigheten kan iverksette personkontroll uten at det er reist tvil om en person er sikkerhetsmessig skikket. Departementet viser til at Datatilsynet mener at en regelmessig innhenting gir bedre personvern enn enkeltvis innhenting som er basert på mistanke, da enkeltvis innhenting vil sende signaler til registereiere om at en person er under mistanke. Departementet understreker at en hjemmel til kontroll ikke innebærer en plikt for klareringsmyndigheten til å føre regelmessig kontroll og foreta fornyet personkontroll med alle som har klarering i klareringens gyldighetstid.

Departementet mener det er et behov for et klart hjemmelsgrunnlag, og foreslår at utvalgets bestemmelse tas inn som ny § 8-5 tredje ledd, men med språklige forenklinger.

12.5.9 Utlevering av informasjon til Politiets sikkerhetstjeneste og konsekvenser for autorisasjonsansvarliges plikter

Departementet støtter utvalgets forslag om en hjemmel for informasjonsdeling mellom sikkerhetsmyndigheten og PST, jf. utvalgets lovforslag § 8-12. Departementet er enig med utvalget i at informasjonsdelingen avgrenses til opplysninger om en persons klareringsstatus, tilknytningen til andre stater og tjenestested. Departementet legger til grunn at EOS-utvalget fører kontroll med praktiseringen av informasjonsutvekslingen. Videre at det framgår av personopplysningsblanketten at nærmere angitt informasjon vil kunne deles med PST.

Flere av høringsinstansene har fremmet et ønske om at deling av opplysninger knyttet til klareringssaker bør muliggjøres utover det som utvalget har foreslått. *NSM* har foreslått en hjemmel for at opplysningene kan benyttes av sikkerhetsmyndigheten og klareringsmyndighetene i den grad det er nødvendig for å ivareta ansvar og oppgaver innen personellsikkerhet. *Forsvarets sikkerhetsavdeling* har foreslått at bestemmelsen utvides i den grad at opplysningene kan deles internt i avdelingen, og med Etterretningstjenesten. Departementet mener imidlertid at det er viktig av personvernmessige hensyn at informasjonsdelingen avgrenses så strengt som mulig og finner det ikke riktig å utvide informasjonsdelingen ytterligere.

Oslo politidistrikt og *BDO* har i sine høringsinnspill pekt på utfordringer ved at virksomheten skal holde sikkerhetsmyndigheten løpende orientert om autorisert personell. *NSM* viser til at dette vil ha ressursmessige konsekvenser knyttet til teknisk tilrettelegging og drift. Dette gjelder både for sikkerhetsmyndigheten og den enkelte virksomhet. Departementet erkjenner at dette vil være utfordrende både for virksomhetene og sikkerhetsmyndigheten, da det i

dag ikke finnes et effektivt system for en slik rapportering.

Departementet støtter samtidig utvalgets vurdering om at et slikt system bør utvikles slik at sikkerhetsmyndigheten har en oppdatert oversikt over hvor klarert personell til enhver tid tjenestegjør. Sett hen til at det er både tekniske og administrative utfordringer både hos sikkerhetsmyndighet og virksomhetene, bør en plikt for virksomhetene til å holde sikkerhetsmyndigheten løpende orientert, ikke inntre før problemstillingene er nærmere utredet. Departementet foreslår derfor å endre bestemmelsen fra en plikt for virksomheten til at sikkerhetsmyndigheten kan kreve at virksomheten avgir slike opplysninger. Ileggelse av slik plikt vil være særlig aktuelt der særlige omstendigheter ved trusselsituasjonen tilsier det. Videre mener departementet at en slik plikt bør ilegges for virksomheter der dette kan gjennomføres innenfor gjeldende rammevilkår.

En oppdatert oversikt over autoriserte personer og deres tjenestested er en forutsetning for at PST skal kunne stole på at de får korrekt informasjon, slik utvalgets forslag til § 8-12 første ledd bokstav c er utformet. Så lenge virksomhetene ikke har en plikt til å holde sikkerhetsmyndigheten løpende oppdatert, kan heller ikke PST gis en uforbeholden rett til å få utlevert denne informasjonen fra sikkerhetsmyndigheten. Både virksomheter og sikkerhetsmyndigheter bør derfor tilstrebe å oppdatere en liste over autorisert personell, innenfor de til enhver tid gjeldende rammer. PST skal få informasjon om tjenestested der denne er tilgjengelig, men bør samtidig få opplysninger om i hvilken grad opplysningene er oppdatert. I denne sammenheng mener departementet at PST i det minste må kunne få opplyst om hvilken myndighet som har anmodet om sikkerhetsklarering. Departementet foreslår derfor at omtalen av *tjenestested* i § 8-12 første ledd endres til *tjenestested eller hvilken virksomhet som har anmodet om klarering*. Departementet foreslår enkelte språklige forenklinger i bestemmelsens ordlyd. Departement foreslår å videreføre utvalgets forslag til § 8-2 fjerde ledd i forslaget til § 8-9 tredje ledd, med de endringene som framgår ovenfor.

12.5.10 Sikkerhetssamtale

Departementet viser til at plikten til å gjennomføre en sikkerhetssamtale ble forsterket ved lovendringen i 2006. Ordlyden ble endret fra «søke og avklare uklare forhold, eventuelt gjennom å avholde en sikkerhetssamtale» til «skal sikkerhetssamtale gjennomføres der dette ikke anses som åpenbart unødvendig». Utvalget viser til at den forsterkede plikten til å avholde sikkerhetssamtaler i forarbeidene ble begrunnet med en harmonisering med forvaltningsorganers utredningsog informasjonsplikt i medhold av forvaltningsloven § 17, og innebærer at klareringsmyndigheten bør gjennomføre en slik samtale dersom det er tvil om vedkommende skal gis klarering. Departementet støtter en slik begrunnelse av sikkerhetssamtalens funksjon og foreslår å endre ordlyden slik at den i størst mulig grad tydeliggjør dette. Departementet understreker at en sikkerhetssamtale skal avholdes i klareringssaker der det er tvil om personen er sikkerhetsmessig skikket. Det er kun i de tilfeller hvor det er åpenbart at en slik samtale ikke vil kunne endre avgjørelsen, at klareringsmyndigheten kan unnlate å gjennomføre en sikkerhetssamtale.

Departementet foreslår å ta inn bestemmelsen om når det skal gjennomføres en sikkerhetssamtale i § 8-4 tredje ledd andre punktum.

13 Sikkerhetsgraderte anskaffelser

13.1 Gjeldende rett

Gjeldende bestemmelser om sikkerhetsgraderte anskaffelser står i sikkerhetsloven kapittel 7, §§ 27 til 29 a. En sikkerhetsgradert anskaffelse er definert som en «anskaffelse, foretatt av anskaffelsesmyndighet som innebærer at leverandøren av varen eller tjenesten vil kunne få tilgang til skjermingsverdig informasjon eller objekt, eller som innebærer at anskaffelsen må sikkerhetsgraderes av andre årsaker», jf. gjeldende sikkerhetslov § 3 første ledd nr. 17. Leverandører i forbindelse med sikkerhetsgraderte anskaffelser blir automatisk underlagt sikkerhetslovens bestemmelser, jf. sikkerhetsloven § 2 andre ledd, noe som medfører at et større antall private rettssubjekter er underlagt sikkerhetslovens bestemmelser.

Gjeldende § 27 oppstiller krav om at det skal inngås en sikkerhetsavtale mellom anskaffelsesmyndigheten og leverandøren før leverandøren får tilgang til skjermingsverdig informasjon. Dersom det skal gis tilgang til skjermingsverdig objekt praktiseres det i dag bare krav om sikkerhetsavtale dersom Nasjonal sikkerhetsmyndighet (NSM) krever det, eller det av andre grunner er nødvendig å sikkerhetsgradere anskaffelsen.

Skal det inngås en sikkerhetsavtale med en utenlandsk leverandør, kan det først skje etter godkjenning fra NSM, jf. § 27 første ledd tredje punktum. Det kreves at det foreligger en bi- eller multilateral avtale eller annen type arrangement om utveksling og plikt til gjensidig beskyttelse av sikkerhetsgradert informasjon mellom norske myndigheter og hjemstaten til leverandøren, jf. forskrift 1. juli 2001 nr. 753 (forskrift om sikkerhetsgraderte anskaffelser), kapittel 4. De nærmere kravene til innholdet i en sikkerhetsavtale framgår av § 27 andre ledd, og av forskrift om sikkerhetsgraderte anskaffelser § 2-5.

Gjeldende § 28 oppstiller krav om at en leverandør skal leverandørklareres dersom denne skal gis tilgang til informasjon gradert KONFIDENSIELT eller høyere, eller dersom det av andre grunner anses nødvendig. En leverandørklarering innebærer at det foretas en vurdering av leverandørens sikkerhetsmessige skikkethet og evne til forsvarlig håndtering av skjermingsverdig informasjon. Leverandørklarering skal kun gis dersom det ikke foreligger rimelig tvil om at leverandøren er sikkerhetsmessig skikket. For at en utenlandsk leverandør skal kunne leverandørklareres må det foreligge en bi- eller multilateral avtale om utveksling og plikt til gjensidige beskyttelse av sikkerhetsgradert informasjon mellom norske myndigheter og hjemstaten til leverandøren. I dag er det NSM som er klareringsmyndighet for leverandørklareringer.

En leverandørklarering gjaldt tidligere kun for det enkelte oppdrag, og falt automatisk bort når oppdraget var utført. 1. januar 2017 ble bestemmelsen endret slik at den nå gir Kongen myndighet til å bestemme varigheten av leverandørklareringen, se gjeldende sikkerhetslov § 28 første ledd andre punktum. Det følger av forskrift om sikkerhetsgraderte anskaffelser § 3-1 fjerde ledd at leverandørklareringen har en varighet på inntil fem år. Bakgrunnen for endringen var å bringe praksis i Norge nærmere praksis i sammenlignbare land, gjøre prosessen med leverandørklarering enklere og redusere antall søknader om leverandørklarering, jf. Prop. 97 L (2015–2016) kapittel 10.5.

§ 28 tredje ledd oppstiller en plikt for leverandøren til uten ugrunnet opphold å orientere NSM om alle relevante opplysninger av betydning for klareringsspørsmålet. De nærmere kriteriene og krav til egenopplysninger fra leverandøren er nærmere regulert i forskrift om sikkerhetsgraderte anskaffelser §§ 3-2 og 3-3.

Etter at leverandørklarering er gitt skal NSM blant annet informeres om endringer i styre eller ledelse, forandringer i eierstrukturen, flytting av lokaliteter og utstyr, åpning av gjeldsforhandlinger eller begjæring om konkurs, og om andre forhold som kan ha betydning for leverandørens sikkerhetsmessige skikkethet. Dersom forholdene representerer en sikkerhetsrisiko som ikke kan elimineres gjennom forebyggende sikkerhetstiltak, kan NSM inndra leverandørklareringen, jf. § 28 fjerde ledd. Det følger også av § 28 fjerde ledd siste punktum, at skjermingsverdig informasjon eller objekt ikke kan overføres til ny eier eller inngå i bobehandling ved gjeldsforhandling eller

konkurs, med mindre NSM samtykker til dette. Saksbehandlingsreglene i sikkerhetsloven kapittel 6 om personellsikkerhet, herunder bestemmelsen om begrunnelse og klage, gjelder så langt de passer for leverandørklareringer, jf. § 28 femte ledd.

1. januar 2017 trådte ny § 29 a i kraft. Bakgrunnen for bestemmelsen er redegjort for i Prop. 97 L (2015–2016), kapittel 11. I korte trekk oppstiller § 29 a en varslingsplikt ved alle anskaffelser til kritisk infrastruktur, uavhengig av om virksomheten som foretar anskaffelsen er underlagt sikkerhetsloven. Kritisk infrastruktur er i sikkerhetsloven § 3 første ledd nr. 21 definert som «anlegg og systemer som er nødvendige for å opprettholde samfunnets grunnleggende behov og funksjoner». Dersom anskaffelsen «innebærer en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført mot eller ved bruk av infrastrukturen», skal overordnet departement varsles. Dersom virksomheten ikke er underlagt noe departement skal varselet sendes til Forsvarsdepartementet. Det departementet som mottar varsel etter andre ledd, bør innhente en rådgivende uttalelse fra relevante organer om leveransens risikopotensial, og leverandørens sikkerhetsmessige pålitelighet. I Prop. 97 L (2015–2016), side 65 nevnes Politiets sikkerhetstjeneste, Etterretningstjenesten og NSM som aktuelle organer. Dersom anskaffelsen ikke bør gjennomføres, eller det bør stilles nærmere vilkår for gjennomførelsen, skal saken fremmes for Kongen i statsråd. I proposisjonen presiseres det også at vedtaket må være innrettet på en slik måte at lovens formål ivaretas. Det presiseres at formålsbegrensningen blant annet vil innebære at det ikke er hjemmel for å gripe inn ved risiko for industrispionasje som kun er egnet til å skade en enkeltbedrifts forretningsvirksomhet. Det vises for øvrig til utvalgets gjennomgang av gjeldende rett i NOU 2016: 19 kapittel 11.1 til 11.3.

13.2 Utvalgets forslag

Utvalget har vurdert hvorvidt det eksisterende regelverket om sikkerhetsgraderte anskaffelser har en balansert og hensiktsmessig tilnærming når det gjelder sikkerhetshensyn på den ene siden og bedriftsøkonomiske hensyn på den andre. Utvalget har også tatt stilling til hvorvidt innretningen på forslaget til ny lov, herunder utvidelsen av lovens virkeområde, nødvendiggjør endringer i regelverket om sikkerhetsgraderte anskaffelser.

Utvalget har i kapittel 11.3, side 223–224 gjennomgått gjeldende sikkerhetslov, anskaffelsesloven, forskrift om offentlige anskaffelser, forskrift om forsvars- og sikkerhetsanskaffelser, energiloven, beredskapsforskriften og finanstilsynsloven. Utvalget har også gjennomgått vurderingene om tidsbasert leverandørklarering, og varslingsplikt ved anskaffelser til kritisk infrastruktur i Prop. 97 L (2015–2016).

Utvalget kom til at *«det fortsatt er behov for regelverk for sikkerhetsgraderte anskaffelser.»* Det vises i NOU 2016: 19 kapittel 11.4, side 224 til at regelverket er et:

> «viktig virkemiddel for å kunne sikre at leverandører til virksomheter av kritisk betydning for *grunnleggende nasjonale funksjoner*, sikkerhetsmessig er til å stole på. Regelverket for sikkerhetsgraderte anskaffelser bør således gjelde for alle virksomheter som omfattes av loven.»

Utvalget foreslår å videreføre reguleringen som framgår av dagens §§ 27 og 28, for alle virksomheter som omfattes av loven.

Utvalget støtter videre endringen fra oppdragsbasert til tidsbasert leverandørklarering:

> «Endringen vil, slik utvalget ser det, være et viktig bidrag for å effektivisere prosessene knyttet til sikkerhetsgraderte anskaffelser. Endringer medfører også at regelverket er mer i tråd med hvordan dette er regulert i andre sammenlignbare nasjoner. For norske leverandører vil tidsbasert leverandørklarering også gjøre det lettere å konkurrere om oppdrag på det internasjonale markedet.»

Når det gjelder § 29 a om anskaffelser til kritisk infrastruktur uttaler utvalget:

> «Innretning med at virksomhetene plikter å gjennomføre en risikovurdering ved anskaffelser er, slik utvalget ser det, også i tråd med den innretning utvalget har på forslaget til ny sikkerhetslov. De øvrige endringene utvalget foreslår, særlig når det gjelder de foreslåtte mekanismene om deling av trusselinformasjon, også setter virksomhetene i bedre stand til å kunne gjøre en forsvarlig risikovurdering ved slike anskaffelser.»

Utvalget uttaler imidlertid at

> «plikten til å gjøre risikovurderinger, må avgrenses til de virksomheter som faktisk omfattes av loven, det vil si de virksomheter som råder over skjermingsverdige objekter eller skjermingsverdig infrastruktur.»

Sistnevnte medfører en endring fra gjeldende § 29 a, som gjelder alle anskaffelser til kritisk infrastruktur. Endringen må imidlertid ses i sammenheng med at virkeområdet til loven utvides, jf. kapittel 1. Om dette uttaler utvalget på side 224:

> «Utvalgets forslag til utvidelse av lovens virkeområde, vil medføre at virksomheter som råder over infrastruktur av kritisk betydning for grunnleggende nasjonale funksjoner vil bli underlagt loven. Hvorvidt dette innebærer at alle virksomheter som er ment å omfattes av den foreslåtte § 29 a, også omfattes av bestemmelsen i utvalgets lovforslag, vil avhenge av hvilke vurderinger departementene og Sikkerhetsmyndigheten gjør når det gjelder vedtak overfor virksomheter som skal underlegges loven.»

Om forholdet til anskaffelsesregelverket viser utvalget på side 224 til departementets uttalelse i Prop. 97 L (2015–2016), side 48 hvor det framgår at

> «for offentlige oppdragsgivere må regelverket om sikkerhetsgraderte anskaffelser ses i sammenheng med regelverket for offentlige anskaffelser. En sikkerhetsgradert anskaffelse er i utgangspunktet omfattet av anskaffelsesloven og forskrift om forsvars- og sikkerhetsanskaffelser. Nevnte lov og forskrift gjelder i midlertid ikke der en anskaffelse kan unntas med hjemmel i EØS-avtalen artikkel 123.»

13.3 Høringsinstansenes syn

Avinor, BDO, Forsvars- og sikkerhetsindustriens forening (FSi), Nasjonal sikkerhetsmyndighet (NSM), Norges Ingeniør- og Teknologorganisasjon (NITO), Norges vassdrags- og energidirektorat (NVE), Norsk olje og gass, Olje- og energidepartementet, Oslo politidistrikt, Samferdselsdepartementet, Statnett, Telenor Norge AS, Utenriksdepartementet og Energi Norge har kommentert utvalgets forslag til regelverk for sikkerhetsgraderte anskaffelser. De aller fleste er positive til forslaget. *Statnett* og *Energi Norge* mener imidlertid at behovet for sikkerhet i forbindelse med anskaffelser til kraftsektoren best reguleres gjennom sektorspesifikt regelverk.

Norsk olje og gass har spilt inn at utvalgets forslag til kapittel 9 bør

> «avgrenses mot privat virksomhet som ikke er omfattet av forskrift om forsvars- og sikkehetsanskaffelser. Alternativt må det gjøres en grundig kost-nytte vurdering av hvilken virkning dette forslaget vil kunne få for privat virksomhet.»

Energi Norge, NVE, Statnett og *Olje- og energidepartementet* er opptatt av at kravene i regelverket ikke må medføre en dårligere anskaffelse, og det må heller ikke legge unødvendige hindringer for konkurransen. *Olje- og energidepartementet* viser til viktigheten av å

> «vektlegge hensynet til funksjonalitet og kvalitet ved det som anskaffes. Kravet om sikkerhetsgradering av anskaffelsen, herunder inngåelse av sikkerhetsavtaler, må ikke medføre en dårligere anskaffelse».

Olje- og energidepartementet viser videre til:

> «I mange bransjer er det nødvendig å kunne bruke også utenlandske leverandører eller underleverandører. Det er også viktig at det ikke legges unødvendige hindringer for konkurranse.»

Statnett viser til at mange av deres anlegg vil kunne bli underlagt regimet om skjermingsverdige objekter, jf. forslaget til § 7-1, og at mange av disse har et svært stort antall leverandører, hvor mange er utenlandske:

> «Felles for disse er også i denne sammenheng en avhengighet av utenlandske leverandører. Det finnes ikke norske leverandører for en rekke produkter til disse anleggene og systemene. Det store antallet utenlandske leverandører fører til et sett med utfordringer knyttet til forslaget som kan gå direkte ut over forsyningssikkerheten.»

Energi Norge viser videre til at

> «i Statkrafts kraftanlegg i Norge er det alene over 3100 leverandører. I forhold til antall leverandører til anleggene som er klassifisert i

> «høyeste» klasse er det i underkant 900 ulike leverandører. Bare et av Statkrafts klasse 3 anlegg har færre enn 50 ulike leverandører og det er flere som har opp mot 100. Mange leverandører kan nok forhåndsklareres for leveranse til anlegg som kommer inn under sikkerhetsloven, men det er neppe praktisk mulig å forhåndsklarere alle tenkelige leverandører. Det er derfor en reell bekymring at reparasjonstiden vil øke ved feil i anleggene på grunn av økt byråkrati, i tillegg til økte kostnader knyttet til byråkratiet.»

Statnett og NVE mener det bør være opp til virksomhetene når og hvilke krav som skal gjelde i det enkelte tilfelle. *NVE* uttaler:

> «Forslaget inneholder krav til sikkerhetsavtale, leverandøravklaring og varslingsplikt. Det kan være områder og bransjer hvor alle tre er nødvendige, men NVE stiller spørsmål ved om dette bør være generelle krav. Vi mener det gir en bedre regulering å stille krav til at virksomhetene i sine ROS-analyser må vurdere om det er spesielle anskaffelser hvor sikkerhetsavtaler, leverandørklaringer og varslingsplikt anses nødvendig.»

NSM har uttalt:

> «Det bør vurderes å tydeliggjøre i lovforslaget at eventuelle leverandører må kunne tilfredsstille alle relevante krav i loven for å kunne få tilgang til sikkerhetsgradert informasjon/skjermingsverdig objekt og infrastruktur, før man kan tildeles en gradert kontrakt.»

NSM mener videre at den internasjonale dimensjonen av regelverket bør tydeliggjøres:

> «Det er gjennom dette regelverket at man sikrer norske leverandørers tilgang til det internasjonale markedet som involverer utenlandsk sikkerhetsgradert informasjon, og gjør det mulig for norske virksomheter å benytte leverandører fra utlandet dersom det er behov for dette. De internasjonale sikkerhetsgraderte anskaffelser er nært knyttet opp til bilaterale og multilaterale sikkerhetsavtaler som Norge har inngått med andre stater/organisasjoner. NSM mener at det er viktig at også denne delen av regimet reflekteres på en god måte i regelverket. Det bør vurderes om denne dimensjonen bør tydeliggjøres i lovforslaget eller om det er tilstrekkelig å beskrive dette nærmere i en lovproposisjon. Nærmere konkrete bestemmelser må uansett utformes i forskrifts form.»

NITO har spilt inn at det er behov for å beholde kjernekompetanse nasjonalt i de virksomhetene som er underlagt loven:

> «NITOs mener summen av utsatte (eller privatiserte) tjenester kan være av et slikt omfang at det oppstår en avhengighet. Avhengigheten kan medføre at det over tid er vanskelig å ta denne kunnskapen/kompetansen tilbake til ordinær drift. En stats egen evne til å ivareta funksjoner og støttefunksjoner er viktig elementer i statens samfunnssikkerhet. NITO vil videre påpeke at tjenester som skal outsources må vurderes både enkeltvis og i sum med tanke på kryssavhengigheter og samlet risiko. Det gjelder både for virksomheten, sektoren og for Norge. Fokus må være på at virksomheten skal kunne fortsette å levere de samfunnskritiske tjenestene også dersom de outsourcede tjenestene faller bort (krise/krig) eller kompromitteres (spionasje/sabotasje/terror).
>
> NITO vil spesielt peke på at fortsatt leveranse og funksjon må opprettholdes dersom tjenestene eller driften er outsourcet til utlandet (utflagging). Er tjeneste eller drift samlet innenlands, skal tjenesteleverandøren kunne dokumentere et visst minstenivå av sikkerhet som samsvarer med virksomhetens sikkerhetsbehov.»

Oslo politidistrikt uttaler:

> «Definisjonen omfatter ikke at en leverandør selv kan utarbeide sikkerhetsgradert informasjon. Dette er noe som leverandører gjør både i form av selve leveransen samt i form av intern sikkerhetstjeneste. Det foreslås derfor at teksten gis et tillegg: Med sikkerhetsgradert anskaffelse menes en anskaffelse som innebærer at leverandøren av varen eller tjenesten vil kunne få tilgang til eller selv tilvirke sikkerhetsgradert informasjon.»

Energi Norge mener videre at forholdet mellom regelverket og EU-retten er for dårlig utredet, og viser til:

> «Endringene i sikkerhetsloven setter ikke regelverket om offentlige anskaffelser til side. Om forholdet mellom regelverket for offentlige anskaffelser og sikkerhetslovens bestemmelser viser NOUen til hva Forsvarsdepartemen-

tet skriver om sikkerhetsgraderte anskaffelser i Prop. 97 L (2015–2016): *[f]or offentlige oppdragsgivere må regelverket om sikkerhetsgraderte anskaffelser sees i sammenheng med regelverket for offentlige anskaffelser. En sikkerhetsgradert anskaffelse er i utgangspunktet omfattet av [anskaffelsesloven] og [forskrift om forsvars- og sikkerhetsanskaffelser]. Nevnte lov og forskrift gjelder imidlertid ikke der en anskaffelse kan unntas med hjemmel i EØS-avtalen artikkel 123.* Virksomheter underlagt anskaffelsesregelverket for forsyningssektorene må således følge dette regelverket, selv om anskaffelsen er underlagt varslingsplikt i henhold til sikkerhetslovens bestemmelser. Dette forholdet kompliserer ytterligere anskaffelsesprosessen og åpner for potensielle erstatningskrav og søksmål. Det er uklart i hvilken grad EU-rett om fri flyt av varer og tjenester er vurdert i denne sammenheng. Dette bør tydeliggjøres i den videre behandlingen av lovforslaget.»

Når det gjelder den konkrete utformingen av bestemmelsene har *NVE* og *NSM* spilt inn at det bør presiseres hvem «anskaffelsesmyndigheten» i § 9-2 er, slik at det kommer tydeligere fram at bestemmelsen også gjelder for de private virksomhetene som er underlagt loven. *NSM* foreslår:

«I denne kontekst synes ikke begrepet «anskaffelsesmyndigheten» helt treffende. NSM foreslår derfor at det heller benyttes formuleringen «virksomheten som gjennomfører anskaffelsen».

Når det gjelder forslaget til § 9-3 er alle de høringsinstansene som har uttalt seg positive til at leverandørklarering fra 1. januar 2017 har blitt gjort tidsbasert, med en varighet på 5 år.

BDO og *NSM* mener imidlertid at klareringsmyndigheten bør være den samme som for personklarering. *NSM* viser til sin anbefaling i Sikkerhetsfaglig råd, og uttaler:

«Forsvarsdepartementet bør fremme et forslag om at sikkerhetsloven endres slik at Kongen kan utpeke klareringsmyndigheter og klageinstans for saker om leverandørklarering og andre myndighetsavgjørelser på området. NSM registrerer at utvalget ikke har fulgt opp denne anbefalingen, men anbefaler at det gjøre en fornyet vurdering slik at det åpnes for at klareringsmyndighet for leverandører også kan legges til andre enn Sikkerhetsmyndigheten.»

Telenor AS har videre spilt inn:

«Det må tas hensyn til at elektronisk kommunikasjon både er en samfunnskritisk funksjon, en kommersiell tjeneste, samt del av et globalt økosystem når det skal avgjøres om anskaffelsen omfattes av regelverket for sikkerhetsgradert anskaffelse. Herunder hvilke krav som skal stilles til anskaffende myndighet (det private rettssubjektet) og leverandør, og hvilke leverandører som kan godkjennes for hvilke leveranser. Det bør vurderes å innføre differensiert leverandørklarering hvor det tas hensyn til at det er en forskjell på leverandørgodkjenning for «rikets sikkerhet» og «samfunnssikkerhet».

Utenriksdepartementet har tatt opp:

«Dersom en aktuell leverandør ikke er leverandørklarert kan tidkrevende klareringsprosesser med NSM likevel medføre forsinkelser i konkrete anskaffelsesaker. Det kan derfor være fordelaktig om oppdragsgiver kunne anmode NSM om leverandørklarering av navngitte leverandører også med henblikk på fremtidige anskaffelsessaker, og uavhengig av konkrete anskaffelsesprosesser. Dermed vil oppdragsgivere kunne etablere «lister» over klarerte leverandører som oppdragsgivere uten tidsspille kan innhente tilbud fra og tildele kontrakter til.»

Til forslaget § 9-4 mener *Telenor, Samferdselsdepartementet* og *Statnett* at det er høyst usikkert hvor kapable virksomhetene er til selv å vurdere risiko, særlig gjelder dette de små virksomhetene. *Statnett* uttaler om dette:

«Statnett er usikker på i hvilken grad en virksomhet med kritisk infrastruktur vil være i stand til å vurdere den konkrete risikoen for et konkret objekt eller en infrastruktur. Hvis vi legger trefaktormodellen til grunn (side 44) hvor risiko ses på som forholdet mellom trusler, verdier og sårbarhet, vil en virksomhet kunne angi verdi og sårbarhet. Samtidig vil kunnskap og kompetanse om truslene rettet mot konkrete objekter og infrastrukturer kunne variere. Etter Statnetts syn må virksomhetens risikovurdering derfor kunne avgrenses til hvilken konsekvens bortfall av planlagt anskaffelse har for formål og virkeområde i §§ 1-1 og 1-2, eksempelvis om bortfall vil kunne skade grunnleggende nasjonale funksjoner.

Samtidig er det fremdeles Statnetts primære syn at det er mer hensiktsmessig å la energiloven ivareta formålet § 29a.»

13.4 Departementets vurdering

13.4.1 Generelt

Departementet er langt på vei enig i utvalgets vurderinger og foreslår at regelverket for sikkerhetsgraderte anskaffelser videreføres. Det vil da også i ny lov være et krav om sikkerhetsavtale, leverandørklarering og at virksomhetene pålegges en varslingsplikt ved sikkerhetsgraderte anskaffelser. Anskaffelsen er sikkerhetsgradert hvor leverandøren vil håndtere sikkerhetsgradert informasjon, eller får tilgang til skjermingsverdig objekt eller infrastruktur, jf. § 9-1. Leverandøren i en sikkerhetsgradert anskaffelse blir underlagt loven, jf. § 1-2 andre ledd. Departementet foreslår at bestemmelsene langt på vei utformes i tråd med utvalgets forslag, men med noen språklige forenklinger. Det foreslås også at de nærmere kravene til sikkerhetsavtalen vil fremgår av forskrift, og at det i forskrift kan gjøres unntak fra kravet om sikkerhetsavtale. Departementet ser behov for at det i det videre arbeidet med gjennomføringen av loven utredes nærmere om det skal gjøres tilpasninger slik at også leverandører til skjermingsverdige informasjonssystemer omfattes av loven, jf. § 6-1.

13.4.2 Virkeområde for reglene om sikkerhetsgraderte anskaffelser

Departementet har merket seg at høringsinstansene gjennomgående er positive til forslaget, men at flere har innspill til virkeområdet for og den nærmere utformingen av bestemmelsene om sikkerhetsgraderte anskaffelser. Flere av høringsinstansene har spilt inn at hensynet til sikkerhet ikke må legge unødvendige begrensninger på konkurransen, herunder leverandørtilfanget, særlig ved bruk av utenlandske leverandører.

Norsk olje og gass har i sitt høringsinnspill gitt uttrykk for at bestemmelsene om sikkerhetsgraderte anskaffelser ikke bør gjelde for de private virksomheter som allerede er og vil bli underlagt loven. Departementet deler ikke denne oppfatningen, og viser til at de virksomheter som underlegges sikkerhetsloven anses som så viktige for den nasjonale sikkerheten at det er et klart behov for å kunne føre kontroll med leverandørene til disse, uavhengig av om virksomheten som foretar anskaffelsen er en offentlig eller en privat aktør. Regelverket for sikkerhetsgraderte anskaffelser vil dessuten gi virksomhetene et nødvendig virkemiddel i arbeidet med forbyggende sikkerhetsarbeid i egen virksomhet, jf. lovens kapittel 4 om forebyggende sikkerhetsarbeid. Lovforslaget innebærer derfor at alle virksomhetene som blir underlagt loven, jf. § 1-2 annet ledd, jf. § 1-3, må forholde seg til regelverket om sikkerhetsgraderte anskaffelser.

Hvilke krav som stilles til virksomheten og leverandøren, vil imidlertid variere ut fra graderingsnivået på informasjonen, objektet eller infrastrukturen leverandøren får tilgang til ved anskaffelsen. Kravene vil også variere ut fra om informasjonen skal oppbevares hos leverandøren eller ikke. Slik departementet ser det, vil ikke kravene gå lenger enn det som er nødvendig av hensyn til nasjonale sikkerhetsinteresser i det enkelte tilfelle.

Eksempelvis vil kravet om leverandørklarering i utgangspunktet bare komme til anvendelse hvor leverandøren skal tilvirke eller oppbevare informasjon gradert KONFIDENSIELT eller høyere. I de tilfellene hvor leverandørens personell kun får tilgang til gradert informasjon, skjermingsverdig objekt eller infrastruktur hos virksomheten som foretar anskaffelsen, vil det i utgangspunktet kun være et krav om at personellsikkerhetsreglene i kapittel 8 følges. I tillegg kommer eventuelle krav som følger av det forebyggende sikkerhetsarbeidet i den anskaffende virksomheten, herunder reglene om informasjonssikkerhet og informasjonssystemsikkerhet i kapittel 5 og 6. Departementet understreker imidlertid at leverandørklarering likevel kan være aktuelt dersom det anses som nødvendig av andre grunner. Utvalget har ikke utredet dette nærmere, men skriver i særmerknaden til § 9-3 at det i første rekke vil være

> «de tilfeller der leverandøren kun vil få tilgang til klassifiserte områder innen skjermingsverdig objekt eller infrastruktur, hvor ansvarlig departement har truffet vedtak om krav til adgangsklarering, jf. § 7-3. Hvorvidt det kreves leverandørklarering for anskaffelser til skjermingsverdig objekt eller infrastruktur, må avgjøres konkret. I vurderingen bør det særlig tas hensyn til hvorvidt leverandørens personell får tilgang til deler av objektet eller infrastrukturen som har et høyt skadepotensial.»

Forslaget innebærer at det kan fastsettes i forskrift for hvilke andre tilfeller det vil være et krav om leverandørklarering.

Når det gjelder innspillet fra *NVE* om at det også vil være en sikkerhetsgradert anskaffelse når anskaffelsen medfører at leverandøren får tilgang til skjermingsverdig objekt etter § 7-1, viser departementet til at dette i utgangspunktet er en videreføring av gjeldende rett. Departementet viser også til det som framgår over, at kravene i regelverket vil variere, alt etter hva leverandøren og personellet som skal utføre oppdraget får tilgang til. I tråd med *Oslo politidistrikts* innspill har departementet tatt inn en presisering i § 9-1 for å tydeliggjøre at det også vil være en sikkerhetsgradert anskaffelse i de tilfeller leverandøren selv tilvirker sikkerhetsgradert informasjon.

13.4.3 Sikkerhetsavtale

Når det gjelder utvalgets forslag til § 9-2, understreker departementet at sikkerhetsavtalen skal tydeliggjøre og konkretisere de krav loven og tilhørende forskrifter oppstiller for virksomheten og leverandøren i forbindelse med anskaffelsen. Departementet foreslår at dette tydeliggjøres i § 9-2 andre ledd. Departement foreslår videre at det av lovteksten fremgår at sikkerhetsavtalen skal inneholde hvilken sikkerhetsgrad anskaffelsen skal ha, og hvordan leverandøren skal forholde seg til de krav som gjelder for anskaffelsen. Hvilken sikkerhetsgrad anskaffelsen skal ha vil avhenge av graderingsnivået på den informasjon, objekt eller infrastruktur leverandøren vil kunne få adgang til i forbindelse med anskaffelsen. Etter departementets oppfatning er sikkerhetsavtalen viktig for at leverandøren skal bli bevisst på hvilke av sikkerhetslovens krav som gjelder for den aktuelle anskaffelsen, og hvilke sikkerhetstiltak som må være på plass for å oppfylle disse kravene.

Departementet bemerker at kravet til omfanget av sikkerhetsavtalen vil måtte tilpasses graderingsnivået på anskaffelsen, og omfanget av de sikkerhetstiltak som må være på plass når anskaffelsen gjennomføres. I de tilfellene der hvor personell fra en leverandør skal gis tilgang til en del av et skjermingsverdig objekt med krav om adgangskontroll, jf. § 7-3, og kravet skal oppfylles ved at personellet følges rundt av sikkerhetspersonell, vil kravet til sikkerhetsavtale eksempelvis kunne være oppfylt ved at det tas inn en bestemmelse i kontrakten med leverandøren om dette, se eksempelet i særmerknaden. Hvor anskaffelsen innebærer at leverandøren skal oppbevare høyt gradert informasjon vil det imidlertid være mer omfattende krav til innholdet i avtalen.

Etter departementets syn vil ikke en sikkerhetsavtale i seg selv medføre økt ulempe for leverandørene. Eventuelle ulemper for leverandørene følger av å bli underlagt sikkerhetslovens bestemmelser, jf. § 1-2 andre ledd, herunder de krav til behandling av informasjon og adgangskontroll som gjelder for den informasjon, objekt eller infrastruktur leverandøren får tilgang til gjennom anskaffelsen. Eksempelvis kan det oppstå ulemper for leverandøren ved at det stilles krav til håndtering av sikkerhetsgradert informasjon, eller ved at leverandørens personell må oppfylle krav til adgangs- eller sikkerhetsklarering hvor leverandøren gis tilgang til skjermingsverdig objekt, jf. § 7-1.

Lovforslaget legger opp til at de nærmere kravene til innhold i sikkerhetsavtalen fastsettes i forskrift. Hvilke krav som stilles vil avhenge av anskaffelsens graderingsnivå. Utvalgets forslag til § 9-2 andre ledd, bokstav b og c, og kravene i gjeldende forskrift om sikkerhetsgraderte anskaffelser § 2-5, vil bli vurdert videreført i forskrift. Forskrift om sikkerhetsgraderte anskaffelser trådte i kraft før bestemmelsene om objektsikkerhet. Det vil derfor være naturlig at det i det videre forskriftsarbeidet også utredes hvilke nærmere krav til sikkerhetsavtalen som skal gjelde når leverandøren skal ha tilgang til skjermingsverdig objekt eller infrastruktur. Departementet ser videre at det i enkelte særlige tilfeller vil kunne være behov for å gjøre unntak fra kravet om sikkerhetsavtale, eksempelvis hvor det fremstår som åpenbart unødvendig at en slik avtale inngås. For hvilke tilfeller unntak vil være aktuelt må imidlertid utredes nærmere i det videre forskriftsarbeidet. Det åpnes derfor for at det i forskrift kan fastsettes unntak fra kravet om sikkerhetsavtale.

Flere av høringsinstansene mener det er uklart hva som ligger i «anskaffelsesmyndigheten». Departementet foreslår derfor en omformulering, slik at det klart framgår at sikkerhetsavtalen skal inngås mellom virksomheten som gjennomfører anskaffelsen og leverandøren. Det er også tatt inn en presisering i overskriften for å tydeliggjøre hvem som er partene til sikkerhetsavtalen.

Der hvor utenlandske leverandører, eller personell fra utenlandske leverandører, må klareres eller gis tilgang til sikkerhetsgradert informasjon, oppstiller § 9-2 krav om at sikkerhetsmyndigheten skal godkjenne leverandøren. I disse tilfellene må det, som i dag, foreligge en bi- eller multilateral avtale om utveksling og plikt til gjensidig beskyttelse av sikkerhetsgradert informasjon mellom norske myndigheter og hjemstaten til leverandøren. I dag kontakter NSM sikkerhetsmyndighetene i hjemstaten til leverandøren, som vil

bekrefte eller avkrefte hvorvidt leverandøren eller personell fra leverandøren oppfyller de av sikkerhetslovens krav som gjelder i forbindelse med anskaffelsen, eksempelvis om leverandøren har gyldig leverandørklarering eller om leverandørens personell har nødvendige klareringer. Sikkerhetsmyndigheten i hjemstaten vil også kunne føre sikkerhetsmessig tilsyn med leverandørens utførelse av anskaffelsen i disse tilfellene.

Dersom leverandøren eller personellet ikke har nødvendige klareringer, kan sikkerhetsmyndigheten anmode sikkerhetsmyndigheten i hjemstaten om å foreta nødvendige klareringer. Eventuelt må sikkerhetsmyndigheten og/eller klareringsmyndigheten kunne utveksle nødvendig informasjon med sikkerhetsmyndigheten i hjemstaten for selv å kunne klarere leverandøren eller personellet. Den nærmere prosessen for godkjenning av utenlandsk leverandør må reguleres i forskrift.

13.4.4 Leverandørklarering

Når det gjelder forslaget til § 9-3 om leverandørklarering vil departementet først understreke at dette kun er absolutt hvor leverandøren skal oppbevare sikkerhetsgradert informasjon, gradert KONFIDENSIELT eller høyere. Hvor leverandørens personell bare skal utføre arbeid hos virksomheten som er underlagt sikkerhetsloven, vil det normalt være tilstrekkelig at reglene om personellklarering følges, jf. lovforslagets kapittel 8. Departementet bemerker at i de tilfeller hvor leverandørklarering ikke kan gis, vil hensynet til nasjonal sikkerhet veie tyngre enn hensynet til et eventuelt økonomisk tap hos virksomheten eller leverandøren som er underlagt loven.

NSM og *BDO* har spilt inn at det bør være samme klareringsmyndighet for personell, som for leverandørklarering. Det vises særlig til mulighetene for positive synergieffekter, samtidig som *NSM* rendyrkes som klageinstans. For å gjøre regelverket mer fleksibelt for framtidige organisatoriske endringer, foreslår departementet at Kongen gis myndighet til å utpeke hvem som er klareringsmyndighet for leverandørklareringer.

Når det gjelder leverandørklareringens varighet slutter departementet seg til utvalgets vurdering, og viser samtidig til vurderingene i Prop. 97 L (2015–2016) kapittel 10.5. Slik departementet ser det vil tidsbaserte leverandørklareringer også ivareta innspillet fra *Utenriksdepartementet* som ønsker en mulighet til å kunne forhåndsklarere leverandører. Tidsbasert leverandørklarering videreføres derfor med hjemmel i § 9-3. Departementet bemerker at selv om en leverandør har leverandørklarering, må det inngås en sikkerhetsavtale for hver enkelt anskaffelse, ettersom kravene etter loven og forskriftene vil kunne variere for den enkelte anskaffelse.

13.4.5 Varslingsplikt ved anskaffelser til skjermingsverdige objekter, informasjonssystemer og infrastruktur

Når det gjelder høringsinstansenes innvendinger mot varslingsplikten i § 9-4, viser departementet til de vurderinger som ble gjort i Prop. 97 L (2015–2016), kapittel 11.4. Etter departementets syn ivaretar de vurderinger som ble gjort i proposisjonen også de innvendinger som har kommet i forbindelse med denne høringen. Når det gjelder innspillet fra *Telenor*, *Samferdselsdepartementet* og *Statnett* om usikkerheten knyttet til virksomhetenes evne til å foreta risikovurderinger, viser departementet særlig til kapittel 11.4.2, hvor det blant annet framgår:

> «Alle eierne av kritisk infrastruktur må kunne forventes å ha inngående kunnskap om egen infrastruktur. Dette innebærer både kunnskap om verdien av infrastrukturen, altså dens betydning for samfunnet, og om potensielle sårbarheter ved infrastrukturen. Det kan derimot ikke forventes at alle eiere av kritisk infrastruktur skal ha kunnskap om mulige trusler og aktører som kan utgjøre en trussel. Dette er informasjon som primært besittes av myndighetene, og som i varierende grad deles med andre. Mange virksomheter vil i sine risikovurderinger derfor måtte fokusere på sårbarheter ved infrastrukturen og ikke på trusler. Virksomhetene vil både måtte undersøke om anskaffelsen teknisk eller fysisk sett åpner en mulighet for at noen kan utføre eller legge til rette for sikkerhetstruende virksomhet og vurdere mulige konsekvenser av slik virksomhet.»

For nærmere om den risikovurdering som skal foretas viser departementet til Prop. 97 L (2015–2016) kapittel 11.4.2.

Når det gjelder utvalgets forslag til avgrensning av bestemmelsens virkeområde antar departementet at dette vil være av mindre praktisk betydning, da lovens virkeområde utvides til også å omfatte eiere av skjermingsverdig infrastruktur. Departementet har imidlertid også kommet til at bestemmelsen bør omfatte virksomheter som råder over skjermingsverdige informasjonssystemer, for å tilpasse bestemmelsen til at skjer-

mingsverdige informasjonssystemer nå er omfattet av loven, jf. forslaget § 6-1.

Det er videre tatt inn en justering i § 9-4 *første ledd* for å tilpasse bestemmelsen til endringen i begrepsbruken til «sikkerhetstruende virksomhet», jf. kapittel 6.4.2 og særmerknaden til § 1-1 bokstav b.

13.4.6 Forholdet til annet regelverk

Statnett og *Energi Norge* har spilt inn at behovet for sikkerhet i anskaffelsesprosessen i tilstrekkelig grad ivaretas i eksisterende sektorregelverk, og at det eventuelle behovet for tilpasninger best ivaretas gjennom en revisjon av dette regelverket.

Til dette viser departementet til at både utvalget og flertallet av høringsinstansene er enige om behovet for å utvikle en dynamisk sektorovergripende rammelov, for best mulig å kunne møte dagens risikobilde. Departementet deler denne oppfatningen, og ser det derfor som hensiktsmessig at reguleringen av sikkerhetsgraderte anskaffelser videreføres i en sektorovergripende lov. Loven vil angi de krav som virksomhetene må oppfylle av hensyn til nasjonal sikkerhet, mens sektorregelverket kan ha utfyllende bestemmelser tilpasset egen sektor.

Flere av høringsinstansene har videre stilt spørsmål om forholdet mellom regelverket for sikkerhetsgraderte anskaffelser og regelverket for offentlige anskaffelser. Departementet viser til at regelverket for offentlige anskaffelser gjelder offentlige myndigheter og enkelte private virksomheter, jf. anskaffelsesloven § 2 andre ledd, mens regelverket for sikkerhetsgraderte anskaffelser også vil gjelde for andre private virksomheter som underlegges loven, jf. forslaget til § 1-3. Virksomheter som er underlagt begge regelverkene, bør allerede ved utformingen av konkurransegrunnlaget ta stilling til om en leverandør vil kunne få tilgang til sikkerhetsgradert informasjon, skjermingsverdig objekt eller infrastruktur, og hvilke av sikkerhetslovens krav leverandøren må oppfylle ved anskaffelsen. Der hvor varslingsplikten i § 9-4 kan bli aktuell viser departementet til de forslag til utforming av konkurransegrunnlag og praktiske føringer som framgår av Prop. 97 L (2015–2016), kapittel 11.4.8.

Etter departementets syn vil det ikke oppstå konflikt med våre EØS-forpliktelser, da eventuelle begrensninger for konkurransen ikke vil gå lenger enn strengt nødvendig av hensyn til Norges nasjonale sikkerhet. Ved mange høyt graderte anskaffelser vil antakelig EØS – avtalens artikkel 123 komme til anvendelse, og da slik at anskaffelsen er unntatt kravene i anskaffelsesregelverket i sin helhet.

Når det gjelder innspillet fra *NITO,* om behovet for at virksomheter som er underlagt loven også kan opprettholde sin funksjon i krise og krig, uten bruk av utenlandske leverandører, vil departementet vise til at det er klart uheldig dersom en virksomhet som er av avgjørende betydning for grunnleggende nasjonale funksjoner, ikke kan utføre sine oppgaver i en krise- og krigssituasjon. Departementet antar imidlertid at dette til en viss grad avhjelpes gjennom bestemmelsene om eierskapskontroll i kapittel 10. Disse bestemmelsene gir mulighet til å føre kontroll med aktørene som gjennom eierskap i virksomheten utøver innflytelse på beslutningen om å «outsource» tjenester. Utvalgets forslag til bestemmelse om eierskapskontroll gir imidlertid ikke mulighet til å føre direkte kontroll med forvaltning av virksomhetene, herunder om virksomhetene «outsourcer» tjenestene. En slik bestemmelse har ikke vært nærmere vurdert av utvalget, og departementet har derfor ikke tilstrekkelig grunnlag for å foreslå en slik bestemmelse.

Departementet vil imidlertid bemerke at bestemmelsene om varslingsplikt ved anskaffelser til skjermingsverdig informasjonssystem, objekt og infrastruktur pålegger virksomheten en plikt til å vurdere hvorvidt anskaffelsen kan innebære en risiko for sikkerhetstruende virksomhet. Denne plikten vil naturlig nok også gjelde dersom virksomheten ønsker å «outsource» tjenester til en utenlandsk leverandør. I ytterste konsekvens vil myndighetene kunne fatte vedtak om å nekte at virksomheten «outsourcer» tjenester dersom dette innebærer en uakseptabel risiko. Departementet viser til at forslagets § 6-2 vil kunne medføre begrensninger på bruk av utenlandske leverandører.

14 Eierskapskontroll

14.1 Gjeldende rett

Det finnes i dag en rekke regelverk som har til hensikt å kontrollere eierskapet i norske selskaper, men ingen av disse har som formål å sikre generell kontroll med eierskapet i selskaper som støtter eller ivaretar grunnleggende nasjonale funksjoner.

Gjeldende sikkerhetslov og gjeldende petroleumslovgivning inneholder imidlertid enkelte bestemmelser som i noen tilfeller kan begrunne inngrep i eierstrukturene til et privat rettssubjekt av hensyn til nasjonal sikkerhet.

Gjeldende sikkerhetslov § 5 a pålegger virksomheter «som får kunnskap om en planlagt eller pågående aktivitet som kan medføre en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført», en varslingsplikt til overordnet departement. Bestemmelsen gir da Kongen i statsråd mulighet til å «fatte nødvendige vedtak for å hindre en planlagt eller pågående aktivitet som nevnt i første ledd første punktum.» Bestemmelsen gir således mulighet for myndighetene til å gjøre nødvendige vedtak i de tilfeller hvor en aktivitet medfører en «*ikke ubetydelig risiko*» for at «*sikkerhetstruende virksomhet blir etablert*».

Det kan blant annet innebære å fatte et vedtak som setter til side former for vedtak eller aktiviteter som i utgangspunktet er tillatt, eksempelvis oppkjøp av eierandeler i et strategisk viktig selskap, forutsatt at oppkjøpet anses som en tilstrekkelig stor sikkerhetsrisiko.

Bestemmelsen trådte i kraft 1. januar 2017, og er nærmere omtalt i Prop. 97 L (2015–2016) kapittel 4.4, side 19. Bestemmelsen er foreslått videreført av utvalget, se utvalgets forslag § 2-5.

Gjeldende bestemmelser om sikkerhetsgraderte anskaffelser i sikkerhetsloven kapittel 7 gir myndighetene en viss kontroll med eierskapet til leverandører hvor en anskaffelse medfører at leverandøren kan få tilgang til skjermingsverdig informasjon eller skjermingsverdig objekt, jf. §§ 27 og 28. I forbindelse med leverandørklareringen etter § 28, skal «leverandøren gi alle opplysninger som antas å kunne være av betydning for klareringsspørsmålet». Det følger videre at

> «[l]leverandøren skal uten ugrunnet opphold orientere Nasjonal sikkerhetsmyndighet om endringer i styre eller ledelse, forandringer i eierstrukturen, flytting av lokaliteter og utstyr, åpning av gjeldsforhandling eller begjæring om konkurs og andre forhold som kan ha betydning for leverandørens sikkerhetsmessige skikkethet.»

Dersom forholdene blir ansett å være en sikkerhetsrisiko kan sikkerhetsmyndigheten inndra leverandørklareringen, forutsatt at risikoen ikke kan elimineres gjennom å *utøve forebyggende sikkerhetstjeneste.*

Videre har petroleumslovgivningen, som gjennomfører konsesjonsdirektivet (direktiv 94/22/EF) i norsk rett, noen bestemmelser som kan gi adgang til å kontrollere eierskapet i selskaper som opererer på norsk sokkel. Av petroleumsloven § 10-12 første og andre ledd framgår det at «overdragelse av en tillatelse eller andel i tillatelse til petroleumsvirksomhet», eller «annen direkte eller indirekte interesseoverføring eller deltakelse i tillatelsen, herunder bl.a. overdragelsen av aksjeposter og andre eierandeler som kan gi bestemmende innflytelse over en rettighetshaver som innehar andel i en tillatelse ikke kan skje uten departementets samtykke». I vurderingen av om samtykke skal gis, framgår det av forskrift til lov om petroleumsvirksomhet § 72 at forskriften §§ 8, 10, 28 og 29 kommer til anvendelse så langt de passer. Av § 10 framgår krav til tildelingskriteriene for utvinningstillatelser, herunder at det kan legges vekt på relevante *objektive og ikke-diskriminerende kriterier.* Lest i sammenheng med forskriften § 11 andre ledd, om *vilkår og krav*, og konsesjonsdirektivet artikkel 3(5) a), antar departementet at det vil være adgang til å vektlegge *hensynet til nasjonal sikkerhet* i vurderingen av om samtykke skal gis.

Når det gjelder reglene om eierskapskontroll i konkurranseloven, børsloven, vannfallskonsesjonsloven, beredskapsforskriften, og i den tidli-

gere ervervsloven, viser departementet til NOU 2016: 19 kapittel 12.2. I tillegg viser departementet til kapittel 6 i finansforetaksloven, som gir myndighetene adgang til å føre kontroll med eierskapet i finansforetak. Det framgår av § 6-1:

> «Den som vil gjennomføre erverv som vil medføre at vedkommende blir eier av en kvalifisert eierandel i et finansforetak, må på forhånd sende melding om dette til Finanstilsynet. Det samme gjelder erverv som vil medføre at en kvalifisert eierandel økes slik at den vil utgjøre eller overstige henholdsvis 20, 30 eller 50 prosent av kapitalen eller stemmene i finansforetaket, eller slik at eierandelen gir bestemmende innflytelse som nevnt i allmennaksjeloven § 1-3 i finansforetaket. Som kvalifisert eierandel regnes en eierandel som representer 10 prosent eller mer av kapitalen eller stemmene i finansforetaket, eller som for øvrig gir adgang til å utøve en vesentlig innflytelse i ledelsen av foretaket og dets virksomhet.»

Et slikt erverv kan bare gjennomføres «etter tillatelse gitt av departementet», jf. § 6-1 andre ledd. Ved avgjørelse om tillatelse skal gis etter § 6-1 andre ledd, skal

> «departementet ut fra behovet for å sikre forsvarlig og betryggende ledelse av finansforetaket og dets virksomhet, og i betraktning av den grad av innflytelse som erververen som eier vil kunne utøve i foretaket etter ervervet, vurdere erververens egnethet som innehaver av vedkommende samlede eierandel etter ervervet, og om ervervet av eierandelen er finansielt betryggende.»

I § 6-3 andre ledd listes opp nærmere vurderingskriterier for når ervervet kan stanses. Om bakgrunnen for bestemmelsene framgår det av forarbeidene at disse skal sikre at finansinstitusjoner opprettholder tilstrekkelig finansiell stabilitet ved oppkjøp i institusjonen.

14.2 Utvalgets forslag

Sikkerhetsutvalget foreslår en egen bestemmelse i § 10-1 om eierskapskontroll. Bestemmelsen er foreslått tatt inn i et eget kapittel.

Sikkerhetsutvalgets begrunnelse (NOU 2016: 19 kapittel 12.8, side 246) for en slik bestemmelse er at

> «myndighetene i dag ikke har tilstrekkelige virkemidler for å kunne sikre nasjonal kontroll med strategisk viktige selskaper».

Utvalget har gjennomgått gjeldende sikkerhetslov, konkurranseloven, børsloven, vannfallskonsesjonsloven, beredskapsforskriften og den tidligere ervervsloven.

Utvalget viser til at eksisterende regelverk i stor grad skal ivareta andre hensyn enn nasjonale sikkerhetsinteresser. Videre vises det til at gjeldende bestemmelser om sikkerhetsgraderte anskaffelser bare i en «*viss utstrekning*» gir «*mulighet til å kunne ha kontroll*» over eierskapet til leverandørene til de strategiske selskapene, gjennom kravet om leverandørklarering, jf. gjeldende sikkerhetslov kapittel 7 om sikkerhetsgraderte anskaffelser. Se nærmere om utvalgets vurderinger i utredningen kapittel 12.8.

Leverandørklarering gir sikkerhetsmyndigheten innsikt i leverandørens eierstrukturer, og gir sikkerhetsmyndighetene mulighet til å trekke tilbake leverandørklareringen der eierkonstellasjonen utvikler seg i en retning som utgjør en økt sikkerhetsmessig risiko. Utvalget uttaler i kapittel 12.2:

> «Regelverket er imidlertid avgrenset til konkrete anskaffelser, og er således mindre egnet for å ivareta mer generelle behov for kontroll med eierskapet til strategisk viktige selskaper».

Utvalget viser videre til at gjeldende regelverk ikke vil

> «kunne sikre at grunnleggende nasjonale funksjoner ikke blir skadelidende ved at strategisk viktige selskaper helt eller delvis blir kjøpt opp av utenlandske aktører». Dette gjelder særlig «hensynet til forsyningssikkerhet og beredskap».

Utvalget uttaler videre i kapittel 12.8:

> «Selskaper som leverer varer eller tjenester av kritisk betydning for grunnleggende funksjoner, vil som utgangspunkt kun ha en kontraktuell forpliktelse til slik levering. I en krise- eller krigssituasjon hvor det sannsynligvis vil være knapphet på tilgjengelige ressurser vil det, slik utvalget ser det, ikke være en tilfredsstillende løsning at Norge har basert nødvendig kompetanse, eller produksjons- og vedlikeholdskapasitet på enkelte spesielt kritiske områder, ute-

> lukkende på utenlandske leverandører. Ved knapphet på ressurser må man være forberedt på at en slik kontraktuell forpliktelse ikke vil bli overholdt. Behovet til leverandørens hjemstat kan i slike tilfeller blir prioritert. Særlig vil dette gjelde i de tilfeller selskapets hjemstat er en stat Norge ikke har et sikkerhetsmessig samarbeid med.»

Utvalget ser derfor behov for en mekanisme som setter myndighetene i stand til å kunne kontrollere eierskapet i slike selskaper.

Utvalget har sett på hvordan eierskapskontroll reguleres i andre nasjoner vi vanligvis sammenligner oss med. Utvalget uttaler at:

> «Danmark og Sverige har ikke en slik type regulering. De fleste andre nasjoner utvalget har undersøkt, har imidlertid en eller annen form for mekanisme for å kunne kontrollere eierskapet i strategisk viktige selskaper.»

Finland, USA, England, Frankrike og Canada har lovgivning som gir myndighetene hjemmel til å gripe inn ved utenlandsk kontrollovertakelse i virksomheter hvor overtakelsen er i strid med nasjonale sikkerhetsinteresser. Et av flere fellestrekk er at terskelen for å kunne gripe inn mot et erverv er høy.

Eksempelvis har Finland regulert utlendingers overtakelse av visse finske foretak for å ivareta «ytterst viktige nasjonale interesser», se NOU 2016: 19 kapittel 12.3.6 side 236.

I USA vurderer *Committee on Foreign Investment in the US* (CFIUS) om kontrollovertakelser vil kunne true nasjonal sikkerhet. *The Industry Act* gir britiske myndigheter hjemmel til å gripe inn ved utenlandsk kontrollovertakelse over viktige produksjonsvirksomheter, dersom overtakelsen er i strid med nasjonale interesser. Loven har imidlertid aldri blitt anvendt. *The Enterprise Act* angir at britiske myndigheter kan «stoppe eller sette vilkår for sammenslåinger og overtakelse av britiske selskaper», dersom transaksjonen anses å stride mot offentlige interesser, som f.eks. nasjonal sikkerhet, se NOU 2016: 19 kapittel 12.3.3 side 232. I Frankrike framgår myndighetskontroll med utenlandske investeringer av *Code Monétaire et Financier, Titre V, Articles L151-1 til L151-4.* I utgangspunktet skal finansielle relasjoner med utlandet være uten restriksjoner. Det er imidlertid knyttet restriksjoner til nærmere bestemte virksomhetsområder. Disse framgår av Alstomdekretet Artikkel R153-2, som også angir hvilke investering som skal meldes og forhåndsgodkjennes av sikkerhetsmyndigheten.

For en nærmere gjennomgang av fremmed rett viser departementet til utvalgets utredning kapittel 12.3.

Utvalget har kommet til at eierskapskontroll av hensyn til beskyttelse av grunnleggende nasjonale funksjoner i utgangspunktet vil kunne være i strid med våre EØS-rettslige forpliktelser, blant annet Norges forpliktelse til å sikre fri etableringsrett og fri bevegelighet av kapital, jf. EØS-avtalens artikkel 31 og 40. Dette gjelder selv om restriksjonene rammer likt for innenlandske og utenlandske eiere.

Imidlertid viser utvalget til at unntakene i artikkel 32, 33 og 123 vil være anvendelige i de helt spesielle tilfellene det vil være nødvendig å bruke bestemmelsen om eierskapskontroll. Utvalget legger opp til at hjemmelen om eierskapskontroll bare skal kunne benyttes i de tilfeller hvor EØS-avtalens artikkel 123 er anvendelig.

Utvalget uttaler i NOU 2016: 19 kapittel 12.4.1, side 239:

> «Ved spørsmål om anvendelse av unntaket må det foretas en konkret vurdering i den enkelte sak. Det må vurderes hvilken sikkerhetsinteresse som skal beskyttes, hva som er sammenhengen mellom sikkerhetsinteressen og inngrepet i eierskapet for det relevante selskapet, og endelig hvorfor det er nødvendig å kontrollere eierskapet for å verne om sikkerhetsinteressen.»

Det forutsettes at bruk av unntaket vil være «nødvendig og proporsjonalt», i tråd med EU-domstolens praksis ved bruk av art. 123.

Når det gjelder selve utformingen av bestemmelsen bør den ifølge utvalget «være konkret avgrenset til å omfatte virksomheter som er av kritisk betydning for grunnleggende nasjonale funksjoner, jf. utvalgets lovforslag § 1-2 første ledd bokstav a til e».

Utvalget viser videre til i kapittel 12.4.5 at

> «[...] en usikkerhet om hvilke selskaper som er underlagt kontroll med eierskapet eller usikkerhet om vilkårene for når det vil bli grepet inn kunne ha en begrensende effekt på investeringslysten i Norge.»

Sammenholdt med begrensningen bestemmelsen i EØS-avtalen oppstiller uttaler utvalget at

> «[l]ovgivningen må dermed utformes slik at den kun rammer de tilfellene hvor unntakene fra EØS-avtalen gir adgang til inngripen, er tilstrekkelig presis om hvilke selskaper den rammer og hva som vil være vilkårene for når det vil skje inngripen slik at investorer kan forutberegne sin rettsstilling, og ikke unødvendig pålegger meldeplikt eller andre prosessuelle plikter på investeringer i selskaper hvor det ikke er adgang til å føre kontroll.»

Utvalget understreker:

> «Bestemmelsen er ment å være en snever unntaksbestemmelse, og myndighetene vil måtte dokumentere godt i den enkelte sak hvorfor det er nødvendig å gripe inn. Inngripen skal kun skje av hensyn til sikkerhetsinteresser. Bestemmelsen må ikke brukes for å ivareta andre interesser, herunder næringspolitiske interesser.»

I særmerknaden til bestemmelsen nevner utvalget eksempler på hvilke sikkerhetsinteresser som antas å være relevante:

> «hensynet til forsyningssikkerhet og strategisk produksjon av varer og tjenester for grunnleggende nasjonale funksjoner, behovet for å beholde kritisk nøkkelkompetansen av betydning for slike funksjoner eller av hensyn til beskyttelse av sensitiv og/eller sikkerhetsgradert informasjon.»

Utvalget mener videre at vedtaksmyndigheten etter bestemmelsen bør legges til Kongen i statsråd, både av hensyn til bestemmelsens inngripende karakter, men også av hensyn til likhet med tilsvarende vedtaksbestemmelser ellers i lovforslaget.

14.3 Høringsinstansenes syn

BDO, Fellesforbundet, Forsvars- og sikkerhetsindustriens forening (FSi), Fylkesmannen i Rogaland, Nasjonal kommunikasjonsmyndighet (Nkom), Nasjonal sikkerhetsmyndighet (NSM), Kongsberg Gruppen, Norges vassdrags- og energidirektorat (NVE), Luftfartstilsynet, Politiets sikkerhetstjeneste (PST), Samferdselsdepartementet, Utenriksdepartementet, Direktoratet for nødkommunikasjon (DNK), Abelia og NHO, har kommentert bestemmelsen om eierskapskontroll, og er i hovedsak positive til denne.

BDO, Fellesforbundet, Nkom, NSM og Kongsberg Gruppen tar opp at bestemmelsen kun retter seg mot utenlandske rettssubjekter. *Fellesforbundet* og *Kongsberg Gruppen* mener at både utenlandske og nasjonale oppkjøpere bør omfattes av bestemmelsen. *Kongsberg Gruppen* uttaler:

> «I lovforslaget foreslås det at kun utenlandske rettssubjekter vil omfattes av meldeplikt og godkjenning av oppkjøp. Kongsberg Gruppen er av den oppfatning at også norske rettssubjekter bør innebefattes av dette regelverket da det kan være kompliserte bakenforliggende eierstrukturer som kan innebære at reell(e) oppkjøper(e) ikke blir gjenstand for vurdering. Utvalget trekker riktignok på side 272 frem at det skal gjøres en konkret vurdering av hvorvidt oppkjøperen anses som utenlandsk eller ikke, men Kongsberg Gruppen anbefaler at loven bør omfatte alle slik at den juridiske vurderingen av oppkjøper gjøres uavhengig av oppkjøpers nasjonalitet. Dersom loven også innebefatter norske rettssubjekter vil lovforslaget etter vår mening også unngå mulige utfordringer med hvorvidt loven vil være diskriminerende for EØS-borgere. Loven vil da på dette punktet ikke måtte benytte unntaksbegrunnelser for å bli godkjent i henhold til EØS-regelverket.»

Nkom ber departementet vurdere om meldeplikten også bør tilligge virksomheten som blir ervervet:

> «Nkom stiller spørsmål til om de utenlandske rettssubjektene, som i § 10-1 pålegges å sende melding til ansvarlig departement, har de nødvendige forutsetninger til å gjøre kvalifiserte vurderinger av om virksomheten de planlegger å erverve eierandel i, er en virksomhet av kritisk betydning for grunnleggende nasjonale funksjoner. Nkom ber departementet vurdere om meldingsplikt eller tilsvarende også bør tilligge *virksomheten* som blir ervervet av det utenlandske rettssubjektet, ettersom det er denne virksomheten som (formodentlig) er underlagt loven.»

Fellesforbundet og *Kongsberg Gruppen* mener videre at terskelverdiene er satt for høyt. *Fellesforbundet* uttaler at:

> «Utvalget foreslår en meldeplikt som inntreffer når oppkjøper direkte eller indirekte erverver eller får reelt aksjeeie eller andelseie for minst

> en 1/3-del av aksjekapitalen, andelene eller stemmene. Etter Fellesforbundets syn er terskelen for meldeplikt satt for høyt. Et oppkjøp på tett oppunder en tredjedel vil føre til at oppkjøper kommer i svært nær posisjon til å oppnå negativ kontroll i selskapet uten at dette medfører meldeplikt. Fellesforbundet ber derfor departementet vurdere et første innslagspunkt på oppkjøp av 10 prosent, og deretter ved henholdsvis en tredjedel, halvparten, to tredjedeler, 90 prosent og fullt erverv.»

Kongsberg Gruppen er av den oppfatning at bestemmelsen også bør inneholde gjennomføringsforbud fram til godkjennelsen, og nærmere saksbehandlingsregler:

> «Lovforslagets § 10-1 beskriver at eierskapskontroll utføres når «…rettssubjekter ønsker å erverve…», og at det skal gjennomføres en forhåndskontroll. Lovforslaget inneholder imidlertid ikke gjennomføringsforbud frem til godkjennelsen, ei heller bestemmelser om saksbehandlingsfrist. Vi ber departementet vurdere hvorvidt dette bør inkorporeres i lovteksten for å sikre forutsigbarhet, samt for å unngå at det oppstår vanskelige og uheldige situasjoner ved at oppkjøp som er gjennomført senere nektes godkjenning.»

Nkom uttaler:

> «Ut fra gjeldende ordlyd i bestemmelsen er det uklart hvorvidt myndighetene har anledning til å gripe inn dersom det utenlandske rettssubjektet ikke gir slik melding, enten i form av å gripe inn på eget initiativ for å gjennomføre en vurdering etter 4. ledd, eller eventuelt å sanksjonere bruddet. For eksempel nevnes det i kapittel 12.3.2.1 i utvalgets rapport at den amerikanske *Committee on Foreign Investment in the US* kan gripe inn på eget initiativ og pålegge vilkår eller forby kontrollovertakelsen.»

NHO og *Abelia* uttrykker bekymring for at bestemmelsen vil ha negativ betydning for norsk næringsvirksomhet. *NHO* uttaler om dette:

> «For en selger av eierandeler vil risikoen for inngrep ha betydning for hvordan man gjennomfører en salgsprosess, og dermed for den pris og de vilkårene som er mulig å oppnå ved et salg. En mulig kjøper som regner risikoen som stor for at erverv blir stanset, vil kanskje ikke delta i prosessen, med den konsekvensen for kjøper at etterspørsel blir lavere. Selgere har behov for å kunne vite sikkert før en salgsprosess starter om det som skal selges er omfattet av § 1-2. Vi legger til grunn at § 2-1 blir utformet slik at en innehaver av eierandeler ikke vil være i tvil om det er aktuelt med eierskapskontroll.
>
> Vi er usikre på om den regelen som er foreslått dekker tilstrekkelig erverv av virksomhet (eiendeler, rettigheter og forpliktelser) i motsetning til eierandeler.»

DNK ser behov for en bestemmelse om eierskapskontroll i strategisk viktige selskaper, som er av kritisk betydning for nasjonale funksjoner, men stiller «spørsmål ved om bestemmelsen også bør utvides til å omfatte tjenesteutsetning av drift av slik infrastruktur/systemer».

NVE uttaler:

> «Utvalget har omtalt kravet til offentlig eierskap som følger av industrikonsesjonsloven. NVE slutter seg til utvalgets målsetning om at de virkemidler som foreslås ikke i vesentlig grad skal innskrenke selskapenes muligheter for å konkurrere i et globalt marked. For byggefasen mener NVE at bruk av utenlandske leverandører i byggefasen for nye kraftledninger og kraftverk er nødvendig for effektiv og sikker etablering av slike anlegg. NVE mener på denne bakgrunn at mekanismen for å kunne kontrollere eierskapet må være en snever unntaksregel.»

Samferdselsdepartementet uttaler:

> «En rekke tjenester og oppgaver i samferdselssektoren er konkurranseutsatt, og hvor også utenlandske aktører konkurrer i markedet. SD er derfor opptatt av at sikkerhetsloven ikke virker konkurransevridende, for eksempel ved at utenlandske selskaper må ekskluderes fordi de vil ikke vil kunne underlegges sikkerhetsloven. Tilsvarende vil det være en utfordring dersom enkeltselskap underlegges loven og pålegges kostnadskrevende sikkerhetskrav, mens konkurrerende selskap slipper.»

NVE og *Utenriksdepartementet* mener at forholdet til EØS-regelverk bør framgå klarere av bestemmelsen. *NVE* uttaler:

> «Det bør i selve bestemmelsen henvises til at eierskapskontrollen må skje innen de rammer EØS-avtalen setter. Dette vil bidra til at det mer

konsekvent fremgår i loven hvilke føringer EØS-avtalen setter, slik det er gjort for personopplysninger i § 4-7. For energiforsyningen er det hvem som er reell driver som er viktigst for å ivareta sikkerheten. Anleggskonsesjoner gis til reell driver. Energiloven § 9-2 tredje ledd annet punktum gir hjemmel til å fatte vedtak om at «drift i ekstraordinære situasjoner og gjennomføring av tiltak etter dette kapittel skal kunne skje fra norsk territorium».»

Utenriksdepartementet uttaler:

«Når det gjelder beskrivelsen av EØS-avtalens artikkel 123. pkt. 12.4.1. vil UD bemerke at artikkel 123 er i all hovedsak hentet fra sikkerhetsklausulsformuleringen i EFTAs frihandelsavtaler, med visse suppleringer i bokstav c). Bestemmelsen tilsvarer derfor *ikke* sikkerhetsklausulen i TFEU artikkel 346. Dette vil kunne ha betydning for tolkningen av bestemmelsen og dermed rekkevidden av denne. I motsetning til GATT artikkel XXI (b), inneholder ikke EØS-avtalen noe unntak utelukkende av hensyn til nasjonale sikkerhetshensyn alene, men krever i tillegg at det må foreligge (jf. «*i tilfelle*») indre uro, krig, fare for krig, eller at tiltaket er nødvendig for å oppfylle forpliktelser Norge har påtatt seg for å opprettholde fred og sikkerhet. Bestemmelsen har så vidt departementet kjenner til aldri vært anført for EFTA-domstolen, og det er derfor vanskelig å si noe om hvordan den eventuelt vil bli tolket dersom spørsmålet skulle komme på spissen.»

PST mener at enkelte av begrepene i bestemmelsen bør klargjøres og at dette bør gjøres i forskrift. *PST* uttaler:

«I forslaget til § 10-1 *Eierskapskontroll* benyttes det flere begreper som PST mener med fordel kunne defineres nærmere, for eksempel gjennom bruk av forskriftshjemmelen. Dette gjelder begreper som *«ervervets risikopotensial og erververens sikkerhetsmessige pålitelighet»* i bestemmelsens tredje ledd, men også hva en vurdering av dette skal omfatte. Likeledes mener PST det i forskrift bør klargjøres hvilke undersøkelser relevante myndigheter kan gjøre i forkant av en rådgivende uttalelse til departementet, og hvilke myndigheter som i denne sammenheng anses som relevante.»

14.4 Departementets vurdering

Departementet er langt på vei enig i utvalgets vurderinger og ser behovet for bestemmelser om eierskapskontroll. Departementet har merket seg at høringsinstansene gjennomgående er positive til forslaget, men at flere har innspill til utformingen av bestemmelsen. Departementet foreslår at bestemmelsen deles i tre, og at det gjøres noen språklige justeringer. Departementet ser behov for å tydeliggjøre når meldeplikten inntrer, innholdet av meldingen, hvilke saksbehandlingsregler som gjelder for behandlingen av meldingen og innholdet i vedtakskompetansen. Det foreslås derfor at kapittel 10 deles opp i bestemmelsene §§ 10-1 til 10-3.

Departementet viser innledningsvis til at de virksomheter som blir underlagt loven, jf. § 1-3 er av så sentral betydning for nasjonal sikkerhet at det bør være adgang til å kunne føre kontroll med eierskapet i disse virksomhetene. Adgangen til å kunne stanse ervervet skal imidlertid være snever, slik at vedtakskompetansen kun skal brukes unntaksvis. Dette er etter departementets syn ivaretatt i forslaget §§ 10-1 til 10-3.

Til *NHOs* innspill om at det er usikkert om bestemmelsen også dekker erverv av virksomhet (eiendeler, rettigheter og forpliktelser), vil departementet bemerke at de foreslåtte bestemmelsene vil omfatte erverv av eierandeler som gir erverver betydelig innflytelse over forvaltningen av en virksomhet som er underlagt loven. Bestemmelsene gir imidlertid ikke adgang til å gripe inn i beslutninger som er et resultat av forvaltningen av virksomheten, eksempelvis et salg av eiendeler eller overføring av rettigheter og forpliktelser til uønskede aktører. Skal sistnevnte tilfeller kunne stanses av hensyn til nasjonal sikkerhet må vilkårene i § 2-5 være oppfylt.

Når det gjelder utformingen av § 10-1 støtter departementet innspillet til *Fellesforbundet* og *Kongsberg Gruppen* om at også nasjonale erververe bør ha en meldeplikt. Det vises til at kompliserte eierstrukturer kan innebære at reelle oppkjøpere ikke blir gjenstand for vurdering dersom meldeplikten kun omfatter utenlandske kjøpere. Departementet kan ikke se at det er tungtveiende innvendinger mot at meldeplikten også skal gjelde for nasjonale oppkjøpere. Departementet foreslår derfor at «utenlandske» fjernes fra forslaget til § 10-1.

Departementet kan videre ikke se at det er behov for, eller praktisk, at også virksomheten det gjøres erverv i, underlegges en meldeplikt. Departementet legger til grunn at erververne i til-

nærmet alle tilfeller vil være klar over at virksomhetene hvor de erverver en eierandel på 1/3 eller mer, er underlagt sikkerhetsloven. Det vises særlig til at det i de aller fleste tilfeller vil være en kontakt mellom erverver og selskapet forut for ervervet, samtidig som det vil foreligge et enkeltvedtak som underlegger virksomheten lovens bestemmelser, jf. § 1-3. Informasjon om hvilke virksomheter som er underlagt loven vil imidlertid også være tilgjengelig hos det departement som har truffet vedtak om å underlegge virksomheten loven, og hos sikkerhetsmyndigheten som vil ha en oversikt over alle virksomheter som er underlagt loven. I dag er informasjonen om hvilke virksomheter som er underlagt loven tilgjengelig på NSMs hjemmesider. Det er videre uklart for departementet hvem i virksomheten som vil ha tilstrekkelig kunnskap om ervervet på et like tidlig tidspunkt som erververen, samtidig som det er usikkert om det alltid vil være klart om virksomheten vet hvorvidt noen erverver en eierandel i denne. Departementet antar videre at risikoen for at det blir truffet et vedtak om stans eller omgjøring av ervervet, jf. § 10-3, gjør at meldeplikten vil bli etterlevd. Departementet viser også til at meldeplikten påhviler erverver i regelverkene til de landene som utvalget har sett hen til. I flere av landene er myndighetene også gitt hjemmel til å gripe inn på eget initiativ. Etter den nå opphevede ervervsloven var det også erverver som hadde meldeplikt.

Kongsberg Gruppen og *Fellesforbundet* mener at terskelen for når meldeplikten inntreffer er satt for høyt. Høringsinstansene foreslår et system hvor første innslagspunkt er ved oppkjøp av 10 prosent, og deretter ved henholdsvis en tredjedel, halvparten, to tredjedeler, 90 prosent og fullt erverv. Departementet slutter seg imidlertid til utvalgets forslag, og viser til utvalgets vurdering i NOU 2016: 19 kapittel 12.7.2:

> «En eierandel på over en tredjedel av aksjekapitalen og en tilsvarende andel av stemmene på generalforsamlingen vil således gi negativ kontroll med de beslutninger som krever to tredjedels flertall. Ved negativ kontroll vil eieren således kunne motsette seg vesentlige beslutninger som for eksempel flytting av hovedkontor, andre vedtektsendringer etc.»

Videre finner departementet at terskelen i utvalgets forslag samsvarer bedre med den høye terskelen for stansing av erverv som følger av § 10-3, samtidig som antall meldinger begrenses noe. Departementet bemerker at den foreslåtte terskelen er i samsvar med terskelen i tilsvarende regelverk i Frankrike.

Utvalget har ikke foreslått en regulering av krav til innhold i meldingen. Departementet vil utrede behovet for nærmere krav til innholdet i meldingen i det videre forskriftsarbeidet. Meldingen bør etter departementets syn inneholde opplysninger som gjør mottaker i stand til å vurdere erververens samlede innflytelse på virksomheten, og erververs sikkerhetsmessige pålitelighet. Eksempelvis vil opplysninger om størrelsen på eierandelen og erververs eierstruktur være relevante. Departementet antar at momentene som framgår av gjeldende sikkerhetslov § 28 om leverandørklarering, som i stor grad er videreført i forslaget § 9-3, også vil kunne være relevante i vurderingen.

Når det gjelder den nærmere saksbehandlingen av meldingen, foreslår departementet en egen bestemmelse om dette i § 10-2. Departementet har sett hen til fristreglene for behandling av meldinger etter finansforetaksloven, og til at det i enkelte tilfeller må medregnes noe tid til informasjonsinnhenting, samt til den konkrete vurderingen av meldingen. Departementet ser det derfor som hensiktsmessig at meldingen behandles så snart som mulig, og senest innen 60 arbeidsdager etter at meldingen er mottatt. Departementet ser det også som hensiktsmessig med en bestemmelse om fristavbrudd, og foreslår derfor at fristen avbrytes dersom mottaker av meldingen, før det har gått 50 arbeidsdager, har framsatt skriftlig krav om ytterligere opplysninger. Fristen avbrytes fram til svaret er mottatt.

Departementet foreslår videre at den instansen som mottar meldingen, bør innhente en rådgivende uttalelse fra relevante organer om ervervets risikopotensial, og erververens sikkerhetsmessige pålitelighet. Hvem som anses som relevante organer, og hva uttalelsen bør inneholde, må imidlertid utredes nærmere i det videre forskriftsarbeidet. Eksempelvis vil EOS-tjenestene, med den tilgang de har til trusselinformasjon mot norske virksomheter, være aktuelle.

Departementet ser ikke behov for et gjennomføringsforbud fram til godkjennelse foreligger. Risikoen for at ervervet blir stanset eller reversert, vil etter all sannsynlighet medføre en utsettelse av gjennomføringen til melderen har fått beskjed om ervervet er godkjent, jf. § 10-2, eller om det skal behandles av Kongen i statsråd, jf. § 10-3. Departementet kan heller ikke se at et gjennomføringsforbud vil minske risikoen for erverv med uønsket innflytelse på virksomheten.

Når det gjelder § 10-3 legger departementet til grunn at et vedtak etter bestemmelsen må ligge innenfor formålet med sikkerhetsloven. Vedtaket må også være forholdsmessig, slik at hensynet til nasjonale sikkerhetsinteresser må veie opp for de negative økonomiske konsekvensene av vedtaket. Det forutsettes at vedtaket kan begrunnes, og at denne begrunnelsen kan dokumenteres tilstrekkelig.

Departementet bemerker at Kongen i statsråd, uavhengig av melding, vil kunne fatte vedtak om stans av ervervet, jf. § 10-3.

Når det gjelder innspillene fra *NHO* og *Abelia*, er departementet enig i at det kan være en risiko for at bestemmelsen om eierskapskontroll vil kunne påvirke konkurransekraften til og investeringslysten i norske selskaper underlagt loven. Departementet vil imidlertid påpeke at disse virksomhetene håndterer informasjon, teknologi eller fysiske aktiva som er av så stor betydning for grunnleggende nasjonale funksjoner at det er funnet nødvendig å underlegge dem sikkerhetsloven. Muligheten til å kunne føre kontroll med eierskapet av hensyn til nasjonal sikkerhet, veier etter departementets syn tyngre enn de eventuelle negative konsekvensene for virksomhetenes konkurransekraft. Departementet anser dessuten de eventuelle negative konsekvensene som små, da § 10-3 kun vil bli anvendt helt unntaksvis etter en forholdsmessighetsvurdering i hvert enkelt tilfelle, hvor nettopp de negative konsekvensene for virksomheten må holdes opp mot hensynet til nasjonale sikkerhetsinteresser.

Når det gjelder innspillet fra *NVE* og *Utenriksdepartementet* om forholdet til EØS-retten, slutter departementet seg til utvalgets vurderinger. Stans av et erverv i en virksomhet vil i utgangspunktet være i strid med EØS-avtalens regler om fri etableringsrett og den frie bevegelighet av kapital, jf. EØS-avtalens artikkel 31 og 40. Imidlertid vil et inngrep bare gjøres i særlige tilfeller, hvor formålet med inngrepet ikke kan oppnås på en mindre inngripende måte. Det må videre være forholdsmessighet mellom den konkrete risiko for skadevirkning for nasjonale sikkerhetsinteresser og negative konsekvenser for de involverte aktørene. Departementet antar at artikkel 123, men også i enkelte tilfeller artikkel 33, da vil kunne hjemle inngripen.

15 Kontroll- og tilsynsordninger

15.1 Gjeldende rett

Etter sikkerhetsloven § 30 er den forebyggende sikkerhetstjenesten underlagt kontroll og tilsyn av Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste, i samsvar med lov februar 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjenesten (EOS-kontrolloven). I praksis innebærer dette at alle forvaltningsorganer, og selvstendige rettssubjekter underlagt loven, i prinsippet er gjenstand for kontroll og tilsyn av EOS-utvalget. Hovedformålet med EOS-utvalgets kontroll er å ivareta den enkeltes rettssikkerhet.

Nasjonal sikkerhetsmyndighet (NSM) har etter gjeldende sikkerhetslov § 9 første ledd bokstav c i oppgave å «føre tilsyn med sikkerhetstilstanden i virksomheter, herunder kontrollere at den enkeltes plikter i eller i medhold av loven her overholdes, og eventuelt gi pålegg om forbedringer».

Sikkerhetsloven har i dag en bestemmelse om straff i § 31. Her heter det at den som forsettlig eller uaktsomt overtrer bestemmelser gitt i eller i medhold av konkrete angitte bestemmelser i sikkerhetsloven, eller overtrer pålegg gitt av Nasjonal sikkerhetsmyndighet i medhold av lovens § 9 første ledd bokstav c, straffes med bøter eller fengsel inntil seks måneder, hvis ikke forholdet går inn under en strengere straffebestemmelse. Den som forsettlig eller grovt uaktsomt krenker taushetsplikt etter § 12 første ledd og den som overtrer forbud med hjemmel i § 18 a *Adgang til steder og områder*, straffes med bot eller fengsel inntil 1 år, hvis ikke forholdet går under en strengere straffebestemmelse.

De konkrete bestemmelsene i sikkerhetsloven som § 31 viser til, er § 5 om den enkelte virksomhets plikter etter loven, § 10 om Nasjonal sikkerhetsmyndighets adgangsrett for å kunne gjennomføre sine kontrolloppgaver etter loven, § 12 om plikten til å beskytte sikkerhetsgradert informasjon, § 13 om sikkerhetsmessig godkjenning av informasjonssystemer, § 14 om kryptosikkerhet og § 17 om utvelgelse av skjermingsverdige objekter.

De bestemmelsene som her er gjengitt er ansett for å være de mest sentrale i forbindelse med etablering og etterlevelse av de sikkerhetstiltak som blir fastsatt gjennom sikkerhetsloven eller i medhold av denne, for å sikre et samfunnsmessig forsvarlig sikkerhetsnivå.

I praksis skjer det få tilfeller av anmeldelse for brudd på sikkerhetsloven og forskrifter.

15.2 Utvalgets forslag

Når det gjelder forholdet til EOS-utvalget, foreslår Sikkerhetsutvalget å videreføre gjeldende rett.

Når det gjelder tilsynsmyndighetenes tilsyn med virksomheter underlagt loven, har utvalget, som tidligere beskrevet, kommet til at det beste vil være å etablere en tilsynsmodell som både ivaretar målet om en helhetlig og tverrsektoriell tilnærming til forebyggende sikkerhet, samtidig som samfunnssektorenes særegenheter og behov ivaretas i tilstrekkelig grad. (NOU 2016: 19 kapittel 7.7.4). For å sikre en slik helhetlig, samordnet og tverrsektoriell tilnærming foreslår utvalget at sikkerhetsmyndigheten gis myndighet til å føre tilsyn med sektormyndigheter tillagt tilsynsansvar etter loven (NOU 2016: 19, side 140–141). Utvalget viser i denne forbindelse til forslaget om å lovfeste en samhandlingsplikt mellom sektormyndigheten og aktuelle sektormyndigheter, formalisert gjennom en samarbeidsavtale. Utvalget peker på at tilsynsmyndighetene har myndighet til å gi pålegg om gjennomføring av tiltak, dersom virksomhetene ikke oppfyller sine plikter etter loven. Utvalget foreslår også at sikkerhetsmyndigheten gis påleggsmyndighet overfor de sektormyndighetene som har tilsynsansvar etter loven, slik at det kan gripes inn dersom sikkerhetsnivået i den aktuelle samfunnssektoren utvikler seg på en utilfredsstillende måte.

Utvalget foreslår å innføre hjemmel om tvangsmulkt og overtredelsesgebyr. Utvalget gir uttrykk for at tilsynsmyndighetens virkemiddelportefølje etter dagens sikkerhetslov ikke er tilfredsstillende overfor virksomheter som ikke følger opp kra-

vene etter lov og forskrift, og sier videre i NOU 2016: 19, side 141:

> «Tilsynsmyndigheten har i medhold av dagens lov § 9 første ledd bokstav c), myndighet til å gi pålegg om forbedringer dersom avvik avdekkes. Dersom slike pålegg ikke følges opp av den enkelte virksomhet, er anmeldelse det eneste virkemidlet tilsynsmyndigheten har tilgjengelig. Terskelen for å gå til anmeldelse av en virksomhet, vil i de fleste tilfeller være høy. Utvalget mener derfor at tilsynsmyndighetens virkemiddelporteføljе bør utvides ved at det gis myndighet til å ilegge tvangsmulkt dersom det avdekkes brudd på regelverket, eller der pålegg ikke følges opp innen en gitt tidsfrist. I nærmere angitte tilfeller, bør tilsynsmyndigheten også kunne ilegge overtredelsesgebyr ved brudd på regelverket. På samme måte som for påleggsmyndigheten, foreslår utvalget at myndigheten til å ilegge tvangsmulkt og overtredelsesgebyr bør legges til den myndighet som er tildelt tilsynsansvaret.»

Utvalget foreslår å videreføre gjeldende sikkerhetslovs straffenivå og skyldkrav.

15.3 Høringsuttalelser

Utenriksdepartementet uttaler blant annet at tilsynsfunksjonen til sikkerhetsmyndigheten

> «bør fokusere på tilsynsobjekter som har en sektorovergripende rolle og den enkelte virksomhets egen kontroll- og revisjonsaktivitet. Utvalget av tilsynsobjekter bør skje i samarbeid med ansvarlig sektordepartement.»

Videre uttaler *Utenriksdepartementet*:

> «Sikkerhetsmyndigheten bør tilføres kompetanse slik at den faktiske tilsynskompetansen gjenspeiler lovens utvidede formål og virkeområde. Dette er avgjørende for at tilsyn med virksomheter kan gjennomføres på en måte og etter en metodikk som oppleves som minst mulig belastende for den enkelte virksomhet.»

NSM peker på at erfaringen er at pålegg om å lukke avvik ikke alltid etterkommes av virksomheten, og at NSM har få virkemidler i disse tilfellene. NSM anser det positivt at nye virkemidler foreslås og støtter at det innføres et hjemmelsgrunnlag for tvangsmulkt og overtredelsesgebyr.

Nasjonal kommunikasjonsmyndighet (Nkom) uttaler om tvangsmulkt og overtredelsesgebyr:

> «Nkom bruker denne typen sanksjoner aktivt i forhold til å etterleve ekomregelverket, og under forutsetning av klare regler om forholdsmessighet og klagerett er Nkom enig i innføring av denne type sanksjonsmidler er et viktig verktøy for tilsynsmyndigheten fremfor ensidig fokus på straff.»

Norges vassdrags- og energidirektorat (NVE) foreslår at overskriften på kapittelet og § 11-1 blir «særskilte kontroll- og tilsynsordninger». Dette «[f]or å markere at § 11-1 ikke omhandler tradisjonell tilsynsmyndighet (slik § 3-1 gjør).»

Oslo politidistrikt hevder det er grunnlag for å stille spørsmål ved om dagens straffenivå står i forhold til de samfunnsmessige konsekvensene som kan oppstå som følge av brudd på lovgivningen, og uttaler videre:

> «Generelt ved sanksjoner på dette området vil gjelde at virksomheter kan spekulere å omgå krav og pålegg, dersom sanksjonsnivået ikke står i forhold til investerings- og driftskostnadene ved å etablere nødvendige tiltak.»

Riksadvokaten har ikke innvendinger til utvalgets forslag om å utvide virkemiddelporteføljen til også å omfatte tvangsmulkt og overtredelsesgebyr, og uttaler videre:

> «Et av flere antatt positive utslag av den sektorovergripende tilnærmingen er at tilsynsmyndigheten utvikler en ensartet praksis for så vel administrative sanksjoner som anmeldelse av straffbart forhold. Sett i sammenheng med fagmyndighetsansvaret, som innebærer ansvar for implementering av lovverket, vil det forhåpentligvis gi den nødvendige forutberegnelighet og klarhet for de virksomhetene som er underlagt sikkerhetsloven og som i ytterste konsekvens kan stilles strafferettslig ansvarlig for brudd på denne.»

Riksadvokaten peker videre på at utvalget foreslår samme straffenivå som etter gjeldende lov, og uttaler:

> «Tatt i betraktning utvalgets uttalelser om at terskelen for å anmelde er høy, og tatt i betraktning forslaget om utvidet virkemiddelporteføljе, må en legge til grunn at tilfeller som anmeldes til politiet er av en viss alvorlighets-

grad. På denne bakgrunn tillater en seg å foreslå at straffen etter utkastet § 11-4 første ledd endres til «bot eller fengsel inntil 6 måneder, eller begge deler». En slik endring vil gi mulighet til å pågripe dersom de generelle og spesielle vilkårene etter straffeprosessloven § 171 jf. §170a for øvrig er til stede. Dersom tilsynsmyndigheten først vurderer forholdet som så vidt alvorlig at anmeldelse inngis, må en i praksis ta høyde for at det også er nødvendig og forholdsmessig å benytte de mest vanlige tvangsmidlene. Ransaking vil det være anledning til også etter gjeldende § 9, idet terskelen etter straffeprosessloven § 192 er at handlingen kan medføre «frihetsstraff».»

15.4 Departementets vurdering

Departementet er ikke uenig når *Utenriksdepartementet* uttaler at sikkerhetsmyndigheten bør ha oppmerksomhet særlig knyttet til tilsynsobjekter som har en sektorovergripende rolle og til den enkelte virksomhets egen kontroll- og revisjonsaktivitet. Dette må imidlertid ikke forhindre at sikkerhetsmyndigheten har relevante sanksjonsmidler overfor virksomhetene i de tilfellene der kravene som stilles etter loven, ikke blir fulgt.

Når det gjelder sanksjonsmulighetene, har departementet merket seg høringsuttalelsene til i denne sammenheng sentrale høringsinstanser som *NSM* og politi- og påtalemyndighet. Disse instansene støtter utvalgets forslag om å utvide sanksjonsmulighetene ved brudd på sikkerhetsloven og tilhørende forskrifter til også å omfatte tvangsmulkt og overtredelsesgebyr, i tillegg til de gjeldende strafferettslige reaksjonene bot og fengsel.

Departementet er enig med utvalget i at tilsynsmyndighetens virkemiddelportefølje i dagens lov ikke er tilstrekkelig, særlig fordi praksis tilsier at terskelen for å gå til anmeldelse er høy. Med hjemmel for bruk av administrative sanksjoner som tvangsmulkt og overtredelsesgebyr, vil man få en mer fleksibel måte til å «sette makt» bak de krav som stilles for å ivareta sikkerhetslovens formål. Forutsetningen for innføring av slike administrative sanksjoner må være at det fastsettes nærmere forskrifter og retningslinjer for slik bruk, ikke minst for å sikre forholdsmessighet mellom brudd og sanksjon, og for å sikre forutberegnelighet og likhet.

Når det gjelder straffenivået, er departementet enig i at det kan diskuteres om dette er satt for lavt. Imidlertid mener departementet at det nå er viktigst å få på plass en utvidelse av virkemiddelporteføljen. Departementet følger likevel *Riksadvokatens* forslag som endrer straffenivået i § 11-4 første ledd slik at det gis mulighet for bruk av tvangsmiddelet pågripelse, dersom de generelle og spesielle vilkårene etter straffeprosessloven § 171, jf. § 170 a er oppfylt. Departementet foreslår derfor at «bot eller fengsel inntil 6 måneder» i § 11-4, utvides til «eller begge deler».

Departementet er videre enig med *NVE* i at overskriften på kapittelet og § 11-1 bør endres for å markere at bestemmelsen ikke omhandler tradisjonell tilsynsmyndighet, som er regulert i loven kapittel 3, og har justert overskriften i tråd med dette.

Når det gjelder utvalgets forslag til § 11-1 andre ledd er dette en videreføring av gjeldende sikkerhetslov § 30 andre ledd, som gir Kongen myndighet til å etablere andre kontroll- og tilsynsordninger enn den ordning som gjelder for EOS-utvalget og som er omtalt i bestemmelsens første ledd. I forarbeidene til gjeldende sikkerhetslov, Ot. prp. nr. 49 (1996–97) heter det at det er påkrevet med en lovhjemmel for de tilfeller det er aktuelt å etablere særskilte kontrollordninger for virksomheter som ikke ligger under regjeringens alminnelige instruksjonsmyndighet, som for eksempel overfor kommunene (utover den tilsynsmyndighet som allerede i loven er tillagt NSM). Det har siden sikkerhetslovens ikrafttreden i 2001 aldri vært aktuelt å etablere slike særskilte kontrollordninger, verken overfor kommunene eller andre virksomheter som er underlagt loven. Departementet som overordnet organ fører i dag tilsyn med NSM, og NSM fører tilsyn med virksomheter underlagt loven, inkludert kommunene. Å ha kontrollordninger utover dette, antas det ikke å være behov for. Departementet foreslår derfor å sløyfe denne del av forslaget til bestemmelse om særlige kontroll- og tilsynsordninger.

16 Ikrafttredelse

Loven trer i kraft fra det tidspunktet Kongen bestemmer, jf. § 12-1 første punktum.

På samme måte som gjeldende sikkerhetslov er forslaget en rammelov som forutsetter at det blir utarbeidet nærmere forskrifter, for å få på plass et regelverk som skal gjøre det mulig å praktisere loven og dens intensjoner på en god måte.

Til gjeldende sikkerhetslov er det gitt forskrifter om henholdsvis personellsikkerhet, sikkerhetsadministrasjon, informasjonssikkerhet, sikkerhetsgraderte anskaffelser og objektsikkerhet. Loven trådte først i kraft etter at de fleste av disse forskriftene ble fastsatt.

Også når det gjelder forslaget til ny lov, er det behov for å utarbeide en rekke forskrifter før loven kan ta til å gjelde. Det vil derfor ta tid før loven kan tre i kraft etter at et lovforslag er vedtatt av Stortinget. Imidlertid bør det være åpning for en suksessiv prosess, slik at deler av loven kan tre i kraft på ulike tidspunkter. I § 12-1 andre punktum er det lagt inn en hjemmel for Kongen til å sette i kraft forskjellige bestemmelser til ulik tid.

Fra det tidspunkt som ny lov trer i kraft, vil gjeldende lov bli opphevet, jf. § 12-2. Det vil være behov for å foreta endringer i andre lover som følge av ny lov om nasjonal sikkerhet. Eksempler på slike lover er straffeloven og straffeprosessloven, politiloven, politiregisterloven, domstolsloven og plan- og bygningsloven. Slike endringsforslag vil bli fulgt opp i en tilleggsproposisjon før loven kan tre i kraft. Enkelte bestemmelser kan likevel tre i kraft på et tidligere tidspunkt, dersom det ikke er behov for endringer i andre lover eller behov for endringer i underliggende forskrifter.

17 Kompensatoriske ordninger

17.1 Gjeldende rett

Det finnes i dag ingen kompensatoriske ordninger for virksomheter som er underlagt loven, og som påføres kostnader for å oppfylle lovens krav. Hovedregelen er at virksomhetene selv dekker disse kostnadene.

Av forskrift om objektsikkerhet § 4-1 andre ledd framgår det imidlertid at:

> «Objekteier kan i særlige tilfeller søke om dispensasjon fra sikkerhetstiltak der dette anses forsvarlig».

Bestemmelsen åpner for at det i noen få tilfeller vil være mulig å redusere omfanget av de krav og tilhørende kostnader som oppstilles i forskriften. Av forskrift om sikkerhetsgraderte anskaffelser § 6-2 framgår videre at leverandøren som utgangspunkt skal dekke kostnader forbundet med å oppfylle lovens krav, men at det kan avtales annerledes mellom anskaffende myndighet og leverandøren.

17.2 Utvalgets forslag

Utvalget har i NOU 2016: 19 kapittel 6.7.6, side 118–119, vurdert behovet for kompensatoriske tiltak. Utvalget uttaler at:

> «I enkelte tilfeller vil det ut fra samfunnsøkonomiske betraktninger kunne være behov for å pålegge omfattende sikkerhetstiltak for en spesifikk virksomhet eller innenfor en hel samfunnssektor. Et eksempel kan være en konkret virksomhet som er av helt avgjørende betydning for en eller flere grunnleggende nasjonale funksjoner. Dersom slike pålegg medfører uforholdsmessig stor belastning for den aktuelle virksomhet eller sektor sett i forhold til den egenverdi tiltakene har for virksomheten/sektoren, kan det være behov for kompensatoriske tiltak.»

Utvalget viser til at økonomiske insentiver er blant de virkemidlene staten har tilgjengelig for å oppnå god nasjonal sikkerhet. Utvalget ser det imidlertid ikke som formålstjenlig «å spesifisere eventuelle kompensatoriske tiltak i loven» og påpeker videre at

> «[h]vis slike pålegg skulle bli nødvendig, mener utvalget at dette så langt som mulig bør søkes løst gjennom tett dialog mellom sikkerhetsmyndighetene, aktuelle sektormyndigheter og berørte virksomheter.»

17.3 Høringsinstansenes syn

Næringslivets sikkerhetsråd (NSR) har uttalt at:

> «NSR har tidligere påpekt (høringssvar til objekt sikkerhetsforskriften) at private virksomheter selv må ta kostnaden for å sikre sine kommersielle verdier. Dersom samfunnet har behov for sikring utover det, bør også samfunnet betale for det. Utvalget skriver at kostnadene ved sikringstiltak etter loven skal stå i et rimelig forhold til det som oppnås ved tiltaket. De skriver videre at «Bruk av økonomisk insentiver, eller andre kompensatoriske tiltak, kan da tenkes å være aktuelle virkemidler for å avbøte en uforholdsmessig stor økonomisk belastning for den enkelte virksomhet». NSR er av den oppfatning at virksomheter som underlegges sikkerhetsloven, og spesielt etter pålegg, må gis økonomisk støtte til pålagte sikringstiltak. Statlig økonomisk støtte vil være den beste måten å sikre at alle som bør ha et forsvarlig sikkerhetsnivå etter loven har det, og at tiltakene står i et rimelig forhold til det som oppnås ved tiltaket.»

Abelia har videre uttalt seg om kostnader for næringslivet som en følge av ny lov

> «(...) utvalget påpeker selv i punkt 6.7.1 at med det nye forslaget til virkeområde for loven, vil flere virksomheter bli underlagt den nye sikkerhetsloven. Videre heter det at det for; virksomheter som tidligere ikke har vært underlagt sikkerhetsloven, vil en slik underleggelse

kunne få vesentlige konsekvenser. Dette innebærer økte kostnader som kan virke tyngende for den enkelte bedrift, men utvalget mener de «...sikkerhetsmessige gevinstene i et samfunnsperspektiv overstiger de ulempene en utvidelse av lovens virkeområde vil kunne få for enkelte virksomheter». Spørsmålet blir da hvor stor andel av kostnadene for det samfunnsmessige perspektivet det er rimelig at hver enkelt bedrift skal bære byrden av. Dette er altså kostnader virksomheter blir pålagt, som går ut over de åpenbare kostnadene, sett fra et kommersielt ståsted og disse må finansieres av markedet. Mulige løsninger kan være kostnadsdifferensiering i henhold til størrelse og omsetning i bedriften. En form for kompensasjon kan være en annen. Slike løsninger bør utredes nærmere.»

Direktoratet for forvaltning og IKT (Difi) har videre uttalt at:

«Utredningen tar opp spørsmålet om behov for å pålegge omfattende sikkerhetstiltak kan medføre en uforholdsmessig stor økonomisk belastning for den enkelte virksomhet. I utredningens kapittel 6.7.6 har ikke utvalget sett det som formålstjenlig å spesifisere eventuelle kompensatoriske tiltak i loven. Utvalget mener spørsmål om kompensasjon så langt som mulig bør søkes løst gjennom tett dialog mellom sikkerhetsmyndighetene, aktuelle sektormyndigheter og berørte virksomheter. Difi vil påpeke at dette er spørsmål hvor det vil være behov for å utrede hvordan slike pålegg og eventuelle kompensatoriske tiltak vil forholde seg til regelverket om offentlige anskaffelser.»

17.4 Departementets vurdering

Departementet finner i likhet med utvalget at det ikke er formålstjenlig å spesifisere eventuelle kompensatoriske ordninger i loven. Med kompensatoriske ordninger mener departementet økonomiske insentiver eller andre økonomiske tiltak. Departementet er av den oppfatning at mekanismene i loven i tilstrekkelig grad sikrer at forsvarlig sikkerhetsnivå opprettholdes hos virksomhetene, uavhengig av eventuelle kompensatoriske ordninger. Utgangspunktet er at den enkelte virksomhet selv må dekke kostnadene for sikkerhetstiltak. Dersom disse kostnadene i enkelte tilfeller skulle bli uforholdsmessig store, kan det unntaksvis være aktuelt med økonomiske initiativer eller kompensatoriske tiltak for å sørge for å oppnå et forsvarlig sikkerhetsnivå.

Departementet vil vurdere om det er behov for eventuelle kompensatoriske ordninger i det videre arbeidet med gjennomføring av sikkerhetsloven. Det presiseres imidlertid at eventuelle økte utgifter tilknyttet kompensatoriske ordninger må dekkes innenfor den enkelte samfunnssektor.

I den sammenheng vil også forslaget om en klar hjemmel for å kunne kreve gebyr, jf. Prop. 97 L (2015–2016) kapittel 5, bli vurdert.

Når det gjelder innspillet fra *Difi*, bemerker departementet at dersom kompensatoriske tiltak skulle bli aktuelt, vil forholdet til EØS-regelverket måtte vurderes konkret i det enkelte tilfelle.

18 Økonomiske og administrative konsekvenser

Reguleringen av forebyggende nasjonalt sikkerhetsarbeid har som formål å øke sikkerheten i samfunnet. Regelverket oppstiller krav om forebyggende sikkerhetstiltak som hovedsakelig er rettet mot å redusere sårbarhetene i samfunnet. Sikkerhet og sikringstiltak kan være kostnadskrevende, men manglende sikkerhet kan få svært store samfunnsmessige og økonomiske konsekvenser.

Forslaget til ny sikkerhetslov vil medføre en begrenset utvidelse av lovens virkeområde. Forslaget vil kunne innebære at både nye virksomheter, og større deler av allerede underlagte virksomheters infrastruktur og systemer, blir underlagt lovens bestemmelser. Dette er en følge av at ny lov vil gjelde objekter og infrastruktur av avgjørende betydning for grunnleggende nasjonale funksjoner, som er en utvidelse fra dagens regulering av skjermingsverdige objekter. Det er også en følge av at loven vil omfatte informasjonssystemer som behandler annen skjermingsverdig informasjon, eller som i seg selv er av avgjørende betydning for grunnleggende nasjonale funksjoner, og således ikke er begrenset til gradert informasjon eller graderte informasjonssystemer.

Lovforslaget vil som en følge av ovennevnte medføre økonomiske og administrative konsekvenser. Forslaget har imidlertid som formål å sikre en kostnadseffektiv regulering av forebyggende sikkerhetstiltak. Kostnader til sikkerhetstiltak skal ikke gå lenger enn det som er nødvendig for å sikre et forsvarlig sikkerhetsnivå i de virksomhetene som underlegges loven. Loven legger opp til at det i utgangspunktet er sektormyndighetene, som har kunnskap om egen sektor, som skal legge føringer for hva som er forsvarlig sikkerhet. Dette gir et mulighetsrom for å finne hensiktsmessige og tilpassede løsninger, også i et økonomisk perspektiv. Det legges også opp til at den enkelte virksomheten i sin vurdering av hvilke sikkerhetstiltak som er nødvendige for å opprettholde et forsvarlig sikkerhetsnivå, må vurdere hva som er akseptabel restrisiko holdt opp mot kostnaden ved tiltakene.

Siden tilsynsmyndighet vil kunne legges til myndigheter med sektoransvar, vil det i den utstrekning loven kommer til anvendelse i den enkelte sektor, også kunne innebære ekstra oppgaver og utgifter for sektormyndighetene. Det vil eksempelvis kunne påløpe utgifter knyttet til behov for personell og kompetanse i de ulike sektormyndighetene. Omfanget av nye oppgaver vil avhenge av sikringsnivået som allerede er etablert i den enkelte sektor. Utvidelsen av virkeområdet, og utøvelsen av rollen som sikkerhetsmyndighet, vil også medføre økte utgifter for Nasjonal sikkerhetsmyndighet (NSM).

For de virksomhetene som underlegges loven, vil det påløpe øvrige administrative kostnader, blant annet knyttet til sikkerhetsadministrasjon og personellsikkerhet. Eksempelvis vil kravet om rapportering fra myndigheter med tilsynsansvar til sikkerhetsmyndigheten innebære at det må etableres nye administrative rutiner.

Nedenfor følger en nærmere beskrivelse av forslagets antatte administrative og økonomiske konsekvenser.

18.1 Utvidelsen av virkeområdet

Det er ikke 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. De fleste nye virksomhetene som vil omfattes av loven, vil være i sivil sektor. De økonomiske konsekvensene dette medfører vil imidlertid variere, og må vurderes konkret i hvert enkelt tilfelle.

Utgangspunktet er, som i dag, at det er den enkelte virksomheten som må finansiere utgiftene forbundet med forebyggende sikkerhetstiltak, og at kostnadene dekkes innenfor den enkelte samfunnssektor.

Forsvarsdepartementet har mottatt innspill til vurderinger av økonomiske og administrative konsekvenser fra Arbeids- og sosialdepartementet, Finansdepartementet, Helse- og omsorgsdepartementet, Kommunal- og moderniseringsdepartementet, Justis- og beredskapsdepartementet, Nærings- og fiskeridepartementet, Olje og energi-

departement, Samferdselsdepartementet og Utenriksdepartementet.

Alle de nevnte departementene har kommet til at lovforslaget vil medføre merutgifter, men at det ikke er mulig å gi et konkret anslag av størrelsen på de økonomiske konsekvensene av forslaget. Dette skyldes i hovedsak, som nevnt over, at det ikke vil være mulig å anslå utgiftene før departementene har vurdert hvilke virksomheter som skal omfattes av loven. Det skyldes også at lovforslaget forutsetter et omfattende forskriftsarbeid, og at kravene virksomhetene må forholde seg til ikke vil være endelig fastlagt før dette arbeidet er gjennomført. I tillegg vil det være av betydning hvor mange myndigheter med sektoransvar som vil føre tilsyn etter loven. Også unntaksbestemmelsene i lovforslaget, §§ 1-2, 5-2 og 6-2, bidrar til usikkerhet med hensyn til å kunne vurdere de konkrete konsekvensene av lovforslaget. Det er spesielt i forbindelse med sikring av skjermingsverdige objekter og infrastruktur, informasjons- og informasjonssystemsikkerhet og økte administrative oppgaver at departementene vurderer at det vil oppstå et merbehov.

Eksempelvis anslås det i kraftsektoren at utgifter som følge av lovforslaget først og fremst vil komme i tilknytning til håndtering av gradert informasjon og sikkerhetsgraderte anskaffelser. Det kan imidlertid også påløpe kostnader til fysisk sikring, forutsatt at det vurderes som nødvendig med en økning av eksisterende sikringsnivå.

I justissektoren anslås det at det kan komme økte utgifter i forbindelse med at flere virksomheter enn i dag faller inn under loven. I tillegg vil antakelig den økte aktivitetsplikten for departementet og virksomhetene, utvidelsen til å omfatte skjermingsverdige informasjonssystemer, utvidelsen innen objekt- og infrastruktursikkerhet og adgangsklarering gi merutgifter.

I forsvarssektoren er det særlig forslaget om beskyttelse av skjermingsverdige, men ugraderte, informasjonssystemer som vil kunne medføre økte utgifter. For Nasjonal sikkerhetsmyndighet (NSM) vil særlig opplæring og tilsyn føre til merutgifter, se kapittel 18.5 nedenfor.

På bakgrunn av innspillene over er den begrensede utvidelsen av lovens virkeområde forsøkt klargjort i lovarbeidet. Det er også tatt inn forskriftshjemler i §§ 5-2 og 6-2 om informasjonssikkerhet og informasjonssystemsikkerhet, hvor det i særlige tilfeller kan gjøres unntak fra hovedregelen om gjennomføring av sikkerhetstiltak. Etter departementets syn vil de justeringene som er gjort, sammenholdt med fleksibilitet knyttet til gjennomføringen av sikkerhetstiltak, kunne redusere de økonomiske konsekvensene av loven.

18.2 Informasjonssikkerhet, informasjonssystemsikkerhet og objekt- og infrastruktursikkerhet

Flere systemer, objekter og infrastrukturer vil bli underlagt loven som følge av at virkeområdet utvides. Det må forventes at dette medfører økte utgifter til sikkerhetstiltak, og til administrative og organisatoriske tiltak, spesielt for sivile virksomheter.

Etter departementets vurdering vil tekniske tiltak for skjerming av ulike former for informasjon i systemer og infrastrukturer stå for en merutgift. Hvor stor merutgiften vil bli, er imidlertid forbundet med stor usikkerhet. Det hevdes i flere innspill til lovarbeidet at det allerede i dag er etablert en god grunnsikkerhet i mange infrastrukturer. I hvor stor grad den nye loven vil kreve en økning av sikkerheten, er dermed vanskelig å anslå før loven er trådt i kraft og har tatt til å virke. Det understrekes at lovens bestemmelser på dette området legger til grunn risikobaserte vurderinger ved bestemmelse av hvilke sikkerhetstiltak som er nødvendige.

Som følge av lovens utvidede virkeområde vil det også måtte forventes økte utgifter til beskyttelse av et større antall fysiske objekter enn i dag. Omfanget av kostnadene vil imidlertid være avhengig av eksisterende sikkerhetstiltak i virksomheten og behovet for nye sikkerhetstiltak. Videre vil bestemmelsene om beskyttelse av infrastruktur medføre utgifter til ulike typer sikkerhetstiltak og til økt kompetanse i forvaltningen og vedlikeholdet av tiltakene.

18.3 Personellsikkerhet

Hjemmelen for adgangsklarering til skjermingsverdige objekter og infrastruktur vil øke antall klareringssaker for klareringsmyndighetene. For å kunne gjennomføre en effektiv klareringsprosess vil det være behov for en økning av personellressurser som skal behandle disse sakene. Det konkrete merbehovet kan imidlertid ikke beregnes før det enkelte departementet har avgjort om det skal settes krav til adgangsklarering, jf. § 8-3. Det må i vurderingen av merbehovet tas høyde for at personer i en rekke stillinger i dag allerede er sikkerhetsklarert, og således ikke vil ha behov for adgangsklarering. Det hører med til denne vurde-

ringen at en adgangsklarering i utgangspunktet skal være en enklere prosess enn en sikkerhetsklarering.

Det foreslås at hovedregelen i klareringssakene bør være en digitalisert overføring av registeropplysninger til sikkerhetsmyndigheten fra behandlingsansvarlige i registrene. Det vil påløpe investeringskostnader med å få etablert sikre kommunikasjonslinjer mellom sikkerhetsmyndigheten og de aktuelle registereierne som i dag ikke har slike kommunikasjonslinjer med sikkerhetsmyndigheten, samt å tilrettelegge de aktuelle registrene for en slik overføring. På lengre sikt vil imidlertid forslaget sannsynligvis innebære en effektivisering og redusert ressursbruk knyttet til behandling av denne type saker, både hos sikkerhetsmyndigheten og de aktuelle registereierne.

I tillegg legger forslaget til § 8-9 opp til at sikkerhetsmyndigheten skal kunne kreve rapport fra autorisasjonsansvarlige om hvilket personell som har blitt autorisert i den enkelte virksomhet, slik at opplysninger om dette kan legges inn i det sentrale klareringsregisteret. I den utstrekning sikkerhetsmyndigheten krever dette, vil det medføre administrative kostnader for den enkelte virksomheten.

18.4 Eierskapskontroll

De konkrete økonomiske konsekvensene av forslaget om eierskapskontroll er vanskelige å fastslå før det er bestemt hvilke virksomheter som underlegges loven. Departementet er imidlertid av den oppfatning at eventuelle uheldige konsekvenser for investeringslysten i, og konkurransekraften til, norske virksomheter vil være begrensede. Det vises til at terskelen for at bestemmelsene kommer til anvendelse er høy, og at bestemmelsene er utformet med tanke på at det skal være forutsigbart for virksomhetene når disse kommer til anvendelse, og hvilke saksbehandlingsregler som da gjelder. Før vedtakskompetansen i § 10-3 benyttes, skal det dessuten foretas en forholdsmessighetsvurdering av negative konsekvenser for virksomhetene og erververen, holdt opp mot hensynet til nasjonale sikkerhetsinteresser. I de tilfellene hvor vedtakskompetansen benyttes, forutsettes det at hensynet til nasjonale sikkerhetsinteresser veier tyngre enn de negative økonomiske konsekvensene for virksomhetene og erververen.

18.5 Sikkerhetsmyndigheten

Sikkerhetsmyndigheten er i dag Nasjonal sikkerhetsmyndighet (NSM). I henhold til Kronprinsregentens resolusjon av 4. juli 2003 og Kongelig resolusjon av 22. mars 2013 er NSM et direktorat administrativt underlagt Forsvarsdepartementet. Justis- og beredskapsdepartementet har imidlertid et overordnet ansvar og et samordningsansvar for forebyggende sikkerhetsarbeid i sivil sektor og skal innvirke på prosess og resultat i styringen av NSM. NSM har en faglig rapporteringslinje til Justis- og beredskapsdepartementet for saker som gjelder sivil sektor.

Forslaget får konsekvenser for NSMs ansvarsområde og vil medføre behov for økte personellressurser og potensielt et tilhørende behov for utvidelse av bygningsmassen. Følgende endringer vil i hovedsak kunne få betydning for hvor stort det samlede merbehovet til NSM vil bli:

- Utvidelse av lovens virkeområde
- Utvidelse av objektsikkerhetsregelverket fra skjermingsverdig objekt til også å omhandle skjermingsverdig infrastruktur.
- Utvidelse av virkeområdet til også å gjelde informasjonssystemer som ikke behandler sikkerhetsgradert informasjon, men som behandler annen skjermingsverdig informasjon eller som i seg selv er av avgjørende betydning for grunnleggende nasjonale funksjoner.
- Økning i antallet potensielle råd- og veiledningsobjekter. Antallet objekter NSM skal føre tilsyn med, vil avhenge av hvor mange sektormyndigheter som vil bli tildelt tilsynsansvar innen sin sektor. Videre vil antallet kontrollobjekter øke, i tillegg til at et økt antall virksomheter under sikkerhetsloven vil kunne medføre økt behov, og muligheter for, utplassering av sensorer i varslingssystemet for digital infrastruktur.
- Rapportering fra de autorisasjonsansvarlige til NSM om hvilket personell som har blitt autorisert i den enkelte virksomhet for at opplysninger om dette kan legges inn i det sentrale klareringsregisteret, og anmodninger fra Politiets sikkerhetstjeneste vedrørende dette.

NSM har estimert det økonomiske merbehovet som følge av ny sikkerhetslov til å være i et spenn fra om lag 25 mill. kroner til i underkant av 105 mill. kroner i 2017-kroner. Middelsestimatet gir et netto merbehov for NSM på om lag 60 mill. kroner i 2017-kroner. Sistnevnte tilsvarer en budsjettøkning på 27,5 prosent, sammenholdt med regnskapet for 2016. Estimatene avhenger, som nevnt

over, blant annet av hvor mange og hvilke virksomheter som blir omfattet av loven, hvor mange sektormyndigheter som vil bli tildelt tilsynsansvar innen sin sektor, antall tilsynsobjekter og omfanget av råd og veiledningsarbeidet.

Som et sentralt element i langtidsplanen for den videre utviklingen av forsvarssektoren, jf. Innst. 62 S (2016–2017) til Prop. 151 S (2016–2017), er det lagt opp til en større budsjettramme for NSM, for å styrke det forebyggede sikkerhetsarbeidet som et sentralt ledd i å øke Forsvarets operative evne og for å forbedre sikkerheten i samfunnet for øvrig. Langtidsplanen tar særlig sikte på å forbedre NSMs evne til, og mulighet for, IKT-tilsyn, håndtering av IKT-angrep, råd og veiledning og til å ivareta fagmyndighetsrollen innenfor personellsikkerhet.

Økt behov for økonomiske ressurser til NSM som følge av ny sikkerhetslov vil komme i tillegg til de allerede planlagte økningene som følger av Stortingets tilslutning til langtidsplanen for forsvarssektoren for perioden 2017–2020. Det økonomiske merbehovet for NSM vil måtte avklares nærmere i forbindelse med det videre forskrifts- og veiledningsarbeidet. Det antas i utgangspunktet at hoveddelen av merbehovet først vil realiseres mot slutten av inneværende langtidsplanperiode.

19 Merknader til de enkelte bestemmelsene

19.1 Kapittel 1 Formål og virkeområde

Til § 1-1

Bestemmelsen er en videreføring av det materielle innholdet i utvalgets forslag, men det er gjort språklige og strukturelle endringer.

I *bokstav a* slås det fast at loven skal bidra til å trygge *Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser*. Suverenitet og territoriell integritet skal per definisjon være uavkortet, med de begrensninger og tilpasninger som følger av Norges folkerettslige forpliktelser, herunder EØS-avtalen. Ingen andre land eller organisasjoner skal kunne frata Norge råderett over egne anliggender. Landets øverste statsorganer må ha handlefrihet og kontroll innen norsk territorium. Videre innebærer *suverenitet* evne til å hevde nasjonens interesser internasjonalt ved at Norge fører en selvstendig og egendefinert utenrikspolitikk. En forsvarlig beskyttelse vil være avgjørende for å opprettholde rettsstatens og demokratiets grunnleggende verdier. Det vises for øvrig til beskrivelsen av suverenitet i Meld. St. 32 (2015–2016) (Svalbard-meldingen kapittel 3.1, side 17), der det slås fast at «[s]uverenitet vil si at en stat har eksklusiv råderett over sitt territorium og eksklusiv rett til å utøve myndighet der, f.eks. rett til å vedta og å håndheve lover og andre regler.» *Nasjonale sikkerhetsinteresser* omfatter de tre omtalte og viktigste interessene som framheves i denne bokstaven, i tillegg til kategoriene som oppregnes i legaldefinisjonen av begrepet i § 1-5 nr. 1. Bruken av begrepet *nasjonale sikkerhetsinteresser* i formålsbestemmelsen innebærer en endring sammenliknet med utvalgets lovforslag. Dette er nærmere beskrevet under departementets vurderinger i kapittel 6.4.2.

I *bokstav b* spesifiseres det at loven skal bidra til *å forebygge, avdekke og motvirke sikkerhetstruende virksomhet*. I dette ligger at loven skal fastsette krav til sikkerhetstiltak som skal redusere risikoen for at nasjonale sikkerhetsinteresser rammes av hendelser som skyldes eller er knyttet til sikkerhetstruende virksomhet. Sikkerhetstiltakene skal også redusere skadene eller konsekvensene av slike uønskede hendelser. De nasjonale sikkerhetsinteressene og de grunnleggende nasjonale funksjonene som understøtter dem, hviler på de enkelte virksomhetene som er underlagt loven. Det er dermed i stor grad virksomhetenes sikkerhetstiltak som skal redusere risikoen i forbindelse med uønskede hendelser som følge av eller knyttet til sikkerhetstruende virksomhet. Begrepet *motvirke*, som er brukt i utvalgets forslag, er supplert med *avdekke* og *forebygge* for mer presist å angi hva slags sikkerhetstiltak det kan være tale om og for å dekke flere dimensjoner av etterretnings- og sikkerhetstjenestenes arbeid. For en virksomhet som er underlagt loven, vil tiltakene hovedsakelig dreie seg om å *forebygge* uønskede hendelser knyttet til sikkerhetstruende virksomhet, særlig gjennom å redusere virksomhetens egne sårbarheter. Etterretnings- og sikkerhetstjenestenes arbeid vil i tillegg dreie seg om å *avdekke* og *motvirke* sikkerhetstruende virksomhet.

Begrepet *sikkerhetstruende virksomhet* erstatter utvalgets *tilsiktede uønskede hendelser*. Med sikkerhetstruende virksomhet menes *tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser*, jf. definisjonen i § 1-5 nr. 4. Begrepet er også ment å omfatte hendelser slike handlinger forårsaker. Tilsiktede handlinger som *direkte kan skade* innebærer handlinger der intensjonen er å påføre en eller annen form for skade på nasjonale sikkerhetsinteresser. Dette vil blant annet kunne omfatte sabotasje- eller terroraksjoner der målet er å ramme en viktig samfunnsfunksjon for slik å skade myndighetenes styringsevne eller andre interesser. Med tilsiktede handlinger som *indirekte kan skade* menes handlinger der intensjonen ikke nødvendigvis er å *skade* nasjonale sikkerhetsinteresser, men der konsekvensen eller hendelsen som følger av den tilsiktede handlingen, kan skade sikkerhetsinteressene. Dette vil for eksempel kunne innebære spionasje fra en fremmed stat, der målet ikke først og fremst er å *skade* norske interesser, men snarere å fremme egne interesser. Resultatet av spionasjen kan imidlertid, i en tilspisset situasjon eller

i en forhandlingssituasjon mellom den fremmede staten og Norge, skade norske interesser. I likhet med dagens sikkerhetslov tar loven sikte på å beskytte nasjonale sikkerhetsinteresser mot terrorhandlinger, sabotasje og spionasje. Loven er imidlertid ikke avgrenset til å gjelde for bare disse truslene. Det tas sikte på å beskytte mot alle typer tilsiktede handlinger som kan utgjøre en trussel mot de nasjonale sikkerhetsinteressene. Denne avgrensningen vil i seg selv være styrende for hvilke typer tilsiktede handlinger som vil være aktuelle. Eksempelvis vil annen alvorlig kriminalitet, herunder organisert kriminalitet, også kunne ha store skadefølger for nasjonale sikkerhetsinteresser. Betydningen av *sikkerhetstruende virksomhet* er således noe utvidet sammenliknet med gjeldende sikkerhetslov, jf. definisjonen av begrepet i § 1-5 nr. 4 og beskrivelsen i kapittel 6.4.2.

