Lov om nasjonal sikkerhet (sikkerhetsloven)

Dato	LOV-2018-06-01-24
Departement	Justis- og beredskapsdepartementet
Ikrafttredelse	01.01.2019
Endrer	LOV-1998-03-20-10
Kunngjort	01.06.2018
Rettet	21.06.2021 (faglige noter fjernet)
Korttittel	Sikkerhetsloven – sikkl

Kapitteloversikt:

Jf. *tidligere* lov 20 mars 1998 nr. 10.

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 stortingsrepresentanter, 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 dette. 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 overtredelsesgebyr 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[1] Kongen bestemmer. Kongen kan sette i kraft forskjellige bestemmelser til ulik tid.

1 Fra 1 jan 2019 iflg. res. 20 des 2018 nr. 2052, se dens nr. 2 for overgangsregler.

§ 12-2. *Opphevelse*

Fra det tidspunktet loven trer i kraft, oppheves lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste.