

Hjelp!

Vi er underlagt Sikkerhetsloven

- En enkel veileder

Hva er sikkerhetsloven?

Sikkerhetsloven er myndighetenes fremste juridiske virkemiddel for å ivareta nasjonal sikkerhet. Loven fastsetter en rekke sikkerhetskrav for virksomheter som anses som særlig viktige for Norges nasjonale sikkerhetsinteresser og dermed er underlagt loven. Lovens formål er å styrke evnen til å forebygge, avdekke og motvirke aktiviteter som truer Norges nasjonale sikkerhet.

Denne veilederen retter seg mot virksomheter som er underlagt sikkerhetsloven etter vedtak. Det innebærer at virksomheten har mottatt et vedtak om underleggelse fra departementet med ansvar for den aktuelle sektoren. Veilederen omhandler ikke forpliktelsene til leverandører av sikkerhetsgraderte anskaffelser eller offentlige organer.

Hvordan blir en virksomhet underlagt sikkerhetsloven?

Hvert departement har ansvar for å identifisere hvilke private virksomheter som skal underlegges sikkerhetsloven innenfor sin sektor, samt å fatte vedtak om underleggelse.

Det er betydelige forskjeller mellom sektorene i praktiseringen av sikkerhetsloven. Saksbehandlingen for underleggelse er imidlertid lik og følger vanlig forvaltningspraksis. Dette innebærer blant annet krav om at departementet varsler den aktuelle virksomheten på forhånd før vedtak om underleggelse. Virksomheten vil ha rett til å uttale seg på bakgrunn av et slikt forhåndsvarsel.

Hva innebærer det å være underlagt sikkerhetsloven?

En virksomhet kan enten helt eller delvis underlegges sikkerhetsloven. For de delene av virksomheten som blir underlagt må selskapet iverksette sikkerhetstiltak som angitt i loven. Målet med tiltakene skal være å oppnå og opprettholde det loven omtaler som et "forsvarlig sikkerhetsnivå". Ved en underleggelse er det sentralt at virksomheten setter seg grundig inn i vedtaket. Dette er viktig for å identifisere hvilke deler av virksomheten som er underlagt lovens krav, og for å skaffe seg oversikt over hvilke bestemmelser i loven som er relevante. Hvis vedtaket ikke er tilstrekkelig presist på disse punktene, kan det være hensiktsmessig å gå i dialog med det aktuelle departementet for å få tydeliggjort vedtaket.

Hvilke deler av sikkerhetsloven som er relevante vil i stor grad avhenge av hvilken informasjon/infrastruktur og/eller hvilke objekter virksomheten har som anses skjermingsverdige etter loven (se nærmere beskrivelse under).

Sikkerhetslovens pilarer

Sikkerhetsloven spesifiserer i utgangspunktet ikke konkrete tiltak som skal implementeres, men stiller funksjonelle krav til sikkerheten for å sikre at de underlagte virksomhetene oppnår og opprettholder et "forsvarlig sikkerhetsnivå". Pliktene som følger av loven, blir ytterligere konkretisert og operasjonalisert gjennom kravene i virksomhetssikkerhetsforskriften. Sikkerhetsloven stiller i hovedsak krav innen fem pilarer:

- Informasjon- og informasjonssystemssikkerhet
- Objekt- og infrastrukturens sikkerhet
- Personellsikkerhet
- Sikkerhet i leverandørkjeder
- Sikkerhet ved eierskapskifte

For at en virksomhet skal kunne oppfylle kravene etter sikkerhetsloven, kreves det at virksomheten oppnår et forsvarlig sikkerhetsnivå på tvers av disse fem pilarene. Loven krever dermed at virksomhetens sikkerhetsarbeid baserer seg på en helhetlig tilnærming, med utgangspunkt i risikovurderinger som identifiserer hvilke verdier virksomheten må beskytte. Virksomheten må kontinuerlig vurdere behovet for å iverksette nye tiltak basert på den gjeldende risikovurderingen. Virksomhetens sikkerhetsstyringssystem skal sørge for at virksomheten er i stand til å forebygge, avdekke og motvirke sikkerhetstruende aktiviteter. Virksomheter pålegges også en varslingsplikt under sikkerhetsloven.

Virksomheten får ingen formell bekreftelse eller sertifisering på at selskapet har oppnådd et forsvarlig sikkerhetsnivå. Det er opp til virksomheten selv, basert på jevnlig gjennomganger og grundige risikovurderinger, å vurdere om forsvarlig sikkerhetsnivå er oppnådd og opprettholdt. Slike vurderinger forutsetter god kunnskap til lovens bestemmelser, tilhørende forskrifter og andre relevante regelverk.

På neste side følger en kort introduksjon til hvilke sikkerhetstiltak som gjennomgående er relevante innenfor sikkerhetslovens fem pilarer.

Informasjon- og informasjonssystem-sikkerhet

Deler av informasjonen som tilligger virksomheter underlagt sikkerhetsloven har større verdi for nasjonal sikkerhet enn annen informasjon og skal dermed beskyttes bedre. Sikkerhetsloven omtaler dette som "skjemningsverdig informasjon". Skjemningsverdig informasjon deles videre inn i to kategorier: a) ugradert skjemningsverdig informasjon og b) sikkerhetsgradert informasjon. De strengeste kravene stilles til beskyttelse av sikkerhetsgradert informasjon. For sikkerhetsgradert informasjon stiller loven, sammen med forskriften, en rekke krav med utgangspunkt i hvilken gradering informasjonen har. Kravene knytter seg blant annet til riktig merking og oppbevaring, samt tilgangsstyring av hvem som skal ha tilgang til informasjonen.