Virkemidler som er tilgjengelige for å sikre nasjonale sikkerhetsinteresser, kan på samme tid gjøre at de samme interessene og verdiene det tas sikte på å beskytte, kommer under press. Av bestemmelsens *bokstav c* følger det derfor at sikkerhetstiltak som iverksettes for å ivareta lovens formål, skal gjennomføres på en måte som er *i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn*. Med *grunnleggende rettsprinsipper og verdier* menes blant annet hensynet til den enkeltes personvern og rettssikkerhet. I dette ligger en presisering av at det kun er de sikkerhetsmessige tiltakene som er nødvendige og forholdsmessige, og har en dokumentert effekt, som skal iverksettes. Det ligger også en plikt til å vurdere alternative og mindre inngripende tilnærminger for å oppnå samme effekt. Bokstav c er en videreføring av utvalgets forslag til § 1-1 andre ledd.

Til § 1-2

Bestemmelsen er en videreføring av utvalgets forslag, men det er gjort språklige og strukturelle endringer. Enkelte særbestemmelser om virkeområdet er flyttet fra § 1-3 til § 1-2.

I *første ledd* angis at loven gjelder for alle statlige, fylkeskommunale og kommunale organer. Dette er en videreføring av gjeldende sikkerhetslov, der betegnelsen forvaltningsorganer brukes. I forskriftshjemmelen i *fjerde ledd* ligger det også en mulighet for å unnta enkelte statlige, fylkeskommunale eller kommunale organer, slik gjeldende lov § 2 første ledd, fjerde punktum åpner for.

Bestemmelsens *andre ledd* er en videreføring av gjeldende lov § 2 andre ledd om at leverandører til sikkerhetsgraderte anskaffelser automatisk er omfattet av loven. Leddet er flyttet sammenliknet med utvalgets forslag, der det var plassert i § 1-3.

Bestemmelsens *tredje ledd* er i hovedsak en videreføring av gjeldende lov § 2 åttende ledd, med de tilpasninger som er nødvendige i en modernisert lov. Med *bilandene* menes Bouvetøya, Peter I's øy og Dronning Maud Land, jf. lov 27. februar 1930 nr. 3 om Bouvet-øya, Peter I's øy og Dronning Maud Land m.m. (bilandsloven) § 1. Leddet er flyttet sammenliknet med utvalgets forslag, der det var plassert i § 1-3.

Kongen i statsråd er i *fjerde ledd* gitt myndighet til å gi nærmere forskrifter om lovens virkeområde, der det åpnes for å unnta bestemte virksomheter eller visse typer informasjon, informasjonssystemer, objekter og infrastrukturer. Se blant annet kapittel 10.5.2 og 10.5.3 for omtale av bruk av unntakshjemmelen. Myndigheten kan ikke delegeres, jf. den nærmere omtalen av dette i NOU 2016: 19 i kapittel 7.7.10.

Det vises for øvrig til departementets vurderinger i kapittel 6.4.3

Til § 1-3

Bestemmelsen er en videreføring av utvalgets forslag til § 1-2, men begrenser seg til de virksomhetene som ikke faller inn under *lovforslaget* § 1-2. Bestemmelsen viderefører også vedtaksbestemmelsen i utvalgets forslag til § 2-1 første ledd bokstav c og andre ledd.

Virksomhetsbegrepet i loven skal forstås vidt og omfatter alle former for virksomhet, uavhengig av eierskap og organisasjonsform. Ved vurderingen av om en *virksomhet* omfattes, er det uten betydning om det er tale om et privat selskap, et foretak, en forvaltningsbedrift, et hel- eller deleid statlig selskap, et statsforetak, en ideell organisasjon, en stiftelse eller annet.

Bestemmelsens *første ledd* slår fast at departementene innenfor sitt fagområde skal fatte vedtak om at loven skal gjelde for virksomheter som enten *behandler sikkerhetsgradert informasjon* etter *bokstav a*, *råder over informasjon, informasjonssystemer, infrastruktur eller objekter* etter *bokstav b* eller *driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner* etter *bokstav c*. Det må vurderes konkret i det enkelte tilfelle om bare deler av loven skal gjelde for virksomheten, og i så fall hvilke deler av loven. Loven kan eksempelvis gjøres gjeldende innenfor informasjonssikkerhet og personellsikkerhet, dersom det ikke er relevant å ta med informasjonssystemsikkerhet eller objekt- og infrastruktursikkerhet. Det kan også være slik at loven bare skal

gjelde for deler av den aktuelle virksomheten. For eksempel kan deler av infrastrukturen som en virksomhet råder over være skjermingsverdig, mens andre deler ikke er det.

Hvorvidt en virksomhet *råder over* vil måtte avgjøres konkret i hvert enkelt tilfelle, ut fra en vurdering av om virksomheten har en faktisk og reell innflytelse eller påvirkningsmulighet over informasjonen, informasjonssystemet, objektet eller infrastrukturen.

Også virksomheter som *driver aktivitet* av avgjørende betydning for grunnleggende nasjonale funksjoner skal omfattes. Eksempelvis vil selskaper som har en nøkkelkompetanse som er av betydning for slike funksjoner, kunne tenkes å bli omfattet av loven. Normalt vil virksomheter som driver slik aktivitet, også ha en eller annen form for råderett over informasjon, informasjonssystemer, objekter eller infrastruktur, slik at de uansett vil falle inn under lovens virkeområde.

I begrepet *avgjørende for* grunnleggende nasjonale funksjoner ligger et kvalitetskrav. Det er ikke tilstrekkelig at virksomheter leverer innsatsfaktorer for grunnleggende nasjonale funksjoner, for at de skal falle inn under loven. Det er kun de aktørene som har en så sentral rolle for funksjonene at de må anses som avgjørende for evnen til å opprettholde funksjonsdyktighet, som vil omfattes. Vurderingen skal baseres på hvilken betydning bortfall eller svekkelse av virksomheten har for den funksjonen som virksomheten understøtter. Den nærmere vurderingen av hvilke virksomheter som konkret vil falle inn under lovens virkeområde må gjøres konkret, jf. § 2-1.

Etter bestemmelsens *andre ledd* skal virksomhetene varsles før vedtak fattes, jf. forvaltningsloven § 16. Vedtaket kan påklages til Kongen i statsråd.

Sikkerhetsmyndigheten kan etter *tredje ledd* på eget initiativ fremme forslag overfor et departement om å treffe vedtak etter andre ledd. Med *et departement* menes her det ansvarlige fagdepartementet. Dersom slikt vedtak ikke fattes, og sikkerhetsmyndigheten fastholder sin anbefaling, kan sikkerhetsmyndigheten bringe saken inn for endelig avgjørelse til det departementet som har det overordnede ansvaret for forebyggende sikkerhetsarbeid i sivil sektor, eller det departementet som har det overordnede ansvaret for forebyggende sikkerhetsarbeid i forsvarssektoren. Per i dag følger dette av kronprinsregentens resolusjon 4. juli 2003 om fordeling av ansvar for forebyggende sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet (Justis- og beredskapsdepartementet i sivil sektor og Forsvarsdepartementet i forsvarssektoren).

Etter *fjerde ledd* skal sikkerhetsmyndigheten treffe vedtak etter første ledd overfor virksomheter som ikke anses å falle inn under et departements ansvarsområde. Dette skal fange opp virksomheter som ikke naturlig tilhører en bestemt samfunnssektor. Ett eksempel kan være satelittbaserte tjenester, se nærmere NOU 2016: 19 kapittel 7.4.8.Vedtak kan påklages til departementet, som her skal forstås på samme måte som i tredje ledd andre punktum.

Til § 1-4

Bestemmelsen er en videreføring av utvalgets forslag når det gjelder i hvilken utstrekning loven gjelder for Stortinget, Stortingets organer, regjeringen og domstolene.

I motsetning til gjeldende sikkerhetslov § 2 sjuende ledd gjøres det ikke direkte unntak for Stortinget og dets organer. Bestemmelsens *første ledd* slår i stedet fast at loven gjelder for Stortinget og dets organer i den utstrekning Stortinget bestemmer det. Det forutsettes at Stortinget gjør et formelt vedtak om spørsmålet.

Bestemmelsens *andre ledd* er en videreføring av det vedtatte forslaget i Prop. 97 L (2015–2016) om en lovfesting av en langvarig og fast praksis om at det ikke stilles krav om sikkerhetsklarering og autorisasjon for regjeringens medlemmer og dommere i Høyesterett.

Bestemmelsens *tredje ledd* er en videreføring av gjeldende lov § 2 femte ledd om særregler for sikkerhetsklarering etter domstolloven og straffeprosessloven. Kongen er gitt myndighet til å fastsette ytterligere særregler.

Til § 1-5

Bestemmelsen angir definisjoner av sentrale begreper i loven.

I *nr. 1* defineres *nasjonale sikkerhetsinteresser.* Begrepet er nærmere beskrevet i kapittel 6.4.2. Begrepet er en utvidelse av gjeldende lovs *vitale nasjonale sikkerhetsinteresser* og er brukt for å ramme inn interessene som loven skal beskytte. Bruken av begrepet medfører en språklig endring sammenliknet med utvalgets lovforslag, men er ikke ment å innebære en materiell endring.

Grunnleggende nasjonale funksjoner er definert i *nr. 2*. En funksjon er kun å anse som en grunnleggende nasjonal funksjon dersom den understøtter kategoriene i bokstav a til e i definisjonen av *nasjonale sikkerhetsinteresser,* og et helt eller

delvis bortfall vil kunne få konsekvenser for disse overordnede sikkerhetsinteressene. Begrepet er nærmere beskrevet av utvalget i NOU 2016: 19 kapittel 6.7.2.

I *nr. 3* er begrepet *forebyggende sikkerhetsarbeid* definert. Begrepet tilsvarer i all hovedsak gjeldende lovs *forebyggende sikkerhetstjeneste*. Det vises til beskrivelsen av begrepet i særmerknaden til § 11-1 i NOU 2016: 19.

Begrepet *sikkerhetstruende virksomhet* er definert i *nr. 4*. Begrepet er benyttet i gjeldende lov, men skal forstås videre i departementets lovforslag. Definisjonen, slik den er brukt i departementets lovforslag, er ment å tilsvare utvalgets bruk av *tilsiktede uønskede hendelser*. Begrepet er nærmere beskrevet i kapittel 6.4.2 og i særmerknaden til § 1-1.

Begrepet *nærstående* er definert i *nr. 5* og er nærmere beskrevet i særmerknaden til § 8-5.

19.2 Kapittel 2 Ansvar og myndighet for forebyggende sikkerhetsarbeid

Til § 2-1

Bestemmelsen er utvidet sammenlignet med gjeldende sikkerhetslov § 4 og følger i hovedsak opp utvalgets forslag til § 2-1.

Bestemmelsen etablerer det enkelte departements ansvar for forebyggende sikkerhetsarbeid, og plikten til å identifisere og holde oversikt over grunnleggende nasjonale funksjoner som omfattes av loven og de virksomheter som har en sentral rolle i å understøtte slike funksjoner.

Første ledd slår fast at hvert enkelt fagdepartement er ansvarlig for forebyggende sikkerhetsarbeid innenfor sitt myndighetsområde. Departementenes *ansvarsområde* vil følge den til enhver tid sittende regjerings fordeling av ansvar mellom statsrådene og de ulike departementene. Dette innebærer både at de ansvarlige departementene gis myndighet til å fatte vedtak overfor virksomheter i egen sektor, og et særlig ansvar for å følge opp at det skjer et forsvarlig forebyggende sikkerhetsarbeid i sektoren. Ved endring av departementsstrukturen, må regjeringen ta stilling til mulige konsekvenser for fordeling av ansvarsområder etter loven.

Første ledd bokstav a til *c* slår fast departementenes oppgaver med å identifisere og fatte vedtak overfor de virksomheter som skal omfattes av loven. Det foreslås her en modell som består av tre trinn.

Departementene skal i henhold til *bokstav a,* først identifisere hvilke grunnleggende nasjonale funksjoner som finnes innenfor eget myndighetsområde. Med *holde oversikt over* menes at departementenes identifisering skal være en dynamisk prosess som må oppdateres ved behov.

På bakgrunn av departementenes oversikt over grunnleggende nasjonale funksjoner, plikter departementene etter *bokstav b,* å identifisere og holde oversikt over virksomheter som er av vesentlig betydning for understøttelsen av slike funksjoner.

Det at en virksomhet identifiseres til å være av *vesentlig betydning* innebærer ikke i seg selv at det påhviler virksomheten plikter etter loven. Det er imidlertid viktig at departementene til enhver tid har en oversikt over hvilke innsatsfaktorer de grunnleggende nasjonale funksjonene er avhengige av for å kunne opprettholde sin funksjonalitet. Generelle samfunnsmessige endringer, eller endringer i det gjeldende trusselbildet, kan også medføre at virksomheter som tidligere ikke har blitt ansett til å være av vesentlig betydning, blir det. Systematikken det legges opp til i bestemmelsen er ment å skulle legge til rette for at slike endringer blir fanget opp.

Ut fra den totale oversikten over grunnleggende nasjonale funksjoner og virksomheter av vesentlig betydning for disse, skal departementet treffe enkeltvedtak etter § 1-3.

Etter første ledd *bokstav d* skal departementene melde inn til sikkerhetsmyndigheten oversikter etter bokstavene a og b og vedtak etter § 1-3. På den måten skal sikkerhetsmyndigheten kunne ha en helhetlig nasjonal oversikt over hva som regnes som grunnleggende nasjonale funksjoner, og hvilke virksomheter som loven gjelder for.

I bestemmelsens *andre ledd* foreslås det en hjemmel for Kongen i statsråd til å gi forskrift om departementenes ansvar og myndighet for forebyggende sikkerhetsarbeid.

Til § 2-2

Bestemmelsen er i hovedsak en videreføring av gjeldende sikkerhetslov §§ 8 og 9 og utvalgets forslag til § 2-2.

Bestemmelsen angir sikkerhetsmyndighetens ansvar og myndighet etter loven. I praksis vil funksjonen som sikkerhetsmyndighet ivaretas av den aktøren som blir tildelt myndigheten fra ansvarlig fagdepartement. Ansvaret som tillegges sikkerhetsmyndigheten, er i dag lagt til Nasjonal sikkerhetsmyndighet (NSM). Forslaget innebærer ingen endring av dette.

I *første ledd* slås det fast at sikkerhetsmyndigheten har det sektorovergripende ansvaret for at

forebyggende sikkerhetsarbeid skjer i samsvar med loven. Sikkerhetsmyndighetens ansvar griper ikke inn i de enkelte departementenes ansvar innen eget myndighetsområde. Med *sektorovergripende ansvar* menes i første rekke ansvaret for at forebyggende sikkerhetsarbeid etter loven har en helhetlig tilnærming, og at sikkerhetsarbeidet mellom ulike departementer og ulike relevante sektormyndigheter blir koordinert. Sikkerhetsmyndighetens ansvar og oppgaver er nærmere konkretisert i *andre ledd bokstav a* til *h.*

Etter *bokstav a* plikter sikkerhetsmyndigheten å *påse* at det føres tilsyn med at virksomheter oppfyller krav til forebyggende sikkerhetsarbeid. De nærmere reglene om tilsyn følger av loven kapittel 3.

Bokstav b regulerer ansvaret for å utarbeide og vedlikeholde grunnleggende kriterier for tilsyn. Dette vil være kriterier som både sikkerhetsmyndigheten som tilsynsorgan og myndigheter med tilsynsansvar etter loven, vil måtte etterleve. Dette skal legge til rette for en nasjonal enhetlig tilnærming til tilsyn innen forebyggende sikkerhetsarbeid.

Bokstav c setter en plikt for sikkerhetsmyndigheten til å innhente og vurdere informasjon som har betydning for det forebyggende sikkerhetsarbeidet.

I *bokstav d* reguleres sikkerhetsmyndighetens råd- og veiledningsansvar etter loven. Sikkerhetsmyndigheten skal ha en aktiv rolle når det gjelder konkret rådgivning overfor virksomhetene. Av ressursmessige og praktiske grunner forutsetter departementet at slik rådgivning fortrinnsvis gis gjennom generelle veiledere og felles kursopplegg o.l.

Bokstav e regulerer sikkerhetsmyndighetens plikt til å holde oversikt over de funksjoner og virksomheter som departementene har identifisert etter § 2-1, mens *bokstav f* angir plikten til å holde oversikt over de virksomheter som departementene og sikkerhetsmyndigheten har fattet vedtak om etter § 1-3. Sikkerhetsmyndighetens plikt innebærer å holde en tverrsektoriell og nasjonal oversikt over de funksjoner og virksomheter som er blitt identifisert av departementene. Plikten til å holde en slik oversikt er en sentral del av sikkerhetsmyndighetens sektorovergripende ansvar, og vil også danne grunnlaget for sikkerhetsmyndighetens forslagsrett overfor departementene når det gjelder virksomheter som bør underlegges loven jf. § 1-3 tredje ledd.

Den tverrsektorielle oversikten innbefatter også et særskilt ansvar for å identifisere gjensidige avhengigheter på tvers av samfunnssektorer og på tvers av virksomheter, slik at denne type avhengigheter kan synliggjøres overfor de ansvarlige departementene. Oversikten vil også bidra til å identifisere virksomheter som ikke faller naturlig inn under et departements ansvarsområde.

Bokstav g gir sikkerhetsmyndigheten plikt til å legge til rette for informasjonsdeling etter § 2-3, mens *bokstav h* setter krav til sikkerhetsmyndigheten for å bidra til utviklingen av sikkerhetstiltak, og til fastsettelse av krav til forebyggende sikkerhetsarbeid.

I *tredje ledd* framgår at sikkerhetsmyndigheten er nasjonal fagmyndighet overfor andre land og internasjonale organisasjoner. I denne funksjonen skal sikkerhetsmyndigheten ha nødvendig internasjonalt samarbeid innen forebyggende sikkerhetsarbeid. Med *fagmyndighet overfor andre land og internasjonale organisasjoner* menes at sikkerhetsmyndigheten skal være utøvende organ og ivareta Norges sikkerhetsforpliktelser internasjonalt – herunder de sikkerhetsfunksjoner NATO forutsetter at Norge har etablert. Disse internasjonale forpliktelsene er ikke til hinder for at sektormyndigheter kan ha et internasjonalt samarbeid innen sine fagfelt.

I *fjerde ledd* gis sikkerhetsmyndigheten en rett til uhindret adgang til skjermingsverdig objekt, infrastruktur, informasjonssystem eller informasjon, så langt dette er nødvendig for å gjennomføre oppgavene i eller i medhold av loven.

I *femte ledd* gis Kongen hjemmel til i forskrift å gi utfyllende bestemmelser om sikkerhetsmyndighetens ansvar for forebyggende sikkerhetsarbeid.

Til § 2-3

Bestemmelsen omhandler sikkerhetsmyndighetens ansvar for å legge til rette for utveksling av informasjon om trusselvurderinger. At bestemmelsen er innrettet som en tilretteleggingsplikt, skyldes primært at sikkerhetsmyndigheten ikke vil ha full råderett over all trussel- og sikkerhetsinformasjon. For informasjon som utarbeides av andre relevante aktører, som Politiets sikkerhetstjeneste og Etterretningstjenesten, vil det i siste instans være opp til disse tjenestene hvorvidt de har anledning til å dele denne informasjonen. All informasjonsutveksling etter denne bestemmelsen må skje innenfor rammene av lovbestemt taushetsplikt og innenfor rammene av den enkelte aktørs lovmessige adgang til å dele slik informasjon. Det vises for øvrig til departementets vurderinger når det gjelder virksomhetenes ansvar for å

dele sikkerhetsrelevant informasjon, se kapittel 7.4.3.

Etter *første ledd* plikter sikkerhetsmyndigheten å legge til rette for at virksomheter som loven gjelder for, får tilgang til informasjon om trusselvurderinger og andre opplysninger som er av betydning for virksomhetenes forebyggende sikkerhetsarbeid, som for eksempel virksomhetenes plikt til å foreta en vurdering av risiko, jf. § 4-2.

Etter *andre ledd* skal sikkerhetsmyndigheten påse at det etableres nødvendige arenaer for informasjons- og erfaringsutveksling, i samråd med sektormyndigheter og andre relevante myndigheter. Antakelig kan mye av tilretteleggingsansvaret nevnt i første ledd ivaretas gjennom etablering av slike arenaer eller felles arrangementer med øvrige relevante myndigheter.

I *tredje ledd* gis det hjemmel for Kongen til å gi forskrift om utveksling av trusselvurderinger og annen sikkerhetsinformasjon.

Til § 2-4

Bestemmelsen er en videreføring av gjeldende sikkerhetslov § 9 første ledd bokstav e og § 10 a, med enkelte språklige endringer.

Etter *første ledd* skal Kongen utpeke en myndighet som skal drive en nasjonal responsfunksjon for digitale angrep og et nasjonalt varslingssystem for digital infrastruktur. Både responsfunksjonen og varslingssystemet har et bredere nedslagsfelt enn sikkerhetslovens virkeområde. Funksjonene har likevel så sterk tilknytning til nasjonalt forebyggende sikkerhetsarbeid, at lovfesting av funksjonene passer best i reguleringen av dette. Det vises til departementets vurderinger i kapittel 7.4.4.

Andre ledd gir myndigheten som skal drive den nasjonale responsfunksjonen og det nasjonale varslingssystemet for digital infrastruktur, hjemmel til å behandle personopplysninger i ulike former *når det er nødvendig for å utføre oppgavene etter første ledd*. Opplysningene kan være i form av metadata om IKT-trafikk, informasjon som er nødvendig for å analysere utløste alarmer, IP-adresser mottatt fra samarbeidspartnere, eller logger og infisert maskinvare når det er nødvendig for å bistå en virksomhet med å håndtere alvorlige digitale angrep, så framt virksomheten samtykker til det, jf. bokstavene a til d.

Tredje ledd åpner for at myndigheten også kan behandle personopplysninger i andre tilfeller når det er *strengt nødvendig for å utføre oppgavene etter første ledd*.

Bestemmelsen er ikke ment å innebære noen materiell endring fra fra gjeldende sikkerhetslov § 9 første ledd bokstav e og § 10 a, jf. Innst. 352 S (2015–2016) til Prop. 97 L (2015–2016).

Til § 2-5

Bestemmelsen er i hovedsak en videreføring av gjeldende sikkerhetslov § 5 a og utvalgets lovforslag § 2-5. Departementet har imidlertid ikke fulgt utvalgets forslag til terskel, *stor grad av sannsynlighet* for skade, for at Kongen i statsråd kan fatte vedtak, men beholdt gjeldende retts *ikke ubetydelig risiko*. *Første ledd* gir Kongen i statsråd kompetanse til å fatte vedtak for å hindre en planlagt eller pågående aktivitet som kan innebære en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet.

Begrepet *aktivitet* favner vidt. Både iøynefallende aktiviteter som f.eks. oppføring av bygninger eller utplassering av antenner, og mindre synlige aktiviteter, som f.eks. planer om utbygging, ferdsel i et område eller oppkjøp av virksomheter, omfattes av begrepet. Hva gjelder oppkjøp av virksomheter, vil bestemmelsen kunne være et supplement til loven kapittel 10 om eierskapskontroll, eksempelvis der den aktuelle virksomheten det planlegges oppkjøp av ikke er underlagt loven ved enkeltvedtak. Vedtaksmyndigheten omfatter aktiviteter som er *planlagt eller pågående*, noe som innebærer at den også gjelder aktiviteter som ennå ikke har materialisert seg, men hvor det f.eks. er mottatt en søknad. Dette er viktig for å sikre at potensiell aktivitet som innebærer en risiko kan bli stanset før virksomheten faktisk blir etablert eller gjennomført. Hvilke typer aktivitet bestemmelsen er ment å ramme er verken mulig eller hensiktsmessig å angi nærmere konkret. Bestemmelsen er ment å være en sikkerhetsventil for å kunne hindre enhver aktivitet, uavhengig av hvordan disse materialiserer seg. Det avgjørende vil være hvorvidt aktiviteten har potensial til å innebære en *ikke ubetydelig risiko* mot nasjonale sikkerhetsinteresser. Det er ikke krav om at aktiviteten må rette seg direkte mot virksomheter som er omfattet av loven. Også aktivitet som mer indirekte eller avledet innebærer en ikke ubetydelig risiko mot nasjonale sikkerhetsinteresser, vil etter forholdene kunne omfattes av bestemmelsen.

Bestemmelsen stiller ikke krav om at det må foreligge en viss bestemt sannsynlighet for at aktiviteten vil innebære en risiko mot nasjonale sikkerhetsinteresser dersom den etableres eller gjennomføres. At aktiviteten skal kunne medføre

en *ikke ubetydelig risiko*, innebærer derimot at vedtaksmyndigheten ikke inntrer hvis dette framstår som usannsynlig, eller det kun er en teoretisk mulighet for det. Terskelen for sannsynlighet må ellers ses i sammenheng med de mulige konsekvensene av den aktuelle aktiviteten. Dersom konsekvensen for nasjonale sikkerhetsinteresser kan bli katastrofal, vil også terskelen for når det fattes vedtak bli lav. Motsatt vil terskelen kunne heves dersom konsekvensen av den aktuelle aktiviteten regnes som liten.

Begrepet *nasjonale sikkerhetsinteresser* skal forstås på samme måte som i § 1-1.

Bestemmelsen gir Kongen i statsråd hjemmel til å fatte *nødvendige vedtak*. Hvilke vedtak Kongen i statsråd kan fatte med hjemmel i første ledd, vil avhenge av hvilken type aktivitet det tas sikte på å hindre. Heller ikke for *vedtak* vil det være mulig eller hensiktsmessig å gi en opplisting av hvilke typer vedtak Kongen i statsråd kan fatte med hjemmel i bestemmelsen, ut over at de må være egnet til å kunne hindre den aktuelle aktiviteten. At vedtaket skal være *nødvendig* innebærer imidlertid at Kongen i statsråd ikke skal fatte mer byrdefulle vedtak enn det som er påkrevd, og som vurderes som rimelig i den konkrete saken. Bestemmelsen vil som nevnt over være en sikkerhetsventil, og den forutsettes benyttet kun i helt spesielle tilfeller. Kompetansen til å fatte vedtak er lagt til Kongen i statsråd, og den kan ikke delegeres. Departementet legger til grunn at det vil være tale om et lite antall saker, og at disse sakene etter sin art vil være alvorlige og spesielle, jf. også formålet med sikkerhetsloven. At kompetansen legges til Kongen i statsråd sikrer at eventuelle tiltak som iverksettes, er resultat av en vurdering på høyt nivå, og at de står i et rimelig forhold til den foreliggende risikoen.

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

Etter *andre ledd* bør det før det fattes vedtak innhentes rådgivende uttalelser fra relevante organer med kompetanse innenfor det aktuelle fagområdet. Det vil være det departementet som mottar varsel som må vurdere saken og avgjøre hvordan den skal håndteres. Departementet som mottar varselet har også ansvaret for å innhente rådgivende uttalelser. Både Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet og Etterretningstjenesten kan være aktuelle og naturlige organer å konsultere i slike situasjoner. Etter omstendighetene kan det også være aktuelt å innhente rådgivende uttalelser fra andre virksomheter med særlig kompetanse innen det aktuelle fagområdet. Det klare utgangspunktet skal her være at slike uttalelser skal innhentes. Departementet foreslår likevel ingen lovfestet plikt til dette. Å innhente en uttalelse vil i enkelte tilfeller være åpenbart unødvendig, og må derfor kunne unnlates. Dette kan for eksempel være aktuelt dersom saken vurderes å være tilfredsstillende opplyst gjennom varslingen, eller at varselet vurderes å være åpenbart grunnløst.

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

Etter *fjerde ledd* kan Kongen i statsråd gi forskrift om hvilke vedtak som kan fattes etter første ledd. Forskriftskompetansen er således lagt på samme nivå som kompetansen til å fatte vedtak, og heller ikke denne kompetansen kan delegeres til andre.

19.3 Kapittel 3 Tilsyn

Til § 3-1

Bestemmelsen regulerer fordelingen av tilsynsansvaret etter loven. Bestemmelsen er en videreføring av gjeldende rett, men åpner, i tråd med utvalgets forslag, for at tilsyn kan delegeres til sektormyndigheten i den enkelte sektor.

Det framgår av *første ledd* at det er sikkerhetsmyndigheten som fører tilsyn etter loven.

Etter *andre ledd* kan departementet 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 myndigheten med sektoransvar allerede fører tilsyn innenfor et eller flere av disse fagområdene. *Departementet* er det departement som har det overordnede ansvaret for forebyggende sikkerhetsarbeid i sektoren, jf. § 2-1. Bestemmelsen forutsetter at det foretas en helhetsvurdering i samarbeid med sikkerhetsmyndigheten, hvor det skal vurderes om den aktuelle myndigheten har nødvendige sikkerhetsfaglig kompetanse, eller kan opparbeide seg slik kompetanse uten uforholdsmessig høye utgifter, til å ivareta tilsynsansvaret på en forsvarlig måte. Et moment i denne vurderingen er om sektortilsynet allerede fører tilsyn med sikring gjennom sektorlovgivningen. Myndigheten med sektoransvar må også oppfylle de krav som oppstilles i forskrift, jf. § 3-1 fjerde ledd.

Etter *andre ledd, andre punktum* skal sikkerhetsmyndigheten, dersom det er nødvendig av hensyn til internasjonale forpliktelser, eller det er tvingende nødvendig, føre tilsyn med virksomheter uavhengig av om en myndighet med sektoransvar er gitt tilsynsansvaret for sektoren. Internasjonale forpliktelser kan for eksempel være knyttet til behandling av gradert informasjon gjennom bi- eller multilaterale avtaler med andre stater eller internasjonale organisasjoner. *Tvingende nødvending* forutsetter at det foreligger konkrete sikkerhetsinteresser som tilsier at sikkerhetsmyndigheten skal føre tilsyn. Bestemmelsen er ment som en sikkerhetsventil, som kun skal benyttes i spesielle tilfeller.

Sikkerhetsmyndigheten skal i henhold til *tredje ledd* føre tilsyn med departementene og de myndighetene med sektoransvar som er tillagt tilsynsansvar etter *andre ledd*. Tilsyn med myndighetene med sektoransvar må ses i sammenheng med at sikkerhetsmyndigheten har et sektorovergripende ansvar, som også innebærer å påse at det føres tilsyn med at lovens bestemmelser overholdes.

Fjerde ledd gir Kongen hjemmel til å gi bestemmelser i forskrift om departementenes tildeling av tilsynsansvar, og om fordeling av ansvaret mellom sikkerhetsmyndigheten og aktuelle myndigheter med sektoransvar.

Til § 3-2

Bestemmelsen regulerer samarbeids- og samordningsplikten mellom sikkerhetsmyndigheten og myndigheter med tilsynsansvar etter § 3-1 andre ledd. Bestemmelsen er en videreføring av utvalgets forslag.

Første ledd oppstiller krav om at det skal inngås en avtale om samarbeid mellom sikkerhetsmyndigheten og myndigheten med tilsynsansvar. Samarbeidsavtalen bør inneholde ansvarsfordelingen mellom myndighetene knyttet til gjennomføring av tilsyn i den aktuelle sektoren. Avtalen bør også inneholde rammene for samarbeidet, herunder hvordan tilstrekkelig sikkerhetsfaglig kompetanse skal sikres i den aktuelle sektoren, og hvordan sektorspesifikk kompetanse skal deles med sikkerhetsmyndigheten.

Andre ledd pålegger sikkerhetsmyndigheten å utarbeide og vedlikeholde grunnleggende kriterier for tilsyn etter loven, og legge til rette for opplæring av tilsynspersonell. Kriteriene kan fastsettes i forskrift eller i instruks, og skal ivareta lovens formål innenfor alle sektorene. Forebyggende sikkerhetsarbeid er en kontinuerlig prosess, hvor tilsyn er et av verktøyene for å avdekke behov for nye sikkerhetstiltak. Det forebyggende sikkerhetsarbeidet forutsetter derfor at sikkerhetsmyndigheten gis mulighet til å påvirke hva det skal føres tilsyn med og hvordan tilsyn gjennomføres. Sikkerhetsmyndigheten skal gjennom kriteriene, gi overordnede føringer som skal sikre at lovens formål ivaretas, også i de tilfellene hvor tilsynsansvaret etter loven er gitt til en sektormyndighet. Bestemmelsen legger imidlertid opp til at myndighetene med tilsynsansvar har adgang til å supplere de overordnede føringene, med spesifikke kriterier som er tilpasset den enkelte samfunnssektor.

Det er også en viktig del av det forebyggende sikkerhetsarbeidet at sikkerhetsmyndigheten bidrar til å sikre at tilsynspersonell har tilstrekkelig sikkerhetsfaglig kompetanse. Sikkerhetsmyndigheten skal derfor legge til rette for sikkerhetsfaglig opplæring av tilsynspersonell. Det vil være naturlig at det etableres egne program for tilsynspersonell, eksempelvis på kurssenteret til Nasjonal sikkerhetsmyndighet.

Tredje ledd første punktum gir sikkerhetsmyndigheten adgang til å medvirke til forberedelse og gjennomføring av tilsyn dersom det er nødvendig. Det vil eksempelvis kunne være nødvendig dersom sikkerhetsmyndigheten har behov for innsikt i den enkelte samfunnssektor, for bl.a. å kunne avdekke behov for nye sikkerhetstiltak. Denne

adgangen er begrunnet i sikkerhetsmyndighetens sektorovergripende ansvar for forebyggende sikkerhet. Gjennom deltakelse vil sikkerhetsmyndigheten kunne kvalitetssikre tilsyn og kunne bidra med sikkerhetsfaglige kompetanse. Sikkerhetsmyndigheten kan også kreve å delta på tilsyn dersom det er nødvendig.

Etter *tredje ledd andre punktum* kan myndigheter med tilsynsansvar be sikkerhetsmyndigheten om bistand til forberedelser og gjennomføring av tilsyn. Hva sikkerhetsmyndigheten skal bistå med, og hvordan bistanden skal ytes, bør reguleres i samarbeidsavtalen, jf. første ledd.

Fjerde ledd pålegger myndighetene med tilsynsansvar å orientere sikkerhetsmyndigheten om planlagte tilsyn, rapportere om gjennomførte tilsyn og informere om eventuelle avvik og pålegg. Formålet med rapporteringsplikten er å sikre at sikkerhetsmyndigheten får tilgang til nødvendig informasjon for å kunne utvikle nye sikkerhetskrav, som igjen er nødvendig for at sikkerhetsmyndigheten skal kunne ivareta sitt sektorovergripende ansvar for forebyggende sikkerhet.

Femte ledd gir Kongen hjemmel til å gi forskrift om samarbeid og informasjonsutveksling mellom sikkerhetsmyndigheten og myndighetene med tilsynsansvar. De nærmere reglene for tilsyn vil framgå av forskrift.

Til § 3-3

Bestemmelsen angir generelle prinsipper for gjennomføring av tilsyn etter loven. Bestemmelsen er en videreføring av gjeldende rett, men utvides, i tråd med utvalgets forslag, til også å regulere behandlingen av opplysninger som innhentes ved tilsyn. Med tilsynsmyndighet menes både sikkerhetsmyndigheten og myndigheter med tilsynsansvar etter loven.

I *første ledd* slås det fast at tilsyn etter loven skal skje på en slik måte at tilsynsobjektenes daglige drift ikke forstyrres mer enn nødvendig. Tilsyn kan være en belastning for virksomhetene som utsettes for dette, både ved at det er ressurskrevende å forberede tilsyn og ved at stedlig tilsyn potensielt kan medføre at den daglige driften blir redusert i den perioden tilsynet pågår. En god forutgående dialog mellom tilsynsmyndigheten og tilsynsobjektet, hvor dette er mulig uten å undergrave formålet med tilsynet, vil i de fleste tilfeller redusere unødvendig merarbeid og potensiell negativ innvirkning på daglig drift.

Andre ledd avgrenser bruken av opplysninger som innhentes som ledd i tilsynet, til bruk i forbindelse med tilsynet og i det forebyggende sikkerhetsarbeidet. I *forbindelse med det forebyggende sikkerhetsarbeidet* vil si at opplysningene kan tenkes brukt til å samle erfaring fra tilsyn, i risikovurderinger og i vurderinger av sikkerhetstilstanden i sektorene. Opplysningene kan også brukes til utvikling og forbedring av sikkerhetstiltak, videreutvikling av tilsynsvirksomheten, forbedring av rådgivningsarbeidet og avdekke behov for utarbeidelse av veiledninger mv. Videre kan erfaringer fra tilsyn brukes til utdanning og kompetanseheving av tilsynspersonell. En forutsetning for bruken er at denne skjer innenfor lovens formål.

Til § 3-4

Stedlig tilsyn er tilsyn som gjennomføres hos en virksomhet. Gjennomføring av stedlige tilsyn forutsetter at tilsynsmyndigheten får tilgang til tilsynsobjektet, enten det er informasjon, objekt, infrastruktur eller relevant sikkerhetspersonell i virksomheten. Bestemmelsen er en videreføring av gjeldende rett og utvalgets forslag men med enkelte språklige justeringer.

Første ledd fastslår at tilsynsmyndigheten kan kreve å få tilgang til virksomhetens informasjon, informasjonssystemer, objekter og infrastruktur. *Første ledd andre punktum* pålegger virksomheten som blir underlagt tilsyn å stille med relevant personell under tilsynet, så langt det er nødvendig for å få gjennomført tilsynet.

Andre ledd slår fast at stedlige tilsyn skal varsles skriftlig. Dersom et varsel vil kunne undergrave formålet med tilsynet, kan tilsyn likevel gjennomføres uten varsel.

Til § 3-5

Bestemmelsen inneholder særlige bestemmelser om tilsynsmyndighetens behandling av personopplysninger.

Som ledd i tilsynsvirksomheten vil tilsynsmyndigheten kunne få tilgang til personopplysninger, enten fordi det er behov for å behandle slike opplysninger eller som overskuddsinformasjon.

Første ledd etablerer et generelt hjemmelsgrunnlag for behandling av personopplysninger der dette er nødvendig for å utføre tilsynsoppgavene etter loven.

I *andre ledd* slås det fast at tilsynsmyndighetens behandling av personopplysninger ikke skal utgjøre et uforholdsmessig inngrep i personvernet. Behandling kan skje der det etter en konkret vurdering er nødvendig og proporsjonalt i forhold til det inngrepet behandlingen representerer.

I *tredje ledd* gis det nærmere prosedyreregler for tilsynsmyndighetenes behandling av personopplysninger. Som hovedregel skal personopplysninger kun behandles ved hjelp av virksomhetens egne informasjonssystemer. Tilsynsmyndigheten kan kreve kopi av personopplysninger i den utstrekning dette er nødvendig for å påvise eller avkrefte lovbrudd.

Til § 3-6

Bestemmelsen gir tilsynsmyndigheten hjemmel til å gi pålegg. Bestemmelsen viderefører utvalgets forslag. Et pålegg behøver ikke å omfatte gjennomføring av et konkret tiltak, kun at det må gjennomføres tiltak for å korrigere et avvik fra lovens krav. I de tilfellene hvor det pålegges konkrete tiltak, må disse være nødvendige for å ivareta lovens formål, og kostnadene forbundet med pålegget må være rimelige sett i forhold til det som kan oppnås ved tiltaket. Det må foretas en konkret vurdering av om tiltakene er uforholdsmessig kostbare, sett i forhold til hva som er en akseptabel restrisiko for virksomheten, jf. § 4-3.

Andre ledd gir sikkerhetsmyndigheten mulighet til å gi myndigheter med tilsynsansvar pålegg om å føre tilsyn i samsvar med krav fastsatt i eller i medhold av loven. Adgangen forutsetter at myndigheten med tilsynsansvar ikke fører tilsyn eller at tilsynene ikke er gjennomført i tråd med de fastsatte kriteriene i eller i medhold av loven.

I *tredje ledd* slås det fast at pålegg etter første og andre ledd kan påklages. For selvstendige rettssubjekter gjelder reglene i forvaltningsloven kapittel VI.

19.4 Kapittel 4 Generelle krav til forebyggende sikkerhetsarbeid

Til § 4-1

Første ledd første punktum slår fast at det er ledelsen i virksomheten som har ansvaret for det forebyggende sikkerhetsarbeidet. Ansvaret kan delegeres, men en god forankring hos ledelsen er avgjørende for et godt og tilstrekkelig prioritert sikkerhetsarbeid. Bestemmelsen slår også fast at det skal gjennomføres intern kontroll av sikkerhetstilstanden i virksomheten. Bestemmelsen er en videreføring av gjeldende rett, men tydeliggjøres i tråd med utvalgets forslag. Det er også gjort enkelte språklige justeringer i forhold til utvalgets forslag.

Andre ledd presiserer at virksomheten har et ansvar for å sørge for opplæring av eget personell, og en plikt til å sørge for at leverandører, underleverandører og andre oppdragstakere har tilstrekkelig risiko- og sikkerhetsforståelse. Formålet med bestemmelsen er å slå uttrykkelig fast at en virksomhet ikke kan frasi seg ansvaret for det forebyggende sikkerhetsarbeidet. Leverandører til sikkerhetsgraderte anskaffelser vil ha et selvstendig ansvar for det forebyggende sikkerhetsarbeidet i forbindelse med den konkrete anskaffelsen, herunder en plikt til å sørge for opplæring av eget personell, jf. § 1-2 andre ledd og lovens kapittel 9.

Til § 4-2

Bestemmelsen er ny i den forstand at gjeldende rett ikke oppstiller en eksplisitt plikt for virksomhetene til å foreta en vurdering av risiko. Det framgår av gjeldende sikkerhetslov og av forskrift om sikkerhetsadministrasjon at «[e]nhver virksomhet plikter å utøve forebyggende sikkerhetstjeneste». § 4-2 innebærer således en klargjøring av hva en sentral del av det forebyggende sikkerhetsarbeidet består i. Bestemmelsen er i hovedsak en videreføring av utvalgets forslag til § 4-3. Imidlertid videreføres ikke forslaget om at det skal gjennomføres en risiko- og sårbarhetsanalyse (ROS-analyse).

Første ledd regulerer virksomhetens plikt til å gjennomføre en vurdering av risiko, som grunnlag for virksomhetens plikt til å gjennomføre forebyggende sikkerhetstiltak etter loven.

Vurderingen er ikke knyttet opp mot bruk av en spesiell standard, men skal gjøres for å kartlegge den risikoen virksomheten er utsatt for. Vurderingen skal skape bevissthet og kunnskap om risiko- og sikkerhetsnivået, og danne grunnlaget for målrettet å kunne unngå/redusere virkninger av handlinger som kan skade informasjon, informasjonssystemer, infrastruktur og objekter som er beskyttet av loven. Vurderingen skal gi grunnlag for prioriteringer av hvilke tiltak som bør iverksettes. Med *regelmessig* menes at risikovurderingene må oppdateres slik at det tas høyde for endringer av sårbarheter, trusler eller verdier.

En forutsetning for å kunne gjøre en tilfredsstillende vurdering, er at de ulike virksomhetene blir satt i stand til å forstå det til enhver tid gjeldende trusselbildet. Bestemmelsen må således ses i sammenheng med sikkerhetsmyndighetens plikt til aktiv rådgivning og veiledning, jf. § 2-2, og plikten til å legge til rette for tilgjengeliggjøring av trusselinformasjon og annen sikkerhetsrelevant informasjon, jf. § 2-3.

Av *andre ledd* følger at virksomheten som en del av vurderingen også må kartlegge hvilke andre virksomheter den er avhengig av, for å opprettholde sin funksjon. I lovbestemmelsen fastsettes ingen nærmere avgrensning av kartleggingen. I utgangspunktet vil det imidlertid være de virksomhetene som ved bortfall, vil få en direkte konsekvens for virksomhetens funksjon etter loven.

I bestemmelsens *tredje ledd* pålegges virksomheten å gjennomgå, og om nødvendig revidere, vurderingen av risiko på jevnlig basis. Arbeidet skal være en dynamisk prosess, som skal ta høyde for endringer i gjeldende trusselsituasjon, virksomhetens sårbarheter og andre sikkerhetsrelevante endringer. Når, og hvor ofte, en virksomhet må gjennomføre en slik vurdering vil i stor grad være situasjonsbetinget.

Etter *fjerde ledd* skal den myndigheten som utfører tilsyn, også etter forespørsel gi råd og veiledning knyttet til vurderingen. Som hovedregel vil plikten til å gi råd og veiledning etter bestemmelsen følge fordelingen av tilsynsansvaret etter § 3-1. Råd- og veiledningsplikten er nærmere beskrevet under kapittel 8.4. Det vil imidlertid kunne være forhold som gjør at ansvarsfordelingen bør eller må være annerledes. For enkelte sektormyndigheter vil eksempelvis EØS-rettslige forpliktelser sette begrensninger for hvor langt sektormyndigheten kan gå i forhold til konkret rådgivning overfor virksomheter i egen sektor. Hvorvidt det er sikkerhetsmyndigheten eller aktuelle sektormyndigheter som skal bistå virksomheten i slike situasjoner, bør fastlegges i samarbeidsavtalen mellom dem.

I bestemmelsens *femte ledd* gis Kongen myndighet til å fastsette nærmere bestemmelser om hvordan vurdering av risiko skal gjennomføres. Dette vil blant annet innebære om det skal benyttes standarder, i så fall hvilke, hvor regelmessig vurderinger må gjennomføres, og en nærmere angivelse av kartleggingen av gjensidige avhengigheter mellom virksomheter.

Til § 4-3

Bestemmelsen er en videreføring og klargjøring av gjeldende rett, og regulerer de generelle pliktene til å gjennomføre sikkerhetstiltak for virksomheter som er underlagt loven. Bestemmelsen viderefører i hovedsak utvalgets forslag til §§ 4-1 og 4-5.

Første ledd slår fast at virksomheten plikter å gjennomføre de forebyggende sikkerhetstiltak som må til for å gi et forsvarlig sikkerhetsnivå og redusere risikoen knyttet til sikkerhetstruende virksomhet. Med begrepet *knyttet til* menes at sikkerhetstiltakene både skal omfatte tiltak som reduserer risikoen for at slik virksomhet inntreffer, og tiltak som reduserer konsekvensene av slik virksomhet ved å redusere skadeomfanget. Nødvendig reduksjon av risiko kan både skje ved enkeltstående tiltak eller kombinasjoner av flere typer tiltak. Kombinasjoner av tiltak vil ofte være aktuelt. Tiltak kan være av en art som direkte reduserer sannsynligheten for at hendelser rammer et spesifikt objekt eller en infrastruktur. Eksempler på dette er ulike former for barrierer, systemer for tidlig deteksjon av uønskede hendelser, verifikasjonssystemer og ulike former for reaksjon for å stoppe eller redusere omfanget av slike hendelser. Reduksjon av risiko kan også bestå av tiltak som reduserer skadevirkningene dersom en hendelse inntreffer. Dette kan enten være tiltak som baseres på økt redundans eller økt resiliens, eller en kombinasjon av slike tiltak. Høy redundans innebærer at det er flere enheter eller delsystemer som bidrar til å opprettholde funksjonen. Dersom noen av enhetene eller delsystemene mister sin funksjon, vil de øvrige kunne fylle funksjonen til den eller de som er falt ut, og dermed forhindre alvorlige konsekvenser. Høy resiliens betyr at funksjonen har stor evne til raskt å gjenopprette normaltilstand dersom hele eller deler av funksjonen blir påvirket av en hendelse. Egenberedskap kan også være et nødvendig og hensiktsmessig risikoreduserende tiltak, for eksempel ved bortfall av strømforsyning.

Grunnlaget for virksomhetens sikkerhetstiltak skal være virksomhetens vurdering av risiko, jf. § 4-2.

Begrepet *forsvarlig sikkerhetsnivå* er en rettslig standard som trekker opp rammene for hvilket handlingsrom virksomheten har for etablering av sikkerhetstiltak. Innholdet i den rettslige standarden er nærmere omtalt i kapittel 9.4.

Sikkerhetstiltakene skal inkludere alle tiltak for å ivareta lovens formål, herunder informasjonssikkerhet, informasjonssystemsikkerhet, fysisk sikkerhet og personellsikkerhet, samt andre relevante sikkerhetstiltak. Det er kombinasjonen av relevante tiltak som er avgjørende for om virksomheten kan sies å ha et forsvarlig sikkerhetsnivå, ikke de ulike tiltakene vurdert hver for seg. For enkelte virksomheter vil det være umulig, eller uforholdsmessig kostbart, å etablere sikkerhetstiltak som gjør at tilsiktede uønskede hendelser blir helt forhindret. Redundante systemer vil imidlertid kunne redusere risikoen for at slike hendelser får kritiske konsekvenser, slik at kravet til forsvarlig sikkerhetsnivå er oppfylt.

Første ledd andre punktum presiserer at tiltakene som iverksettes for å motvirke tilsiktede uønskede hendelser, kan ses i sammenheng med behov for tiltak for å håndtere annen type risiko. Bestemmelsen legger opp til at virksomheten har en helhetlig tilnærming, hvor kravene til forebyggende sikkerhetsarbeid etter loven kan ses i sammenheng med krav til sikkerhet i andre regelverk. Forutsetningen for at planlegging og gjennomføring kan ses i sammenheng, er at kravene etter sikkerhetsloven oppfylles.

I *andre ledd* slås det fast at virksomheten, ved vurderingen av hvilke sikkerhetstiltak som skal gjennomføres, skal foreta en forholdsmessighetsvurdering mellom kostnadene ved tiltakene og den sikkerhetsmessige effekten som oppnås. Et absolutt krav er imidlertid at slike vurderinger gjøres innenfor rammen av det som skal til for å oppnå et forsvarlig sikkerhetsnivå etter første ledd.

Bestemmelsens *tredje ledd* oppstiller et krav til å gjennomføre øvelser. Formålet med øvelser er dels å utdanne og trene eget personell, og dels å teste at sikkerhetstiltak er iverksatt og fungerer etter intensjonen.

Bestemmelsens *fjerde ledd* inneholder en forskriftshjemmel til å fastsette nærmere plikter for virksomheter som omfattes av loven, og nærmere bestemmelser om øvelser. For nærmere omtale av øvelser, se kapittel 9.4.

Til § 4-4

Bestemmelsen er ny og regulerer virksomhetens plikt til å dokumentere det forebyggende sikkerhetsarbeidet. Formålet med bestemmelsen er å legge til rette for at tilsyn med virksomhetene etter lovens kapittel 3 kan gjennomføres på en effektiv og hensiktsmessig måte. Bestemmelsen er i hovedsak en videreføring av utvalgets forslag til § 4-4.

I bestemmelsen pålegges virksomheten å dokumentere at vurdering av risiko, jf. § 4-2, er gjennomført. Videre skal virksomheten dokumentere at nødvendige tiltak er iverksatt med sikte på å redusere sannsynligheten for, og konsekvensene av, handlinger som har til mål å skade informasjon, informasjonssystemer, objekter og infrastruktur. Det nærmere omfanget av dokumentasjon som er nødvendig, bør fastsettes i forskrift, jf. *andre ledd*.

Til § 4-5

Bestemmelsen regulerer virksomhetenes varslingsplikt til tilsynsmyndighetene. Bestemmelsen er i hovedsak en videreføring av gjeldende rett, men presiserer at i de tilfellene en sektormyndighet er gitt tilsynsansvar, skal begge myndighetene varsles. En forutsetning for at myndighetene skal kunne ha oversikt over sikkerhetstilstanden i de ulike samfunnssektorene, er at myndighetene får rettidig og tilstrekkelig informasjon om hendelser av betydning, jf. § 2-5.

I *første ledd* slås det fast at virksomhetene plikter å varsle sikkerhetsmyndigheten og andre myndigheter som skal føre tilsyn i medhold av § 3-1 andre ledd. For at sikkerhetsmyndigheten skal kunne ivareta sitt sektorovergripende ansvar, er det nødvendig at denne har en tilstrekkelig informasjonstilgang om relevante hendelser også i samfunnssektorer der den ikke har et direkte tilsynsansvar. Ved at sikkerhetsmyndigheten får tilgang til varsel fra alle samfunnssektorer, vil denne også ha muligheten til å kartlegge og holde oversikt over trusler som rammer flere samfunnssektorer parallelt, og å gi nødvendig råd, veiledning og tidlig varsling til samfunnssektorer som ennå ikke er berørt av de aktuelle truslene. Virksomheten skal gi slikt varsel i tre tilfeller.

Første ledd bokstav a regulerer de tilfeller der det er klarlagt at virksomheten faktisk er rammet av sikkerhetstruende virksomhet, det vil si en tilsiktet handling som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser, jf. definisjonen i § 1-5.

Varslingsplikten inntrer bare der den aktuelle handlingen er rettet mot den aktuelle virksomheten.

Etter *første ledd bokstav b* inntrer varslingsplikten også der det er en begrunnet mistanke om at sikkerhetstruende virksomhet er gjennomført eller planlagt. I begrepet *begrunnet mistanke* ligger et krav om at det må være en viss grad av sannsynlighet før varslingsplikten inntrer. Der det foreligger en mistanke om at slik virksomhet er planlagt, vil virksomheten uansett ha en egeninteresse i å varsle myndighetene slik at nødvendige tiltak for å avverge hendelsen kan iverksettes.

Etter *bokstav c* skal virksomheten også varsle der det har skjedd alvorlige brudd på sikkerhetskrav til beskyttelse av informasjon, informasjonssystemer, infrastruktur eller objektsikkerhet.

Etter *andre ledd* følger en plikt for virksomheten til å varsle tilsynsmyndigheten ved kunnskap om en planlagt eller pågående aktivitet som kan medføre en ikke ubetydelig risiko for at nasjonale

sikkerhetsinteresser blir truet. Det slås fast at det skal varsles selv om dette innebærer videreformidling av opplysninger som i utgangspunktet er omfattet av lovbestemt taushetsplikt. Sett hen til de funksjoner og interesser loven tar sikte på å beskytte, er det avgjørende at taushetsplikt etter annet regelverk ikke er til hinder for varsling om aktivitet som kan medføre en slik risiko for nasjonale sikkerhetsinteresser. Uttrykket *får kunnskap om* stiller ikke krav om visshet eller andre krav til graden av kunnskap om aktiviteten. Både *kjennskap til* og *indikasjoner* på slik aktivitet er tilstrekkelig. Om begrepene *aktivitet, ikke ubetydelig risiko* og *nasjonale sikkerhetsinteresser* vises det til særmerknaden til § 2-5.

Tilsynsmyndigheten skal varsle sikkerhetsmyndigheten og videresende varsel om forhold som angitt i andre ledd til ansvarlig departementet så snart som mulig etter at tilsynsmyndigheten har tilstrekkelig informasjon om saken. Det kan tenkes situasjoner der tilsynsmyndigheten har behov for å innhente ytterligere informasjon før de har et tilstrekkelig informasjonsgrunnlag til å formidle videre.

Etter *tredje ledd* kan Kongen gi nærmere regler om varslingsplikten etter andre ledd i forskrift.

19.5 Kapittel 5 Informasjonssikkerhet

Til § 5-1

Bestemmelsen etablerer begrepet skjermingsverdig informasjon som en samlebetegnelse på all informasjon som skal beskyttes etter loven. Begrepet utvides sammenlignet med tidligere sikkerhetslov. I motsetning til tidligere lov, da det utelukkende var konfidensialitetsbehov som skulle vurderes, skal nå også integritets- og tilgjengelighetsbehov inngå som kriterier i verdivurderingen av informasjonen. Det må vurderes hvilke konsekvenser det vil kunne få for nasjonale sikkerhetsinteresser dersom informasjonen blir kjent for uvedkommende, blir endret av uvedkommende eller er utilgjengelig for personer eller informasjonssystemer som har tjenstlig og lovlig behov for tilgang.

Begrepet *informasjon* skal forstås vidt. Måten informasjonen er tilvirket på og hvilken form informasjonen har, er ikke relevante momenter i vurderingen av om noe er informasjon. Begrepet omfatter for eksempel informasjon i form av fysiske dokumenter, digitale og maskinlesbare signaler, film, lydopptak og muntlige opplysninger.

Til § 5-2

Bestemmelsen fastsetter en plikt for virksomheten til å beskytte skjermingsverdig informasjon. Denne plikten er videre enn den som følger av § 5-4 om taushetsplikt. Virksomhetens vurdering av risiko, jf. § 4-2, sett i sammenheng med § 5-1, vil danne grunnlaget for å angi hvilken informasjon som skal beskyttes etter sikkerhetsloven. *Forsvarlig sikkerhetsnivå* i *første ledd* skal forstås på samme måte som andre steder i loven, se merknadene til § 4-3. *Første ledd* andre punktum bokstavene a til c konkretiserer at det er særlig egenskapene konfidensialitet, integritet og tilgjengelighet som ligger i begrepet informasjonssikkerhet og som skal beskyttes. Informasjonen vil bare kunne endres når det er godkjent av utsteder av informasjonen. Videre er det ofte behov for å begrense tilgjengeligheten til informasjon, slik at det kun er personer og informasjonssystemer som har lovlig og tjenstlig behov for informasjon som har tilgang.

Behovet for å beskytte de ulike egenskapene ved informasjonen må ses i sammenheng. En konkret helhetsvurdering av behovet for beskyttelse må ligge til grunn for å kunne iverksette passende sikkerhetstiltak. Opplistingen i bestemmelsen skal forstås som et minimum av hensyn som må vurderes for å oppnå god informasjonssikkerhet. Andre egenskaper som for eksempel autentisitet, og ikke-benektbarhet må også vurderes der det er relevant. Med ikke-benektbarhet menes å knytte en handling til avsender slik at avsender ikke senere kan benekte å stå bak handlingen. Det må også vurderes om det er behov for å kunne spore brudd på egenskapene. Nødvendighetsvurderingen vil i stor grad avhenge av de nærmere bestemmelser om beskyttelse som blir fastsatt i forskrift, jf. *andre ledd*.

Andre ledd første punktum gir Kongen forskriftshjemmel til å fastsette nærmere bestemmelser om identifisering og sikkerhetskrav for beskyttelse av skjermingsverdig informasjon, herunder hvilke minstekrav til beskyttelse som skal gjelde. I dette ligger også hjemmel til å fastsette regler for beskyttelse av sikkerhetsgradert informasjon, jf. § 5-3. Det kan også gjøres unntak fra hovedregelen om bortfall av gradering etter 30 år, jf. § 5-3 andre ledd andre punktum og gjeldende lov § 11 tredje ledd tredje punktum. Som etter gjeldende rett vil det være nødvendig å regulere nærmere i forskrift hvilke tilfeller det skal gjøres unntak fra hovedregelen.

Bestemmelsens *andre ledd andre punktum* gir Kongen hjemmel til å i særlige tilfeller gjøre unn-

tak fra beskyttelsestiltakene. Det kan ikke gjøres unntak fra plikten til å foreta en verdivurdering og eventuell sikkerhetsgradering av informasjonen. Hva som ligger i s*ærlige tilfeller* er nærmere omtalt i kapittel 10.5.2.

Til § 5-3

Bestemmelsen er i stor grad en videreføring av gjeldende lov § 11 og utvalgets forslag til § 5-1. Den grunnleggende systematikken med verdivurdering, sikkerhetsgradering og merking er den samme. *Første ledd* fastslår hvem som er pliktsubjekt og som dermed har plikt til å foreta en verdivurdering av informasjonen som er utgangspunktet for en eventuell sikkerhetsgradering. Bokstav a til d gir nærmere anvisning på innholdet i verdivurderingen. Det skal vurderes hvilket skadepotensial informasjonen har for nasjonale sikkerhetsinteresser dersom informasjonen blir kjent for uvedkommende.

Plikten til å merke sikkerhetsgradert informasjon gjelder ikke der merking i praksis er umulig. Det gjelder for eksempel for informasjon som ikke har en fysisk tilstand, slik som muntlige opplysninger. Merkingsplikt inntrer imidlertid for den som bringer informasjonen over i et format der merking er mulig.

Ordlyden i bestemmelsen skiller seg noe fra gjeldende lov. Der tidligere lov brukte begrepene *utsteder eller på annen måte tilvirker,* brukes nå bare *tilvirker,* uten at dette utgjør en realitetsforskjell. Begrepet *nasjonale sikkerhetsinteresser* skal forstås på samme måte som i § 1-5 nr. 1.

Tema for skadevurderingen og dermed om informasjonen skal sikkerhetsgraderes, er i hvilken grad en trusselaktør, dersom denne blir kjent med informasjonen, kan påføre nasjonale sikkerhetsinteresser skade. Vurderingen vil være bestemmende for i hvilken grad informasjonens konfidensialitet må beskyttes. Er konklusjonen at konfidensialitetsbrudd *ikke* i noen grad kan få skadefølger, jf. bokstav d, for nasjonale sikkerhetsinteresser, skal informasjonen ikke sikkerhetsgraderes. Informasjonen skal dermed heller ikke beskyttes etter de særlige bestemmelsene for sikkerhetsgradert informasjon i §§ 5-4 til 5-6. Dette utelukker imidlertid ikke at informasjonen skal beskyttes etter andre regler som følger av sikkerhetslovens bestemmelser om skjermingsverdig informasjon, eller av andre regelverk slik som for eksempel personopplysningsloven eller beredskapsforskriften.

Innholdet i og forholdet mellom de ulike sikkerhetsgradene videreføres. Dette innebærer blant annet at forarbeidene (Ot.prp. nr. 49 (1996–97) Om lov om forebyggende sikkerhetstjeneste (sikkerhetsloven)) til tidligere lov fortsatt er relevante, og at tilknytningen til NATO systemet videreføres. Endringen fra *skade* i tidligere lov bokstav b og c til *skadefølge* i ny lov er kun en språklig justering som ikke innebærer realitetsendring. Det samme gjelder endringen i bokstav d fra *medføre* i tidligere lov til *få* i ny lov. Se også NOU 2016:19 kapittel 8.2.1 som beskriver nærmere hvilken informasjon som omfattes av BEGRENSET.

Sikkerhetshensyn skal være styrende for nødvendighetsvurderingen etter *andre ledd* første punktum. Bestemmelsen skal sikre at det faktisk foretas en grundig vurdering av beskyttelsesbehovet og at andre relevante hensyn, slik som hensynet til offentlighet, tas i betraktning.

Andre ledd viderefører gjeldende sikkerhetslov § 11 tredje ledd første punktum. 30-årsregelen må anses som en hovedregel. For enkelte typer informasjon vil det imidlertid være nødvendig å gjøre unntak fra denne. Kongens myndighet som følger av dagens § 11 tredje ledd andre og tredje punktum, foreslås videreført i lovforslaget § 5-2 andre ledd.

Tredje ledd viderefører i all hovedsak gjeldende § 11 fjerde ledd. Leddet inneholder ikke lenger en uttrykkelig hjemmel for Kongen til å inngå avtaler med fremmed stat eller organisasjon. Det innebærer ikke en realitetsendring, ettersom Grunnloven § 26 gir Kongen denne kompetansen. Se nærmere merknadene til gjeldende § 11, jf. Ot.prp. nr. 49 (1996–97), side 67.

Til § 5-4

Bestemmelsen er en videreføring av gjeldende lov §§ 11 andre ledd og 12 første ledd, og utvalgets forslag til § 5-3. Endringene innebærer ingen realitetsendring fra gjeldende sikkerhetslov.

Første ledd fastsetter uttømmende og absolutte vilkår for å kunne overlate sikkerhetsgradert informasjon til en annen. Se merknadene til § 8-1 om *autorisasjon*.

A*ndre ledd* fastsetter en plikt til å bevare taushet om sikkerhetsgradert informasjon i alle andre tilfeller enn det som følger av første ledd. Den som skal overlate sikkerhetsgraderte informasjon til en annen må forsikre seg om at vilkårene er oppfylt. Formuleringen *arbeidet eller tjenesten* skal forstås vidt, og omfatter både *oppdrag, verv eller aktivitet for,* og andre formaliserte relasjoner til, virksomheten.

Til § 5-5

Bestemmelsen er i hovedsak en videreføring av gjeldende lov § 16 og utvalgets forslag til § 5-4.

Første ledd hjemler at det kan foretas kontroll hos virksomheten med sikte på å avdekke om uvedkommende kan skaffe seg tilgang til sikkerhetsgradert informasjon. Begrepet *innsyn* erstatter *avtitting*, uten at det er ment å utgjøre en realitetsforskjell.

Andre ledd setter begrensning for hva informasjonen som sikkerhetsmyndigheten tilegner seg gjennom kontrollen, kan brukes til. For det første kan informasjonen brukes til gjennomføring av selve kontrollen og til rapporteringen som følger av tredje ledd. For det andre kan informasjonen brukes i sikkerhetsmyndighetens øvrige forebyggende sikkerhetsarbeid. Dette skal særlig dekke sikkerhetsmyndighetens behov for å kunne samle og analysere funn og erfaringer fra kontrollen, som igjen kan brukes i risikovurderinger, til å forbedre sikkerhetstiltak, til utvikling av metodikk for undersøkelser og i rådgivningsarbeidet. De nærmere vilkårene for bruken skal fastsettes i forskrift, og vil måtte ta tilstrekkelig hensyn til personvern og virksomhetssensitiv informasjon.

Tredje ledd pålegger den som utfører kontrolleren en rapporteringsplikt overfor virksomheten som blir kontrollert. Formålet er å bidra til å bedre virksomhetens sikkerhet.

Det følger av *fjerde ledd* at andre enn sikkerhetsmyndigheten kan utføre tekniske sikkerhetsundersøkelser. Det kan være virksomheten selv eller andre egnede private eller offentlige virksomheter. Det er en nødvendig forutsetning at slik aktivitet gjennomføres i tråd med vilkår fastsatt i forskrift.

Til § 5-6

Bestemmelsen er en videreføring av gjeldende lov § 14. *Første ledd* setter begrensninger for hvilke kryptosystemer som kan brukes til å beskytte sikkerhetsgradert informasjon. *Andre ledd* fastsetter sikkerhetsmyndighetens rolle som nasjonal forvalter av kryptomateriell og leverandør av kryptosikkerhetstjenester til virksomheter, som brukes til å beskytte sikkerhetsgradert informasjon.

Krypto er en kortform for kryptografi, og handler om prinsipper og teknikker for å skjule informasjon slik at bare de(n) som er autorisert har mulighet til å avsløre innholdet.

Bestemmelsen gjelder bruk av krypto for beskyttelse av skjermingsverdig informasjon. Nærmere bestemmelser om kryptosikkerhet kan gis i forskrift.

19.6 Kapittel 6 Informasjonssystemsikkerhet

Til § 6-1

Bestemmelsen viderefører i all hovedsak forslaget i utvalgets § 6-1. Bestemmelsen definerer hvilke informasjonssystemer som skal beskyttes etter loven, og etablerer begrepet *skjermingsverdige informasjonssystemer* som en samlebetegnelse for disse.

Skjermingsverdige systemer kan defineres på to måter. Enten ved å fastslå at systemet behandler skjermingsverdig informasjon, jf. § 5-1, eller ved å fastslå av systemet har en særlig viktig rolle i virksomhetens leveranse av sine kritiske tjenester. Alle systemer som behandler sikkerhetsgradert informasjon, jf. § 5-3, er skjermingsverdige.

Det legges til grunn samme definisjon av begrepet *informasjonssystem* og begrepet *behandler* som utvalget, se NOU 2016: 19, side 262–263 :

> «Med begrepet *informasjonssystem* menes systemer som anvendes for å løse en oppgave eller utføre en funksjon i en organisasjon. Det omfatter menneskelige, organisatoriske og tekniske ressurser, metoder og teknikker.
>
> *Informasjonssystem* skal i sikkerhetsloven forstand forstås vidt. Begrepet omfatter både manuelle og digitale informasjonssystemer, og favner alt fra saksbehandlingssystemer, kontorstøttesystemer og rene kommunikasjonssystemer til kontroll- og styringssystemer.
>
> […]
>
> Med begrepet *behandler* menes alle former for behandling av informasjon i et informasjonssystem, blant annet transport, lagring og prosessering.»

Et system kan falle inn under begge beskrivelsene av skjermingsverdige informasjonssystemer. For eksempel kan et system ha en særlig viktig rolle i en virksomhet, samtidig som det behandler sikkerhetsgradert informasjon.

Til § 6-2

Bestemmelsen viderefører i all hovedsak forslaget til § 6-2 i NOU 2016: 19.

Første ledd fastsetter en plikt for virksomheten til å beskytte virksomhetens skjermingsverdige informasjonssystemer. Virksomhetens vurdering

av risiko, jf. § 4-2, vil sammen med verdivurderingen av informasjonssystemer etter § 6-1, danne grunnlaget for å angi hvilke av virksomhetens informasjonssystemer som skal beskyttes. Virksomheten plikter å sørge for et *forsvarlig sikkerhetsnivå* for informasjonssystemene. Begrepet *forsvarlig sikkerhetsnivå* skal forstås på samme måte som i §§ 4-3 og i 5-2, se merknaden til § 4-3.

Som nevnt i merknaden til § 6-1 kan skjermingsverdige informasjonssystemer defineres på to ulike måter, med to tilhørende hovedformål for beskyttelsestiltakene. Ivaretakelse av de to hovedformålene må ses i sammenheng. Funksjonaliteten vil ofte henge tett sammen med ivaretakelsen av konfidensialitet, integritet og tilgjengelighet. For eksempel er det ikke tilstrekkelig å kun se på graderingsnivået for et sikkerhetsgradert informasjonssystem. Hvis systemet i tillegg til å behandle BEGRENSET informasjon, også spiller en viktig rolle for at en sentral myndighet skal kunne ivareta sin rolle under en krise, kan det være at sikkerhetsnivået må være høyere for dette systemet enn det som er vanlig for systemer som behandler BEGRENSET informasjon. Virksomhetens vurdering av risiko, jf. § 4-2, vil være sentral i vurderingen av hvilke sikkerhetstiltak som er tilstrekkelige for å oppnå et forsvarlig sikkerhetsnivå.

Det vil kunne variere fra system til system hva som skal til for å oppnå et forsvarlig sikkerhetsnivå. Ved utarbeidelse av tilstrekkelige sikkerhetstiltak bør det ses hen til internasjonale standarder for beskyttelse av informasjonssystemer.

Andre ledd første punktum gir Kongen hjemmel til å fastsette nærmere bestemmelser om identifisering og sikkerhetskrav for beskyttelse av skjermingsverdige informasjonssystemer, herunder minstekrav, i forskrift. Etter *andre ledd andre punktum* kan Kongen i særlige tilfeller gjøre unntak i forskrift fra beskyttelsestiltak som følger av lov eller forskrift. Eksempelvis kan det være behov for spesielle tilpasninger i enkelte skarpe militære oppdrag, eller hvor store komplekse systemer skal behandle sikkerhetsgradert informasjon. Unntakshjemmelen tilsvarer § 5-2 andre ledd andre punktum, se merknadene til § 5-2 og kapittel 10.5.2.

Til § 6-3

Bestemmelsen viderefører i all hovedsak forslaget til § 6-3 i NOU 2016: 19.

Første ledd fastslår at alle skjermingsverdige informasjonssystemer, jf. § 6-1, skal godkjennes. Det er imidlertid ikke krav om at systemene godkjennes før de tas i bruk, da det eksempelvis kan være svært vanskelig å gjennomføre en forhåndsgodkjenning av informasjonssystemer i virksomheter som nylig er blitt utpekt til å omfattes av sikkerhetsloven, samtidig som at beskyttelsesbehovet ikke nødvendigvis er like stort som for systemer som behandler sikkerhetsgradert informasjon.

Det følger imidlertid av *første ledd andre punktum* et krav om at informasjonssystemer som behandler sikkerhetsgradert informasjon forhåndsgodkjennes. Dette er en videreføring av gjeldende rett, jf. gjeldende lov § 13 første ledd.

Det følger av *andre ledd* at Kongen i forskrift kan bestemme hvem som skal være godkjenningsmyndighet, hvilke vilkår som skal gjelde for godkjenning, og hvilke krav som skal gjelder for leverandører til skjermingsverdige informasjonssystemer. Eksempelvis kan det være grunn til å videreføre dagens ordning i en del tilfeller, jf. gjeldende forskrift om informasjonssikkerhet § 5-28 andre ledd, der virksomhetenes leder kan godkjenne enkelte systemer. Gjennomføring av verifikasjoner kan utføres av godkjenningsmyndigheten, uavhengig av om denne har tilsynsansvar.

Til § 6-4

Virksomhetens overvåking av sine egne skjermingsverdige informasjonssystemer, kan innebære mange former for sikkerhetstiltak. Eksempelvis er logging av aktivitet i systemet, automatiserte alarmer og manuell sammenstilling og analyse av innhentet data, aktuelle tiltak. Bestemmelsen er i hovedsak en videreføring av gjeldende sikkerhetslov § 13 a og forslaget til § 6-4 i NOU 2016: 19.

Første ledd oppstiller en plikt for virksomheten til å foreta sikkerhetsmessig overvåking av virksomhetens skjermingsverdige informasjonssystemer, jf. § 6-1. Med begrepene *forebygge*, *avdekke* og *motvirke* menes sikkerhetstiltak som omfatter hele livssyklusen til en uønsket hendelse, herunder evne til å oppdage (detektere) og gjenopprette sikker tilstand etter hendelsen, jf. merknaden til §1-1. Med *hendelse som kan skade* menes potensiell eller faktisk kompromittering av systemet. Det kan også være tale om at systemet blir brukt til å skade andre systemer, eller at systemet blir brukt som utgangspunkt for virksomhet som truer nasjonale sikkerhetsinteresser. Bestemmelsens siste punktum erstatter gjeldende lov § 13a om sikkerhetsrelevante hendelser. Dette innebærer ikke en realitetsendring. Selv om lovens virkeområde bruker begrepet *sikkerhets-*

truende virksomhet, brukes begrepet *hendelse* i bestemmelsen fordi virksomheten ofte må iverksette tiltak før det er kjent om hendelsen er tilsiktet eller ei, eller om den er resultat av en handling eller en teknisk feil.

Andre ledd gir hjemmel for og pålegger en plikt til lagring, registrering og analyse av ulike former for utveksling av informasjon. Omfanget av overvåkingen, herunder lagring og registrering, strekker seg til og begrenses av formålet med overvåkningen. For nærmere omtale av andre ledd, se NOU 2016: 19 kapittel 8.6.4.

Ved overvåking av systemer som behandler personopplysninger, stiller *tredje ledd* ytterligere krav til at virksomhetens vurdering av formåls- og forholdsmessigheten av overvåkningen. For det første stilles det strengere krav til vurderingen av om overvåkingen ivaretar formålet, enn det krav som følger av andre ledd. Videre må virksomheten i hvert enkelt tilfelle foreta en forholdsmessighetsvurdering der behovet for overvåking ses i sammenheng med eventuelle negative virkninger for personvernet. Omfanget av overvåkingen må være begrunnet og nødvendig. Virksomheten må dessuten – der det er valgmuligheter – velge den metoden som er minst inngripende for personvernet til brukerne av systemet. I noen tilfeller kan for eksempel automatisert overvåking, med et innhold som er utilgjengelig for mennesker, være mindre inngripende enn manuell overvåking.

I *fjerde ledd* gis det hjemmel til å lagre informasjon fra overvåkingen i inntil fem år. Loven setter ikke begrensninger for bruken av informasjon som ikke er personopplysninger. *Femte ledd* er i hovedsak en videreføring av gjeldende sikkerhetslov § 13 a tredje ledd. *Femte ledd andre punktum* fastsetter at lagrede personopplysninger bare kan benyttes i den grad formålet med overvåkningen krever det.

Sjette ledd er en videreføring av gjeldende sikkerhetslov § 13 a femte ledd. Her pålegges virksomheten en informasjonsplikt overfor brukerne av systemet i samsvar med personopplysningsloven § 19. *Sjuende ledd* er en videreføring av gjeldende sikkerhetslov § 13 a sjette ledd, men med noen presiseringer.

Til § 6-5

Bestemmelsen er i all hovedsak en videreføring av gjeldende sikkerhetslov § 15, andre ledd, om inntrengingstesting og utvalgets forslag til § 6-6.

Det framgår av *første ledd* at virksomheten kan be sikkerhetsmyndigheten om inntrengningstesting, men at denne ikke har en plikt til å gjennomføre en slik test. Ordningen er et tilbud til virksomhetene som er omfattet av loven. Det er opp til den enkelte virksomhet å vurdere behovet for tiltaket. Se nærmere om dette i kapittel 10.5.3.

Første ledd andre punktum fastsetter at formålet med inntrengningstesten skal være å bedre virksomhetens sikkerhet. Virksomhetens orienteringsplikt etter *første ledd tredje punktum* er generelt utformet, og innebærer eksempelvis at det er tilstrekkelig at de ansatte er klar over at slike kontroller tidvis kan forekomme.

Av *andre ledd* framgår det at i de tilfellene hvor inntrengingstesten gjelder informasjonssystemer som behandler personopplysninger, skal formåls- og forholdsmessigheten av testen vurderes. Det må foretas en vurdering av konsekvensene for personvernet, i tillegg til den vurdering skal gjøres etter første ledd.

Tredje ledd fastslår at informasjonen bare kan brukes til å ivareta formålet med kontrollen. Dette innebærer for det første at informasjonen kan brukes til gjennomføring av selve kontrollen og til rapportering etter *femte ledd*. I de tilfellene hvor det oppdages alvorlige avvik, bør informasjonen videreformidles til det departementet som har det overordnede sektoransvaret for virksomheten. For det andre, jf. tredje punktum, kan informasjonen brukes i sikkerhetsmyndighetens øvrige forebyggende sikkerhetsarbeid. Dette skal særlig dekke behovet for at sikkerhetsmyndigheten kan samle og analysere funn og erfaringer fra kontrollen, slik at dette kan brukes i risikovurderinger, for å forbedre sikkerhetstiltak, til utvikling av metodikk for undersøkelser og i rådgivningsarbeidet. De nærmere vilkårene for slik bruk må fastsettes i forskrift, og det må tas tilstrekkelig hensyn til personvern og virksomhetssensitiv informasjon, jf. sjette ledd.

Fjerde ledd tilsvarer deler av gjeldende § 11-8 i forskrift om informasjonssikkerhet. Rapporteringen må ses i sammenheng med sikkerhetsmyndighetens plikter, jf. § 2-2. Hovedformålet med rapporten er å forbedre virksomhetens sikkerhet. Se for øvrig kapittel 10.5.3.

Det følger av *femte ledd* at andre enn sikkerhetsmyndigheten kan utføre inntrengingstesting. Det kan være virksomheten selv eller andre offentlige eller private virksomheter. Det er en nødvendig forutsetning for slik aktivitet at nærmere vilkår for aktiviteten fastsettes i forskrift.

Til § 6-6

Bestemmelsen er i all hovedsak en videreføring av gjeldende sikkerhetslov § 15 første ledd om monitoring, og utvalgets forslag til § 6-5.

Etter *første ledd* kan virksomheten be sikkerhetsmyndigheten gjennomføre kontroll av om systemet behandler gradert informasjon det ikke er godkjent for. Ordningen skal kun være et supplement til øvrige relevante sikkerhetstiltak, og er et tilbud til de virksomhetene som ser behov for slik kontroll av sine informasjonssystemer. Hjemmelen til å bestemme om og når andre enn sikkerhetsmyndigheten kan utføre kommunikasjons- og innholdskontroll, er lagt til Kongen, jf. åttende ledd.

Formålet med kontrollen er å undersøke om det behandles sikkerhetsgradert informasjon i systemer utover det systemet er godkjent for. Eksempelvis kan systemer godkjent for sikkerhetsgradert informasjon gradert opp til KONFIDENSIELT, undersøkes med sikte på å finne ut om de behandler informasjon som er gradert HEMMELIG eller høyere, eller tilsvarende for utenlandsk gradert informasjon. Informasjonssystemer som er helt åpne og som ikke er kategorisert som skjermingsverdig etter sikkerhetsloven, kan undersøkes for å se om de likevel behandler sikkerhetsgradert informasjon gradert BEGRENSET eller høyere, eller tilsvarende for utenlandsk gradert informasjon. Bestemmelsen gir hjemmel til å undersøke *alle* virksomhetens informasjonssystemer, ikke bare de som er *skjermingsverdige*. Virksomhetens orienteringsplikt etter *første ledd andre punktum* er generelt utformet og innebærer at det er tilstrekkelig at de ansatte er klar over at slike kontroller tidvis kan forekomme.

Andre ledd setter rammene for hvilke metoder som kan inngå i kontrollen. Både avlytting og avlesing av informasjon er tillatt.

Tredje ledd viderefører forbudet etter gjeldende sikkerhetslov § 15, mot å kontrollere privat kommunikasjon og kommunikasjon med virksomheter som ikke omfattes av sikkerhetsloven. Kontroll av kommunikasjon mellom skjermingsverdige informasjonssystemer i ulike virksomheter som er omfattet av sikkerhetsloven, er likevel tillatt.

Fjerde ledd fastsetter taushetsplikt for den som blir kjent med slik informasjon som det er forbud mot å samle inn. For en nærmere beskrivelse av hva som ligger i begrepene *arbeid* og *tjeneste*, se merknadene til § 5-4.

Femte ledd skal sikre at virksomhetens ledelse foretar en grundig vurdering av behovet for, og konsekvensene av kontrollen. Det følger forutsetningsvis av første punktum at sikkerhetsmyndigheten må vurdere faren for at kontrollen fanger opp kommunikasjon som beskrevet i tredje ledd. Virksomhetens ledelse må godta både metodene for kontrollen, og sikkerhetsmyndighetens vurdering, før kontrollen kan settes i gang. Virksomhetens ledelse må i sin avgjørelse vurdere betydningen kontrollen vil kunne ha for sikkerheten i virksomhetens informasjonssystemer, opp mot faren for brudd på personvernet.

Sjette ledd regulerer sikkerhetsmyndighetens behandling og bruk av informasjon som den blir kjent med gjennom kontrollen. Blant annet kan informasjonen brukes til gjennomføring av selve kontrollen og til rapporteringen som følger av *sjuende ledd*. Etter *tredje punktum* kan informasjonen brukes i sikkerhetsmyndighetens øvrige forebyggende sikkerhetsarbeid. Dette skal særlig dekke behovet for at sikkerhetsmyndigheten kan samle og analysere funn og erfaringer fra kontrollen, slik at dette kan brukes i risikovurderinger, for å forbedre sikkerhetstiltak, til utvikling av metodikk for undersøkelser og i rådgivningsarbeidet. De nærmere vilkårene for slik bruk må fastsettes i forskrift, og det må tas tilstrekkelig hensyn til personvern og virksomhetssensitiv informasjon.

Sjuende ledd tilsvarer deler av dagens forskrift om informasjonssikkerhet § 11-8. Rapporteringen må ses i sammenheng med sikkerhetsmyndighetens plikter, jf. forslaget til § 2-2. Hovedformålet med kontrollen er å forbedre virksomhetens sikkerhet.

Det følger av *åttende ledd* at andre enn sikkerhetsmyndigheten kan utføre kommunikasjons- og innholdskontroll. Det kan være virksomheten selv eller andre offentlige eller private virksomheter. Det er en nødvendig forutsetning for slik aktivitet at nærmere vilkår for aktiviteten fastsettes i forskrift.

19.7 Kapittel 7 Objekt- og infrastruktursikkerhet

Til § 7-1

Bestemmelsen er i hovedsak en videreføring av gjeldende sikkerhetslov § 17, med den viktige forskjell at begrepet infrastruktur er lagt som tillegg til begrepet objekt. Materielt sett er innholdet en videreføring av utvalgets forslag til § 7-1, bortsett fra forslaget om å gi sikkerhetsmyndigheten en adgang til å påklage et departementsvedtak inn

for et tvisteorgan. I stedet kan sikkerhetsmyndigheten med dette lovforslaget bringe saken inn for det departement som har overordnet ansvar for forebyggende sikkerhetsarbeid i sivil sektor eller det departement som har overordnet ansvar for forebyggende sikkerhetsarbeid i forsvarssektoren, dersom departementet ikke fatter vedtak i tråd med sikkerhetsmyndighetens forslag, jf. redegjørelsen for sjette ledd nedenfor.

Bestemmelsen regulerer departementenes og sikkerhetsmyndighetens ansvar og myndighet til å utpeke, klassifisere og holde oversikt over skjermingsverdige objekter og infrastruktur. Begrepene skjermingsverdig objekt og skjermingsverdig infrastruktur er nærmere omtalt i kapittel 11.2 ovenfor.

Bestemmelsen må ses i forlengelsen av departementenes og sikkerhetsmyndighetens myndighet til å treffe enkeltvedtak etter § 1-3 første og fjerde ledd.

Det heter i *første ledd* at objekter og infrastruktur er skjermingsverdige dersom det kan skade grunnleggende nasjonale funksjoner om de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse. Det avgjørende for relevans til sikkerhetsloven er at enhetene, enkeltvis eller en sammensetning eller en samling av enheter, har et beskyttelsesbehov for å hindre skade på grunnleggende nasjonale funksjoner. Det må gjøres en konkret vurdering hvorvidt et objekt eller en infrastruktur er skjermingsverdig. I en slik vurdering skal det legges vekt på redundans og desentralisering der dette er naturlig. I enkelte særlige tilfeller vil loven også kunne omfatte virksomheter som forvalter objekter som ikke anses å ha avgjørende betydning for grunnleggende nasjonale funksjoner, jf. § 1-1. Dette gjelder objekter som, dersom de blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse, har et skadepotensial som direkte kan ha konsekvenser for nasjonale sikkerhetsinteresser.

Etter bestemmelsens *andre ledd* gis departementene myndighet til å utpeke og klassifisere skjermingsverdige objekter og infrastruktur innen egne ansvarsområder. Hva gjelder skjermingsverdige objekter, er dette en videreføring av departementenes myndighet etter gjeldende sikkerhetslov kapittel 5. Departementene pålegges også en plikt til å holde oversikt over slike objekter og slik infrastruktur. Plikten må ses i sammenheng med departementenes overordnede ansvar for forebyggende sikkerhet i egen sektor, jf. § 2-1 første ledd. De objekter og den infrastruktur som utpekes og klassifiseres, skal dessuten meldes inn til sikkerhetsmyndigheten med angivelse av klassifiseringsgrad. På den måten kan sikkerhetsmyndigheten ha en helhetlig og sektorovergripende oversikt over skjermingsverdige objekter og infrastruktur, og får muligheten til å kunne se gjensidige sammenhenger og avhengigheter.

I bestemmelsens *tredje ledd* gis sikkerhetsmyndigheten en tilsvarende myndighet og plikt som departementene har etter andre ledd første punktum, overfor objekter og infrastruktur som ikke ligger innenfor et departements ansvarsområde, se også merknad til § 1-3 fjerde ledd.

Etter *fjerde ledd* skal virksomheter som råder over objekter eller infrastruktur som utpekes etter andre eller tredje ledd, varsles om utpekingen. Etter *femte ledd* kan en avgjørelse om slik utpeking overfor et selvstendig rettssubjekt påklages til overordnet organ etter reglene i forvaltningsloven kapittel VI, på samme måte som klage etter enkeltvedtak etter § 1-3 første ledd og etter § 2-2 fjerde ledd, se merknad til disse bestemmelsene. Vedtak fattet av et departement kan påklages til Kongen i statsråd, mens vedtak av sikkerhetsmyndigheten kan påklages til departementet.

Etter bestemmelsens *sjette ledd* kan sikkerhetsmyndigheten på eget initiativ fremme forslag overfor ansvarlig departement om at det bør treffes vedtak etter andre ledd. Med *et departement* menes her det ansvarlige fagdepartementet. Dersom slikt vedtak ikke fattes, og sikkerhetsmyndigheten fastholder sin anbefaling, kan sikkerhetsmyndigheten bringe saken inn for endelig avgjørelse til det departementet som har det overordnede ansvaret for forebyggende sikkerhetsarbeid i sivil sektor, eller det departementet som har det overordnede ansvaret for forebyggende sikkerhetsarbeid i forsvarssektoren. Per i dag følger dette av kronprinsregentens resolusjon 4. juli 2003 om fordeling av ansvar for forebyggende sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet (Justis- og beredskapsdepartementet i sivil sektor og Forsvarsdepartementet i forsvarssektoren).

I *sjuende ledd* gis det en hjemmel til Kongen om å gi forskrift om utpeking og klassifisering av objekter og infrastruktur, og om melding til sikkerhetsmyndigheten.

Til § 7-2

Bestemmelsen er i hovedsak en videreføring av utvalgets forslag til § 7-2. Imidlertid er begrepet «risiko- og sårbarhetsanalyse» erstattet med «skadevurdering», som skal forstås som en mindre omfattende vurdering.

Bestemmelsen regulerer hvordan skjermingsverdige objekter eller infrastruktur skal klassifiseres. Myndigheten til å klassifisere objekter og infrastruktur tilligger ansvarlig departement eller sikkerhetsmyndigheten, jf. § 7-1 andre og tredje ledd. Formålet med klassifisering av objekter og infrastruktur er dels at det er styrende for hvilke sikkerhetstiltak som skal iverksettes, jf. § 7-3, og dels at det gir myndighetene anledning til å kunne prioritere mellom ulike objekt eller infrastruktur, avhengig av hvor store skadefølger redusert funksjonalitet vil kunne ha for grunnleggende nasjonale funksjoner.

Første ledd i bestemmelsen slår fast at skjermingsverdige objekter og infrastruktur skal klassifiseres dersom det kan skade grunnleggende nasjonale funksjoner at de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse.

Etter første ledd *bokstav a* skal MEGET KRITISK benyttes dersom redusert funksjonalitet kan få helt avgjørende skadefølger. Begrepet *helt avgjørende skadefølger* skal forstås på samme måte som i § 5-3 første ledd bokstav a.

Etter første ledd *bokstav b* skal KRITISK benyttes dersom redusert funksjonalitet kan få alvorlige skadefølger. Begrepet *alvorlige skadefølger* skal forstås på samme måte som i § 5-3 første ledd bokstav b.

Etter første ledd *bokstav c* skal VIKTIG benyttes dersom redusert funksjonalitet kan få skadefølger. Begrepet *kan få skadefølger* skal forstås på samme måte som i § 5-3 første ledd bokstav c.

Bestemmelsens *andre ledd* slår fast at klassifiseringen skal skje på grunnlag av en skadevurdering, og det skal spesifiseres hvilke grunnleggende nasjonale funksjoner objektet eller infrastrukturen understøtter og hva konsekvensene av redusert funksjonalitet vil være. Som en konsekvens av dette er det nødvendig at ansvarlig departement eller sikkerhetsmyndigheten får tilgang til virksomhetens vurdering på dette punkt i klassifiseringsarbeidet, siden klassifiseringen vil bygge på den foretatte skadevurderingen og inngå i begrunnelsen i den oversikt som skal sendes til sikkerhetsmyndigheten. Disse begrunnelsene vil være av sentral betydning for sikkerhetsmyndighetens mulighet til å kunne kvalitetssikre departementenes klassifisering av objekter og infrastruktur i medhold av bestemmelsen. Selve begrunnelsen vil i seg selv være meget sensitiv informasjon, og vil måtte behandles deretter, jf. kapittel 5 om informasjonssikkerhet.

I bestemmelsens *tredje ledd* presiseres det at klassifiseringsnivået kan være forskjellig for ulike deler av et objekt eller en infrastruktur. I den utstrekning dette er tilfelle, skal slike deler defineres som selvstendige objekter eller infrastruktur. Det er altså mulig å definere *objekt i objekt*, *infrastruktur i infrastruktur* og *objekt i infrastruktur*. Dette innebærer at det kan være ulike klassifiseringsnivåer for ulike deler innad i samme objekt eller infrastruktur, med ulike beskyttelsesbehov. Sikkerhetstiltakene, jf. § 7-3, vil da også kunne differensieres avhengig av de ulike delenes klassifisering.

I *fjerde ledd* gis hjemmel for Kongen til å gi forskrift om klassifisering av skjermingsverdige objekter og infrastruktur.

Til § 7-3

Bestemmelsen er i all hovedsak en videreføring av utvalgets forslag til § 7-3.

Bestemmelsen regulerer virksomhetenes plikt til å iverksette sikkerhetstiltak for utpekt og klassifisert objekt eller infrastruktur. Bestemmelsen må ses i sammenheng med de generelle kravene til forebyggende sikkerhet i § 4-3.

Etter *første ledd* plikter virksomheten å iverksette de sikkerhetstiltak som er nødvendige for å opprettholde et forsvarlig sikkerhetsnivå. Begrepet forsvarlig sikkerhetsnivå viser tilbake på den rettslige standarden i § 4-3 første ledd, og skal forstås på samme måte. Slike tiltak kan bestå av fysiske, elektroniske, menneskelige eller organisatoriske barrierer, systemer som skal oppdage og varsle om aktivitet eller hendelser (deteksjon), systemer og rutiner for avklaring vedrørende aktiviteter og hendelser og bakgrunnen for dem (verifikasjon) eller oppfølging av uønskede aktiviteter og hendelser (reaksjon), eller en kombinasjon av slike tiltak, jf. bokstavene a til e. Tiltakene skal være funksjonsbaserte og derfor vil også andre passende tiltak kunne være aktuelle.

I *andre ledd* presiseres det at de nødvendige sikkerhetstiltakene skal bygge på en vurdering av risiko, jf. § 4-2. Vurderingen skal bidra til å avklare hvilke tiltak som er nødvendige for å beskytte objektet eller infrastrukturen.

I *tredje ledd* angis det at beskyttelse av objekter og infrastruktur også kan omfatte krav til personers adgangsklarering etter § 8-3, for tilgang til hele eller deler av skjermingsverdige objekter eller infrastruktur. Med *tilgang* menes i denne sammenheng både fysisk og logisk tilgang til objekt eller infrastruktur. For enkelte typer objekt eller infrastruktur vil det ikke være nødvendig med fysisk tilgang for å gjøre skade. En logisk (digital) tilgang kan i noen tilfeller gi like gode

muligheter til å gjøre skade av betydning for objektets eller infrastrukturens funksjonalitet.

I *fjerde ledd* gis hjemmel for Kongen til å gi forskrift om beskyttelse av objekter og infrastruktur innenfor hvert klassifiseringsnivå og om bruk av sikringsstyrker.

Til § 7-4

Bestemmelsen er i hovedsak en videreføring av utvalgets forslag til § 7-4. Departementet foreslår et nytt fjerde ledd om rapportering av resultatet av den kontroll som paragrafen omhandler. Utvalgets fjerde og femte ledd blir derfor femte og sjette ledd her.

Bestemmelsen regulerer i *første ledd* virksomhetens adgang til å be sikkerhetsmyndigheten om å gjøre forsøk på å forsere virksomhetens etablerte sikkerhetstiltak for tilgang til skjermingsverdig objekt eller infrastruktur. Bestemmelsen korresponderer og må ses i sammenheng med hjemmelen for inntrengingstesting av skjermingsverdige informasjonssystemer, jf. § 6-5.

Slik testing er et frivillig tilbud til den enkelte virksomhet, og kan bare gjøres på anmodning fra ledelsen i den aktuelle virksomheten. Formålet med denne typen testing er å forsøke å avdekke svakheter ved de tiltak som en virksomhet har iverksatt for å hindre at uvedkommende får tilgang til objektet eller infrastrukturen. Virksomhetens orienteringsplikt etter første ledd *tredje punktum* er generelt utformet og innebærer at det er tilstrekkelig at de ansatte er klar over at slike kontroller tidvis kan forekomme.

Bestemmelsens *andre ledd* hjemler behandling av personopplysninger ved testing, og fastslår at det skal gjøres en nødvendighets- og forholdsmessighetsvurdering av behovet for slik kontrollvirksomhet, ved at kontrollen ikke skal gjøres *mer omfattende enn det som formålet med kontrollen krever*.

Tredje ledd angir en formålsavgrensing for bruk av informasjon som testingen gir tilgang til. Med informasjon menes i denne sammenheng både personopplysninger og opplysninger om virksomheten. Bestemmelsens formål om å kontrollere og eventuelt forbedre virksomhetens sikkerhetsnivå, vil være styrende for hva informasjonen kan brukes til. Den læring og kunnskap som sikkerhetsmyndigheten tilegner seg gjennom slike kontroller, kan brukes til myndighetens videreutvikling av sitt generelle sikkerhetsarbeid.

Etter bestemmelsens *fjerde ledd* skal sikkerhetsmyndigheten gi rapport om resultatet av kontrollen til virksomheten, der innholdet i rapporten bare skal være informasjon som kan bidra til en bedre sikkerhet hos virksomheten.

Etter *femte ledd* kan Kongen i forskrift gi nærmere bestemmelser om testing av sikkerhetstiltak for skjermingsverdige objekter og infrastruktur, og at slik testing kan gjennomføres av andre enn sikkerhetsmyndigheten.

Til § 7-5

Bestemmelsen viderefører i hovedsak gjeldende sikkerhetslov § 18 a første ledd bokstav a, b og c, men i en modernisert språkdrakt og tilpasset øvrig innretning på lovforslaget.

Begrepene *militære øvelser og forsøk* skal forstås som øvelser og forsøk som gjøres av, eller i regi av aktører i forsvarssektoren (Forsvarsdepartementet og underliggende etater), og vil ikke utelukkende gjelde øvelser og forsøk som utføres av etaten Forsvaret. Den til enhver tid gjeldende organiseringen av forsvarssektoren vil være styrende for hvordan bestemmelsen må forstås og praktiseres. Det avgjørende vil være om aktiviteten det tas sikte på å skjerme ved et adgangsforbud, direkte eller indirekte har betydning for Forsvarets operative evne. Eksempelvis vil etatene Forsvarets forskningsinstitutt og Forsvarsmateriell kunne gjennomføre øvelser og forsøk som har eller vil få betydning for Forsvarets operative evne.

Formuleringen «bestemte angitte steder eller områder» behøver ikke å knytte seg til militær virksomhet, men avgrenses til aktiviteter eller virksomhet som ligger innenfor sikkerhetslovens ramme.

Endringene er ikke ment å gjøre store realitetsendringer i dagens rettstilstand på området.

19.8 Kapittel 8 Personellsikkerhet

Til § 8-1

Bestemmelsen er i hovedsak en videreføring av gjeldende sikkerhetslov § 19 første ledd, og regulerer når *sikkerhetsklarering*, *adgangsklarering* og *autorisasjon* skal gjennomføres.

Med *sikkerhetsklarering* menes en avgjørelse fra klareringsmyndigheten om at en person er sikkerhetsmessig skikket til å kunne håndtere sikkerhetsgradert informasjon opp til et gitt sikkerhetsnivå.

Med *adgangsklarering* menes en avgjørelse om at en person er sikkerhetsmessig skikket for tilgang til klassifiserte områder innenfor skjermingsverdige objekter eller infrastruktur jf. § 8-3.

Med *autorisasjon* menes avgjørelse fra autorisasjonsansvarlig i den enkelte virksomhet om at en person, etter en konkret helhetsvurdering, gis tilgang til sikkerhetsgradert informasjon eller tilgang til klassifiserte områder innen objekter eller infrastruktur.

Første ledd er en videreføring av utvalgets forslag til § 8-1 første ledd og slår fast at autorisasjon i medhold av § 8-9 skal gjennomføres for to kategorier personell. For det første gjelder det for personer som skal gis tilgang til sikkerhetsgradert informasjon, jf. første ledd *første punktum*. *[S]kal få tilgang* indikerer at vedkommende gjennom sitt arbeid har tjenstlig behov for tilgang til slik informasjon. For det andre gjelder kravet til autorisasjon, i henhold til første ledd *andre punktum*, personer som skal ha tilgang til klassifiserte områder innen objekter og infrastruktur, der det er fattet vedtak etter § 8-3. Med *adgang* menes både fysisk og logisk tilgang til slike objekter eller infrastruktur, se merknad til § 8-3. Adgangsklarering for laveste klassifiseringsgrad er ment å være en mindre omfattende og enklere klareringsprosess enn for de høyere klassifiseringsgradene, som kan være tilnærmet lik klareringsprosessen for sikkerhetsklarering.

Andre ledd er en videreføring av utvalgets forslag til § 8-1 andre ledd og gjeldende sikkerhetslov § 19 andre ledd, og slår fast at personer som skal autoriseres for tilgang til sikkerhetsgradert informasjon KONFIDENSIELT eller høyere, på forhånd skal sikkerhetsklareres. Andre ledd *andre punktum* er ny og slår fast at personer som skal ha adgang til skjermingsverdige objekter eller infrastruktur som det er truffet vedtak om etter 8-3 tredje ledd, på forhånd må adgangsklareres.

Etter *tredje ledd* kan Kongen gi forskrift om behandling av klareringssaker og gyldighetstiden til klareringer. På samme måte som etter dagens regelverk, vil det være behov for nærmere regler for saksbehandlingen, blant annet når og på hvilken måte autorisasjon og sikkerhetsklarering skal gjennomføres.

Til § 8-2

Bestemmelsen er i hovedsak en videreføring av gjeldende sikkerhetslov § 19 andre til fjerde ledd. Bestemmelsen regulerer bruk av sikkerhetsklarering og de ulike nivåene som sikkerhetsklarering gjelder for. Bestemmelsen er utledet av utvalgets forslag til § 8-1 fjerde og femte ledd. Reguleringen av sikkerhetsgrader i NATO videreføres i forskrift, jf. tredje ledd.

Første ledd slår fast at en person må sikkerhetsklareres før vedkommende kan få tilgang til informasjon gradert KONFIDENSIELT eller høyere etter § 5-3.

Andre ledd gjelder personer som gjennom sitt arbeid *vil kunne få* tilgang til sikkerhetsgradert informasjon. Bestemmelsen er en videreføring av gjeldende sikkerhetslov § 19 tredje ledd. Det er ikke et vilkår for sikkerhetsklarering at vedkommende faktisk vil få tilgang til slik informasjon. I forarbeidene til gjeldende sikkerhetslov vises det som eksempel til vakter, rengjøringspersonell og andre som forutsetningsvis ikke skal ha tilgang til slik informasjon, men som gjennom sitt arbeid er i en posisjon hvor en lett kan skaffe seg slik tilgang. Et vilkår for sikkerhetsklarering av slikt personell er at andre risikoreduserende tiltak som kan kompensere for bruk av sikkerhetsklarering skal vurderes først.

Etter *tredje ledd* kan Kongen gi forskrift om forholdet mellom nasjonale sikkerhetsgrader og sikkerhetsgrader i NATO, andre nasjoner, eller andre internasjonale organisasjoner.

Til § 8-3

Bestemmelsen er ny og regulerer forutsetningene for bruk av adgangsklarering.

Første ledd er en videreføring av utvalgets forslag til § 7-3 tredje ledd og slår fast at det enkelte ansvarlige departement innen sitt myndighetsområde kan fatte vedtak om krav til adgangsklarering. Dette gjelder tilgang til hele eller deler av skjermingsverdige objekter eller infrastruktur. Det slås også fast at sikkerhetsmyndigheten kan fatte slike vedtak overfor virksomheter som ikke ligger innenfor et departements myndighetsområde.

I bestemmelsens *andre ledd* slås det fast at adgangsklarering ikke skal brukes dersom det finnes andre sikringstiltak som er bedre egnet og kan kompensere for bruk av klarering. For eksempel kan visse områder skjermes for innsyn eller dersom adgangsbehovet er sjeldent forekommende, kan sikkerhetsbehovet dekkes ved at vedkommende følges av sikkerhetspersonell. *Tredje ledd* slår fast at avgjørelse om adgangsklarering som gjelder selvstendige rettssubjekter kan påklages.

Fjerde ledd slår fast at adgangsklarering gjelder for personer som skal ha tilgang til objekter og infrastruktur klassifisert etter § 7-2. I bestemmelsen *andre punktum* slås det fast at departementet kan bestemme at personer med sikkerhetsklarering for et bestemt nivå også er klarert

for adgang til et bestemt skjermingsverdig objekt eller en bestemt skjermingsverdig infrastruktur. Adgangsklarering skal være et forenklet supplement til sikkerhetsklarering og ikke en erstatning. Det er det konkrete behovet som skal avgjøre hvilken klarering som velges.

Etter *femte ledd* kan Kongen gi forskrift om krav til adgangsklarering og forholdet mellom sikkerhetsklarering og adgangsklarering. Det vil være behov for nærmere å regulere bruken av de to klareringstypene, blant annet for å klargjøre forholdet mellom sikkerhetsgradert informasjon og den type informasjon tilgang til skjermingsverdig objekt eller infrastruktur kan gi.

Til § 8-4

Bestemmelsen angir det nærmere vurderingstemaet for når klarering skal gis eller opprettholdes. Bestemmelsen skiller seg fra utvalgets forslag til § 8-5 ved at opplistingen av vurderingstemaene er tatt inn i bestemmelsens fjerde ledd, som er en videreføring av gjeldende sikkerhetslov § 21. Vurderingstemaene er omredigert noe, slik at opplistingen går fra a til o.

Hvorvidt en person skal gis en sikkerhetsklaring beror på en helhetsvurdering av om en person er sikkerhetsmessig skikket. Etter *første ledd* skal klarering bare gis eller opprettholdes dersom det ikke foreligger rimelig grunn til å tvile på om en person er sikkerhetsmessig skikket. Vurderingen av *rimelig tvil* må ses i sammenheng med det nivået vedkommende skal klareres for. Desto høyere klareringsnivå, desto mindre grad av tvil kan aksepteres.

Andre ledd slår fast at i vurderingen om personen er *sikkerhetsmessig skikket, skal* det legges vekt på personens pålitelighet, lojalitet og dømmekraft i forbindelse med behandlingen av sikkerhetsgradert informasjon og tilgang til skjermingsverdige objekter eller infrastruktur. En personkontroll etter § 8-5, skal være grunnlaget for vurderingen.

Tredje ledd slår fast at klareringssaken skal være så godt opplyst som mulig, og at dersom det er tvil om en person er sikkerhetsmessige skikkethet skal det gjennomføres en sikkerhetssamtale. Det er klareringsmyndigheten som er ansvarlig for at saken er tilstrekkelig opplyst.

Fjerde ledd lister opp forhold som det i vurderingen kan legges vekt på i forbindelse med personkontrollen.

I fjerde ledd *bokstav a* er *terror* lagt til som en naturlig del av hva som kan vektlegges, jf. gjeldende sikkerhetslov § 21 første ledd bokstav a. I bokstav c er ordlyden endret i tråd med endret definisjon av nærstående, jf. § 1-5 nr. 5 og merknad til § 8-5. I bokstav h er *unnlatelse* lagt til som en naturlig del av hva som kan vektlegges, jf. dagens sikkerhetslov § 21 første ledd bokstav g. Videre er bokstav g splittet opp hvor den delen som omhandler unnlatelse av å gi autorisasjonsansvarlig løpende underretning er ny bokstav i, nektelse av å gi taushetsløfte eller delta i sikkerhetssamtale er ny bokstav j. De påfølgende bokstavhenvisingene er dertil endret. I ny bokstav k er ordlyden endret fra *friste til utroskap* til *å handle i strid med nasjonale sikkerhetsinteresser.* Dette er ikke en materiell endring men en tydeliggjøring av hva som er hensikten med vurderingskriteriet.

Etter *femte ledd* er det et totalforbud mot å legge vekt på lovlig politisk engasjement og annet lovlig samfunnsengasjement i vurderingen av sikkerhetsmessig skikkethet.

I bestemmelsens *sjette ledd* avgrenses klareringsmyndighetens anledning til å vektlegge opplysninger om nærstående personer til tilfeller der det antas at disse forholdene vil kunne påvirke om en person er sikkerhetsmessig skikket.

Etter *sjuende ledd* kan Kongen gi forskrift om klarering og gjennomføring av sikkerhetssamtale. Bestemmelsen er en videreføring av forskriftshjemmelen i gjeldende sikkerhetslov § 26 andre ledd og utvalgets forslag til § 17 andre ledd bokstav a og c.

Til § 8-5

Bestemmelsen er i hovedsak en videreføring av gjeldende sikkerhetslov § 20 og utvalgets forslag til § 8-7. Bestemmelsen regulerer gjennomføring av personkontroll som grunnlag for klareringsmyndighetens vurdering av om en person er sikkerhetsmessig skikket etter § 8-4.

Etter *første ledd første punktum* skal sikkerhetsmyndigheten gjennomføre personkontroll av alle som skal adgangs- eller sikkerhetsklareres. Med *personkontroll* menes i denne sammenhengen både opplysninger fra vedkommende selv og de opplysninger klareringsmyndigheten selv besitter eller innhenter fra relevante registre eller andre kilder.

Etter *andre ledd* er det et vilkår for å igangsette personkontroll at den aktuelle personen er gjort oppmerksom på, og har *samtykket* til, at slik kontroll igangsettes. I *tredje punktum* slås det fast at samtykket også omfatter muligheten for fornyet personkontroll innenfor gyldighetstiden, dersom det er behov for det, jf. tredje ledd. Utvalget har i sitt forslag erstattet s*amtykke* med *aksept* og

begrunnet dette med at en person som søkes klarert i de fleste tilfeller er i en arbeids-/arbeidstakerrelasjon, noe som gjør det vanskelig til å oppfylle kravene til et frivillig samtykke. Departementets vurdering er at det kun er unntaksvis at krav til klarering inntreffer etter at en person er tilsatt i en stilling. I de aller fleste tilfeller har den enkelte et valg om hvorvidt man vil søke på en stilling som har krav til klarering. Et samtykke til gjennomføring av en personkontroll anses derfor som frivillig og informert, og videreføres fra gjeldende lov.

Tredje ledd er i all hovedsak en videreføring av utvalgets forslag til § 8-8, men med språklige forenklinger, jf. kapittel 12.5.8. Bestemmelsen regulerer klareringsmyndighetens adgang til å kunne anmode om fornyet personkontroll ved behov, når som helst i klareringens gyldighetstid. Retten til å anmode om slik fornyet personkontroll gjelder både ved mistanke om nye forhold som kan påvirke om en person er sikkerhetsmessig skikket, og som et ledd i regelmessig oppfølging av klarert personell. Med klareringsmyndigheten menes også klagemyndigheten ved behandling av klager på avgjørelse om klarering, jf. § 8-17.

Etter *fjerde ledd* skal personkontrollen omfatte opplysninger gitt av personen selv, og som plikter å gi fullstendige opplysninger som kan ha betydning for den sikkerhetsmessige skikketheten, jf. § 8-4. Bestemmelsens *andre punktum* er ny og slår fast at en klareringssak kan avsluttes uten realitetsbehandling dersom en person ikke svarer på henvendelser fra klareringsmyndigheten. Departementet viser til at det i noen særskilte tilfeller ikke er mulig for en person å besvare henvendelser fra klareringsmyndigheten. Under slike omstendigheter kan saken avsluttes uten realitetsbehandling. Dette til forskjell for unnlatelsestilfellene nevnt i § 8-4 bokstav h, som regulerer de tilfellene som gjelder nektelse eller aktiv handling av ikke å forholde seg til de krav som settes til medvirkning i klareringsprosessen.

Etter *femte ledd* kan det gjennomføres personkontroll av nærstående personer dersom det søkes om sikkerhetsklarering for HEMMELIG eller høyere sikkerhetsgrader. Det samme gjelder for adgangsklarering for objekter og infrastruktur med klassifiseringsgraden MEGET KRITISK. Det kan også gjennomføres personkontroll av nærstående i andre særlige tilfeller. Med begrepet *nærstående* menes personer som er i nær familie eller som har annen nær tilknytning som kan ha betydning for om en person er sikkerhetsmessig skikket, jf. § 1-5 nr. 5. Dette omfatter i første rekke vedkommendes ektefelle, partner, samboer, barn, foreldre og søsken, og andre personer vedkommende er knyttet til ved familiebånd. Begrepet nærstående omfatter imidlertid ikke bare de personer vedkommende har en familiær tilknytning til. Det avgjørende er hvorvidt den aktuelle personen har en relasjon til vedkommende av en slik art at den reelt påvirker om en person er sikkerhetsmessig skikket.

I sjette ledd heter det at personkontrollen også skal omfatte andre opplysninger som klareringsmyndigheten sitter med, og opplysninger fra relevante registre. Med *relevante registre* omfattes også opplysninger som virksomheten har lagret på annen måte, eksempelvis i elektroniske saksarkiv. I bestemmelsens *andre punktum*, vises det til at personkontrollen også kan omfatte andre kilder. Dette kan for eksempel være opplysninger fra private kredittopplysingsregistre, jf. gjeldende forskrift om personellsikkerhet § 3-4.

I *sjuende ledd* slås det fast at det ikke skal innhentes, registreres eller videreformidles opplysninger om politisk engasjement som nevnt i § 8-4 femte ledd.

Etter *åttende ledd* plikter behandlingsansvarlige for relevante registre å utlevere registeropplysninger uten hinder av taushetsplikt. Opplysningene skal gis skriftlig, og det kan ikke kreves vederlag for denne type tjeneste. *Behandlingsansvarlig* skal forstås på samme måte som registereier i gjeldende sikkerhetslov § 20 fjerde ledd andre punktum. Det vil være sikkerhetsmyndigheten som forestår personkontrollen på vegne av de ulike klareringsmyndighetene.

Niende ledd slår fast at behandlingsansvarlige for relevante registre skal legge til rette for en digitalisert overføring av personkontrollopplysninger. Se omtale under 12.5.7.

Tiende ledd slår fast at opplysningene i klareringssakene ikke benyttes til andre formål enn vurdering av klarering. *Andre punktum* viser til at klareringsmyndigheten kan gi autorisasjonsansvarlige opplysninger dersom det av sikkerhetsmessige hensyn er nødvendig. Se omtale under 12.5.9.

I *ellevte ledd* kan Kongen gi forskrift om personkontroll av nærstående, fornyet personkontroll, hvilke registre som er relevante for personkontroll, framgangsmåten ved registerundersøkelser i utlandet, utlevering av opplysninger ved tilsvarende personkontroll som utføres av andre lands myndigheter og arkivering, oppbevaring, forsendelse og digitalisert overføring av personkontrollopplysninger. Bestemmelsen viderefører blant annet gjeldende hjemmel i sikkerhetsloven § 26 andre ledd bokstav b.

Til § 8-6

Første ledd er en videreføring av utvalgets forslag til § 8-9 og er i utgangspunktet også en videreføring av gjeldende lov § 21 siste ledd. Med begrepet *særlige tilfeller* menes at det skal være en viss tilbakeholdenhet med å gi klarering på vilkår eller stillingsklarering, blant annet av likebehandlingshensyn. Men i de tilfeller der alternativet er å avslå klareringsanmodningen, vil bruk av vilkår kunne benyttes dersom dette vurderes som et tilstrekkelig risikoreduserende tiltak. Bruk av vilkår for klarering, herunder stillingsklarering, vil blant annet kunne bidra til et mer fleksibelt system hvor verdifull kompetanse kan rekrutteres, uten at dette innebærer en uakseptabel risiko.

Etter *andre ledd* kan Kongen i forskrift gi nærmere bestemmelser om bruk av vilkår ved klarering.

Til § 8-7

Bestemmelsen er i all hovedsak en videreføring fra gjeldende sikkerhetslov § 22 og utvalgets forslag til § 8-10. *Utenlandske statsborgere* i gjeldende lov § 22 er endret til klarering av *personer med utenlandsk statsborgerskap*. Dette for å tydeliggjøre at det avgjørende er at personen har et utenlandsk statsborgerskap. Personer med både norsk statsborgerskap og utenlandsk statsborgerskap skal vurderes etter denne bestemmelsen. Det samme gjelder statsløse personer.

Vurderingen om klarering kan gis til utenlandsk statsborger skal baseres på en konkret helhetsvurdering, der tilknytning til Norge, tilknytning til hjemlandet og hjemlandets sikkerhetsmessige betydning skal vektlegges i vurderingen, i tillegg til vurderingstemaene i § 8-4, jf. kapittel 12.5.2.

I *andre ledd* er det presisert at bruk av vilkår, som for eksempel stillingsklarering, skal vurderes særskilt ved klarering av personer som har utenlandsk statsborgerskap, hvis slik avgrensning kan være et risikoreduserende tiltak, jf. kapittel 12.5.4.

I *tredje ledd* er Kongen gitt myndighet til i forskrift å gi nærmere bestemmelser om klarering av personer med utenlandsk statsborgerskap

Til § 8-8

Bestemmelsen regulerer i hvilke tilfeller klareringsmyndigheten plikter å vurdere klareringen tilbakekalt, nedsatt eller suspendert for å iverksette nærmere undersøkelser, dersom klareringsmyndigheten får opplysninger som gir grunn til å tvile på at en klarert person fortsatt er sikkerhetsmessig skikket. Klareringsmyndigheten har en plikt til ved slike tilfeller å varsle sikkerhetsmyndigheten og autorisasjonsansvarlig. Bestemmelsen er en videreføring av gjeldende sikkerhetslov § 24 andre og tredje ledd, og utvalgets forslag til § 8-6, og skal forstås på samme måte.

Til § 8-9

Bestemmelsen regulerer hvem som har ansvaret for autorisasjon etter loven, og det nærmere vurderingstemaet for om personer kan gis autorisasjon. Bestemmelsen er videreføring av utvalgets forslag til § 8-2, men med språklige endringer.

Første ledd slår fast at virksomhetens leder er ansvarlig for autorisasjon og den sikkerhetsmessige ledelse og kontroll av autorisert personell i virksomheten. Ansvaret for forebyggende sikkerhetsarbeid er et lederansvar, jf. 4-1 første ledd første punktum. Myndigheten til å gi autorisasjon kan ved behov delegeres, men det presiseres at det er virksomhetens ledelse som har ansvaret. Myndigheten til å ha sikkerhetsmessig ledelse og kontroll av personellet, vil i praksis følges opp av den som har fått delegert myndighet etter første ledd, eksempelvis autorisert personells nærmeste foresatte. Med *sikkerhetsmessig ledelse og kontroll* menes blant annet ansvaret for å påse at autorisert personell har tilstrekkelig opplæring og kompetanse på forebyggende sikkerhetsarbeid, og å påse at personellet faktisk etterlever sikkerhetsbestemmelsene i sitt daglige virke. Autorisasjonsansvarlig skal foreta en tilstrekkelig identitetskontroll av personer som skal autoriseres.

Andre ledd første punktum slår fast at det ikke kan gis autorisasjon før autorisasjonssamtale er avholdt. Andre ledd andre punktum angir vurderingstemaet for avgjørelser om autorisasjon og er en videreføring av gjeldende sikkerhetslov § 23 første ledd. Hvorvidt vedkommende er *sikkerhetsmessig skikket*, må baseres på en konkret helhetsvurdering av de opplysninger autorisasjonsansvarlig har tilgjengelig, og på det inntrykket som gis i autorisasjonssamtalen.

I *tredje ledd* slås det fast at sikkerhetsmyndigheten kan kreve at virksomheten skal holde sikkerhetsmyndigheten orientert om hvilke personer som er autoriserte, jf. kapittel 12.5.9. Bestemmelsen er nødvendig for at PST skal kunne be om opplysninger etter § 8-12. Nærmere bestemmelser om utleveringen av opplysningene kan gis i forskrift.

I *fjerde ledd* er Kongen gitt myndighet til å gi nærmere bestemmelser om autorisasjon, autorisa-

sjonsansvarliges plikter og virksomhetens plikt til å holde sikkerhetsmyndigheten orientert om hvilke personer som er autorisert i forskrift.

Til § 8-10

Første ledd regulerer i hvilke tilfeller autorisasjonsansvarlig plikter å vurdere autorisasjonen opprettholdt, tilbakekalt, nedsatt eller suspendert. Etter første ledd andre punktum framgår det at autorisasjonsansvarlig skal melde fra om avgjørelser til klareringsmyndigheten. Bestemmelsen ivaretar utvalgets forslag til varslingsplikt i § 8-11 andre ledd, jf. kapittel 12.5.6. *Andre ledd* regulerer i hvilke tilfeller autorisasjon automatisk bortfaller.

Bestemmelsen er en videreføring av utvalgets forslag til § 8-3, og av gjeldende sikkerhetslov § 24 andre og fjerde ledd, men med enkelte språklige endringer.

Til § 8-11

Bestemmelsen er en videreføring av utvalgets forslag til § 8-11 første ledd. Bestemmelsen er en presisering av gjeldende sikkerhetslov § 24 første ledd, jf. kapittel 12.5.6.

Til § 8-12

Bestemmelsen er en videreføring av utvalgets forslag til § 8-12, men med språklige endringer. Bestemmelsen er ny og regulerer sikkerhetsmyndighetens adgang til å utlevere opplysninger fra klareringssaker til Politiets sikkerhetstjeneste.

Etter *første ledd* er det et vilkår for utlevering av informasjon at det foreligger en forutgående *anmodning* fra Politiets sikkerhetstjeneste. Anmodningen må i en viss utstrekning ha et presist innhold, slik at utleveringen av informasjon begrenses til det som er nødvendig. Anmodningen kan eksempelvis være avgrenset til å gjelde informasjon om personer som har tilknytning til en bestemt nasjon, eller personer med utenlandsk tilknytning som tjenestegjør innen nærmere definerte virksomheter. Anmodningen bør normalt være avgrenset til å gjelde en nærmere avgrenset tidsperiode. Sikkerhetsmyndigheten vil kunne oppdatere informasjonsgrunnlaget dersom det skjer endringer innenfor den angitte tidsperioden. Anmodningene vil uansett måtte tilpasses det konkrete informasjonsbehovet Politiets sikkerhetstjeneste har på tidspunktet for anmodningen.

De tre typene opplysninger som informasjonsdelingen omhandler framgår av første ledd.

Med *klareringsstatus* menes hvilket nivå de aktuelle personene er klarert for og klareringens gyldighetstid.

Begrepet *tilknytning til andre stater* skal forstås vidt, i den forstand at ulike slags tilknytninger vil kunne være relevante. Det kan for eksempel dreie seg om personene har familiær tilknytning til en fremmed stat eller økonomiske interesser i en fremmed stat. Samtidig vil ikke enhver tilknytning til en annen stat være tilstrekkelig til å oppfylle kravet. Det avgjørende i vurderingen vil være om personen har en slik tilknytning til en annen stat, at denne vil kunne utgjøre et effektivt pressmiddel overfor personen eller på annen måte ha betydning for personens lojalitet til Norge. Praksis vedrørende forståelsen av tilknytningskriteriene etter gjeldende sikkerhetslov § 21 første ledd bokstav k vil være relevant i denne sammenheng. Kriteriene er videreført i § 8-4 femte ledd bokstav n.

Utvalgets forslag til bokstav c *tjenestested* er endret til *tjenestested eller hvilken virksomhet som har anmodet om klarering*. Det vises til omtalen i kapittel 12.5.9. Med tjenestested menes hvor de aktuelle personene arbeider, og viser til konkret virksomhet og hvilken stilling personene innehar i denne virksomheten.

Etter *andre ledd* er det et vilkår for utlevering av informasjon som nevnt i første ledd, at Politiets sikkerhetstjeneste anfører at det er nødvendig for å ivareta tjenestens oppgaver etter politiloven §§ 17 b og 17 c nr. 1. Begrunnelsen for hvorfor utlevering er *nødvendig* i de enkelte tilfellene vil ofte være av slik karakter at Politiets sikkerhetstjeneste ikke kan, eller ikke ønsker, å dele denne begrunnelsen med andre. Når Politiets sikkerhetstjeneste anfører at slik informasjon er nødvendig, skal derfor sikkerhetsmyndigheten legge til grunn at vilkårene for utlevering av informasjon er oppfylt. Begrunnelsen vil i ettertid kunne kontrolleres av EOS-utvalget.

Tredje ledd inneholder en forskriftshjemmel for Kongen til å gi nærmere bestemmelser om utlevering av informasjon til Politiets sikkerhetstjeneste.

Til § 8-13

Bestemmelsen er en videreføring av gjeldende sikkerhetslov § 25 og utvalgets forslag til § 8-13, men med strukturelle og språklige forenklinger.

I *andre ledd* er ordlyden endret, jf. utvalgets forslag til 8-13 tredje ledd andre punktum. Det presiseres at det er opplysningene som kan røpe forhold, jf. bokstav a til e, som ikke skal inngå i *begrunnelsen*.

I *andre ledd bokstav a* er *grunnleggende nasjonale funksjoner* i utvalgets forslag til § 8-17 erstattet med *nasjonale sikkerhetsinteresser*, jf. § 1-5 nr. 1

I *tredje ledd* slås det fast at klareringsmyndigheten skal utarbeide en begrunnelse hvor alle relevante forhold skal inngå. Begrunnelsen må vise til reglene og de faktiske omstendighetene som avgjørelsen bygger på, og de hensyn som har vært vektlagt. I den interne begrunnelsen må også alle vesentlige omstendigheter tas med, også de som er unntatt etter andre ledd.

Til § 8-14

Bestemmelsen er en videreføring av utvalgets forslag til § 8-14 og gjeldende sikkerhetslov § 25 a.

Etter først ledd kan en person kreve å få innsyn i sin klareringssak når det er fattet avgjørelse i saken. Begrepet *sakens dokumenter* skal forstås på samme måte som offentleglova § 4 første ledd, jf. andre ledd.

Etter andre ledd kan personen ikke kreve innsyn i opplysninger som nevnt i § 8-13 andre ledd. Det kan heller ikke kreves innsyn i dokumenter som er utarbeidet for den interne saksforberedelsen. Dette skal forstås på samme måte som etter forvaltningsloven § 18 a. Det kan ikke nektes innsyn i faktiske opplysninger, jf. andre ledd tredje punktum.

Det er tatt inn en forskriftshjemmel i fjerde ledd.

