Deres referanse	Vår referanse	Dato
2015/3139-7/FD V 3/MAY	HOW	19.1.2017

Innspill til NOU 2016:19 Samhandling for sikkerhet

Det vises til brevdatert 17.10.2016, der det es om innspill til 'NOU 2016:19 Samhandling for sikkerhet' – og forslag til revidert sikkerhetslov.

Energi Norge er en interesse- og arbeidsgiverorganisasjon for norsk energinæring. Energi Norge representerer ca. 280 bedrifter som produserer, frakter og selger strøm og varme. Medlemsbedriftene står for 99 prosent av kraftproduksjonen og dekker 90 prosent av nettkundene i Norge. Energi Norge arbeider for bedre klima, sikker forsyning og grønn vekst.

Energi Norges overordnede innspill

Kraftsektoren utgjør en samfunnskritisk infrastruktur hvis overordnede målsettinger er å sikre en robust og effektiv kraftforsyning. Dette har gitt et velfungerende beredskaps- og sikkerhetskonsept organisert i Kraftforsyningens beredskapsorganisasjon (KBO).

Generelt er Energi Norge positivt innstilt til tiltak som ytterligere kan styrke sikkerhet og beredskap i sektoren, men er opptatt av at tiltakene ikke går på bekostning av dagens entydige ansvarsfordeling, svekker forsyningssikkerheten, eller medfører uforholdsmessige økonomiske konsekvenser. *Derfor anbefaler Energi Norge at det endelige ansvaret for sikkerhet og beredskap ligger hos sektormyndighetene som har den nødvendige fagkompetanse og kjenner sektorens sikkerhetsmessige utfordringer.*

Videre består Energi Norges overordnede anbefalinger i det følgende:

- **Videreføre dagens entydige ansvarsforhold.** 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. Dette innebærer at det endelige ansvaret for sikkerhet og beredskap fortsatt legges til sektormyndigheten, og at NSM ikke gis anledning til å overstyre denne. Følgelig fraråder Energi Norge forslaget om å etablere et tvisteorgan med kompetanse til å overprøve sektormyndigheten.

- **Gjennomføre samfunnsøkonomiske kost- /nyttevurderinger.** Energi Norge anbefaler at tiltak for å fremme tverrsektoriell koordinering og strengere krav til beredskap og sikkerhet baseres på grundige samfunnsøkonomiske avveininger som sikrer forholdsmessighet mellom kostnader og nytte. Eventuelle krav om system- og objektsikring bør også begrunnes ut fra disse kriteriene.

- **Bredere beslutningsgrunnlag og revidert forslag.** Energi Norge anbefaler at forslaget bearbeides mye grundigere før det fremmes for Stortinget. Etter en gjennomgang av høringsinnspillene ber vi derfor om at regjeringen innhenter ytterligere konsekvensutredninger før et revidert forslag til lov sendes ut på høring.

Disse hovedpunktene er nærmere utdypet i det følgende. I vedlegg 1 følger Energi Norges konkrete forslag til endringer av lovteksten.

1. Sikkerhet i kraftforsyningen

I utvalgsrapportens digitale vedlegg 3 "*Vurdering av forebyggende sikkerhet innenfor kraft, petroleum og luftfart*", slås det fast at kraftsektorens sektorregelverk er dekkende for forebyggende sikkerhet.

«*Dagens sektorregelverk er i stor grad dekkende for forebyggende sikkerhet. Regelverket sikrer god håndtering av sektorens leveringssikkerhet. På noen områder er beredskapsforskriften og veilederen til forskriften for detaljert, noe som medfører at bransjen i begrenset grad inviteres til å finne gode løsninger. Regelverket regulerer tydelige ansvars- og myndighetsroller i beredskapsorganisasjonen. Dette er viktig og må beholdes*.»

Energi Norge vil derfor ikke anbefale å introdusere et ytterligere sektorovergripende forvaltningsledd med fullmakter til å overstyre sektormyndighetens kompetanse. For at dette skal gjøres på en faglig forsvarlig måte, vil det kreve et betydelig løft i kompetanse og ressursbruk hos sikkerhetsmyndigheten. Det foreligger ingen vurderinger av hvilken kompetanse og ressursnivå som må bygges opp hos sikkerhetsmyndigheten for å ivareta det foreslåtte ansvaret. Det foreligger heller ikke kost-/nyttevurderinger som dokumenterer at de økte kostnadene forslaget innebærer, oppveies av en tilsvarende økt samfunnsøkonomisk nytteverdi og utfordringer knyttet til økt byråkratisering og potensiell kompetansestrid mellom sikkerhetsmyndigheten og øvrige sektormyndigheter.

For norsk kraftforsyning ligger de største truslene erfaringsmessig i skader forårsaket av naturgitte forhold som storm, tunge snøfall, flom og lynaktivitet. Økt fokus og kompetanseoppbygging knyttet til IKT sårbarheter er viktig, men det er avgjørende å se dette i sammenheng med de øvrige truslene i kraftsystemet og sette inn ressursene der de gir størst nytte for samfunnet. Rettes fokuset for ensidig inn mot områder som har lavt skadepotensial i kombinasjon med en regulering som rettes mot økt effektivisering av sektoren, kan det lede til en uheldig dreining av fokuset vekk fra de mest sentrale utfordringene sektoren står overfor når det gjelder sikkerhet og beredskap.

1.1. Objektsikkerhet, systemsikkerhet og redundans

En infrastruktur som det norske kraftsystemet kan ikke sikres fullstendig, noe utvalget også slår fast. Nytteeffekten av ulike tiltak må vurderes, og avveiningen mellom objektsikring og systemsikring vil være sentral i slike vurderinger.

Det norske kraftsystemet er i utgangspunktet robust mot de fleste typer hendelser. I motsetning til andre land, er systemet basert på vannkraft og har en distribuert struktur med mange produksjonsenheter i ulike størrelser, som ligger spredt geografisk og nettmessig. Av totalt ca. 1570 vannkraftverk er 1233 < 10 MW, 257 mellom 10 og 100 MW, 75 mellom 100 og 500 MW. Kun seks enheter er større enn 500 MW. Disse seks utgjør ca. 15 % av den totale kapasiteten på ca. 32 000 MW.

I kraftsystemet er det sammensetningen av de ulike komponentene som avgjør sikkerheten og ikke enkeltkomponentene. Om en enkelt stasjon blir gjenstand for omfattende sikring, vil den fortsatt være avhengig av sikkerheten i tilknyttede tilførselslinjer. Dagens beredskapskrav tar høyde for dette. Anlegg i kraftsystemet er klassifisert og sikret i henhold til regelverk hjemlet i energiloven med forskrifter. N-1-kriteriet[1] er et grunnleggende prinsipp i kraftsystemet, og det er få enkelt-anlegg både i produksjons- og overføringssystemet som ved utfall, utgjør en vesentlig trussel mot forsynings- og leveringssikkerheten. Eksempelvis er det innebygd redundans i de fleste stasjoner i sentral- og regionalnettet i form av antall linjer inn, flere transformatorer, samt oppdekningsreserve i underliggende nett og nabostasjoner. Det er følgelig krevende å sette kraftforsyningen ut av spill med fysiske virkemidler på en slik måte at det vil true grunnleggende nasjonale funksjoner. For systemsikkerheten er beskyttelse av sensitiv informasjon om redundansforholdene vel så viktig som sikring av særskilte anlegg.

I utvalgsrapporten beskrives forhold knyttet til bortfall av driftskontrollsystemer. I den forbindelse vil vi peke på at kraftsystemet fortsetter å fungere selv om aktørene mister muligheten for fjernstyring og

[1] N-1 kriteriet – utfall av en komponent, som for eksempel en linje eller en transformator, skal ikke medføre overlast eller svikt i det øvrige strømnettet.

fjernovervåkning av ett eller flere av sine anlegg. Systemsikkerheten ivaretas gjennom krav om redundans i driftskontrollsystemene ut fra anleggenes kritikalitet, samt krav til virksomhetene om å forberede tiltak for fortsatt drift av anleggene ved svikt i driftskontrollsystemene (utrykning og bemanning av anlegg). I praksis betyr dette oftest bemanning av kritiske anlegg og lokal styring av produksjon og strømnettet, som sikrer at disse kan drives i lang tid, selv om feil eller havarier oppstår i driftskontrollsystemene.

2. Informasjon og samordning

Virksomhetene i kraftsektoren trenger tilgang til relevante scenarier og trusselbilder, som grunnlag for ROS analyser, planer og tiltak. Øvrig sensitiv informasjon kan håndteres gjennom sektormyndigheten. NSMs kompetanse innenfor IKT sikkerhet og trusselvurderinger bør derfor tilflyte sektorene gjennom en organisert informasjonsutveksling mellom NSM og sektormyndighetene, på et nivå som ikke nødvendiggjør underleggelse av loven. Slik kan kompetansenivået løftes hos de ulike sektorene og virksomhetene. NSMs oppgaver bør derfor rettes inn mot deres primærområder og sørge for at de ulike sektormyndigheter (som OED og NVE) og virksomheter underlagt sektormyndighetenes regulering gis tilgang til nødvendig informasjon og kompetanse. Slik kan også samarbeidet mellom NORCERT og KraftCert utvikles. Med en slik organisering kan nødvendige tiltak for systemer og objekter innføres på en kostnadseffektiv måte, samtidig som de sektorovergripende behovene, ansvar og roller ivaretas.

2.1. Varslingsrutiner

Utvalget anbefaler at NSM varsles parallelt i de tilfeller en sektormyndighet er tillagt tilsynsansvar etter loven. En slik dobbeltrapportering vil medføre økt ressursbruk hos NSM, ved at kapasiteten for å motta og behandle slike varsler må være tilstrekkelig dimensjonert. Utvalget mener imidlertid at den sikkerhetsmessige gevinsten ved at NSM har et mer fullstendig bilde over hendelser av sikkerhetsmessig betydning, overstiger de kostnadsmessige ulempene. Det foreligger ingen dokumentasjon for denne påstanden. I kraftsektoren har det i mange år vært et sterkt ønske om å effektivisere og redusere rapporteringskravene. Erfaringsmessig er dette ressurskrevende for sektoren, og begrunnelsene for at data og informasjon skal rapporteres oppfattes ofte å være dårlig fundert. 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.

3. Roller og myndighet

3.1. Ansvaret for forebyggende sikkerhet

Energi Norge støtter utvalgets konklusjon om at de generelle prinsippene for krisehåndtering og beredskap bør ligge fast, og også bør gjelde for innretningen på en ny sektorovergripende lov om forebyggende nasjonal sikkerhet. Dette innebærer, i tråd med ansvarsprinsippet, at det primære ansvaret for forebyggende sikkerhet i de ulike samfunnssektorene tillegges det enkelte fagdepartement. Det er det enkelte fagdepartement som kjenner sin sektor best, og har de beste forutsetningene for å identifisere grunnleggende nasjonale funksjoner og virksomheter av kritisk betydning for disse, samt gjøre nødvendige samfunnsmessige prioriteringer innad i sektoren og nødvendig koordinering overfor relevante tilgrensende sektorer.