Loven stiller også sikkerhetskrav til informasjonssystemene som behandler ugradert skjemningsverdig eller sikkerhetsgradert informasjon.

Objekt- og infrastrukturens sikkerhet

Sikkerhetsloven stiller krav til at hvert departement skal føre oversikt over skjemningsverdige objekter og infrastruktur innenfor sitt ansvarsområde. Disse skal klassifiseres i henhold til skalaen: VIKTIG, KRITISK eller MEGET KRITISK. I tillegg til å ivareta sikkerheten til objektet eller infrastrukturen gjennom tiltak innenfor de øvrige pilarene, vil kravet til forsvarlig sikkerhet forutsette at virksomheten iverksetter nødvendige tiltak knyttet til blant annet fysisk sikring og eventuelle rutiner for adgangskontroll eller lignende.

Personellsikkerhet

Medarbeidere i en virksomhet underlagt sikkerhetsloven med tjenstlig behov for tilgang til sikkerhetsgradert informasjon må være autorisert for informasjon gradert opp til BEGRENSET, og i tillegg ha gyldig sikkerhetsklarering for tilgang til informasjon på nivå KONFIDENSIELT eller høyere.

Virksomheter underlagt sikkerhetsloven vil også kunne ha medarbeidere i stillinger som ikke krever autorisering og sikkerhetsklarering, men som likevel får tilgang til kritiske deler av virksomheten. Disse stillingene bør omfattes av flere personellsikkerhetstiltak enn øvrige medarbeidere som ikke krever spesielle personellsikkerhetstiltak. Det er imidlertid opp til virksomheten selv å definere relevante personellsikkerhetstiltak for medarbeiderne i kritiske stillinger hvor det ikke er krav til sikkerhetsklarering.

Dette dokumentet er ment som en introduksjon til sikkerhetsloven og enkelte av bestemmelsene som er relevant for virksomheter som er underlagt loven. Veilederen er ikke å anse som juridisk rådgivning.

I leverandørkjeder

Underlagte virksomheter er pålagt å gjennomføre tiltak for å ivareta forsvarlig sikkerhet i sine leverandørkjeder. De mest omfattende kravene stilles til såkalte sikkerhetsgraderte anskaffelser. Dette er anskaffelser hvor leverandøren kan få tilgang til eller tilvirker sikkerhetsgradert informasjon, eller anskaffelser hvor leverandøren kan få tilgang til et skjemningsverdig objekt eller skjemningsverdig infrastruktur. Virksomheter underlagt sikkerhetsloven har ansvaret for at deres leverandører oppfyller relevante krav i sikkerhetsloven

Ved eierskapsskifte

Kjøpere av en virksomhet underlagt sikkerhetsloven er pålagt en meldeplikt dersom eierskapsskiftet involverer en "kvalifisert eierandel" i virksomheten. En "kvalifisert eierandel" defineres som eierskap til, eller rett til å bli eier av, minst en tredjedel av aksjekapitalen, andelene eller stemmerettighetene i virksomheten. Meldeplikten gjelder også dersom erververen på annen måte oppnår "betydelig innflytelse" over forvaltningen av virksomheten. Meldingen skal sendes til det overordnede departementet, alternativt til sikkerhetsmyndigheten.

Det er vedtatt endringer i reglene for eierskapsskifte som reduserer grensen for hva som regnes som en kvalifisert eierandel til ti prosent. Det innføres også meldeplikt dersom eierandelen økes til bestemte terskelverdier. I tillegg vil de nye reglene pålegge både kjøper og den berørte virksomheten meldeplikt.

Andre regelverk

Det finnes en rekke andre lovverk som regulerer sikkerhet, både på sektorspesifikt og sektorovergripende nivå. For virksomheter underlagt sikkerhetsloven, er det imidlertid viktig å være klar over at sikkerhetsloven ofte stiller strengere og mer omfattende krav til sikkerhet enn annet regelverk. Implementering av sikkerhetstiltak i henhold til andre regelverk, som for eksempel NIS-direktivene, garanterer derfor ikke at kravene i sikkerhetsloven er oppfylt.

Kommersielt fortrinn

I dagens alvorlige trusselbilde er det tydelige forventninger fra både myndigheter og aktører i sikkerhetssensitive sektorer til at norske virksomheter må prioritere sikkerhetstiltak for å kunne håndtere potensielle trusler. Sikkerhetsloven gir et solid rammeverk for hvordan virksomheter kan styrke sikkerheten på en helhetlig måte. Dette kan også benyttes av virksomheter som ikke er underlagt loven, men som ønsker å styrke eget sikkerhetsarbeid. Prioritering av sikkerhetsarbeid kan gi virksomheter et kommersielt fortrinn ved å posisjonere dem som sikkerhetsbevisste aktører som oppfyller strenge krav til egen sikkerhet.



Næringslivets
sikkerhets-
råd

THOMMESSEN