Henvisningen i gjeldende lov til «audiovisuelt opptak av egen sikkerhetssamtale», jf. § 25 a første ledd andre punktum og tredje ledd andre punktum, er ikke videreført. Audiovisuelle opptak omfattes av offentleglovas sitt dokumentbegrep, og nærmere regler om framgangsmåten for gjennomsyn av slike opptak vil bli fastsatt i forskrift etter *fjerde* ledd.

Til § 8-15

Bestemmelsen er en videreføring av utvalgets forslag til § 8-15 og av gjeldende sikkerhetslov § 25 b, med enkelte språklige endringer.

Første ledd gir en person som har fått avslag på innsyn etter 8-14 eller har fått en begrunnelse hvor opplysninger som nevnt i § 8-13 andre ledd er utelatt, rett til å få bistand fra en advokat. Formålet med bestemmelsen er å ivareta rettsikkerheten til den avgjørelsen gjelder. Advokaten kan få innsyn i de dokumentene som er unntatt etter § 8-13 andre ledd. Advokaten har ikke rett til innsyn i dokumenter som er utarbeidet i den interne saksforberedelsen, jf. *andre ledd*.

Det er i dag Forsvarsdepartementet som er ansvarlig for oppnevningen av advokater, jf. *fjerde ledd*.

I *femte ledd* er Kongen gitt myndighet til å gi forskrift om retten til bistand fra advokat, oppnevning av advokater og hvilke opplysninger advokatene kan få tilgang til.

Til § 8-16

Bestemmelsen viderefører gjeldende sikkerhetslov § 23 andre ledd og utvalgets forslag til § 8-4, jf. Prop. 97 L (2015-2016) om endring av klareringsmyndighetsstrukturen. Gjeldende sikkerhetslov § 26 første ledd og utvalgets forslag til § 8-17 første ledd er videreført i tredje ledd.

Til§ 8-17

Bestemmelsen er i stor grad en videreføring av gjeldende sikkerhetslov § 25 c og utvalgets forslag til § 8-6 med strukturelle og språklige endringer.

Begrepet «negativ avgjørelse» er ikke videreført. *Første ledd* viser til hvilke avgjørelser som kan påklages. Avgjørelser om klarering, klaring på vilkår, fastsettelse av tidspunkt for når klaringssaken tidligst kan tas opp på nytt, avslag på begrunnelse og avslag på innsyn påklages. Det er kun den avgjørelsen retter seg mot som kan klage.

Andre ledd regulerer hvem som er klageinstans. Klagen sendes til klareringsmyndigheten som behandler sakene i første instans. Det er sikkerhetsmyndigheten som er klageinstans, med mindre sikkerhetsmyndigheten har fattet vedtaket. I de tilfellene er det departement som er klageinstans.

I *tredje ledd* fremgår hvilke klagefrister som gjelder.

19.9 Kapittel 9 Sikkerhetsgraderte anskaffelser mv.

Til § 9-1

Bestemmelsen regulerer hva som skal anses som en sikkerhetsgradert anskaffelse.

Bestemmelsen er en videreføring av gjeldende sikkerhetslov § 3 nr. 17, men utvides også til å gjelde hvor leverandøren får tilgang til skjermingsverdig infrastruktur i tråd med utvalgets forslag. Det er også inntatt en presisering om at det vil være en sikkerhetsgradert anskaffelse i de tilfellene der leverandører tilvirker sikkerhetsgradert informasjon, jf. kapittel 13.4.2. Det vil være

opp til virksomheten som anskaffer en vare eller tjeneste å vurdere om den leverandøren som skal gjennomføre anskaffelsen vil kunne få tilgang til sikkerhetsgradert informasjon, skjermingsverdig objekt eller infrastruktur.

Det vil også være en sikkerhetsgradert anskaffelse hvor leverandøren bruker underleverandører, eller personell fra underleverandører, som kan få tilgang til eller tilvirker sikkerhetsgradert informasjon, jf. § 5-3, eller som kan få tilgang til et skjermingsverdig objekt eller infrastruktur, jf. § 7-1.

Det er for øvrig gjort mindre språklige endringer for å gjøre bestemmelsen enklere å forstå.

Til § 9-2

Bestemmelsen er i hovedsak en videreføring av gjeldende sikkerhetslov § 27, og utvalgets forslag til § 9-2. Det er inntatt enkelte presiseringer for å tydeliggjøre at en sikkerhetsavtale skal konkretisere de kravene loven og tilhørende forskrifter oppstiller for virksomheten og leverandøren i den sikkerhetsgradert anskaffelsen, jf. §§ 9-1 og 1-2 andre ledd. Utvalgets forslag til andre ledd bokstav b og c er tatt ut av bestemmelsen, og vil bli vurdert tatt inn i forskrift.

For å synliggjøre at sikkerhetsavtalen skal inngås mellom virksomheten som anskaffer varen eller tjenesten, og leverandøren, er det tatt inn et tillegg i overskriften. Videre er *anskaffelsesmyndighet* i *første ledd* erstattet med *virksomheten*.

Av *andre ledd* framgår det hva sikkerhetsavtalen skal inneholde. Sikkerhetsavtalen skal tydeliggjøre og konkretisere hvilke av lovens krav som gjelder for virksomheten og leverandøren i den konkrete anskaffelsen, og hvordan disse skal oppfylles. Hvilke krav som gjelder for den enkelte anskaffelsen vil avhenge av graderingsnivået på informasjonen, jf. lovens kapittel 5, og klassifiseringsgraden og sikringstiltakene for objektet eller infrastrukturen, jf. lovens kapittel 7, som leverandøren får tilgang til ved anskaffelsen. Det vil også kunne gjelde krav som følge av det forebyggende sikkerhetsarbeidet i den aktuelle virksomhet. Kravene vil variere ut fra om gradert informasjon skal oppbevares hos leverandøren eller ikke. Kravene vil dessuten kunne oppfylles gjennom forskjellige typer sikkerhetstiltak.

Eksempelvis vil det i de tilfellene hvor leverandørens personell bare får tilgang til gradert informasjon, skjermingsverdig objekt eller infrastruktur hos virksomheten som foretar anskaffelsen, i utgangspunktet kun være et krav om at leverandørens personell oppfyller kravene etter personellsikkerhetsreglene i lovens kapittel 8. Hvilket krav som stilles til personellet i disse tilfellene, avhenger av om personellet må klareres, jf. §§ 8-2 og 8-3, jf. § 7-3. I tillegg kommer eventuelle krav som følger av det forebyggende sikkerhetsarbeidet i den anskaffende virksomheten, bl.a. reglene om informasjonssikkerhet og informasjonssystemsikkerhet i lovens kapittel 5 og 6. I disse tilfellene kan kravet til sikkerhetsavtale være oppfylt ved at det avtales hvilket personell som eventuelt skal klareres, for hvilken sikkerhetsgrad, og hvilke andre krav som følger av det forebyggende sikkerhetsarbeidet i den anskaffende virksomheten. Dersom leverandørens personell i utgangspunktet skal klareres, jf. §§ 8-2 eller § 8-3, men dette kravet heller skal oppfylles ved at personellet følges rundt av sikkerhetspersonell hos virksomheten, må det framgå av avtalen. Bestemmelsen er ikke ment å være uttømmende, jf. kapittel 13.4.2 og 13.4.3, og vil suppleres av bestemmelser i forskrift.

I *første ledd* framgår det at i de tilfellene der anskaffelsen innebærer at en utenlandsk leverandør, eller personell fra den utenlandske leverandøren, må adgangs- eller sikkerhetsklareres, eller kan få tilgang til sikkerhetsgradert informasjon, skal sikkerhetsmyndigheten godkjenne leverandøren og/eller personellet. Sikkerhetsmyndigheten kontakter sikkerhetsmyndighetene i hjemstaten til leverandøren, som vil bekrefte eller avkrefte hvorvidt leverandøren eller personell fra leverandøren oppfyller de av sikkerhetslovens krav som gjelder i forbindelse med anskaffelsen. Eksempelvis om leverandøren har gyldig leverandørklarering eller om leverandørens personell har nødvendige klareringer. Sikkerhetsmyndigheten i hjemstaten vil også kunne føre sikkerhetsmessig tilsyn med leverandørens utførelse av anskaffelsen i disse tilfellene.

Dersom leverandøren eller personellet ikke har nødvendige klareringer, kan sikkerhetsmyndigheten anmode sikkerhetsmyndigheten i hjemstaten om å foreta nødvendige klareringer. Eventuelt må sikkerhetsmyndigheten og/eller klareringsmyndigheten kunne utveksle nødvendig informasjon med sikkerhetsmyndigheten i hjemstaten for å selv kunne klarere leverandøren eller personellet. Kontakten mellom sikkerhetsmyndigheten og sikkerhetsmyndigheten i hjemstaten til leverandøren forutsetter at det foreligger en bi- eller multilateral avtale om utveksling og plikt til gjensidig beskyttelse av sikkerhetsgradert informasjon mellom norske myndigheter og hjemstaten til leverandøren, jf. kapittel 13.4.3.

En leverandør vil anses som utenlandsk dersom den driver sin virksomhet fra et annet land og under et annet lands jurisdiksjon, og hvor den sikkerhetsmessige oppfølging av leverandøren vil måtte foretas av et annet lands sikkerhetsmyndighet.

Tredje ledd slår fast at leverandøren selv som utgangspunkt skal dekke kostnadene forbundet med å oppfylle sikkerhetslovens krav ved anskaffelsen.

I *fjerde ledd* gis Kongen hjemmel til å bestemme nærmere krav til innholdet i en sikkerhetsavtale, og for hvilke tilfeller det kan gjøres unntak fra kravet om sikkerhetsavtale.

Det er for øvrig gjort mindre språklige endringer for å gjøre bestemmelsen enklere å forstå.

Til § 9-3

Bestemmelsen er i hovedsak en videreføring av gjeldende sikkerhetslov § 28, og utvalgets forslag til § 9-3.

Det følger av *første ledd* at før leverandøren kan få tilgang til sikkerhetsgradert informasjon som er gradert KONFIDENSIELT eller høyere, eller det av andre grunner anses nødvendig, skal leverandøren ha gyldig leverandørklarering for den aktuelle sikkerhetsgraden. I utgangspunktet kreves leverandørklarering kun dersom leverandøren skal ha tilgang eller tilvirke sikkerhetsgradert informasjon i egne lokaler. Der hvor den enkelte leverandørens ansatte bare skal ha innsyn i sikkerhetsgradert informasjon hos virksomheten som gjennomfører anskaffelsen, er det normalt tilstrekkelig at personellet klareres i tråd med reglene for personellsikkerhet i kapittel 8. I tillegg kommer eventuelle bestemmelser om sikkerhetsadministrasjon, informasjonssikkerhet, informasjonssystemsikkerhet m.m., som gjelder hos virksomheten som gjennomfører anskaffelsen.

Med *andre grunner anses nødvendig* i *første ledd andre punktum* menes i første rekke de tilfeller der leverandøren kun vil få tilgang til klassifiserte områder innen skjermingsverdig objekt eller infrastruktur, hvor ansvarlig departement har truffet vedtak om krav til adgangsklarering, jf. § 7-3. Hvorvidt det kreves leverandørklarering for anskaffelser til skjermingsverdig objekt eller infrastruktur, må avgjøres i hvert enkelt tilfelle. I vurderingen bør det særlig tas hensyn til hvorvidt leverandørens personell får tilgang til hele eller deler av objektet eller infrastrukturen som har et høyt skadepotensial. Hvilke andre momenter som skal vektlegges kan fastsettes i forskrift.

Leverandørklarering forutsetter at klareringsmyndigheten faktisk og rettslig har mulighet til å vurdere om en leverandør er sikkerhetsmessig skikket. For utenlandske leverandører har myndighetene bare denne muligheten hvor det foreligger en bi- eller multilateral sikkerhetsavtale mellom Norge og leverandørens hjemstat. Denne avtalen etablerer en gjensidig forpliktelse for myndighetene til å beskytte den annen parts sikkerhetsgraderte informasjon som sin egen og til å bistå hverandre ved sikkerhetsgraderte anskaffelser. Sikkerhetsmyndigheten er kontaktpunktet mot utenlandske sikkerhetsmyndigheter, jf. § 9-2. Ved leverandørklarering av utenlandske leverandører vil derfor sikkerhetsmyndigheten måtte undersøke om leverandøren har gyldig leverandørklarering i hjemstaten. En bi- eller multilateral sikkerhetsavtale gjør at klareringsmyndigheten kan legge leverandørklarering fra leverandørens hjemstat til grunn for vurderingen av sikkerhetsmessig skikkethet. Hva som menes med utenlandsk leverandør framgår av merknaden til § 9-2.

Bestemmelsen *andre til og med femte ledd* skal forstås på samme måte som gjeldende sikkerhetslov § 28 andre til og med femte ledd. Med *ledelse* i *andre ledd siste punktum*, menes daglig leder eller de som har ansvaret for den daglige ledelsen av virksomheten.

Femte ledd viser hovedsakelig til bestemmelsene om begrunnelse og klage i kapittel 8.

For å gjøre regelverket mer fleksibelt for framtidige organisatoriske endringer er det i *sjette ledd første punktum* foreslått at Kongen utpeker hvem som er klareringsmyndighet for leverandørklareringer. Endringen er ikke ment å innebærer materielle endringer.

Det er for øvrig gjort mindre språklige endringer for å gjøre bestemmelsen enklere å forstå.

Til § 9-4

Bestemmelsen er en videreføring av gjeldende sikkerhetslov § 29 a, og utvalgets forslag til § 9-4. Bestemmelsen er imidlertid utvidet til også å omfatte virksomheter som råder over skjermingsverdige informasjonssystemer, for å tilpasse bestemmelsen til at skjermingsverdige informasjonssystemer nå er omfattet av loven. Bestemmelsen pålegger virksomheter som er underlagt loven, og som råder over skjermingsverdig informasjonssystem, objekt eller infrastruktur, jf. §§ 6-1 og 7-1, en varslingsplikt. *Første ledd* er endret for

å tilpasse bestemmelsen til endring i begrepsbruken til *sikkerhetstruende virksomhet*, jf. omtalen under kapittel 6.4.2.

For nærmere om innholdet i bestemmelsen vises til kapittel 13.4.5 og til merknaden til § 29 a i Prop. 97 L (2015–2016), side 75 til 77.

Det er for øvrig gjort mindre språklige endringer for å gjøre bestemmelsen enklere å forstå.

19.10 Kapittel 10 Eierskapskontroll

Til § 10-1

Bestemmelsen er ny, og viderefører meldeplikten i utvalgets forslag til § 10-1.

Bestemmelsens *første ledd* omfatter erverv av eierandeler som gir erverver betydelig innflytelse over forvaltningen av en virksomhet som gjennom enkeltvedtak, jf. § 1-3, er underlagt loven. Informasjon om hvilke virksomheter som er underlagt loven vil være tilgjengelig hos det departement som har truffet vedtak om å underlegge virksomheten loven, eller hos sikkerhetsmyndigheten som skal ha oversikt over alle virksomheter som er underlagt loven, jf. § 2-1 første ledd bokstav d.

Bestemmelsen gir ikke meldeplikt ved beslutninger som er et resultat av forvaltningen av virksomheten, eksempelvis et salg av eiendeler eller overføring av rettigheter og forpliktelser til uønskede aktører, jf. kapittel 14.4.

Bestemmelsens *andre ledd* definerer når det foreligger kvalifisert eierandel. Det er erververs totale innflytelse på forvaltningen av selskapet som er avgjørende. Ved en eierandel på over en tredjedel vil eieren kunne motsette seg beslutninger om forvaltningen av selskapet som det fra et sikkerhetsperspektiv er viktig å kunne ha en viss kontroll over. Eksempelvis flytting av hovedkontor, vedtektsendringer etc. Se kapittel 14.4. Eierandelen vil også kunne anses som kvalifisert dersom den er mindre enn en tredjedel, så lenge eierposten gir rett til å velge et flertall av styret eller motsette seg overnevnte beslutninger på bakgrunn av vedtekter eller aksjonæravtale, eller på annen måte gir mulighet til å utøve betydelig innflytelse over forvaltningen av selskapet.

Meldingen skal som hovedregel gå til det departementet som har truffet vedtaket om at virksomheten er underlagt loven, jf. § 1-3 første ledd. Ved erverv i virksomheter som ikke faller inn under ansvarsområdet til et departement, skal meldingen gå til sikkerhetsmyndigheten.

Nærmere krav til innholdet i meldingen kan reguleres i forskrift, jf. kapittel 14.4, avsnitt sju.

Til § 10-2

Bestemmelsen viderefører utvalgets forslag til § 10-1 tredje ledd. I tillegg angir bestemmelsen frister for behandlingen av meldingen.

Det følger av *første ledd* at meldingen skal behandles så snart som mulig. Utgangspunktet er forvaltningslovens saksbehandlingsregler, jf. forvaltningsloven § 11 a.

Av *andre ledd* framgår det at departementet eller sikkerhetsmyndigheten som hovedregel bør innhente uttalelse fra relevante organer som grunnlag for vurderingen av ervervets risikopotensial og om erverver er sikkerhetsmessig pålitelig. Eksempelvis vil graden av erververens tilknytning til land Norge ikke har et sikkerhetssamarbeid med, kunne være relevant. Det vil også kunne være relevant å se hen til hvilken relasjon erververen har til andre eiere i virksomheten, og hvordan erververen samlet vil kunne ha innflytelse på forvaltningen av selskapet. Hvilke momenter som er relevante i vurderingen av risikopotensialet og erververens sikkerhetsmessige pålitelighet, vil framgå av forskrift. Relevante organer vil eksempelvis være EOS-tjenestene.

Av *tredje ledd* framgår det at melder innen 60 arbeidsdager skal bli orientert om ervervet er godkjent eller om det skal behandles av Kongen i statsråd. Fristen tar høyde for at det i noen tilfeller vil måtte medregnes noen tid for informasjonsinnhenting og vurdering av meldingen. Fristen avbrytes dersom departementet eller sikkerhetsmyndigheten har bedt om ytterligere opplysninger før det har gått 50 arbeidsdager.

Kongen er i *fjerde ledd* gitt myndighet til å gi nærmere bestemmelser om behandlingen av meldingen i forskrift.

Til § 10-3

Bestemmelsen er en videreføring av utvalgets forslag til § 10-1 fjerde ledd, med noen presiseringer.

Bestemmelsen gir Kongen i statsråd adgang til å stanse et erverv som anses som en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet. Begrepet *ikke ubetydelig risiko* skal forstås på samme måte som i § 2-5. Det oppstilles heller ikke i § 10-3 krav om sannsynlighetsovervekt.

Et vedtak må ligge innenfor formålet med sikkerhetsloven, samtidig som det må være forholdsmessighet mellom den økonomiske ulempen for erverver og virksomheten, og hensynet til nasjonale sikkerhetsinteresser. Det er ikke av betydning om det er mottatt melding om ervervet, eller om ervervet alt er gjennomført. Det forutsettes at

vedtaket kan begrunnes og at denne begrunnelsen kan dokumenteres i tilstrekkelig grad.

19.11 Kapittel 11 Særskilte kontroll- og tilsynsordninger. Tvangsmulkt, overtredelsesgebyr og straff

Til § 11-1

Bestemmelsen viderefører gjeldende sikkerhetslov § 30 første ledd og utvalgets forslag til § 11-1 første ledd. Andre ledd i § 30 er en etterlevning fra tidligere bestemmelser, som forarbeidene til sikkerhetsloven, Ot.prp. nr. 49 (1996–97), ikke gir nærmere rede for, bortsett fra behov for en hjemmel til å kunne utøve særskilt kontroll eksempelvis med den kommunale forvaltningen når det gjelder forebyggende sikkerhetsarbeid. Slike særskilte ordninger utover EOS-utvalget har ikke blitt etablert siden sikkerhetsloven trådte i kraft i 2001. I dag utøver departementet tilsyn med NSM, som dens overordnede organ, mens NSM fører tilsyn med virksomheter underlagt loven, inkludert kommunene. Departementet ser derfor ikke behov for bestemmelsen og foreslår at andre ledd ikke blir videreført i det nye lovforslaget.

Bestemmelsen fastslår gjennom begrepet *underlagt* at forebyggende sikkerhetsarbeid etter sikkerhetsloven kan bli gjenstand for kontroll og tilsyn av EOS-utvalget. Bestemmelsen gir ikke direkte føringer for verken organiseringen, gjennomføringen eller omfanget av EOS-utvalgets kontroll.

Med *forebyggende sikkerhetsarbeid* etter loven menes planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av sikkerhetstruende virksomhet, jf. § 1-5 nr. 3. Begrepet tilsvarer i all hovedsak begrepet *forebyggende sikkerhetstjeneste* slik det er definert i gjeldende sikkerhetslov § 3 første ledd nr. 1.

Bestemmelsen må ses i sammenheng med EOS-kontrolloven (lov 3. februar 1995 nr. 7), herunder § 1, som angir EOS-utvalgets kontrollområde til «etterretnings-, overvåkings- og sikkerhetstjeneste som utføres av den offentlige forvaltning eller under styring eller på oppdrag fra denne». Kontrollområdet er funksjonelt og ikke organisatorisk definert, se nærmere Dokument 16 (2015–2016) Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste, kapittel 17.3.

Til § 11-2

Bestemmelsen er en videreføring av utvalgets forslag til § 11-2, men konkretisert for hvilke bestemmelser sanksjonen tvangsmulkt kan anvendes på. Det er videre i andre ledd tatt inn at et vedtak om tvangsmulkt kan påklages til departementet.

Bestemmelsen gir hjemmel til å ilegge en virksomhet som har overtrådt loven, med konkret angitte bestemmelser som setter plikter på virksomheter som loven gjelder for, jf. tilsvarende § 11-3, en løpende mulkt for å tvinge virksomheten til å rette opp i forholdet og å etterleve de plikter som loven setter. Tvangsmulkt forutsetter at det er truffet gyldig enkeltvedtak som pålegger virksomheten å endre sin praksis, jf. § 3-6. Vedtaket må være rettskraftig før mulkten kan begynne å løpe. Mulighetene for å angripe vedtaket ved klage eller rettslige skritt, må altså være uttømt. Med *tilsynsmyndigheten* menes i denne sammenheng sikkerhetsmyndigheten eller den sektormyndighet som har fått tildelt tilsynsansvaret etter § 3-1.

Tvangsmiddelet må være forholdsmessig, jf. blant annet § 1-1 bokstav c. Vedtaket må ikke være mer tyngende enn det som er nødvendig for å oppnå formålet med mulkten, og må dessuten være egnet til å oppnå formålet.

Bestemmelsen er en videreføring av utvalgets forslag til § 11-2, men det er tatt inn i andre ledd at vedtak om tvangsmulkt kan påklages til departementet.

Til § 11-3

Bestemmelsen er en videreføring av utvalgets forslag til § 11-3.

Bestemmelsen gir tilsynsmyndigheten hjemmel til å ilegge overtredelsesgebyr ved overtredelse av lovbestemmelsene angitt i første ledd.

Begrepet *noen som handler på dennes vegne* i *første ledd* angir virksomhetens ansvar utover egen organisasjon. Det må være en viss tilknytning mellom virksomheten og den som har overtrådt bestemmelsen, jf. også § 5-4.

Oppregningen av lovens bestemmelser der overtredelsesgebyr er aktuelt omfatter de bestemmelser i loven som anses særlig viktig å overholde og som dessuten er tilstrekkelig klart formulert ved å legge plikter for de virksomhetene som loven gjelder for, til at denne type sanksjon lar seg forsvare.

Ileggelse av gebyr er inngripende og må være forholdsmessig. Bestemmelsens *andre ledd* angir relevante momenter som skal tas i betraktning

ved fastsettelse av gebyrets størrelse. Momentene er relevante også ved vurderingen av om gebyr skal ilegges.

Bestemmelsens *tredje ledd* fastsetter foreldelsesfristen for adgangen til å pålegge overtredelsesgebyr. Utover det som er regulert i tredje ledd gjelder alminnelige regler om foreldelse.

Til § 11-4

Bestemmelsen er i hovedsak en videreføring av gjeldende sikkerhetslov § 31 og utvalgets forslag til § 11-4.

Bestemmelsens *første ledd* fastslår at overtredelse av nærmere angitte bestemmelser – de samme som i § 11-3 første ledd bokstav a og b – er straffbart, se merknadene til denne bestemmelsen. *Første ledd* retter seg i første rekke mot virksomheter som er ansvarlig for overholdelse av de enkelte bestemmelsene. I første ledd er det tilføyd *eller begge deler* slik at bestemmelsen også gir adgang til å bruke tvangsmiddelet pågripelse, dersom de generelle og spesielle vilkårene etter straffeprosessloven § 171, jf. § 170 a er oppfylt. Strafferammen blir da bot eller fengsel inntil 6 måneder eller begge deler.

Bestemmelsens *andre* og *tredje ledd* retter seg mot enkeltpersoner som ikke overholder § 5-4 eller § 6-6 eller forbud gitt i medhold av § 7-5. Strafferammen her er bot eller fengsel inntil 1 år.

19.12 Kapittel 12 Ikrafttredelse og endringer i andre lover

Til § 12-1

Bestemmelsens *første punktum* fastslår at loven trer i kraft fra det tidspunkt Kongen bestemmer. Det ligger blant annet i dette at ikraftsettelse forutsetter at det først må utarbeides nærmere forskrifter, se f.eks. §§ 3-2, 4-3, 5-5, 5-6, 6-2, 6-6, 7-1, 7-2, 8-3, 8-6 og 10-2. I tillegg vil det være behov for gjennomføring av et informasjons- og opplæringsprogram for berørt personell, særlig i forbindelse med den foreslåtte tilsynsmodellen, jf. §§ 3-1 til 3-6, før loven kan tre i kraft.

I bestemmelsens *andre punktum* slås det fast at Kongen kan sette i kraft forskjellige bestemmelser til ulik tid. Dette innebærer at det ikke vil være påkrevet å vente med ikrafttredelse av loven til alle forskrifter er på plass, men at deler av loven kan ta til å gjelde når det foreligger forskrifter som hører til tilsvarende deler av loven.

Til § 12-2

Når den nye loven trer i kraft, oppheves lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven). Dersom forskjellige bestemmelser i den nye loven blir satt i kraft til ulik tid, jf. § 12-1 andre punktum, skjer tilsvarende delvis opphevelse av 1998-loven, så langt det passer.

Forsvarsdepartementet

t i l r å r :

At Deres Majestet godkjenner og skriver under et framlagt forslag til proposisjon til Stortinget om lov om nasjonal sikkerhet (sikkerhetsloven).

Vi HARALD, Norges Konge,

s t a d f e s t e r :

Stortinget blir bedt om å gjøre vedtak til lov om nasjonal sikkerhet (sikkerhetsloven) i samsvar med et vedlagt forslag.

Forslag
til lov om nasjonal sikkerhet (sikkerhetsloven)

Kapittel 1. Formål og virkeområde

§ 1-1 *Formål*

Loven skal bidra til

a) å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser
b) å forebygge, avdekke og motvirke sikkerhetstruende virksomhet
c) at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.

§ 1-2 *Hvem loven gjelder for*

Loven gjelder for statlige, fylkeskommunale og kommunale organer.

Loven gjelder for leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser etter kapittel 9.

For virksomheter på Svalbard, Jan Mayen og i bilandene gjelder loven i det omfanget og med de stedlige tilpasningene Kongen bestemmer.

Kongen i statsråd kan gi forskrift om lovens virkeområde og helt eller delvis unnta bestemte virksomheter eller visse typer informasjon, informasjonssystemer, objekter og infrastruktur.

§ 1-3 *Vedtak om at loven skal gjelde for andre virksomheter*

Et departement skal innenfor sitt ansvarsområde fatte vedtak om at loven helt eller delvis skal gjelde for virksomheter som

a) behandler sikkerhetsgradert informasjon
b) råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner
c) driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner.

Virksomhetene skal forhåndsvarsles om vedtak etter første ledd.

Sikkerhetsmyndigheten kan på eget initiativ fremme forslag overfor et departement om å fatte vedtak etter første ledd. Dersom departementet ikke fatter vedtak i samsvar med sikkerhetsmyndighetens anbefaling, 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.

Sikkerhetsmyndigheten skal fatte vedtak etter første ledd overfor virksomheter som ikke omfattes av noe departements ansvarsområde. Departementet er klageinstans.

§ 1-4 *Lovens anvendelse for Stortinget, Stortingets organer, regjeringen og domstolene*

Loven gjelder for Stortinget og Stortingets organer så langt Stortinget bestemmer det.

Bestemmelsene som er gitt i og i medhold av kapittel 8, gjelder ikke for regjeringens medlemmer og dommere i Høyesterett.

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

§ 1-5 *Definisjoner*

I denne loven menes med

1. nasjonale sikkerhetsinteresser: landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser knyttet til
   a) de øverste statsorganers virksomhet, sikkerhet og handlefrihet
   b) forsvar, sikkerhet og beredskap
   c) forholdet til andre stater og internasjonale organisasjoner
   d) økonomisk stabilitet og handlefrihet
   e) samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet
2. grunnleggende nasjonale funksjoner: 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
3. forebyggende sikkerhetsarbeid: planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende tiltak mot sikkerhetstruende virksomhet og følger av slik virksomhet

4. sikkerhetstruende virksomhet: tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser
5. nærstående: personer som er i nær familie eller som har annen nær tilknytning som kan ha betydning for om en person er sikkerhetsmessig skikket.

Kapittel 2. Ansvar og myndighet for forebyggende sikkerhetsarbeid

§ 2-1 *Departementenes ansvar og myndighet for forebyggende sikkerhetsarbeid*

Departementene er ansvarlige for forebyggende sikkerhetsarbeid innenfor sine ansvarsområder og skal

a) identifisere og holde oversikt over grunnleggende nasjonale funksjoner
b) identifisere og holde oversikt over virksomheter som har vesentlig betydning for grunnleggende nasjonale funksjoner
c) fatte vedtak etter § 1-3 første ledd
d) melde inn oversikter til sikkerhetsmyndigheten etter bokstav a og b og vedtak etter bokstav c.

Kongen i statsråd kan gi forskrift om departementenes ansvar og myndighet for forebyggende sikkerhetsarbeid.

§ 2-2 *Sikkerhetsmyndighetens ansvar for forebyggende sikkerhetsarbeid*

Sikkerhetsmyndigheten har det sektorovergripende ansvaret for at forebyggende sikkerhetsarbeid i virksomhetene utføres i samsvar med loven.

Sikkerhetsmyndigheten har det overordnede ansvaret for at sikkerhetstilstanden i alle sektorer kontrolleres, og skal se til at virksomhetene oppfyller sine plikter etter loven. Sikkerhetsmyndigheten skal blant annet

a) se til at det føres tilsyn med at virksomheter oppfyller krav til forebyggende sikkerhetsarbeid
b) utarbeide og vedlikeholde grunnleggende kriterier for tilsyn
c) innhente og vurdere informasjon som har betydning for forebyggende sikkerhetsarbeid
d) gi informasjon, råd og veiledning om forebyggende sikkerhetsarbeid og krav til tiltak
e) holde oversikt over de funksjonene og virksomhetene departementene har identifisert etter § 2-1
f) holde oversikt over virksomheter som det er fattet vedtak om etter § 1-3
g) legge til rette for informasjonsdeling etter § 2-3
h) bidra til å utvikle sikkerhetstiltak og fastsette krav til forebyggende sikkerhetsarbeid.

Sikkerhetsmyndigheten er nasjonal fagmyndighet overfor andre land og internasjonale organisasjoner.

Så langt det er nødvendig for å gjennomføre oppgavene i eller i medhold av loven, skal sikkerhetsmyndigheten gis uhindret adgang til skjermingsverdig informasjon, informasjonssystem, objekt eller infrastruktur.

Kongen kan gi forskrift om sikkerhetsmyndighetens ansvar for forebyggende sikkerhetsarbeid.

§ 2-3 *Utveksling av trusselvurderinger og annen sikkerhetsinformasjon*

Sikkerhetsmyndigheten skal legge til rette for at virksomheter som loven gjelder for, får tilgang til informasjon om trusselvurderinger og andre opplysninger som er av betydning for virksomhetenes forebyggende sikkerhetsarbeid.

Sikkerhetsmyndigheten skal i samråd med sektormyndigheter og andre relevante myndigheter sikre at det etableres nødvendige fora for informasjons- og erfaringsutveksling.

Kongen kan gi forskrift om utveksling av trusselvurderinger og annen sikkerhetsinformasjon.

§ 2-4 *Responsfunksjon og varslingssystem for digital infrastruktur*

Kongen utpeker en myndighet som skal drive en nasjonal responsfunksjon for alvorlige digitale angrep og et nasjonalt varslingssystem for digital infrastruktur.

Når det er nødvendig for å utføre oppgaver etter første ledd, kan denne myndigheten behandle personopplysninger i form av

a) metadata om IKT-trafikk til og fra virksomheter som er knyttet til det nasjonale varslingssystemet for digital infrastruktur
b) informasjon som er nødvendig for å analysere utløste alarmer i varslingssystemet
c) IP-adresser mottatt fra nasjonale og internasjonale samarbeidspartnere
d) logger og infisert maskinvare, når det er nødvendig for å bistå en virksomhet i håndteringen av alvorlige digitale angrep og virksomheten samtykker til det.

Når det er strengt nødvendig for å utføre oppgaver etter første ledd, kan også andre personopplysninger enn det som er nevnt i andre ledd, behandles.

Behandlingen av personopplysninger og inngrepet i personvernet skal ikke være mer omfattende enn det som er nødvendig for å oppnå formålet.

Kongen kan gi forskrift om nasjonal responsfunksjon og nasjonalt varslingssystem for digital infrastruktur.

§ 2-5 *Vedtak ved risiko for skadevirkninger for nasjonale sikkerhetsinteresser*

Kongen i statsråd kan fatte nødvendige vedtak for å hindre sikkerhetstruende virksomhet eller annen planlagt eller pågående aktivitet som kan innebære en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet. Et slikt vedtak kan fattes uten hensyn til begrensningene i forvaltningsloven § 35 og uavhengig av om aktiviteten er tillatt etter annen lov eller annet vedtak.

Før det fattes vedtak, bør det innhentes rådgivende uttalelser fra relevante organer med kompetanse innenfor det aktuelle fagområdet.

Vedtak etter første ledd er særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

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

Kapittel 3. Tilsyn

§ 3-1 *Tilsyn med virksomheter*

Sikkerhetsmyndigheten fører tilsyn med virksomheter som er omfattet av loven.

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. Sikkerhetsmyndigheten skal likevel gjennomføre tilsyn når det følger av internasjonale forpliktelser eller når det er tvingende nødvendig.

Sikkerhetsmyndigheten skal føre tilsyn med departementene og myndigheter med tilsynsansvar etter andre ledd.

Kongen kan gi forskrift om tildeling av tilsynsansvar og om fordeling av ansvaret mellom sikkerhetsmyndigheten og aktuelle myndigheter med sektoransvar.

§ 3-2 *Samarbeid mellom sikkerhetsmyndigheten og andre myndigheter med tilsynsansvar*

Sikkerhetsmyndigheten og myndigheter med tilsynsansvar etter § 3-1 andre ledd skal inngå en avtale om samarbeid. Gjennomføring av tilsyn skal så langt det er mulig samordnes med andre tilsynsmyndigheter.

Sikkerhetsmyndigheten skal utarbeide og utvikle grunnleggende kriterier for tilsyn etter loven, og legge til rette for felles opplæring av tilsynspersonell.

Sikkerhetsmyndigheten kan om nødvendig medvirke til forberedelse og gjennomføring av tilsyn som utføres av myndigheter med tilsynsansvar. Myndigheter med tilsynsansvar kan be sikkerhetsmyndigheten om slik bistand.

Myndigheter med tilsynsansvar skal orientere sikkerhetsmyndigheten om planlagte tilsyn, redegjøre for gjennomførte tilsyn og informere om eventuelle avvik og pålegg.

Kongen kan gi forskrift om samarbeid og informasjonsutveksling mellom sikkerhetsmyndigheten og myndigheter med tilsynsansvar.

§ 3-3 *Generelle prinsipper for tilsyn*

Tilsyn etter § 3-1 skal ikke forstyrre tilsynsobjektenes daglige drift mer enn nødvendig.

Opplysninger som tilsynsmyndigheten innhenter, kan bare brukes i forbindelse med tilsynet og i det forebyggende sikkerhetsarbeidet.

§ 3-4 *Adgangsrett og varslingsplikt ved stedlige tilsyn*

Tilsynsmyndigheten kan kreve tilgang til virksomhetens informasjon, informasjonssystemer, objekter og infrastruktur. Virksomheten skal stille med relevant personell under tilsynet så langt det er nødvendig.

Stedlige tilsyn skal varsles skriftlig. Tilsyn kan likevel gjennomføres uten varsel dersom sikkerhetshensyn gjør det nødvendig.

Kongen kan gi forskrift om stedlige tilsyn.

§ 3-5 *Tilsynsmyndighetens behandling av personopplysninger*

Tilsynsmyndigheten kan behandle personopplysninger dersom det er nødvendig for å utføre sine oppgaver.

Behandlingen av personopplysninger må ikke utgjøre et uforholdsmessig inngrep i personvernet.

Personopplysninger skal om mulig behandles ved hjelp av virksomhetens informasjonssystem, uten at de blir kopiert eller overført til tilsynsmyndigheten. Tilsynsmyndigheten kan likevel kreve kopi av personopplysninger når dette er nødvendig for å dokumentere om bestemmelser i loven er brutt.

Kongen kan gi forskrift om tilsynsmyndighetens behandling av personopplysninger.

§ 3-6 *Pålegg*

Tilsynsmyndigheten kan gi virksomheter pålegg om gjennomføring av tiltak som er nødvendige for å ivareta lovens formål. Pålegg om konkrete tiltak kan bare gis dersom kostnadene som påføres virksomheten, framstår som rimelige sett i forhold til det som kan oppnås ved tiltaket.

Dersom myndigheter med tilsynsansvar ikke fører tilsyn i samsvar med krav fastsatt i eller i medhold av loven, kan sikkerhetsmyndigheten gi pålegg om å utføre slikt tilsyn.

Pålegg etter første og andre ledd kan påklages. Reglene i forvaltningsloven kapittel VI gjelder for selvstendige rettssubjekters klageadgang.

Kapittel 4. Generelle krav til forebyggende sikkerhetsarbeid

§ 4-1 *Sikkerhetsstyring*

Virksomhetens leder har ansvaret for det forebyggende sikkerhetsarbeidet. Forebyggende sikkerhetsarbeid skal være en del av virksomhetens styringssystem. Sikkerhetstilstanden i virksomheten skal regelmessig kontrolleres.

Virksomheten skal sørge for at ansatte, leverandører og oppdragstakere har tilstrekkelig risiko- og sikkerhetsforståelse. For leverandører til sikkerhetsgraderte anskaffelser gjelder kapittel 9.

Kongen kan gi forskrift om sikkerhetsstyring.

§ 4-2 *Vurdering av risiko*

Virksomheten skal regelmessig gjennomføre vurdering av risiko. Vurderingen skal danne grunnlag for iverksetting av forebyggende sikkerhetstiltak.

Virksomheten skal som del av vurderingen kartlegge hvilke virksomheter den er avhengig av for å fungere som den skal.

Vurderingen skal gjennomgås jevnlig og om nødvendig revideres.

Tilsynsmyndigheten skal etter forespørsel gi råd og veiledning i forbindelse med vurderingen.

Kongen kan gi forskrift om hvordan en vurdering av risiko skal gjennomføres.

§ 4-3 *Plikt til å gjennomføre sikkerhetstiltak og øvelser*

Virksomheten skal gjennomføre de forebyggende sikkerhetstiltakene som må til for å gi et forsvarlig sikkerhetsnivå og redusere risikoen knyttet til sikkerhetstruende virksomhet. Slike tiltak kan gjennomføres i sammenheng med andre forebyggende sikkerhetstiltak i virksomheten, så lenge kravene i denne loven oppfylles.

Kostnadene ved et sikkerhetstiltak skal stå i et rimelig forhold til det som kan oppnås ved tiltaket.

Virksomheten skal regelmessig gjennomføre øvelser for å vurdere effekten av iverksatte sikkerhetstiltak.

Kongen kan gi forskrift om plikter for virksomheter som omfattes av loven, og om øvelser.

§ 4-4 *Krav til dokumentasjon*

Virksomheten skal dokumentere vurderingen av risiko og de gjennomførte og planlagte sikkerhetstiltakene.

Kongen kan gi forskrift om krav til dokumentasjon.

§ 4-5 *Varslingsplikt*

Virksomheten skal straks varsle sikkerhetsmyndigheten og andre myndigheter som skal utføre tilsyn i medhold av § 3-1 andre ledd, dersom

a) den har blitt rammet av sikkerhetstruende virksomhet
b) det er begrunnet mistanke om at sikkerhetstruende virksomhet har rammet eller vil kunne ramme virksomheten eller andre virksomheter
c) det har skjedd alvorlige brudd på krav til sikkerhet etter kapittel 5, 6 eller 7.

Virksomheten skal uten hinder av taushetsplikt varsle tilsynsmyndigheten dersom den får kunnskap om en planlagt eller pågående aktivitet som kan medføre en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet. Tilsynsmyndigheten skal uten ugrunnet opphold varsle sikkerhetsmyndigheten og videresende varselet til ansvarlig departement for vurdering av vedtak etter § 2-5.

Kongen kan gi forskrift om varslingsplikten etter andre ledd.

Kapittel 5. Informasjonssikkerhet

§ 5-1 *Skjermingsverdig informasjon*

Informasjon er skjermingsverdig dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.

§ 5-2 *Beskyttelse av skjermingsverdig informasjon*

Virksomheten skal sørge for et forsvarlig sikkerhetsnivå for skjermingsverdig informasjon, slik at informasjonen

a) ikke blir kjent for uvedkommende
b) ikke går tapt eller blir endret
c) er tilgjengelig ved tjenstlig behov.

Kongen kan gi forskrift om identifisering og beskyttelse av skjermingsverdig informasjon. I særlige tilfeller kan det i en slik forskrift gjøres unntak fra sikkerhetskrav som er fastsatt i eller i medhold av denne loven.