Vi deler utvalgets syn om at en helhetlig tilnærming til forebyggende sikkerhet på tvers av samfunnssektorene er viktig og at dette gjøres i tråd med samvirkeprinsippet. Dette innebærer at myndigheter, virksomheter og etater bør ha et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering. Et avklart ansvar for å sikre koordinering og informasjonsutveksling er viktig. Det er imidlertid uheldig å skape uklarhet om selve sektoransvaret ved å innføre hjemler til å overstyre de sektorer som har vel etablert kompetanse, regelverk og systemer for å ivareta sikkerhet og beredskap innenfor sitt sektoransvar.

Alle samfunnssektorer har i større eller mindre utstrekning særegenheter og særlige behov som må ivaretas i det forebyggende sikkerhetsarbeidet. Gjensidige avhengigheter på tvers av samfunnssektorene vil være ulike og variere mellom de ulike sektorene. Vi deler utvalgets syn om behovet for en bredere helhetlig tilnærming til arbeidet med forebyggende sikkerhet. Vi mener derimot at dette best ivaretas gjennom en koordinert sektorvis tilnærming, med spesielt fokus på de sektorer hvor beredskap og sikkerhet er viktig men svakt regulert i sektorlovgivningen. Utvalget har ikke sett dette som en aktuell løsning, uten at denne konklusjonen er gjort nærmere rede for i utredningen.

Utvalget vurderer i liten grad de konkrete tverrsektorielle koordineringsbehovene og hvorfor det er nødvendig å kunne formelt gripe inn og overprøve de ulike sektorene. Spesielt problematisk blir dette dersom fagkompetansen i sikkerhetsmyndigheten er lavere enn den sektoren de skal forvalte. I de sektorene som mangler eller har en svak sektorregulering på sikkerhet og beredskap, bør det derfor vurderes først å styrke aktuell sektorregulering på området, noe som naturlig følger av nærhetsprinsippet. Den tverrsektorielle reguleringen bør rettes inn på områder som sektormyndigheten ikke kan ivareta i egen regi.

3.2. System for å identifisere grunnleggende nasjonale funksjoner og hvilke virksomheter som er av kritisk betydning for disse

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.

Energi Norge støtter utvalgets forslag om at dagens etablerte system legges til grunn. Her har det enkelte fagdepartement ansvaret for å identifisere 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. 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, og nødvendig for en rasjonell koordinering med andre relevante sektorer.

3.3. Uavhengig tvisteorgan

Formålet med tvisteorganets virksomhet er å komme frem til de sikkerhetsmessig beste løsningene, sett i et helhetlig samfunnsmessig perspektiv, i tilfeller av uenighet mellom sektormyndigheter og NSM, samt tilfeller av uenighet mellom den enkelte virksomhet og relevante myndigheter. 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. Behovet for samfunnsøkonomisk kompetanse kan ivaretas ved at det stilles krav om at ett eller flere av medlemmene må ha slik kompetanse. Behovet for relevant sektorkompetanse kan ivaretas ved at minst ett medlem må ha slik kompetanse, men da slik at dette ene medlemmet ambulerer fra sak til sak avhengig av hvilken sektor som skal behandles. Dette kan løses ved at hver enkelt sektormyndighet utpeker representanter fra "sin" sektor, som kan tre inn i utvalget når klagesaker knyttet til denne sektoren behandles.

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. Dette gjelder ikke minst all den tid tvisteorganets leder/nestleder sammen med kun to øvrige medlemmer skal ha anledning til å treffe midlertidige vedtak i hastesaker. Energi Norge mener derfor at det må fremgå klart hvem som faktisk skal ha anledning til å utpeke tvisteorganets medlemmer. Etter Energi Norges oppfatning er det hensiktsmessig at denne kompetansen i tilfelle legges til SMK, slik utvalget foreslår.

4. Kostnader og samfunnsnytte

4.1. Lovens formål og virkeområde

Loven tar sikte på å beskytte mot tilsiktede uønskede hendelser, som kan utgjøre en trussel mot grunnleggende nasjonale funksjoner, herunder; terrorhandlinger, sabotasje, spionasje, og annen alvorlig kriminalitet. Listen over tilsiktede uønskede hendelser, som NOUen og lovforslaget tar mål å beskytte mot, er ikke uttømmende. Snarere er de eksempler på interessene utvalget mener er avgjørende å ivareta. NOUen og loven åpner dermed for et betydelig større omfang enn det som konkret fremgår.

Grunnleggende for utvalgets arbeid var å sikre en kostnadseffektiv regulering. Samfunnsøkonomisk lønnsomhet skulle være en grunnleggende forutsetning. Vi kan ikke se at denne grunnleggende forutsetningen er tatt inn i lovens formål og virkeområde og foreslår at lovens formål utvides for å inkludere dette.

4.2. Sikkerhetsmyndighetens oppgaver og utfordringer knyttet til kompetansestrid, dobbeltregulering og byråkratisering

Dersom energisektoren underlegges sikkerhetsloven som beskrevet i NOUen, vil dette kunne føre til kompetansestrid, dobbeltregulering og byråkratisering.

Utvalget foreslår at NSM tildeles et omfattende sektorovergripende ansvar. Så langt vi erfarer har ikke NSM i dag kompetanse knyttet til kraftsystemet, forsyningssikkerhet i kraftsystemet og hvilke objekter/systemer som er kritiske for å opprettholde strømforsyningen i de ulike regioner av landet. Denne kompetansen og de nødvendige ressursene må de tilegne seg dersom de skal ha et sektorovergripende forvaltningsansvar med kompetanse til å klage inn sektormyndighetenes/selskapenes avgjørelser/prioriteringer. 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.

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. Dette er ressurser og kompetanse det tar lang tid å bygge opp, og det er uklart hvilke sikkerhetsventiler sektormyndighetene har for å sikre at ikke NSM blir et forsinkende og byråkratiserende ledd i beredskapsarbeidet. Utvalget har ikke vurdert konsekvensene av at beredskapsarbeidet i de ulike sektorene blir forsinket i tvistesaker mellom NSM og sektormyndighetene/virksomhetene.

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.

All erfaring viser at tildelte hjemler brukes og de nye hjemler som forslaget åpner for må derfor forventes å påføre sektoren ytterligere kostnader gjennom krav om økt rapportering, tilsyn, kostnadskrevende pålegg, tvistebehandling og oppbygging av parallell kompetanse. Tilsyn fra ytterligere forvaltnings-organer, og spesielt i de tilfelle det oppstår uenighet mellom fagdepartement og NSM, vil påføre virksomhetene økt usikkerhet og ytterligere ulikheter mellom virksomhetene. Spesielt gjelder dette nettselskapene hvor myndigheten måler selskapenes effektivitet, som igjen vil påvirke selskapenes inntektsrammer, kundenes nettleietariffer og virksomhetens avkastning. Bransjen opplever allerede i dag at enkelte enheter i bransjen har større belastninger vedrørende tilsyn og kontroll enn andre.

4.3. Forholdet til anskaffelsesregelverket

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 Forsvarsdepartementet 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.

Vi gjør for øvrig oppmerksom på at produksjon av energi og grossistsalg er fritatt fra regelverket om offentlig anskaffelser, ved ESAs[2] vedtak av 22. mai 2012.

Norske kraftselskaper har ofte mange leverandører og underleverandører og svært få komponenter leveres fra norske selskaper. Eksempelvis 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.

4.4. Kompensasjon

Loven åpner opp for at det kan gis kompensasjon dersom en virksomhet får sin rettslige posisjon svekket. *Kongen i statsråd skal gi forskrift om vedtak etter første ledd, herunder om eventuell kompensasjon til personer og virksomheter som får sin rettslige posisjon svekket som følge av Kongens vedtak.*

Ettersom de regulatoriske og kostnadsmessige konsekvenser av forslaget ikke er utredet, er det heller ikke mulig å vurdere potensielle økonomiske tap for virksomhetene ved å bli underlagt sikkerhetsloven. Norsk kraftsektor ble deregulert tidlig på nitti-tallet og all kraftproduksjon og kraftomsetning ble konkurranseutsatt i frie markeder. Nettvirksomhetene er underlagt en konkurransebasert

[2] EFTA`s overvåkningsorgan

reguleringsmodell, som medfører at økte kostnader for et nettselskap medfører konkurransemessige ulemper i forhold til andre nettselskaper.

Nye kostnadsdrivende sikkerhetskrav kan derfor påføre enkeltaktører store tap i tillegg til svekket konkurranseevne. Dette er elementer som må tas i betraktning i de samfunnsøkonomiske kost-/nyttevurderingene. Fortolkningen av hva en svekket rettslig posisjon innebærer og hvilke andre typer for kompensasjon enn erstatning det siktes til, fremgår ikke av utredningen og bør tydeliggjøres.

4.5. Sentrale definisjoner og konsekvenser av disse

NOUen og lovforslaget opererer med en rekke definisjoner som danner grunnlaget for lovens omfang og forståelse. De sentrale begrepene er rundt formulert og bidrar således ikke til å gi en nærmere avklaring av lovens omfang og betydning for de som underlegges loven. Snarere har utvalget lagt opp til at dette skal avklares i senere forskriftsarbeider. Dette forskriftsarbeidet vil for alle praktiske formål bli tillagt Sikkerhetsmyndigheten, til tross for at utvalget har konkludert med at det er sektormyndighetene som har fagkunnskapen til å avgjøre hva som vil være et *forsvarlig sikkerhetsnivå* for den enkelte virksomhet, og på de enkelte fagfeltene loven dekker. Det er med andre ord sektormyndighetene som kan gi definisjonene innhold og avgjøre hva et forsvarlig sikkerhetsnivå faktisk innebærer, ikke Sikkerhetsmyndigheten.

Definisjonene som skal fortolkes av Sikkerhetsmyndigheten, sektormyndighetene og de ulike virksomhetene er uklare. Dette gjelder for eksempel hvilke virksomheter som vil være av *kritisk betydning* for *grunnleggende samfunnsfunksjoner*, når de overordnede interesser er truet, når informasjon, informasjonssystemer, objekter eller infrastruktur, aktivitet, har kritisk betydning for *grunnleggende nasjonale funksjoner* og hvordan redundans og alternative tiltak/virkemidler vil påvirke denne vurderingen. Likeledes er det ikke avklart når infrastruktur og informasjonssystemer vil være av kritisk betydning for samfunnsfunksjonene.

Et sentralt spørsmål utvalget ikke har besvart er hvordan definisjoner og tiltak på tvers av samfunnssektorer og virksomheter skal forstås og koordineres, slik at tiltak blir iverksatt der det er mest samfunnsøkonomisk lønnsomt. Hvilke lønnsomhetskriterier og metodikk som skal legges til grunn for slike tverrsektorielle vurderinger er heller ikke avklart.

Utvalget vurderer at det ikke er mulig, ønskelig eller hensiktsmessig å gjennomføre sikkerhetstiltak som eliminerer risikoen for at tilsiktede uønskede hendelser inntreffer. Vi deler dette synet. En konkret grenseavklaring på dette området er imidlertid ikke foretatt i utredningen. Konsekvensene av lovforslaget er derfor uoverskuelig, ikke bare fordi den tekstlige beskrivelsen og definisjonene er tunge å trenge igjennom, men spesielt fordi de detaljerte og konkrete konsekvensene av forslaget ikke fremkommer. De faktiske konsekvensene vil i beste fall bli synlige når de underliggende forskriftene som loven åpner for, totalt inntil 44 stykker, utarbeides.

4.6. Samfunnsøkonomiske kost-/nyttevurderinger

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.

Utvalget har heller ikke vurdert konkret hvor mange virksomheter som vil bli underlagt loven. For virksomheter som ikke tidligere har vært underlagt sikkerhetsloven, vil en underleggelse kunne få vesentlige konsekvenser. Utvalget erkjenner at økte krav til sikkerhet også vil innebære økte kostnader, som kan virke tyngende for den enkelte virksomhet sett ut fra et bedriftsøkonomisk perspektiv. Utvalget mener likevel at de sikkerhetsmessige gevinstene i et samfunnsperspektiv overstiger de ulempene en utvidelse av lovens virkeområde vil kunne få for enkelte virksomheter. Hvor mye sikkerhetsnivået faktisk vil øke av de foreslåtte lovendringene og den tilhørende nytteverdien av dette, er ikke nærmere beskrevet i NOUen.

Det er med andre ord ikke mulig å overskue de faktiske implikasjonene av forslaget eller å kvantifisere de samfunnsøkonomiske kostnader og nytteverdier som forslaget forventes å gi. For sikkerhetsmyndighetene vil konsekvensene av et sektorovergripende forvaltningsansvar og at flere virksomheter underlegges loven, medføre økt ressursbruk blant annet knyttet til rådgivning, oppfølging og kontroll med virksomhetene. Allerede i perioden 2012 – 2015 har NSMs bemanning økt fra 144 til 218 årsverk og driftsutgiftene fra 171 mill.kr. til 254 mill.kr.[3] Det må forventes en betydelig økning utover dette dersom NSM skal ivareta de foreslåtte nye ansvarsområdene som utvalget foreslår, men ikke kvantifiserer. I tillegg kommer økte kostnader i alle de ulike sektorene knyttet til økt administrasjon, innføring av rapporteringssystemer, kvalitetskontroll med leverandører og underleverandører etc.

Utvalgsrapporten berører ikke de kostnadsmessige sidene ved å stille strengere sikkerhetskrav til ulike anlegg. For å anskueliggjøre potensielle kostnadskonsekvenser i kraftforsyningen har vi søkt å eksemplifisere kostnader forbundet ved å oppklassifisere anlegg til et høyere nivå, referert til NVEs klassifiseringskrav til ulike anlegg, ref. Beredskapsforskriften, ref. vedlegg 2 tabell 3. Eksempelvis kan investeringskostnadene for oppklassifisering av anlegg i klasse 1 og 2 ligge i størrelsesorden 14 mrd. kr. I tillegg påløper økte årlige driftskostnader i størrelsesorden 600 mill.kr. Investeringskostnader og økte driftskostnader knyttet til eventuelle nye sikringstiltak for dagens klasse 3 anlegg vil komme i tillegg. Konsekvenser for øvrige anlegg, som i dag ikke er klassifisert, er ikke medregnet. Dette er kostnader som må dekkes av nettkundene eller som redusert avkastning til produksjons- og netteierne (primært Staten, fylker og kommuner).

Forslaget og de potensielle konsekvensene knyttet til kostnader og økt byråkratisering står i sterk kontrast til Regjeringens erklærte ønske og mål om *en mest mulig effektiv bruk av fellesskapets ressurser*, at *samfunnet må bli mindre byråkratisk*, og *redusere næringslivets kostnader ved å etterleve myndighetspålagte rapporteringskrav*, ref. Regjeringserklæringen.

4.7. Ikrafttredelse

Med bakgrunn i de uklarheter som er beskrevet ovenfor og at lovens omfang og konsekvens først vil bli avklart når underliggende forskrifter utarbeides, bør ikrafttredelse av revidert sikkerhetslov utsettes. Den reviderte lovens ikrafttredelse og utpekning av skjermingsverdige objekter og systemer bør først skje når forskriftsarbeidet er gjennomført og de kostnads- og nyttemessige forhold avklart.

Kraftforsyningen er et av samfunnets mest gjennomregulerte sektorer gitt den sentrale funksjonen det har for samfunnet. Kraftforsyningsberedskap og forsyningssikkerhet, herunder IKT-sikkerhet, er naturlig nok også et sentralt tema for kraftforsyningen og Energi Norges medlemmer. Det er et område Energi Norge ønsker å følge tett opp. Ta derfor gjerne kontakt om det er andre områder vi kan bidra på eller om det er spørsmål vedrørende vårt innspill.

Vennlig hilsen
Energi Norge

Einar Westre
Direktør nett og marked

Hans Olav Ween
Næringspolitisk rådgiver - kraftsystemer

Kopi: OED, NVE, Statnett SF

[3] NSMs årsrapport for 2015 "Kappløp om sikkerhet"

Vedlegg 1

Konkrete endringsforslag til lovteksten

Kapittel 1. Formål og virkeområde

§ 1-1 *Lovens formål*

Loven skal bidra til å trygge Norges suverenitet, territorielle integritet og demokratiske styreform ved å motvirke tilsiktede uønskede hendelser som kan skade grunnleggende nasjonale funksjoner.

Loven skal sikre at tiltak som iverksettes for å ivareta lovens formål, gjennomføres på en måte som er samfunnsøkonomisk forsvarlig og forenlig med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.

§ 1-2 *Lovens virkeområde*

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

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

Loven kommer til anvendelse med mindre det er sektorlovgivning som dekker samme formål og virkeområde.

Kongen i statsråd kan gi forskrift om lovens virkeområde og kan herunder helt eller delvis unnta bestemte rettssubjekter eller visse typer informasjon, informasjonssystemer, objekter og infrastruktur.

§ 1-3 *Særbestemmelser om lovens virkeområde*

Loven gjelder for Stortinget og Stortingets organer i den utstrekning Stortinget bestemmer det.

Bestemmelsene gitt i og i medhold av kapittel 8 om personellsikkerhet gjelder ikke for regjeringens medlemmer og dommere i Høyesterett.

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

Loven gjelder for leverandører av varer eller tjenester i forbindelse med en sikkerhetsgradert anskaffelse etter loven kapittel 9.

For virksomheter på Svalbard, Jan Mayen og i bilandene gjelder loven i det omfang og med de stedlige tilpasninger Kongen bestemmer.

Kapittel 2. Myndigheter etter loven

§ 2-1 *Departementenes ansvar og myndighet etter loven*

Hvert enkelt departement er ansvarlig for forebyggende sikkerhet innenfor sitt myndighetsområde, og skal

a) identifisere og holde oversikt over grunnleggende nasjonale funksjoner innenfor sitt myndighetsområde
b) identifisere og holde oversikt over virksomheter som direkte eller indirekte er av vesentlig betydning for opprettholdelse av grunnleggende nasjonale funksjoner
c) treffe enkeltvedtak om at virksomheter, eller deler av virksomheten, er av kritisk betydning for grunnleggende nasjonale funksjoner, jf. § 1-2, slik at loven, eller deler av loven, gjelder for dem.

Virksomheter som vurderes å være av kritisk betydning for grunnleggende nasjonale funksjoner, jf. første ledd bokstav c, skal forhåndsvarsles, jf. forvaltningsloven § 16. Selvstendige rettssubjekter kan påklage vedtaket til Tvisteorganet etter reglene i forvaltningsloven kapittel VI.

Ansvarlig departement skal holde Sikkerhetsmyndigheten orientert om oversikter og vedtak etter første ledd bokstav a til c.

~~Sikkerhetsmyndigheten kan på eget initiativ fremme forslag overfor ansvarlig departement om at det bør treffes vedtak etter første ledd bokstav c. Dersom Sikkerhetsmyndigheten finner at et departements unnlatelse av å treffe slikt vedtak er uforsvarlig, kan departementets avgjørelse bringes inn for Tvisteorganet.~~

Kongen i statsråd kan gi forskrift om departementenes ansvar og myndighet etter loven.

§ 2-2 *Sikkerhetsmyndigheten*

Sikkerhetsmyndigheten ~~har det sektorovergripende ansvaret for at~~ skal koordinere gjennomføring av forebyggende sikkerhet i virksomhetene slik at dette skjer i samsvar med denne loven. Sikkerhetsmyndigheten skal herunder

a) påse at det føres tilsyn med virksomheters gjennomføring av de kravene til forebyggende sikkerhet som følger av loven
b) gi informasjon, råd og veiledning til virksomheter om forebyggende sikkerhet og aktuelle tiltak for å gjennomføre de kravene som følger av loven
c) utarbeide og gjøre tilgjengelig generell informasjon om loven og praktiseringen av den
d) holde en tverrsektoriell oversikt over departementenes identifisering og enkeltvedtak etter § 2-1 første ledd bokstav a til c
e) treffe enkeltvedtak, jf. § 2-1 første ledd bokstav c, overfor virksomheter som ikke anses å falle innenfor et departements myndighetsområde.
For vedtak etter første ledd bokstav e gjelder § 2-1 andre ledd tilsvarende.

Kongen kan gi forskrift om Sikkerhetsmyndighetens ansvar etter loven.

§ 2-3 *Informasjon om trusselvurderinger og risikohåndtering*

Sikkerhetsmyndigheten skal legge til rette for at sektormyndigheter og virksomheter omfattet av loven får informasjon om trusselvurderinger og annen sikkerhetsinformasjon som er av betydning for myndighetenes og virksomhetenes gjennomføring av loven.

Sikkerhetsmyndigheten skal koordinere tilgjengeliggjøring av informasjon som nevnt i første ledd, og i samråd med sektormyndigheter og andre relevante myndigheter påse at det etableres nødvendige arenaer for informasjons- og erfaringsutveksling.

Kongen kan gi forskrift om utveksling av informasjon etter denne bestemmelsen.

§ 2-4 *Nasjonal responsfunksjon for alvorlige dataangrep*

Kongen utpeker en nasjonal responsfunksjon for alvorlige dataangrep mot skjermingsverdig infrastruktur og et nasjonalt varslingssystem for digital infrastruktur. Når det er nødvendig for å beskytte grunnleggende nasjonale funksjoner, kan den nasjonale responsfunksjonen behandle personopplysninger i form av

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

Behandling av andre former for personopplysninger er kun tillatt når det er strengt nødvendig for å beskytte grunnleggende nasjonale funksjoner. Behandlingen skal i alle tilfeller være proporsjonal med det inngrepet den representerer i personvernet.

Kongen kan gi forskrift om den nasjonale responsfunksjonens behandling av personopplysninger.

§ 2-5 *Vedtaksmyndighet for Kongen i statsråd*

Kongen i statsråd kan fatte enkeltvedtak som er nødvendig for å stanse, begrense eller endre en planlagt eller pågående aktivitet, dersom denne aktiviteten med stor grad av sannsynlighet kan få kritiske skadevirkninger for grunnleggende nasjonale funksjoner. Vedtaket kan fattes uten hensyn til begrensningene i forvaltningsloven § 35 om adgangen til å omgjøre tidligere fattede vedtak, og uavhengig av om aktiviteten ellers er tillatt etter lov eller annet vedtak.

Vedtak etter første ledd skal om mulig være midlertidig og skal ikke ha lengre varighet enn hva som er strengt nødvendig. Vedtaket skal stå i rimelig forhold til den risiko aktiviteten utgjør. Det skal ikke fattes vedtak som er mer inngripende enn det som er strengt nødvendig for å redusere risikoen ved den aktuelle aktiviteten til et akseptabelt nivå.

Før vedtak etter første ledd treffes skal saken utredes så godt som tiden og situasjonen tillater. Berørte parter skal om mulig få anledning til å uttale seg. Den risikoreduserende effekten av vedtaket skal kunne dokumenteres.

Blir vedtak etter første ledd truffet i en situasjon der det ikke er mulig å gjennomføre fullt ut tilfredsstillende saksbehandling, skal slike mangler så snart som mulig rettes. Fremkommer det nye og vesentlige opplysninger i saken, skal det første vedtaket vurderes på nytt, og nytt enkeltvedtak eventuelt treffes.

Vedtak etter første ledd er særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Kongen i statsråd skal gi forskrift om vedtak etter første ledd, herunder om eventuell kompensasjon til personer og virksomheter som får sin rettslige posisjon svekket som følge av Kongens vedtak.

~~§ 2-6 *Klage og tvisteløsning*~~

~~Vedtak etter loven kan bringes inn for Tvisteorganet for forebyggende nasjonal sikkerhet, jf. § 2-7. Dette gjelder ikke vedtak fattet av Kongen i statsråd med hjemmel i §§ 2-5, 9-4 eller 10-1, og vedtak som nevnt i andre ledd.~~

~~Vedtak etter loven kapittel 8 kan påklages til Sikkerhetsmyndigheten. I saker der Sikkerhetsmyndigheten er klareringsmyndighet, kan vedtak påklages til departementet.~~

~~Reglene i forvaltningsloven kapittel VI gjelder for selvstendige rettssubjekters klageadgang etter denne loven.~~

~~§ 2-7 *Tvisteorgan for forebyggende nasjonal sikkerhet*~~

~~Kongen utpeker et kollegialt organ med fem medlemmer som oppnevnes for fire år med adgang til gjenoppnevning for ytterligere fire år.~~

~~Ved oppnevning av organets medlemmer skal det, i tillegg til sikkerhetsfaglig kompetanse, også legges vekt på kompetanse innen personvern og selvstendige rettssubjekters rettssikkerhet.~~

~~Tvisteorganet kan bestemme at leder eller nestleder, sammen med to andre medlemmer, kan treffe midlertidige vedtak i saker som må avgjøres uten opphold.~~

~~Tvisteorganet skal avgi en årlig rapport om sin virksomhet.~~

~~Kongen i statsråd kan i forskrift gi nærmere bestemmelser om Tvisteorganets organisering og saksbehandling.~~

Kapittel 3. Tilsyn etter loven

§ 3-1 *Tilsyn med virksomheter*

Sikkerhetsmyndigheten skal føre tilsyn med departementenes gjennomføring av loven.

Innenfor samfunnssektorer der det finnes andre offentlige myndigheter som har tilsynsfunksjoner som omfatter beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur, kan ansvarlig departement, jf. § 2-1, bestemme at disse sektormyndighetene skal føre tilsyn med virksomheter omfattet av loven.

Innenfor samfunnssektorer der det ikke finnes myndigheter med tilsynsfunksjoner som nevnt i andre ledd, skal Sikkerhetsmyndigheten føre tilsyn med virksomheter omfattet av loven.

Sikkerhetsmyndigheten skal føre tilsyn med sektormyndigheter, som er tillagt tilsynsansvar etter andre ledd.

Kongen kan gi forskrift om fordeling av tilsynsansvaret mellom Sikkerhetsmyndigheten og aktuelle sektormyndigheter.

§ 3-2 *Sikkerhetsmyndighetens samarbeid med sektormyndigheter*

Sikkerhetsmyndigheten skal samarbeide med andre offentlige myndigheter som i medhold av lov har tilsynsfunksjoner innenfor sin samfunnssektor som omfatter beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur.

Gjennomføring av tilsyn skal i størst mulig grad samordnes med andre tilsynsmyndigheter.

For områder der sektormyndigheter har tilsynsansvar etter § 3-1, skal det inngås samarbeidsavtaler mellom Sikkerhetsmyndigheten og sektormyndighetene.

Som grunnlag for sektormyndighetenes tilsyn etter loven, skal Sikkerhetsmyndigheten

a) utarbeide og vedlikeholde grunnleggende kriterier for tilsyn etter loven med forskrifter
b) forestå felles opplæring av tilsynspersonell.

~~Sikkerhetsmyndigheten kan, dersom den anser det nødvendig, medvirke til forberedelse og gjennomføring av tilsyn.~~ Sektormyndighetene kan anmode Sikkerhetsmyndigheten om å medvirke til forberedelser og gjennomføring av tilsyn.~~om slik bistand.~~

Sektormyndigheter som har tilsynsansvar etter loven, jf. § 3-1, skal orientere Sikkerhetsmyndigheten om hovedfunn.

Kongen kan gi forskrift om samarbeidet mellom Sikkerhetsmyndigheten og sektormyndighetene.

§ 3-3 *Generelle prinsipper for tilsyn*

Tilsyn etter loven skal planlegges og gjennomføres på en slik måte at tilsynet virker minst mulig forstyrrende på tilsynsobjektenes daglige drift.

Opplysninger som tilsynsmyndigheten innhenter som ledd i tilsynsvirksomheten skal bare nyttes i direkte forbindelse med tilsynet.

Forvaltningslovens bestemmelser om taushetsplikt gjelder for personell som på vegne av tilsynsmyndigheten gjennomfører tilsyn etter loven.

§ 3-4 *Stedlig tilsyn*

I den grad det er nødvendig for å gjennomføre tilsyn etter loven, kan tilsynsmyndigheten kreve nødvendig adgang til virksomhetens informasjon, informasjonssystemer, objekter og infrastruktur.

Stedlig tilsyn som nevnt i første ledd skal normalt varsles skriftlig. Forvaltningsloven § 15 gjelder tilsvarende.

Kongen kan gi forskrift om tilsynsmyndighetens stedlige tilsyn.

§ 3-5 *Tilsynsmyndighetens behandling av personopplysninger*

Når det er nødvendig for å utføre oppgavene etter loven, kan tilsynsmyndigheten behandle opplysninger som direkte eller indirekte kan knyttes til en fysisk enkeltperson (personopplysninger).

Behandlingen av personopplysninger etter første ledd må være proporsjonal med det inngrepet den representerer i personvernet.

Behandlingen av personopplysninger etter første ledd skal om mulig skje ved hjelp av virksomhetens informasjonssystem, og uten at personopplysninger blir kopiert eller overført til tilsynsmyndigheten. Tilsynsmyndigheten kan likevel kreve kopi av personopplysninger som er nødvendige for å bekrefte, avkrefte eller dokumentere at bestemmelser i loven er brutt. Virksomheten skal varsles om hvilke opplysninger det blir tatt kopi av.

Kongen kan gi forskrift om tilsynsmyndighetens behandling av personopplysninger.

§ 3-6 *Pålegg*

Pålegg etter loven kan bare gis dersom det er utvilsomt at tiltaket er nødvendig for å ivareta lovens formål, og de kostnadene som påføres virksomheten, står i et rimelig forhold til det som kan oppnås ved tiltaket.

Sektormyndighet med tilsynsansvar etter loven kan gi pålegg om gjennomføring av tiltak innenfor sin sektor. Sikkerhetsmyndigheten kan gi virksomheter som ikke er underlagt tilsyn fra en sektormyndighet, pålegg om gjennomføring av tiltak.

Sikkerhetsmyndigheten kan gi en sektormyndighet med tilsynsansvar etter loven nødvendige pålegg for å sikre at lovens formål ivaretas.

~~Pålegg kan påklages til Tvisteorganet. Reglene i forvaltningsloven kapittel VI gjelder for selvstendige rettssubjekters klageadgang.~~

Kapittel 4. Generelle krav til forebyggende sikkerhet

§ 4-1 *Plikt til å gjennomføre sikkerhetstiltak*

Virksomheten skal, på grunnlag av risiko- og sårbarhetsanalysen, jf. § 4-3, gjennomføre forebyggende sikkerhetstiltak. Tiltakene skal gi et forsvarlig sikkerhetsnivå, og

a) bidra til å hindre tilsiktede uønskede hendelser som kan skade informasjon, informasjonssystemer, objekter, infrastruktur eller aktivitet av kritisk betydning for grunnleggende nasjonale funksjoner
b) redusere skadevirkningene dersom slike hendelser inntreffer

Kostnader ved sikkerhetstiltak etter loven skal stå i et rimelig forhold til det som oppnås ved tiltaket.

Forutsatt at kravene som følger av første ledd og loven for øvrig oppfylles, kan planlegging og gjennomføring av forebyggende tiltak mot tilsiktede uønskede hendelser skje i sammenheng med forebyggende tiltak mot annen risiko som foreligger for virksomheten.

Kongen kan gi forskrift om plikter for virksomheter som omfattes av loven.

§ 4-2 *Sikkerhetsstyring*

Ansvaret for forebyggende sikkerhet etter loven påhviler leder for virksomheten. Forebyggende sikkerhet skal innarbeides som en del av virksomhetens styringssystem.

Virksomheten skal påse at dens ansatte, leverandører og oppdragstakere har tilstrekkelig opplæring i sikkerhetsspørsmål, og skal regelmessig kontrollere sikkerhetstilstanden i virksomheten. For leverandører til sikkerhetsgraderte anskaffelser gjelder loven kapittel 9.

Kongen kan gi forskrift om sikkerhetsstyring, herunder om bruk av standarder.

§ 4-3 *Risiko- og sårbarhetsanalyse*

Som grunnlag for virksomhetens forebyggende sikkerhetstiltak skal det gjennomføres en risiko- og sårbarhetsanalyse. Virksomheten skal herunder kartlegge hvilke andre virksomheter den er avhengig av for å opprettholde sin funksjonalitet.

Risiko- og sårbarhetsanalysen skal jevnlig gjennomgås, og om nødvendig revideres.

Sikkerhetsmyndigheten, eller sektormyndighet som er gitt tilsynsansvar etter loven, skal på anmodning rådgi og veilede virksomheten ved gjennomføring av risiko- og sårbarhetsanalyser.

Kongen kan gi forskrift om risiko- og sårbarhetsanalyse, herunder om bruk av standarder.

§ 4-4 *Krav til dokumentasjon*

Virksomheten skal dokumentere at

a) risiko- og sårbarhetsanalyse er gjennomført
b) nødvendige sikkerhetstiltak for å redusere risikoen for og konsekvensene av tilsiktede uønskede hendelser er iverksatt.

Kongen kan gi forskrift om krav til dokumentasjon.

§ 4-5 *Øvelser*

Virksomheten skal gjennomføre regelmessige øvelser for å sikre at kompetansen til å forebygge og håndtere tilsiktede uønskede hendelser vedlikeholdes og utvikles.

Kongen kan gi forskrift om øvelser.

§ 4-6 *Varsling*

Virksomheten skal omgående varsle tilsynsmyndigheten dersom

a) en tilsiktet uønsket hendelse har rammet virksomheten, som kan ha betydning for virksomhetens evne til å ivareta oppgaver knyttet til grunnleggende nasjonale funksjoner
b) det er begrunnet mistanke om at det har inntruffet eller er fare for at det vil inntreffe en hendelse som nevnt i bokstav a

c) det er begrunnet mistanke om at det har inntruffet eller er fare for at det vil inntreffe en tilsiktet uønsket hendelse som kan ha kritiske skadevirkninger for grunnleggende nasjonale funksjoner, selv om dette ikke er rettet mot virksomheten
d) det har skjedd brudd på krav til sikkerhet i kapittel 5, 6 eller 7, med forskrifter.

I samfunnssektorer der sektormyndigheter er gitt tilsynsansvar i medhold av § 3-1, skal Sikkerhetsmyndigheten varsles parallelt.

Tilsynsmyndigheten skal uten ugrunnet opphold videresende varsel etter første ledd bokstav c til ansvarlig departement for vurdering av enkeltvedtak etter § 2-5. Der Sikkerhetsmyndigheten er tilsynsmyndighet skal varsel uten ugrunnet opphold videresendes til departementet.

Varslingsplikten etter denne bestemmelsen gjelder uten hinder av lovbestemt taushetsplikt.

Kongen kan gi forskrift om virksomhetenes varslingsplikt etter loven.

§ 4-7 *Behandling av personopplysninger*

Behandling av personopplysninger som skjer med det formål å etterleve bestemmelsene i denne loven, skal skje i samsvar med prinsippene i Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 artikkel 5, jf. Artikkel 23.

Kapittel 5. Informasjonssikkerhet

§ 5-1 *Sikkerhetsgradert informasjon*

Den som utsteder eller på annen måte tilvirker informasjon skal, på bakgrunn av en skadevurdering, sikkerhetsgradere og merke informasjonen på følgende måte:

a) STRENGT HEMMELIG benyttes dersom det kan få helt avgjørende skadefølger for grunnleggende nasjonale funksjoner, jf. § 1-2, om informasjonen blir kjent for uvedkommende
b) HEMMELIG benyttes dersom det kan få alvorlige skadefølger for grunnleggende nasjonale funksjoner, jf. § 1-2, om informasjonen blir kjent for uvedkommende
c) KONFIDENSIELT benyttes dersom det kan få skadefølger for grunnleggende nasjonale funksjoner, jf. § 1-2, om informasjonen blir kjent for uvedkommende
d) BEGRENSET benyttes dersom det i noen grad kan få skadefølger for grunnleggende nasjonale funksjoner, jf. § 1-2, om informasjonen blir kjent for uvedkommende.

Sikkerhetsgradering skal ikke skje i større utstrekning eller for lengre tid enn nødvendig. Sikkerhetsgraderingen skal bortfalle senest etter 30 år. I særskilte tilfeller kan Kongen beslutte unntak fra 30-års-regelen i andre punktum.

Kongen kan gi forskrift om sikkerhetsgradering.

Innenfor rammen av gjensidig overenskomst med fremmed stat eller internasjonal organisasjon kan Kongen i forskrift gi nærmere bestemmelser om sikkerhetsgradering og beskyttelse av informasjon som mottas fra eller avgis til vedkommende stat eller internasjonale organisasjon.

§ 5-2 *Beskyttelse av sikkerhetsgradert informasjon*

Virksomheten skal iverksette nødvendige sikkerhetstiltak slik at sikkerhetsgradert informasjon
a) ikke blir kjent for uvedkommende
b) ikke går tapt eller blir endret uten at dette er autorisert
c) er tilgjengelig for autoriserte personer der tjenstlige behov tilsier dette.

Kongen kan gi forskrift om minstekrav for beskyttelse av sikkerhetsgradert informasjon.

§ 5-3 *Tilgang til og taushetsplikt for sikkerhetsgradert informasjon*

Sikkerhetsgradert informasjon skal bare overlates til personer som har tjenstlig behov og er autorisert for slik tilgang.

Enhver som får tilgang til sikkerhetsgradert informasjon som ledd i arbeid, oppdrag, verv eller aktivitet for en virksomhet som omfattes av loven har taushetsplikt om innholdet. Taushetsplikten gjelder også etter at vedkommende har avsluttet arbeidet, oppdraget, vervet eller aktiviteten.

§ 5-4 *Tekniske sikkerhetsundersøkelser*

Sikkerhetsmyndigheten, eller den Sikkerhetsmyndigheten bemyndiger, kan foreta undersøkelser av lokaler, bygninger og andre objekter som en virksomhet alene eller sammen med andre råder over, i den hensikt å fastslå om uvedkommende med eller uten tekniske hjelpemidler kan skaffe seg tilgang til sikkerhetsgradert informasjon ved avlytting av tale, avlesning av signaler eller ved innsyn.

Sikkerhetsmyndigheten skal informere sektormyndigheter som har tilsynsansvar etter loven, jf. §3-1, om sikkerhetsundersøkelser før de foretas.

Sikkerhetsmyndigheten skal orientere sektormyndigheter som har tilsynsansvar etter loven, jf. §3-1, om hovedfunn.

Kongen kan gi forskrift om tekniske sikkerhetsundersøkelser.

Kapittel 6. Informasjonssystemsikkerhet

§ 6-1 *Skjermingsverdige informasjonssystemer*

Med skjermingsverdige informasjonssystemer menes

a) informasjonssystemer som er av kritisk betydning for grunnleggende nasjonale funksjoner
b) informasjonssystemer som behandler sikkerhetsgradert informasjon.

§ 6-2 *Beskyttelse av skjermingsverdige informasjonssystemer*

Virksomheten skal gjennomføre nødvendige tiltak for å oppnå et forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer. Tiltakene skal sikre at

a) informasjonssystemene opprettholder sin funksjonalitet
b) konfidensialiteten, integriteten og tilgjengeligheten til informasjon som behandles, ivaretas.

Kongen kan gi forskrift om beskyttelse av skjermingsverdige informasjonssystemer.

§ 6-3 *Godkjenning av skjermingsverdige informasjonssystemer*

Skjermingsverdige informasjonssystemer skal godkjennes av en ansvarlig godkjenningsmyndighet.

Informasjonssystemer som skal behandle sikkerhetsgradert informasjon skal forhåndsgodkjennes.

Kongen kan gi forskrift om godkjenning av skjermingsverdige informasjonssystemer, herunder utpeking av ansvarlige godkjenningsmyndigheter og krav til leverandører.

§ 6-4 *Overvåking av skjermingsverdige informasjonssystemer*

Virksomheten skal kontinuerlig overvåke sine skjermingsverdige informasjonssystemer for å forebygge og håndtere tilsiktede uønskede hendelser som kan skade informasjonssystemet. Hendelser som er relevante for sikkerhetsarbeidet skal registreres.

I den grad det er nødvendig for å ivareta formålet med overvåkningen skal utveksling av informasjon til, fra og i skjermingsverdige informasjonssystemer registreres, lagres og analyseres.

Overvåkning av informasjonssystemer som behandler personopplysninger skal begrenses til de metoder og det omfang som er strengt nødvendig for å ivareta formålet med overvåkningen.

Informasjon etter første og andre ledd kan lagres i inntil fem år. Lagrede personopplysninger kan kun benyttes i den utstrekning det er nødvendig for å ivareta formålet med overvåkningen.

Flere virksomheter som er tilknyttet samme informasjonssystem, kan avtale at en av virksomhetene skal forestå overvåkningen etter første og andre ledd på vegne av de øvrige virksomhetene. Den virksomheten som forestår overvåkningen plikter å sikre at kravene til informasjonssikkerhet i § 5-2 etterleves også for den informasjon den blir kjent med som følge av avtalen om felles overvåkning.

Virksomheten skal påse at autoriserte brukere av informasjonssystemer som overvåkes i henhold til denne bestemmelse, får informasjon om formålet med behandlingen, om de tiltak som er iverksatt, herunder metode og omfang, om informasjonen blir utlevert og eventuelt om hvem som er mottaker.

Kongen kan i forskrift gi nærmere bestemmelser om overvåkning av skjermingsverdige informasjonssystemer, herunder

a) hvilke typer informasjon som kan eller skal registreres, lagres og analyseres i forbindelse med eller som resultat av overvåkningen
b) hvem som skal ha tilgang til informasjon som er registrert og lagret i forbindelse med eller som resultat av overvåkningen
c) hvordan tilgang til registrert eller lagret informasjon skal gis
d) unntak fra lagringstid på fem år, jf. fjerde ledd.

§ 6-5 *Kommunikasjons- og innholdskontroll av informasjonssystemer*

Ledelsen i virksomheten kan anmode Sikkerhetsmyndigheten om å kontrollere om virksomhetens informasjonssystemer kun behandler slik informasjon som sikkerhetsgodkjenningen tillater. Virksomhetens ansatte skal orienteres om at slike kontroller kan forekomme.

Kontrollen kan gjennomføres ved å avlytte og avlese informasjon som behandles i eller kommuniseres mellom informasjonssystemer.

Iverksettelse av kontrollen kan ikke skje før virksomhetens ledelse har godtatt metodene som tenkes benyttet og Sikkerhetsmyndighetens vurdering av faren for at kontrollen kan fange opp kommunikasjon som nevnt i fjerde ledd.

Kontrollen skal ikke omfatte privat kommunikasjon eller kommunikasjon med virksomheter som ikke er omfattet av loven. Avdekker kontrollen at slik kommunikasjon likevel fanges opp skal kontrollen straks opphøre og informasjon som kontrollen har gitt tilgang til slettes.

Det er forbudt for tjenestepersoner som får tilgang til informasjon som nevnt i fjerde ledd, å bringe informasjonen videre til andre tjenestepersoner. For øvrig gjelder taushetsplikt etter § 5-3.

Når informasjon som er samlet inn i samsvar med første ledd ikke lenger har betydning for det angitte kontrollformålet, skal Sikkerhetsmyndigheten straks slette informasjonen.

Kongen kan i forskrift gi nærmere bestemmelser om kommunikasjons- og innholdskontroll av informasjonssystemer.

§ 6-6 *Inntrengningstesting av skjermingsverdige informasjonssystemer*

Ledelsen i virksomheten kan anmode Sikkerhetsmyndigheten om å forsøke å trenge inn i virksomhetens skjermingsverdige informasjonssystemer. Formålet kan bare være å kontrollere om motstandskraften til etablerte sikkerhetstiltak er tilfredsstillende, i den hensikt å forbedre sikkerheten.

Virksomhetens ansatte skal orienteres om at slike kontroller kan forekomme.

Dersom kontrollen innebærer behandling av personopplysninger skal den begrenses til de metoder og det omfang som er strengt nødvendig for å ivareta formålet med kontrollen.

Informasjon som kontrollen gir tilgang til kan kun benyttes til å ivareta formålet med kontrollen. Når det ikke lenger er behov for informasjonen skal den slettes.

Dersom Sikkerhetsmyndigheten klarer å trenge inn i informasjonssystemet, skal fremgangsmåte og resultat dokumenteres, og operasjonen avsluttes.

Sikkerhetsmyndigheten skal gi rapport om resultatet av kontrollen til virksomheten. Rapporten skal kun inneholde informasjon som er av betydning for forbedring av virksomhetens sikkerhet.

Kongen kan gi nærmere forskrifter om inntrengning i skjermingsverdige informasjonssystemer, herunder gjennomføring av inntrengningstesting av andre enn Sikkerhetsmyndigheten.

Kapittel 7. Objekt- og infrastruktursikkerhet

§ 7-1 *Skjermingsverdige objekter og infrastruktur*

Hver enkelt departement skal innen sitt myndighetsområde utpeke, klassifisere og holde oversikt over objekter og infrastruktur av kritisk betydning for grunnleggende nasjonale funksjoner, hensyn tatt til redundansforhold til objekter og systemer.

Sikkerhetsmyndigheten skal utpeke, klassifisere og holde oversikt over objekter og infrastruktur som ikke ligger innenfor et departements myndighetsområde.

Virksomheter som råder over objekter eller infrastruktur som utpekes etter første eller andre ledd, skal varsles om dette. ~~Avgjørelse om utpeking som berører selvstendige rettssubjekter kan påklages til Tvisteorganet etter reglene i forvaltningsloven kapittel VI.~~

~~Sikkerhetsmyndigheten kan på eget initiativ foreslå utpeking av objekter og infrastruktur overfor ansvarlig departement. Dersom Sikkerhetsmyndigheten finner at et departements unnlatelse av å utpeke objekter eller infrastruktur er uforsvarlig, kan departementets avgjørelse bringes inn for Tvisteorganet for endelig avgjørelse.~~

Kongen kan gi forskrift om identifisering og utpeking av objekter og infrastruktur.

§ 7-2 *Klassifisering*

Skjermingsverdige objekter og infrastruktur skal klassifiseres i en av følgende klassifiseringsgrader:

a) MEGET KRITISK nyttes dersom det kan få helt avgjørende skadefølger for grunnleggende nasjonale funksjoner, jf. § 1-2, om objektet eller infrastrukturen får redusert funksjonalitet
b) KRITISK nyttes dersom det kan få alvorlige skadefølger for grunnleggende nasjonale funksjoner, jf. § 1-2, om objektet eller infrastrukturen får redusert funksjonalitet
c) VIKTIG nyttes dersom det kan få skadefølger for grunnleggende nasjonale funksjoner, jf. § 1-2, om objektet eller infrastrukturen får redusert funksjonalitet.

Klassifiseringen skal skje på grunnlag av virksomhetens risiko- og sårbarhetsanalyse, jf. § 4-3, og skal begrunnes ut ifra hvilke konsekvens redusert funksjonalitet objektet eller infrastrukturen har for grunnleggende nasjonale funksjoner ~~objektet eller infrastrukturen understøtter og konsekvensene av redusert funksjonalitet~~. Begrunnelsen skal inngå i departementenes og Sikkerhetsmyndighetens oversikt over skjermingsverdige objekter og infrastruktur.

Dersom en del av et objekt eller infrastruktur har en høyere klassifisering enn objektet eller infrastrukturen for øvrig, skal denne 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 sikkerhets – og beredskapstiltak for å opprettholde et forsvarlig sikkerhetsnivå.

Ved vurderingen av hva som er nødvendig skal virksomheten ta hensyn til klassifiseringsnivået på objektet eller infrastrukturen, og konsekvensen ved bortfall eller reduksjon av funksjonalitet. Sikkerhets – og beredskapstiltakene skal ses i sammenheng og tilpasses det enkelte objekts, eller den enkelte infrastrukturs, konkrete beskyttelsesbehov.

Ansvarlig departement kan treffe enkeltvedtak om krav til adgangsklarering etter loven kapittel 8, for tilgang til hele eller deler av skjermingsverdige objekter eller infrastruktur, innen sitt myndighetsområde. Sikkerhetsmyndigheten kan treffe slike vedtak overfor virksomheter som ikke ligger innenfor et departements myndighetsområde.

~~Avgjørelse om adgangsklarering etter tredje ledd som berører selvstendige rettssubjekter, kan påklages til Tvisteorganet etter reglene i forvaltningsloven kapittel VI.~~

Kongen kan gi forskrift om beskyttelse av objekter og infrastruktur innenfor hvert klassifiseringsnivå.

§ 7-4 *Testing av sikkerhetssystemer*

Ledelsen i virksomheten kan anmode Sikkerhetsmyndigheten om å forsøke å forsere etablerte sikkerhetstiltak for tilgang til skjermingsverdige objekter eller infrastruktur. Formålet kan bare være å forbedre sikkerhetsnivået gjennom å kontrollere motstandskraften til sikkerhetstiltakene. Virksomhetens ansatte skal orienteres om at slike kontroller kan forekomme.

Dersom kontrollen innebærer behandling av personopplysninger skal den begrenses til de metoder og det omfang som er strengt nødvendig for å ivareta formålet med kontrollen.

Informasjon som kontrollen gir tilgang til kan kun benyttes til å ivareta formålet med kontrollen. Når det ikke lenger er behov for informasjonen skal den slettes.

Dersom Sikkerhetsmyndigheten klarer å forsere sikkerhetstiltakene for tilgang til objekt eller infrastruktur, skal operasjonen avsluttes.

Kongen kan gi forskrift om testing av sikkerhetssystemer for skjermingsverdige objekter og infrastruktur, herunder gjennomføring av slik testing av andre enn Sikkerhetsmyndigheten.

§ 7-5 *Adgang til steder og områder*

Kongen kan av hensyn til forsvars-, sikkerhets og beredskapsmessige forhold, jf. § 1-2 første ledd bokstav b, forby uvedkommende adgang til bestemt angitte områder og å overvære militære øvelser eller forsøk.

Kapittel 8. Personellsikkerhet

§ 8-1 *Når klarering og autorisasjon skal gjennomføres*

Person som skal gis tilgang til sikkerhetsgradert informasjon, skal ha autorisasjon i samsvar med § 8-2. Det samme gjelder person som skal ha adgang til klassifiserte områder innen objekter eller infrastruktur som er av kritisk betydning for grunnleggende nasjonale funksjoner, og det er truffet vedtak

etter § 7-3 tredje ledd.

Person som skal autoriseres for tilgang til informasjon gradert KONFIDENSIELT eller høyere, skal på forhånd sikkerhetsklareres, jf. § 8-5. Sikkerhetsklarering må foreligge før autorisasjon kan gis. Person som har gyldig sikkerhetsklarering skal også anses adgangsklarert.

Person som gjennom sitt arbeid vil kunne få tilgang til sikkerhetsgradert informasjon gradert KONFIDENSIELT eller høyere, skal sikkerhetsklareres. Dette gjelder likevel ikke dersom risikoen for slik tilgang kan fjernes ved å iverksette sikkerhetstiltak.

Sikkerhetsklarering gis for følgende nasjonale sikkerhetsgrader, eventuelt også for tilsvarende sikkerhetsgrader i NATO eller annen internasjonal organisasjon:

a) STRENGT HEMMELIG (eventuelt COSMIC TOP SECRET/tilsvarende)
b) HEMMELIG (eventuelt NATO SECRET/ tilsvarende)
c) KONFIDENSIELT (eventuelt NATO CONFIDENTIAL/tilsvarende).

§ 8-2 *Sikkerhetsautorisasjon*

Virksomhetens leder er ansvarlig for autorisasjon.

Autorisasjonsansvarlig har ansvaret for den daglige sikkerhetsmessige ledelse og kontroll av autorisert personell i egen virksomhet.

Autorisasjon kan gis dersom autorisasjonsansvarlig etter en konkret helhetsvurdering ikke har opplysninger som gjør det tvilsomt om vedkommende sikkerhetsmessig er til å stole på. Autorisasjon skal ikke gis før det foreligger melding om klarering, der dette er påkrevd etter § 8-1 andre ledd. Autorisasjonssamtale skal i alle tilfeller avholdes før autorisasjon gis.

Virksomheten skal løpende orientere Sikkerhetsmyndigheten om hvilke personer som er autorisert.

Kongen kan gi forskrift om autorisasjon og autorisasjonsansvarliges plikter etter loven.

§ 8-3 *Nedsettelse, suspensjon og tilbakekallelse av autorisasjon*

Får autorisasjonsansvarlig opplysninger som gir grunn til tvil om en autorisert person fortsatt kan anses sikkerhetsmessig skikket, skal autorisasjonen vurderes tilbakekalt, nedsatt eller suspendert. Avgjørelse om dette skal innberettes til vedkommende klareringsmyndighet.

Autorisasjon bortfaller automatisk når

a) personen fratrer den stilling som autorisasjonen er knyttet til
b) behovet for autorisasjon ikke lenger er til stede
c) personen ikke lenger har tilstrekkelig klarering.

§ 8-4 *Klareringsmyndigheter etter loven*

Kongen utpeker én klareringsmyndighet for forsvarssektoren og én for sivile sektorer. Klareringsmyndighetene avgjør om det er grunn til å anta at en person er sikkerhetsmessig skikket til å håndtere sikkerhetsgradert informasjon opp til et gitt sikkerhetsnivå eller for adgang til klassifiserte områder innen objekter eller infrastruktur som er av kritisk betydning for grunnleggende nasjonale funksjoner. Etterretnings- og sikkerhetstjenestene klarerer eget personell.

Når særlige grunner taler for det kan Kongen utpeke andre klareringsmyndigheter enn de som er nevnt i første ledd.

§ 8-5 *Sikkerhets- og adgangsklarering*

Klarering skal bare gis eller opprettholdes dersom det ikke foreligger rimelig tvil om vedkommendes sikkerhetsmessige skikkethet. Som grunnlag for vurderingen av en persons sikkerhetsmessige skikkethet skal det gjennomføres en personkontroll, jf. § 8-7.

Klareringsavgjørelser skal baseres på en konkret og individuell helhetsvurdering av de foreliggende opplysninger. Klareringsmyndigheten skal påse at klareringssaken er så godt opplyst som mulig før avgjørelse fattes. Sikkerhetssamtale skal gjennomføres der dette ikke anses som åpenbart unødvendig.

I vurderingen skal det bare legges vekt på forhold som er relevante for vedkommendes pålitelighet, lojalitet og sunne dømmekraft med hensyn til behandling av gradert informasjon, og tilgang til skjermingsverdige objekter og infrastruktur. Politisk engasjement og annet lovlig samfunnsengasjement, herunder medlemskap i, sympati med eller aktivitet for lovlige politiske partier eller organisasjoner, skal ikke ha betydning for vurderingen av en persons sikkerhetsmessige skikkethet.

Negative opplysninger om nærstående personer, jf. § 8-7 tredje ledd, skal bare tas i betraktning dersom det antas at nærståendes forhold vil kunne påvirke vedkommendes sikkerhetsmessige skikkethet.

Kongen kan gi forskrift om hvilke forhold som kan tillegges betydning for vurderingen av sikkerhetsmessig skikkethet.

§ 8-6 *Nedsettelse, suspensjon og tilbakekallelse av klarering*

Får klareringsmyndigheten opplysninger som gir grunn til tvil om en sikkerhetsklarert persons sikkerhetsmessige skikkethet, skal klareringsmyndigheten vurdere å tilbakekalle eller nedsette klareringen, eller suspendere klareringen og iverksette nærmere undersøkelser for å avklare forholdet.

Er en sikkerhets- eller adgangsklarering besluttet tilbakekalt, nedsatt eller suspendert, skal begrunnet melding om dette sendes til Sikkerhetsmyndigheten. Autorisasjonsansvarlig skal varsles umiddelbart.

§ 8-7 *Gjennomføring av personkontroll*

Personkontroll skal gjennomføres som grunnlag for sikkerhets- eller adgangsklarering. Med mindre annet er bestemt av Sikkerhetsmyndigheten, skal personkontroll iverksettes etter anmodning fra autorisasjonsansvarlig. Før personkontroll igangsettes skal den som klareres motta informasjon om at slik kontroll vil bli foretatt, og skal ha akseptert dette. Aksepten skal også omfatte muligheten for personkontroll av nærstående personer etter tredje ledd, og fornyet kontroll etter § 8-8.

Personkontroll skal alltid omfatte opplysninger gitt av vedkommende selv. Vedkommende plikter å gi fullstendige opplysninger om forhold som den antar vil kunne være av betydning for vurderingen av sikkerhetsmessig skikkethet etter § 8-5.

Ved sikkerhetsklarering for HEMMELIG/tilsvarende eller høyere sikkerhetsgrader, og i andre særlige tilfeller, kan det gjennomføres personkontroll av nærstående personer.

I tillegg til opplysninger som personen gir, skal kontrollen omfatte opplysninger som vedkommende klareringsmyndighet selv har, samt opplysninger fra offentlige registre, jf. Åttende ledd. Behandlingsansvarlig plikter å utlevere registeropplysninger uten hinder av taushetsplikt. Registeropplysninger skal meddeles skriftlig. Kontrollen kan også omfatte andre kilder, herunder uttalelser fra tjenestesteder eller arbeidsplasser, offentlige myndigheter eller oppgitte eller supplerende referanser. Opplysninger som gis i forbindelse med personkontroll skal gis vederlagsfritt til klareringsmyndigheten.

Behandlingsansvarlige for relevante registre plikter å legge til rette for digitalisert overføring av personkontrollopplysningene til Sikkerhetsmyndigheten.

Opplysninger som er gitt klareringsmyndigheten i forbindelse med personkontroll, skal ikke benyttes til andre formål enn vurdering av klarering. Autorisasjonsansvarlig kan likevel meddeles opplysninger dersom dette anses påkrevet av hensyn til den sikkerhetsmessige ledelse og kontroll av vedkommende.

Personkontroll etter denne bestemmelsen skal for øvrig skje i samsvar med § 4-7.

Kongen gir forskrift om hvilke registre som er relevante for personkontroll for henholdsvis sikkerhetsklarering og adgangsklarering, samt fastsetter nærmere bestemmelser for digitalisert overføring av personkontrollopplysninger.

Kongen kan gi forskrift om fremgangsmåten ved registerundersøkelser i utlandet og om utlevering av opplysninger i forbindelse med andre lands myndigheters tilsvarende personkontroll. Under ingen omstendighet skal det innhentes, registreres eller videreformidles opplysninger om politisk engasjement som omfattes av § 8-5 andre ledd.

§ 8-8 *Fornyet personkontroll*

Klareringsmyndigheten kan be Sikkerhetsmyndigheten om å iverksette ny personkontroll, jf. § 8-7, av klarert personell når som helst innenfor en klarerings gyldighetstid, i den hensikt å kontrollere om det har skjedd endringer av betydning for vedkommendes sikkerhetsmessige skikkethet.

§ 8-9 *Bruk av vilkår og stillingsklarering*

En klarering kan i særlige tilfeller gis på nærmere angitte vilkår, og kan herunder være avgrenset til å kun gjelde en konkret stilling. Ved vurderingen av om det skal settes vilkår for klareringen, skal det særlig tas stilling til om andre tiltak vil kunne ha tilsvarende risikoreduserende effekt.

Kongen kan gi forskrift om bruk av vilkår og stillingsklarering.

§ 8-10 *Klarering av personer som ikke er norske statsborgere*

En person som ikke er norsk statsborger kan etter en konkret helhetsvurdering gis klarering. Klarering skal bare gis eller opprettholdes dersom det ikke foreligger rimelig tvil om vedkommendes sikkerhetsmessige skikkethet. I vurderingen skal det legges vekt på hjemlandets sikkerhetsmessige betydning og vedkommendes tilknytning til hjemlandet, samt vedkommendes eventuelle tilknytning til Norge. Ved klarering av personer som ikke er norske statsborgere skal det vurderes særskilt om bruk av vilkår eller stillingsklarering kan være risikoreduserende tiltak, jf. § 8-9.

Kongen kan gi forskrift om klarering av personer som ikke er norske statsborgere.

§ 8-11 *Varslingsplikt*

Klarert og autorisert person skal umiddelbart varsle autorisasjonsansvarlig om forhold som antas å kunne være av betydning for vedkommendes sikkerhetsmessige skikkethet.

Autorisasjonsansvarlig skal orientere vedkommende klareringsmyndighet dersom forholdet antas å kunne få betydning for vedkommendes klarering.

§ 8-12 *Informasjonstilgang for Politiets sikkerhetstjeneste*

I klareringssaker hvor personen eller nærstående har tilknytning til andre stater, kan Sikkerhetsmyndigheten på anmodning fra Politiets sikkerhetstjeneste gi informasjon om aktuelle personers

a) klareringsstatus
b) tilknytning til andre stater
c) tjenestested.

Utlevering av informasjon etter første ledd kan kun skje der 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 informasjonstilgang

§ 8-13 *Begrunnelse og underretning*

Forvaltningsloven kapittel IV og V gjelder ikke for avgjørelser om klarering eller autorisasjon.

Den som har vært vurdert klarert, har rett til å bli gjort kjent med resultatet. Ved negativ avgjørelse skal vedkommende uoppfordret underrettes om resultatet og opplyses om klageadgangen.

Begrunnelse for en avgjørelse skal gis samtidig med underretningen om utfallet av klareringssaken. Vedkommende har ikke krav på begrunnelse dersom den ikke kan gis uten å røpe opplysninger som

a) er av betydning for grunnleggende nasjonale funksjoner, jf. § 5-1
b) er av betydning for kildevern
c) det av hensyn til vedkommendes helse eller dennes forhold til personer som står denne nær, må anses utilrådelig at vedkommende får kjennskap til
d) 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 i tillegg utarbeide en intern samtidig begrunnelse hvor alle relevante forhold inngår, herunder forhold som nevnt i tredje ledd.

§ 8-14 *Innsyn*

Etter at avgjørelse om klarering er fattet, har den som har vært vurdert klarert rett til å gjøre seg kjent med sakens dokumenter.

Vedkommende har ikke krav på innsyn i de deler av et dokument som inneholder opplysninger som nevnt i § 8-13 tredje ledd. Vedkommende har heller ikke krav på innsyn i et dokument som er utarbeidet for den interne saksforberedelsen ved klareringsmyndigheten eller klageinstansen, med unntak av faktiske opplysninger eller sammendrag eller annen bearbeidelse av faktum.

Den som har krav på innsyn skal på anmodning gis kopi av dokumentet.

§ 8-15 *Oversendelse av sak til særskilt oppnevnt advokat*

Departementet oppnevner en gruppe advokater som skal sikkerhetsklareres for høyeste nivå, og som skal gi råd i samsvar denne bestemmelsen.

Dersom begrunnelse ikke gis, jf. § 8-13 tredje ledd, eller avslag er gitt på begjæring om innsyn, jf. § 8-14 andre ledd første punktum, og den som har vært gjenstand for vurdering begjærer det, skal klareringsmyndigheten gjøre sakens dokumenter tilgjengelig for en advokat som nevnt i første ledd. Før retten til advokat inntrer må vedkommende ha benyttet retten til klage på nektet begrunnelse eller avslag på begjæring om innsyn, jf. § 8-16. Advokaten gir råd til personen som er vurdert klarert om hvorvidt personen bør klage.

Advokaten skal ha tilgang til faktiske opplysninger og begrunnelser i saken, herunder begrunnelser som er ukjente for den som har vært vurdert klarert. Dokument som er utarbeidet for den interne saksforberedelsen ved klareringsmyndigheten eller klageinstansen, jf. § 8-14 andre ledd siste punktum, skal ikke gis advokaten.

§ 8-16 *Klage*

Forvaltningsloven kapittel VI gjelder tilsvarende i klareringssaker om ikke annet følger av denne lov eller forskrift om personellsikkerhet.

Negativ avgjørelse om klarering, herunder om vilkår og om når klareringssaken tidligst kan tas opp på nytt, kan påklages av den avgjørelsen retter seg mot. Det samme gjelder nektet begrunnelse og avslag på begjæring om innsyn.

Klagen sendes vedkommende klareringsmyndighet. Sikkerhetsmyndigheten er klageinstans. Departementet er klageinstans for klareringsavgjørelser truffet av Sikkerhetsmyndigheten i første instans.

Fristen for å klage er tre uker fra den dag underretningen om avgjørelsen, nektet begrunnelse eller avslag på begjæring om innsyn har kommet frem til vedkommende. Dersom det klages på nektet begrunnelse eller avslag på begjæring om innsyn, avbrytes klagefristen. Ny klagefrist løper fra det tidspunkt underretning om begrunnelse eller innsyn er kommet frem eller vedkommende på annen måte er gjort kjent med den. I saker der advokat har gjennomgått saken etter § 8-15, løper ny klagefrist fra den dag rådet fra advokaten har kommet frem til vedkommende.