§ 5-3 *Sikkerhetsgradert informasjon*

En virksomhet som tilvirker informasjon, skal sikkerhetsgradere og merke informasjonen dersom det kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende. Følgende sikkerhetsgrader skal benyttes:

a) STRENGT HEMMELIG dersom det kan få helt avgjørende skadefølger
b) HEMMELIG dersom det kan få alvorlige skadefølger
c) KONFIDENSIELT dersom det kan få skadefølger
d) BEGRENSET dersom det i noen grad kan få skadefølger.

Sikkerhetsgradering skal ikke brukes i større utstrekning eller for lengre tid enn nødvendig. Dersom ikke annet er bestemt, bortfaller sikkerhetsgraderingen etter 30 år.

Kongen kan gi forskrift om sikkerhetsgradering og beskyttelse av informasjon som mottas eller gis innenfor rammen av en gjensidig overenskomst med en fremmed stat eller en internasjonal organisasjon.

§ 5-4 *Tilgang til og taushetsplikt med hensyn til sikkerhetsgradert informasjon*

Sikkerhetsgradert informasjon skal bare overlates til personer som har tjenstlig behov og er autorisert for tilgang til slik informasjon.

Alle som får tilgang til sikkerhetsgradert informasjon som ledd i arbeidet eller tjenesten for en virksomhet som omfattes av loven, har taushetsplikt om innholdet. Taushetsplikten gjelder også etter at arbeidet eller tjenesten er avsluttet.

§ 5-5 *Tekniske sikkerhetsundersøkelser*

Sikkerhetsmyndigheten kan undersøke lokaler, bygninger og andre objekter som en virksomhet alene eller sammen med andre råder over, for å fastslå om uvedkommende kan skaffe seg tilgang til sikkerhetsgradert informasjon ved avlytting, innsyn eller avlesning av signaler.

Informasjon som kontrollen gir tilgang til, kan bare benyttes til det som formålet med kontrollen krever. Når det ikke lenger er behov for informasjonen, skal den slettes. Kunnskap og erfaringer som sikkerhetsmyndigheten tilegner seg gjennom undersøkelsen, kan brukes til videreutvikling av sikkerhetsmyndighetens generelle sikkerhetsarbeid.

Sikkerhetsmyndigheten skal gi virksomheten en rapport om resultatet av kontrollen. Rapporten skal bare inneholde informasjon som kan bidra til å bedre virksomhetens sikkerhet.

Kongen kan gi forskrift om tekniske sikkerhetsundersøkelser, og om at slike undersøkelser kan utføres av andre enn sikkerhetsmyndigheten.

§ 5-6 *Kryptosikkerhet*

Kryptosystemer som skal brukes for å beskytte sikkerhetsgradert informasjon, må være godkjent av sikkerhetsmyndigheten.

Sikkerhetsmyndigheten er nasjonal forvalter av kryptomateriell og leverandør av kryptosikkerhetstjenester til virksomheter. Sikkerhetsmyndigheten kan godkjenne andre leverandører av kryptosikkerhetstjenester.

Sikkerhetsmyndigheten skal godkjenne kryptoalgoritmer som brukes i utstyr som tenkes eksportert.

Kongen kan gi forskrift om kryptosikkerhet.

Kapittel 6. Informasjonssystemsikkerhet

§ 6-1 *Skjermingsverdige informasjonssystemer*

Et informasjonssystem er skjermingsverdig dersom det behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner.

Kongen kan gi forskrift om identifisering av skjermingsverdige informasjonssystemer.

§ 6-2 *Beskyttelse av skjermingsverdige informasjonssystemer*

Virksomheten skal sørge for et forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer, slik at

a) informasjonssystemene fungerer slik de skal
b) uvedkommende ikke får tilgang til informasjonen som behandles i systemene
c) informasjonen som behandles i systemene, ikke endres eller går tapt
d) informasjonen som behandles i systemene, er tilgjengelig ved tjenstlig behov for tilgang.

Kongen kan gi forskrift om identifisering og beskyttelse av skjermingsverdige informasjonssystemer. I særlige tilfeller kan det i en slik forskrift gjøres unntak fra sikkerhetskrav som er fastsatt i eller i medhold av denne loven.

§ 6-3 *Godkjenning av skjermingsverdige informasjonssystemer*

Skjermingsverdige informasjonssystemer skal godkjennes av en godkjenningsmyndighet. Informasjonssystemer som skal behandle sikkerhetsgradert informasjon, skal godkjennes før de tas i bruk.

Kongen kan gi forskrift om godkjenning av skjermingsverdige informasjonssystemer, utpeking

av godkjenningsmyndigheter og krav til leverandører.

§ 6-4 *Overvåking av skjermingsverdige informasjonssystemer*

Virksomheten skal kontinuerlig overvåke sine skjermingsverdige informasjonssystemer for å forebygge, avdekke og motvirke hendelser som kan skade nasjonale sikkerhetsinteresser. Hendelser som er relevante for sikkerhetsarbeidet, skal registreres.

I den grad formålet med overvåkingen krever det, skal sending av informasjon til, fra og innenfor skjermingsverdige informasjonssystemer registreres, lagres og analyseres.

Informasjonssystemer som behandler personopplysninger, skal bare overvåkes med de metodene og i det omfanget som formålet med overvåkingen krever.

Informasjon etter første og andre ledd kan lagres i opptil fem år. Lagrede personopplysninger kan bare benyttes i den grad formålet med overvåkingen krever det.

Flere virksomheter som er tilknyttet samme informasjonssystem, kan avtale at en av virksomhetene skal ta seg av overvåkingen etter første og andre ledd for alle virksomhetene. Den virksomheten som gjennomfører overvåkingen, skal sikre at kravene til informasjonssikkerhet i § 5-2 følges.

Virksomheten skal se til at autoriserte brukere av informasjonssystemer som overvåkes, får vite hva som er formålet med behandlingen av personopplysningene og hvilke overvåkingstiltak som er iverksatt. De skal også få vite om personopplysningene blir utlevert og i så fall til hvem.

Kongen kan gi forskrift om overvåking av skjermingsverdige informasjonssystemer, blant annet om

a) hva slags informasjon som kan eller skal registreres, lagres og analyseres i forbindelse med overvåkingen
b) hvem som skal ha tilgang til informasjon som er registrert og lagret i forbindelse med overvåkingen
c) hvordan tilgang til registrert eller lagret informasjon skal gis
d) at informasjonen etter første og andre ledd skal ha en annen lagringstid enn fem år.

§ 6-5 *Inntrengingstesting av skjermingsverdige informasjonssystemer*

Virksomheten kan be sikkerhetsmyndigheten om å forsøke å trenge inn i virksomhetens skjermingsverdige informasjonssystemer. Formålet skal være å kontrollere om sikkerhetstiltakene er tilstrekkelige. Virksomhetens ansatte skal orienteres om at slike kontroller kan forekomme.

Dersom kontrollen innebærer behandling av personopplysninger, skal den ikke være mer omfattende enn det som formålet krever.

Informasjon som kontrollen gir tilgang til, kan bare benyttes til det som formålet med kontrollen krever. Når det ikke lenger er behov for informasjonen, skal den slettes. Kunnskap og erfaringer som sikkerhetsmyndigheten tilegner seg gjennom inntrengingstestingen, kan brukes til videreutvikling av sikkerhetsmyndighetens generelle sikkerhetsarbeid.

Sikkerhetsmyndigheten skal gi virksomheten en rapport om resultatet av kontrollen. Rapporten skal bare inneholde informasjon som kan bidra til å bedre virksomhetens sikkerhet.

Kongen kan gi forskrift om inntrenging i skjermingsverdige informasjonssystemer, og om at slik kontroll kan utføres av andre enn sikkerhetsmyndigheten.

§ 6-6 *Kommunikasjons- og innholdskontroll av informasjonssystemer*

Virksomheten kan be sikkerhetsmyndigheten kontrollere om virksomhetens informasjonssystemer behandler sikkerhetsgradert informasjon utover det systemets sikkerhetsgodkjenning tillater. Virksomhetens ansatte skal orienteres om at slike kontroller kan forekomme.

Sikkerhetsmyndigheten kan gjennomføre kontrollen ved å avlytte og avlese informasjon som behandles i eller sendes mellom informasjonssystemer.

Kontrollen skal ikke omfatte privat kommunikasjon eller kommunikasjon med virksomheter som ikke er omfattet av loven. Fanger kontrollen likevel opp slik kommunikasjon, skal kontrollen straks opphøre, og informasjon som kontrollen har gitt tilgang til, skal slettes.

Alle som får tilgang til informasjon som nevnt i tredje ledd i forbindelse med arbeid eller tjeneste for sikkerhetsmyndigheten, har taushetsplikt om innholdet.

Sikkerhetsmyndigheten skal informere virksomhetens ledelse om metodene som skal benyttes i kontrollen og sikkerhetsmyndighetens vurdering av risikoen for at kontrollen kan fange opp kommunikasjon som nevnt i tredje ledd. Dersom virksomhetens ledelse finner at hensynet til informasjonssystemsikkerheten ikke kan begrunne metodene og risikoen, skal kontrollen ikke utføres.

Informasjon som kontrollen gir tilgang til, kan benyttes bare til det som formålet med kontrollen

krever. Når det ikke lenger er behov for informasjonen, skal den slettes. Kunnskap og erfaringer som sikkerhetsmyndigheten tilegner seg gjennom kontrollen, kan brukes til videreutvikling av sikkerhetsmyndighetens generelle sikkerhetsarbeid.

Sikkerhetsmyndigheten skal gi virksomheten en rapport om resultatet av kontrollen. Rapporten skal bare inneholde informasjon som kan bidra til å bedre virksomhetens sikkerhet.

Kongen kan gi forskrift om kommunikasjons- og innholdskontroll av informasjonssystemer, og om at slik kontroll kan utføres av andre enn sikkerhetsmyndigheten.

Kapittel 7. Objekt- og infrastruktursikkerhet

§ 7-1 *Skjermingsverdige objekter og infrastruktur*

Objekter og infrastruktur er skjermingsverdige dersom det kan skade grunnleggende nasjonale funksjoner om de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse.

Et departement skal innenfor sitt ansvarsområde utpeke, klassifisere og holde oversikt over skjermingsverdige objekter og infrastruktur. Alle utpekte og klassifiserte objekter og infrastruktur skal meldes inn til sikkerhetsmyndigheten med angivelse av klassifiseringsgrad.

Sikkerhetsmyndigheten skal utpeke, klassifisere og holde oversikt over skjermingsverdige objekter og infrastruktur som ikke omfattes av noe departements ansvarsområde.

Virksomheter som råder over objekter eller infrastruktur som utpekes etter andre eller tredje ledd, skal varsles om utpekingen.

Vedtak om utpeking og klassifisering som berører selvstendige rettssubjekter, kan påklages. Departementet er klageinstans for vedtak fattet av sikkerhetsmyndigheten.

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.

Kongen kan gi forskrift om utpeking av objekter og infrastruktur, og om melding til sikkerhetsmyndigheten.

§ 7-2 *Klassifisering av skjermingsverdige objekter og infrastruktur*

Skjermingsverdige objekter og infrastruktur skal klassifiseres dersom det kan skade grunnleggende nasjonale funksjoner om de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse. Følgende klassifiseringsgrader skal benyttes:

a) MEGET KRITISK dersom det kan få helt avgjørende skadefølger
b) KRITISK dersom det kan få alvorlige skadefølger
c) VIKTIG dersom det kan få skadefølger

Klassifiseringen skal bygge på en skadevurdering, og det skal spesifiseres hvilke grunnleggende nasjonale funksjoner objektet eller infrastrukturen understøtter og hva konsekvensene av redusert funksjonalitet vil være. Begrunnelsen for klassifiseringen skal inngå i departementenes og sikkerhetsmyndighetens oversikt over skjermingsverdige objekter og infrastruktur.

Dersom en del av et objekt eller en infrastruktur har en høyere klassifisering enn resten av objektet eller infrastrukturen, skal denne delen defineres som selvstendig objekt eller infrastruktur.

Kongen kan gi forskrift om klassifisering av skjermingsverdige objekter og infrastruktur.

§ 7-3 *Beskyttelse av objekter og infrastruktur*

Virksomheten skal iverksette nødvendige sikkerhetstiltak for å opprettholde et forsvarlig sikkerhetsnivå. Sikkerhetstiltakene kan være

a) fysiske, elektroniske, menneskelige eller organisatoriske barrierer
b) systemer som skal oppdage og varsle om aktivitet eller hendelser
c) systemer og rutiner for avklaring vedrørende 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.

Virksomheten skal foreta en vurdering av risiko for å avgjøre hvilke tiltak som er nødvendige for å beskytte objektet eller infrastrukturen.

Beskyttelse av objekter og infrastruktur kan også omfatte krav til adgangsklarering etter § 8-3.

Kongen kan gi forskrift om beskyttelse av objekter og infrastruktur innenfor hvert klassifiseringsnivå og om bruk av sikringsstyrker.

§ 7-4 *Testing av sikkerhetstiltak*

Virksomheten kan be sikkerhetsmyndigheten om å forsøke å forsere etablerte sikkerhetstiltak for å få tilgang til skjermingsverdige objekter eller infrastruktur. Formålet skal være å kontrollere om sikkerhetstiltakene er tilstrekkelige. Virksomhetens ansatte skal orienteres om at slike kontroller kan forekomme.

Dersom kontrollen innebærer behandling av personopplysninger, skal kontrollen ikke være mer omfattende enn det som formålet krever.

Informasjon som kontrollen gir tilgang til, kan bare benyttes til det som formålet med kontrollen krever. Når det ikke lenger er behov for informasjonen, skal den slettes. Kunnskap og erfaringer som sikkerhetsmyndigheten tilegner seg gjennom kontrollen, kan brukes til videreutvikling av sikkerhetsmyndighetens generelle sikkerhetsarbeid.

Sikkerhetsmyndigheten skal gi virksomheten en rapport om resultatet av kontrollen. Rapporten skal bare inneholde informasjon som kan bidra til å bedre virksomhetens sikkerhet.

Kongen kan gi forskrift om testing av sikkerhetstiltak for skjermingsverdige objekter og infrastruktur og om at slik testing kan gjennomføres av andre enn sikkerhetsmyndigheten.

§ 7-5 *Forbud mot adgang til steder og områder*

Kongen kan av hensyn til forsvar, sikkerhet og beredskap gi forskrift om eller fatte enkeltvedtak om at personer nektes

a) adgang til eller opphold i nærheten av militære områder
b) adgang til eller opphold i nærheten av bestemt angitte steder eller områder
c) adgang til å overvære militære øvelser eller forsøk, militære operasjoner eller annen militær aktivitet.

Kapittel 8. Personellsikkerhet

§ 8-1 *Krav om sikkerhetsklarering, adgangsklarering og autorisasjon*

Personer som skal få tilgang til sikkerhetsgradert informasjon, skal autoriseres i samsvar med § 8-9. Det samme gjelder personer som skal ha adgang til skjermingsverdige objekter og infrastruktur som det er fattet vedtak om etter § 8-3.

Personer som skal autoriseres for tilgang til informasjon gradert KONFIDENSIELT eller høyere, må ha gyldig sikkerhetsklarering. Personer som skal autoriseres for tilgang til skjermingsverdige objekter og infrastruktur som det er fattet vedtak om etter § 8-3, må ha gyldig adgangsklarering.

Kongen kan gi forskrift om behandling av klareringssaker og gyldighetstiden for klareringer.

§ 8-2 *Sikkerhetsklarering*

Personer skal sikkerhetsklareres dersom de skal ha tilgang til informasjon gradert KONFIDENSIELT eller høyere etter § 5-3.

Det samme gjelder personer som gjennom arbeidet sitt vil kunne få tilgang til slik informasjon. Sikkerhetsklarering skal likevel ikke gjennomføres dersom risikoen for tilgang til slik informasjon kan fjernes gjennom andre og enklere sikkerhetstiltak.

Kongen kan gi forskrift om forholdet mellom nasjonale sikkerhetsgrader og sikkerhetsgrader i NATO, andre nasjoner eller internasjonale organisasjoner.

§ 8-3 *Adgangsklarering*

Et departement kan innenfor sitt ansvarsområde fatte vedtak om krav til adgangsklarering, for tilgang til hele eller deler av skjermingsverdige objekter eller infrastruktur. Sikkerhetsmyndigheten kan fatte slike vedtak overfor virksomheter som ikke er omfattet av noe departements ansvarsområde.

Det skal ikke fattes vedtak om krav til adgangsklarering dersom det kan iverksettes andre egnede sikkerhetstiltak.

Avgjørelsen om krav til adgangsklarering som berører selvstendige rettssubjekter, kan påklages.

Personer kan gis adgangsklarering dersom de skal ha tilgang til objekter eller infrastruktur som er klassifisert etter § 7-2. Departementet kan bestemme at personer med sikkerhetsklarering for et bestemt nivå også er klarert for adgang til et bestemt skjermingsverdig objekt eller en bestemt skjermingsverdig infrastruktur.

Kongen kan gi forskrift om krav til adgangsklarering og om forholdet mellom adgangsklarering og sikkerhetsklarering.

§ 8-4 *Avgjørelse om klarering*

En person kan bare klareres dersom det ikke finnes rimelig grunn til å tvile på at personen er sikkerhetsmessig skikket. Klareringsmyndigheten fatter avgjørelse om klarering.

I vurderingen skal det legges vekt på forhold som er relevante for personens pålitelighet, lojalitet og dømmekraft i forbindelse med behandling av gradert informasjon og tilgang til skjermingsverdige objekter og infrastruktur. Vurderingen skal gjøres på grunnlag av en personkontroll.

Klareringsmyndigheten skal se til at klareringssaken er så godt opplyst som mulig. Dersom det er tvil om en person er sikkerhetsmessig skikket, skal klareringsmyndigheten holde en sikkerhetssamtale med personen.

Opplysninger om følgende forhold kan tillegges vekt:

a) spionasje, planlegging eller gjennomføring av terror, sabotasje, attentat eller lignende, og forsøk på slik virksomhet
b) straffbare handlinger eller forberedelser eller oppfordringer til straffbare handlinger
c) forhold som kan føre til at personen selv, eller personens nærstående, utsettes for trusler mot liv, helse, frihet eller ære, slik at personen kan bli presset til å handle i strid med nasjonale sikkerhetsinteresser
d) forfalskning av eller feilaktig eller unnlatt framstilling av faktiske forhold som personen måtte forstå har betydning for sikkerhetsklareringen
e) misbruk av alkohol eller andre rusmidler
f) enhver sykdom som på medisinsk grunnlag kan gi forbigående eller varig svekkelse av påliteligheten, lojaliteten eller dømmekraften
g) kompromittering av skjermingsverdig informasjon eller brudd på sikkerhetsbestemmelser
h) nektelse eller unnlatelse av å gi personopplysninger om seg selv
i) ikke å orientere den autorisasjonsansvarlige om egne forhold av betydning for sikkerheten
j) nektelse av å gi taushetsløfte, tilkjennegivelse av ikke å ville være bundet av taushetsløfte eller nektelse eller unnlatelse av å delta i sikkerhetssamtale
k) økonomiske forhold som kan friste ham eller henne til å handle i strid med nasjonale sikkerhetsinteresser
l) forbindelse med organisasjoner som har ulovlig formål, og som kan true den demokratiske samfunnsordenen eller som anser vold eller terrorhandlinger som akseptable virkemidler
m) manglende mulighet til å gjennomføre en tilfredsstillende personkontroll
n) tilknytning til andre stater
o) annet som kan gi grunn til å frykte at en person vil kunne opptre i strid med nasjonale sikkerhetsinteresser.

Politisk engasjement og annet lovlig samfunnsengasjement, som medlemskap i, sympati med eller aktivitet for lovlige politiske partier eller organisasjoner, skal ikke tillegges vekt i vurderingen av om en person er sikkerhetsmessig skikket.

Opplysninger om nærstående personer skal bare tillegges vekt dersom de er sikkerhetsmessig relevante.

Kongen kan gi forskrift om klarering og gjennomføring av sikkerhetssamtale.

§ 8-5 *Gjennomføring av personkontroll*

Sikkerhetsmyndigheten skal gjennomføre en personkontroll av alle som skal klareres.

Den som skal klareres, må ha gitt samtykke til kontrollen. Samtykket skal omfatte fornyet kontroll etter tredje ledd. Personkontrollen gjennomføres etter anmodning fra klareringsmyndigheten med mindre sikkerhetsmyndigheten har bestemt noe annet.

Klareringsmyndigheten skal be om en ny personkontroll innenfor gyldighetstiden til en klarering dersom det er behov for det.

En personkontroll skal omfatte opplysninger gitt av personen som skal klareres. Personen plikter å gi fullstendige opplysninger om forhold som kan ha betydning for vurderingen av om personen er sikkerhetsmessig skikket. En klareringssak kan avsluttes uten realitetsavgjørelse dersom en person ikke svarer på henvendelser fra klareringsmyndigheten.

Dersom personen skal sikkerhetsklareres for HEMMELIG eller høyere sikkerhetsgrader eller adgangsklareres til objekter eller infrastruktur klassifisert MEGET KRITISK, og i andre særlige tilfeller, kan det gjennomføres personkontroll av nærstående personer.

Personkontrollen skal også omfatte andre opplysninger som klareringsmyndigheten sitter med, og opplysninger fra relevante registre. Den kan også omfatte opplysninger fra andre kilder, som offentlige myndigheter, tjenestesteder, arbeidsplasser og andre referanser.

Det skal ikke innhentes, registreres eller videreformidles opplysninger om politisk engasjement som nevnt i § 8-4 femte ledd.

Den behandlingsansvarlige for relevante registre plikter å utlevere registeropplysninger uten hinder av taushetsplikt. Registeropplysninger skal meddeles skriftlig. Det kan ikke kreves vederlag for registeropplysningene.

Behandlingsansvarlige for relevante registre skal legge til rette for digitalisert overføring av registeropplysninger til sikkerhetsmyndigheten.

Opplysninger som klareringsmyndigheten har fått i forbindelse med personkontroll, skal ikke benyttes til andre formål enn vurdering av om personen er sikkerhetsmessig skikket. Klareringsmyndigheten kan likevel gi opplysninger til den

autorisasjonsansvarlige dersom det er nødvendig for sikkerhetsmessig oppfølging av personen.

Kongen kan gi forskrift om

a) personkontroll av nærstående
b) fornyet personkontroll
c) hvilke registre som er relevante for personkontroll
d) framgangsmåten ved registerundersøkelser i utlandet
e) utlevering av opplysninger ved tilsvarende personkontroll som utføres av andre lands myndigheter
f) arkivering, oppbevaring, forsendelse og digitalisert overføring av personkontrollopplysninger.

§ 8-6 *Bruk av vilkår ved klarering*

En klarering kan i særlige tilfeller gis på nærmere angitte vilkår, for eksempel at den skal være avgrenset til bare å gjelde en konkret stilling.

Kongen kan gi forskrift om bruk av vilkår ved klarering.

§ 8-7 *Klarering av personer med utenlandsk statsborgerskap*

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.

Kongen kan gi forskrift om klarering av personer med utenlandsk statsborgerskap.

§ 8-8 *Tilbakekallelse, nedsettelse eller suspensjon av klarering*

Dersom klareringsmyndigheten får opplysninger som gir grunn til å tvile på at en klarert person er sikkerhetsmessig skikket, skal klareringsmyndigheten vurdere å tilbakekalle eller nedsette klareringen, eller suspendere klareringen og iverksette nærmere undersøkelser. Er en klarering besluttet tilbakekalt, nedsatt eller suspendert, skal den autorisasjonsansvarlige varsles umiddelbart. Klareringsmyndigheten skal sende sikkerhetsmyndigheten begrunnet melding om beslutningen.

§ 8-9 *Autorisasjon*

Virksomhetens leder er autorisasjonsansvarlig og har ansvaret for sikkerhetsmessig ledelse og kontroll av autoriserte personer.

Det skal gjennomføres en autorisasjonssamtale før det gis autorisasjon. Autorisasjon kan bare gis dersom den autorisasjonsansvarlige ikke har opplysninger som gir rimelig grunn til å tvile på om en person er sikkerhetsmessig skikket.

Sikkerhetsmyndigheten kan kreve at virksomheten skal holde sikkerhetsmyndigheten orientert om hvilke personer som er autorisert.

Kongen kan gi forskrift om autorisasjon, autorisasjonsansvarliges plikter og virksomhetens plikt til å holde sikkerhetsmyndigheten orientert om hvilke personer som er autorisert.

§ 8-10 *Nedsettelse, suspensjon og tilbakekallelse av autorisasjon*

Dersom den autorisasjonsansvarlige får opplysninger som gir rimelig grunn til å tvile på at en autorisert person er sikkerhetsmessig skikket, skal den autorisasjonsansvarlige vurdere om autorisasjonen skal opprettholdes, tilbakekalles, nedsettes eller suspenderes. Den autorisasjonsansvarlige skal melde fra til klareringsmyndigheten om avgjørelsen.

En autorisasjon bortfaller dersom

a) personen fratrer stillingen som autorisasjonen er knyttet til
b) behovet for autorisasjonen ikke lenger er til stede
c) personen ikke lenger har tilstrekkelig klarering.

§ 8-11 *Varslingsplikt om forhold som kan påvirke sikkerhetsmessig skikkethet*

En klarert og autorisert person skal umiddelbart varsle den autorisasjonsansvarlige om forhold som kan være av betydning for om personen er sikkerhetsmessig skikket.

§ 8-12 *Utlevering av informasjon til Politiets sikkerhetstjeneste*

I klareringssaker hvor personer har tilknytning til andre stater, skal sikkerhetsmyndigheten på anmodning fra Politiets sikkerhetstjeneste gi informasjon om personers klareringsstatus, tilknytning til andre stater, tjenestested eller hvilken virksomhet som har anmodet om klarering.

Utlevering av informasjon etter første ledd kan bare skje når Politiets sikkerhetstjeneste anfører at dette er nødvendig for å ivareta tjenestens oppgaver etter politiloven § 17 b og § 17 c nr. 1.

Kongen kan gi forskrift om utlevering av informasjon i klareringssaker til Politiets sikkerhetstjeneste.

§ 8-13 *Begrunnelse for og melding om avgjørelse i klareringssaker*

Den som har vært vurdert klarert, har rett til å få vite resultatet av vurderingen. Hvis det blir avgjort at personen ikke får den ønskede klaringen, skal klareringsmyndigheten uoppfordret informere personen om resultatet og begrunnelsen for denne. Samtidig skal klareringsmyndigheten opplyse om retten til å klage på avgjørelsen.

Begrunnelsen skal ikke inneholde opplysninger som kan røpe forhold

a) som har betydning for nasjonale sikkerhetsinteresser
b) som er av betydning for kildevern
c) som personen ikke bør få kjennskap til av hensyn til helsen
d) som gjelder personens nærstående, og som personen ikke bør få kjennskap til
e) som angår tekniske innretninger, produksjonsmetoder, forretningsmessige analyser og beregninger og forretningshemmeligheter ellers, når de er av en slik art at andre kan utnytte dem i sin næringsvirksomhet.

Klareringsmyndigheten skal utarbeide en intern begrunnelse der alle relevante forhold inngår.

Forvaltningsloven kapittel IV og V gjelder ikke for avgjørelser om klarering eller autorisasjon.

§ 8-14 *Innsyn i klareringssaker*

Etter at en avgjørelse om klarering er fattet, har personen som har vært vurdert klarert, rett til å gjøre seg kjent med sakens dokumenter.

Personen har ikke krav på innsyn i hele eller deler av dokumenter som inneholder opplysninger som nevnt i § 8-13 andre ledd. Personen har heller ikke krav på innsyn i dokumenter som er utarbeidet for den interne saksforberedelsen ved klareringsmyndigheten eller klageinstansen. Unntaket i andre ledd gjelder ikke faktiske opplysninger eller sammendrag eller annen bearbeidelse av faktum.

Den som har krav på innsyn, skal få kopi av dokumentene dersom hun eller han ber om det.

Kongen kan gi forskrift om innsyn i klareringssaker.

§ 8-15 *Oversendelse til særskilt oppnevnt advokat*

En person som har fått en begrunnelse etter § 8-13 første ledd, hvor opplysninger som nevnt i § 8-13 andre ledd er utelatt, eller som har fått avslag på anmodning om innsyn etter § 8-14 andre ledd første punktum, har rett på bistand fra en særskilt oppnevnt advokat.

Advokaten skal ha tilgang til sakens faktiske opplysninger og de delene av begrunnelsen som er ukjent for den som er vurdert klarert, men ikke til dokumenter som er utarbeidet for den interne saksforberedelsen ved klareringsmyndigheten eller klageinstansen.

Advokaten skal gi den som har vært vurdert klarert, råd om hvorvidt han eller hun bør klage.

Departementet oppnevner advokater som skal sikkerhetsklareres for høyeste nivå.

Kongen kan gi forskrift om retten til bistand fra advokat, oppnevningen av advokater og hvilke opplysninger advokatene kan få tilgang til.

§ 8-16 *Klareringsmyndigheter og sentralt register for klareringsavgjørelser*

Kongen utpeker én klareringsmyndighet for forsvarssektoren og én for sivile sektorer. Etterretnings- og sikkerhetstjenestene klarerer sitt eget personell.

Når særlige grunner taler for det, kan Kongen utpeke andre klareringsmyndigheter enn dem som er nevnt i første ledd.

Kongen kan gi forskrift om opprettelsen av et sentralt register for klareringsavgjørelser.

§ 8-17 *Klage på avgjørelse om klarering*

Avgjørelsen om klarering, klarering på vilkår og fastsettelse av tidspunktet for når klareringssaken tidligst kan tas opp på nytt, kan påklages av den avgjørelsen retter seg mot. Det samme gjelder avslag på begrunnelse og avslag på anmodning om innsyn.

Klagen skal sendes til klareringsmyndigheten. Sikkerhetsmyndigheten er klageinstans. Departementet er klageinstans for klareringsavgjørelser som er truffet av sikkerhetsmyndigheten i første instans.

Fristen for å klage er tre uker fra den dagen meldingen om avgjørelsen kom fram til mottakeren. Dersom det klages på avslag på begrunnelse eller avslag på anmodning om innsyn, blir klagefristen avbrutt. Ny klagefrist for avgjørelse om klarering løper fra den dagen klageinstansens avgjørelse er kommet fram, eller mottakeren på annen måte er gjort kjent med den. I saker der en advokat har gjennomgått saken etter § 8-15, løper ny klagefrist fra den dagen rådet fra advokaten har kommet fram til mottakeren.

Forvaltningsloven kapittel VI gjelder i klareringssaker dersom ikke noe annet følger av eller i medhold av denne loven.

Kapittel 9. Sikkerhetsgraderte anskaffelser mv.

§ 9-1 *Sikkerhetsgradert anskaffelse*

En sikkerhetsgradert anskaffelse er en anskaffelse som innebærer at leverandøren av varen eller tjenesten kan få tilgang til eller tilvirker sikkerhetsgradert informasjon, jf. § 5-3, eller få tilgang til et skjermingsverdig objekt eller infrastruktur, jf. § 7-1.

§ 9-2 *Sikkerhetsavtale med leverandør*

Før en sikkerhetsgradert anskaffelse iverksettes, skal virksomheten inngå en sikkerhetsavtale med leverandøren. Dersom en utenlandsk leverandør eller dennes personell må klareres eller gis tilgang til sikkerhetsgradert informasjon, skal sikkerhetsmyndigheten godkjenne leverandøren før det inngås en sikkerhetsavtale.

Sikkerhetsavtalen skal tydeliggjøre og konkretisere partenes plikter og ansvar etter loven. Sikkerhetsavtalen skal alltid inneholde hvilken sikkerhetsgrad anskaffelsen skal ha, jf. §§ 5-3 og 7-2, spesifisert for hver del av oppdraget, og hvordan leverandøren skal forholde seg til de av lovens krav som gjelder for anskaffelsen.

Leverandøren må selv dekke utgifter til å oppfylle krav som følger av lovens bestemmelser, hvis ikke noe annet følger av sikkerhetsavtalen.

Kongen kan gi forskrift om innholdet i en sikkerhetsavtale og om unntak fra kravet om sikkerhetsavtale.

§ 9-3 *Leverandørklarering*

Før en leverandør kan få tilgang til informasjon gradert KONFIDENSIELT eller høyere, skal leverandøren ha gyldig klarering for angitt sikkerhetsgrad. Leverandøren skal også klareres dersom det er nødvendig av andre grunner.

En leverandørklarering skal bare gis dersom det ikke er noen rimelig grunn til å tvile på at leverandøren er sikkerhetsmessig skikket. I vurderingen skal det bare legges vekt på forhold som kan innvirke på leverandørens evne og vilje til å gjøre forebyggende sikkerhetsarbeid etter loven. En personkontroll av personer i leverandørens styre og ledelse skal være en del av vurderingsgrunnlaget.

Leverandøren skal gi klareringsmyndigheten alle opplysninger som kan ha betydning for leverandørklareringen.

Leverandøren skal så snart som mulig orientere klareringsmyndigheten om endringer i styret eller ledelsen, endringer i eierstrukturen, flytting av lokaliteter og utstyr, åpning av gjeldsforhandling, begjæring om konkurs og annet som kan påvirke vurderingen av om leverandøren er sikkerhetsmessig skikket. Dersom det oppstår en sikkerhetsrisiko som ikke kan fjernes med forebyggende sikkerhetstiltak, kan klareringsmyndigheten inndra leverandørklareringen. Sikkerhetsgradert informasjon eller skjermingsverdige objekter eller infrastruktur kan ikke overføres til en ny eier eller inngå i bobehandling ved gjeldsforhandling eller konkurs hvis ikke klareringsmyndigheten har samtykket til det.

For øvrig gjelder reglene i kapittel 8 så langt de passer.

Kongen utpeker en klareringsmyndighet for leverandørklarering. Kongen kan gi forskrift om krav til leverandørklarering og varigheten av klareringen.

§ 9-4 *Varslingsplikt og myndighet til å fatte vedtak ved anskaffelser til skjermingsverdig informasjonssystem, objekt og infrastruktur*

Ved anskaffelser til skjermingsverdig informasjonssystem, objekt eller infrastruktur skal virksomheten vurdere om anskaffelsen kan innebære en ikke ubetydelig risiko for at informasjonssystemet, objektet eller infrastrukturen kan bli rammet av eller brukt til sikkerhetstruende virksomhet. Plikten til å foreta en slik vurdering gjelder ikke dersom anskaffelsen åpenbart ikke innebærer noen slik risiko.

Virksomheten skal varsle departementet dersom vurderingen viser at anskaffelsen innebærer en risiko som nevnt i første ledd. Virksomheter som ikke er underlagt noe departement, skal varsle sikkerhetsmyndigheten. Varslingsplikten gjelder uten hinder av taushetsplikt. Plikten gjelder ikke dersom virksomheten selv iverksetter tiltak som fjerner risikoen, eller gjør den ubetydelig.

Departementet som mottar et varsel etter andre ledd, kan be relevante organer uttale seg om risikoen ved anskaffelsen og om leverandørens sikkerhetsmessige pålitelighet.

Dersom en anskaffelse til et skjermingsverdig informasjonssystem, objekt eller infrastruktur kan innebære en ikke ubetydelig risiko som nevnt i første ledd, kan Kongen i statsråd fatte vedtak om at anskaffelsen ikke skal gjennomføres, eller om at det skal settes vilkår for den. Dette gjelder også dersom det er inngått avtale om anskaffelsen. Dersom det ikke fattes vedtak etter første punktum, skal departementet orientere virksomheten om det. Et vedtak etter første punktum er et særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Kongen i statsråd kan gi forskrift om varslingsplikten og om myndigheten til å fatte vedtak.

Kapittel 10. Eierskapskontroll

§ 10-1 *Meldeplikt ved erverv av virksomhet*

Den som vil erverve en kvalifisert eierandel i en virksomhet som er underlagt loven, jf. § 1-3, skal sende melding til departementet om dette. I de tilfellene hvor virksomheten ikke omfattes av noe departements ansvarsområde, skal meldingen sendes til sikkerhetsmyndigheten.

En kvalifisert eierandel innebærer at ervervet direkte eller indirekte samlet vil føre til at erververen oppnår

a) minst en tredjedel av aksjekapitalen, andelene eller stemmene i virksomheten
b) rett til å bli eier av minst en tredjedel av aksjekapitalen eller andelene, eller
c) betydelig innflytelse over forvaltningen av selskapet på annen måte.

Likt med aksjeeierens egne aksjer regnes de aksjene som eies eller overtas av aksjeeierens nærstående, jf. verdipapirhandelloven § 2-5. Det samme gjelder for andeler som eies eller overtas av andelseierens nærstående.

Kongen kan gi forskrift om meldeplikten.

§ 10-2 *Behandling av melding om erverv av virksomhet*

Departementet eller sikkerhetsmyndigheten som mottar en melding etter § 10-1, skal ta stilling til meldingen så raskt som mulig.

Den som mottar en melding etter § 10-1, kan be relevante organer uttale seg om ervervets risikopotensial og erververens sikkerhetsmessige pålitelighet.

Departementet eller sikkerhetsmyndigheten skal innen 60 arbeidsdager orientere melderen om ervervet er godkjent, eller om at saken skal behandles av Kongen i statsråd etter § 10-3. Fristen regnes fra det tidspunktet departementet eller sikkerhetsmyndigheten har mottatt meldingen. Har departementet eller sikkerhetsmyndigheten innen 50 arbeidsdager framsatt et skriftlig krav om ytterligere opplysninger, avbrytes fristen inntil svaret fra erververen er mottatt.

Kongen kan gi forskrift om departementenes og sikkerhetsmyndighetens behandling av meldingen.

§ 10-3 *Vedtak om stans av erverv av virksomhet*

Dersom et erverv etter § 10-1 kan medføre en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet, kan Kongen i statsråd fatte vedtak om at ervervet ikke kan gjennomføres, eller om at det skal settes vilkår for gjennomføringen. Dette gjelder også dersom det allerede er inngått avtale om ervervet. Dersom det ikke fattes vedtak etter første punktum, skal departementet orientere erververen om dette.

Et vedtak etter første punktum er særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Kongen kan gi forskrift om stans av erverv av virksomhet.

Kapittel 11. Særskilte kontroll- og tilsynsordninger. Tvangsmulkt, overtredelsesgebyr og straff

§ 11-1 *Særskilte kontroll- og tilsynsordninger*

Forebyggende sikkerhetsarbeid i medhold av loven er underlagt kontroll og tilsyn av Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste, i samsvar med bestemmelsene i og i medhold av EOS-kontrolloven.

§ 11-2 *Tvangsmulkt*

Ved overtredelse av bestemmelser gitt i eller i medhold av §§ 3-4, 4-3, 4-4, 4-5, 5-2, 6-2, 6-3, 7-3, § 9-2 første ledd, § 9-4 første ledd første punktum eller § 9-4 andre ledd første eller andre punktum, kan tilsynsmyndigheten fastsette en tvangsmulkt som løper inntil forholdet er brakt i orden. Det samme gjelder for pålegg gitt i medhold av § 3-6.

Et vedtak om tvangsmulkt kan påklages til departementet.

Et vedtak etter første ledd er særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Kongen kan gi forskrift om tvangsmulkt.

§ 11-3 *Overtredelsesgebyr*

Tilsynsmyndigheten kan pålegge en virksomhet overtredelsesgebyr dersom virksomheten eller noen som handler på dennes vegne, forsettlig eller uaktsomt

a) overtrer bestemmelser gitt i eller i medhold av §§ 3-4, 4-3, 4-4, 4-5, 5-2, 6-2, 6-3, 7-3, 9-2 første ledd, 9-4 første ledd første punktum eller 9-4 andre ledd første eller andre punktum
b) overtrer et pålegg gitt med hjemmel i § 3-6
c) gir uriktige eller ufullstendige opplysninger til tilsynsmyndigheten etter §§ 3-4 eller 4-5
d) medvirker til overtredelser som nevnt i bokstav a til c.

Ved fastsettelse av overtredelsesgebyrets størrelse skal det særlig legges vekt på overtredelsens grovhet, overtredelsens varighet, utvist skyld og virksomhetens omsetning. Et vedtak om overtre-

delsesgebyr er et særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Adgangen til å pålegge overtredelsesgebyr foreldes etter fem år. Fristen avbrytes når tilsynsmyndigheten meddeler virksomheten at denne er mistenkt for overtredelse av loven eller vedtak fastsatt med hjemmel i loven.

Et vedtak om overtredelsesgebyr kan påklages til departementet.

Kongen kan gi forskrift om overtredelsesgebyr.

§ 11-4 *Straff*

Den som forsettlig eller uaktsomt overtrer bestemmelser gitt i eller i medhold av §§ 3-4, 4-3, eller 5-2, § 5-3 første ledd, §§ 6-2, 6-3, 7-3, § 9-2 første ledd, § 9-4 første ledd første punktum eller § 9-4 andre ledd første eller andre punktum, eller overtrer et pålegg gitt av tilsynsmyndigheten i medhold av § 3-6, straffes med bot eller fengsel inntil 6 måneder eller begge deler, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Den som forsettlig eller grovt uaktsomt bryter taushetsplikt etter § 5-4 andre ledd eller § 6-6 femte ledd, straffes med bot eller fengsel inntil 1 år eller begge deler, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Den som overtrer et forbud fastsatt med hjemmel i § 7-5, straffes med bot eller fengsel inntil 1 år eller begge deler, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Forsøk på overtredelser som nevnt i første til tredje ledd straffes på samme måte.

Kapittel 12. Ikrafttredelse og endringer i andre lover

§ 12-1 *Ikrafttredelse*

Loven trer i kraft fra det tidspunktet Kongen bestemmer. Kongen kan sette i kraft forskjellige bestemmelser til ulik tid.

§ 12-2 *Opphevelse*

Fra det tidspunktet loven trer i kraft, oppheves lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste.

Bestilling av publikasjoner

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

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

Publikasjonene er også tilgjengelige på
www.regjeringen.no

Trykk: 07 PrintMedia AS – 06/2017