§ 8-17 *Utfyllende bestemmelser*

Kongen kan gi forskrift om opprettelse av et sentralt register for klareringsavgjørelser. Kongen kan gi forskrift om personellsikkerhet, herunder om

a) klarering av bestemte kategorier personell, bl.a. vernepliktige mannskaper i Forsvaret
b) arkivering, oppbevaring og forsendelse av dokumenter i klarerings- og personkontrollsaker
c) avholdelse av sikkerhetssamtaler.

Kapittel 9. Sikkerhetsgraderte anskaffelser mv.

§ 9-1 *Sikkerhetsgradert anskaffelse*

Med sikkerhetsgradert anskaffelse menes en anskaffelse som innebærer at leverandøren av varen eller tjenesten vil kunne få tilgang til sikkerhetsgradert informasjon, jf. § 5-1, eller til et skjermingsverdig objekt eller infrastruktur, jf. § 7-1.

§ 9-2 *Inngåelse av sikkerhetsavtale*

Ved sikkerhetsgraderte anskaffelser skal det inngås en sikkerhetsavtale mellom anskaffelsesmyndigheten og leverandøren. Sikkerhetsavtale skal være inngått før leverandøren kan få tilgang til gradert informasjon eller et skjermingsverdig objekt eller infrastruktur. Sikkerhetsavtale med utenlandske leverandører kan bare inngås etter godkjenning av Sikkerhetsmyndigheten.

Sikkerhetsavtalen skal fastsette nærmere regler om ansvar og plikter etter bestemmelsene i og i medhold av loven her, herunder om

a) anskaffelsens sikkerhetsgrad, jf. §§ 5-1 og 7-2, spesifisert for de enkelte deler av oppdraget
b) undersøkelser hos leverandøren og annen kontroll med denne for å vurdere sikkerhetstilstanden og om leverandøren overholder sikkerhetsbestemmelsene og øvrige plikter etter loven
c) konsekvenser ved brudd på sikkerhetsavtalen.

Utgifter eller krav leverandøren måtte ha for å oppfylle bestemmelsene i eller i medhold av loven her og inngått sikkerhetsavtale, er anskaffelsesmyndigheten og Sikkerhetsmyndigheten uvedkommende, med mindre annet er uttrykkelig avtalt i sikkerhetsavtalen.

§ 9-3 *Leverandørklarering*

Før en leverandør kan få tilgang til sikkerhetsgradert informasjon gradert KONFIDENSIELT eller høyere, eller dersom det av andre grunner anses nødvendig, skal leverandøren ha gyldig leverandørklarering for angitt sikkerhetsgrad. Kongen gir forskrift om gyldighetstiden for leverandørklareringer. Sikkerhetsmyndigheten er klareringsmyndighet.

Leverandørklarering skal bare gis dersom det ikke foreligger rimelig tvil om leverandørens sikkerhetsmessige skikkethet. I vurderingen skal det bare legges vekt på forhold som er relevante for

leverandørens evne og vilje til å utøve forebyggende sikkerhetstjeneste etter bestemmelsene i eller i medhold av loven. I vurderingen skal inngå personkontroll av personer i leverandørens styre og ledelse.

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

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

For øvrig gjelder reglene i kapittel 8, herunder reglene om begrunnelse og klage, så langt de passer.

§ 9-4 *Varslingsplikt og myndighet til å fatte vedtak ved anskaffelser til skjermingsverdig objekt og infrastruktur*

Ved anskaffelser til skjermingsverdig objekt eller infrastruktur skal virksomheten foreta en risikovurdering. Det skal tas stilling til om anskaffelsen medfører en ikke ubetydelig risiko for at tilsiktede uønskede hendelser kan inntreffe mot eller ved bruk av objektet eller infrastrukturen. Plikten til å foreta en risikovurdering gjelder ikke dersom det framstår som åpenbart at anskaffelsen ikke kan innebære slik risiko.

Virksomheten skal varsle ansvarlig departement dersom risikovurderingen konkluderer med 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 risikoreduserende tiltak som fjerner risikoen eller gjør den ubetydelig.

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

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

Kongen i statsråd kan gi forskrift om varslingsplikt og myndighet til å fatte vedtak.

§ 9-5 *Utfyllende bestemmelser mv.*

Kongen kan gi forskrift om sikkerhetsgraderte anskaffelser, samt fastsette særskilte regler for gjennomføring av internasjonale sikkerhetsgraderte anskaffelser.

Kapittel 10. Eierskapskontroll

§ 10-1 *Eierskapskontroll*

Utenlandske rettssubjekter som ønsker å erverve eierandel i en virksomhet som er av kritisk betydning for grunnleggende nasjonale funksjoner som nevnt i § 1-2, skal sende melding til ansvarlig departement om dette. For virksomheter som ikke ligger innenfor et departements myndighetsområde,

skal melding sendes til Sikkerhetsmyndigheten. Meldeplikten gjelder når ervervet direkte eller indirekte samlet gjør 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 når dette må anses som reelt aksjeeie eller andelseie
c) betydelig innflytelse over forvaltningen av selskapet på annen måte.

Likt med aksjeeierens egne aksjer regnes de aksjer som eies eller overtas av aksjeeierens nærstående, jf. verdipapirhandelloven § 2-5. Det samme gjelder for andeler som eies eller overtas av andelseierens nærstående.

Et departement som mottar melding etter første ledd, bør innhente en rådgivende uttalelse fra relevante organer om ervervets risikopotensiale og erververens sikkerhetsmessige pålitelighet.

Dersom et erverv som nevnt i første ledd kan medføre en ikke ubetydelig risiko for skade på grunnleggende nasjonale funksjoner, kan Kongen i statsråd fatte enkeltvedtak om at ervervet nektes gjennomført, eller om at det 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 underrette erververen om dette. Vedtak etter første punktum er særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Kongen kan gi forskrift om erverv av virksomheter omfattet av loven.

Kapittel 11. Kontroll- og tilsynsordninger. Tvangsmulkt, overtredelsesgebyr og straff

§ 11-1 *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 EOS-kontrolloven.

Kongen kan i tillegg etablere særskilte ordninger for å kontrollere og føre tilsyn med Sikkerhetsmyndigheten og andre virksomheters arbeid med forebyggende sikkerhet, i den hensikt å påse at utøvelsen holdes innen rammen av gjeldende lov, administrative eller militære direktiver og ulovfestet rett, eller for å sørge for at rettssikkerhetsmessige og andre hensyn ivaretas.

§ 11-2 *Tvangsmulkt*

Ved overtredelse av bestemmelser gitt i eller i medhold av denne loven, kan tilsynsmyndigheten fastsettes en tvangsmulkt som løper inntil forholdet er brakt i orden. Det samme gjelder for pålegg gitt i medhold av § 3-6.

Vedtak etter første ledd er særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Kongen kan gi forskrift om tvangsmulkt etter loven.

§ 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, 4-1, 4-4, 4-6, 5-2, 6-2, 6-3, 7-3, 9-2 første ledd, 9-4 første ledd første og andre punktum eller 9-4 andre ledd første eller andre punktum
b) overtrer pålegg gitt med hjemmel i § 3-6
c) gir uriktige eller ufullstendige opplysninger til tilsynsmyndigheten
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. Vedtak om overtredelsesgebyr er 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.

Kongen kan gi forskrift om overtredelsesgebyr.

§ 11-4 *Straff*

Den som forsettlig eller uaktsomt overtrer bestemmelser gitt i eller i medhold av §§ 3-4, 4-1, 5-1 første ledd, 5-2, 6-2, 6-3, 7-3, 9-2 første ledd, 9-4 første ledd første og andre punktum eller 9-4 andre ledd første eller andre punktum, eller overtrer pålegg gitt av tilsynsmyndigheten i medhold av § 3-6, straffes med bot eller fengsel inntil 6 måneder, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Den som forsettlig eller grovt uaktsomt krenker taushetsplikt etter § 5-3 andre ledd, straffes med bot eller fengsel inntil 1 år, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Den som overtrer forbud med hjemmel i § 7-5 straffes med bot eller fengsel inntil 1 år, 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 den tid Kongen bestemmer.

§ 12-2 *Opphevelse av lov*

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

Kostnadseksempel ved oppklassifisering av anlegg i kraftforsyningen

For å anskueliggjøre potensielle kostnadskonsekvenser er det søkt, basert på erfaringer, å eksemplifisere kostnader forbundet ved å oppklassifisere anlegg til et høyere nivå, referert til NVEs klassifiseringskrav til ulike anlegg, ref. Beredskapsforskriften, i tabellene 1 – 3 nedenfor. Som det fremgår av kostnadsoversikten kan endringer i klassifiseringsgrad medføre betydelig kostnadsøkninger. Dette er kostnader som i tilfelle må dekkes av nettkundene eller som redusert avkastning til produksjons- og netteierne (primært Staten, fylker og kommuner).

Antall anlegg	**Kl. 1**	**Kl. 2**	**Kl. 3**	**Sum anlegg**
Kraftverk	150	70	25	245
Driftssentraler	70	26	20	116
Koplingsstasjoner/Transformatorstasjoner	560	330	110	1000

Tabell 1 - Antall anlegg med ulik klassifisering

Som det fremgår av tabell 1 er omlag 245 av i alt 1570 produksjonsanlegg i dag klassifisert ihht. Beredskapsforskriften.

Enhetskostnader for oppklassifisering pr. anleggstype	**Engangskostnad** [mill. kr.]		**Driftskostnad** [mill. kr./år]	
	Kl. 1-2	Kl. 2-3	Kl. 1-2	Kl. 2-3
Kraftstasjon	6	3	0,09	0,045
Driftssentral	6,5	8	4	4
Koplings-/transformatorstasjon (gj.sn.)	8	25	0,1125	0,375

Tabell 2 - Erfaringsmessige enhetskostnader ved omklassifisering

Kostnader ved oppklassifisering av anleggstyper	**Engangskostnad** [mill. kr.]		**Driftskostnad** [mill. kr./år]	
	Kl. 1-2	Kl. 2-3	Kl. 1-2	Kl. 2-3
Kraftstasjon	900	210	13,50	3
Driftssentral	455	208	280	104
Koplings-/transformatorstasjon	4 200	8 250	63	124
Sum	**5 555**	**8 668**	**357**	**231**

Tabell 3 - Potensielt kostnadsspenn ved oppklassifisering av anlegg

Som det fremgår av tabell 3 kan eksempelvis investeringskostnadene for oppklassifisering av anlegg i klasse 1 og 2 ligge i størrelsesorden 14 mrd. kr. I tillegg påløper økte årlige driftskostnader i størrelsesorden 600 mill.kr. Investeringskostnader og økte driftskostnader knyttet til eventuelle nye sikringstiltak for dagens klasse 3 anlegg vil komme i tillegg. Konsekvenser for øvrige anlegg, som i dag ikke er klassifisert, er ikke medregnet.