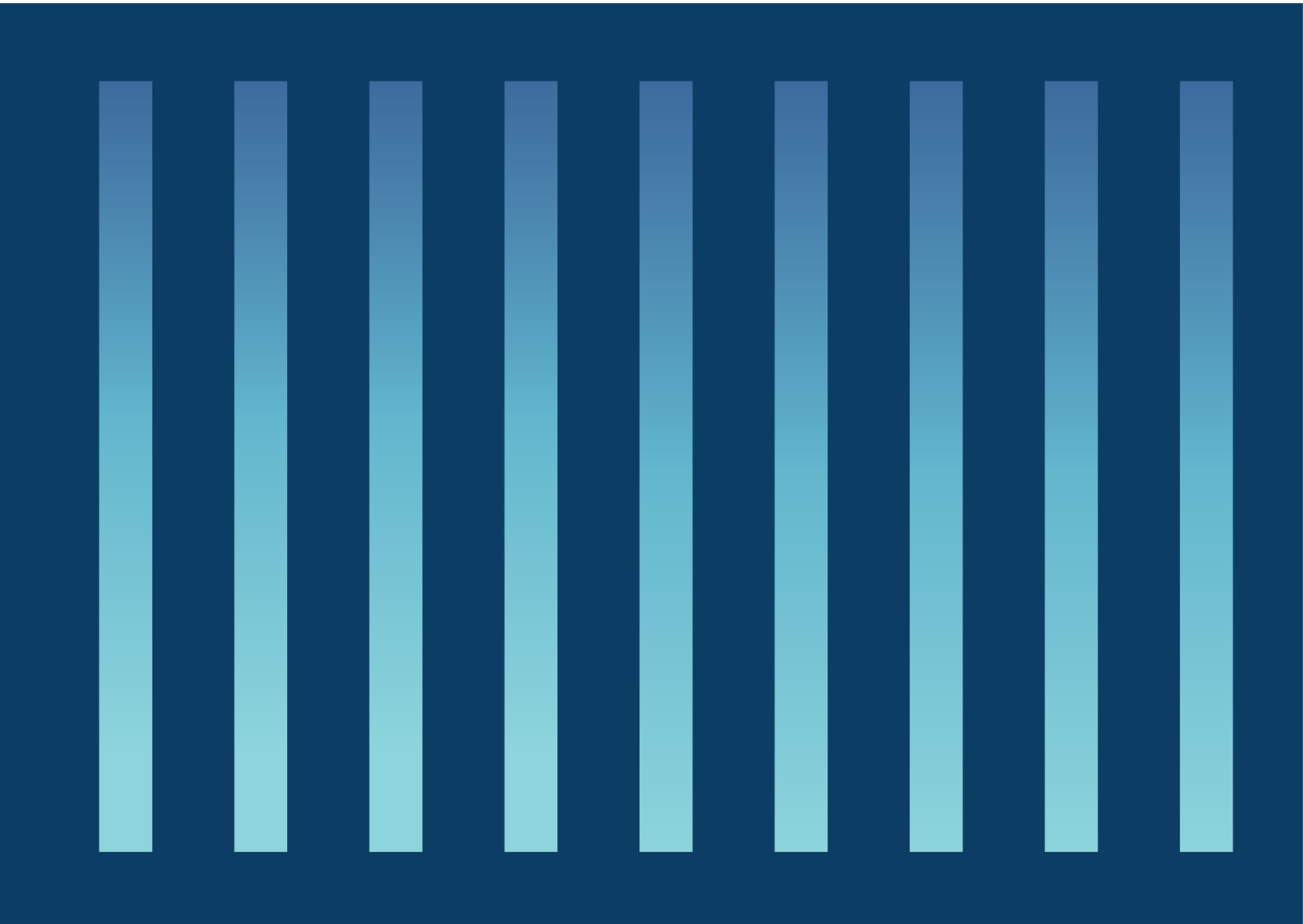
NASJONAL
SIKKERHETSMYNDIGHET

Veileder i anskaffelser etter sikkerhetsloven

Versjon: 1



Nasjonal sikkerhetsmyndighet (NSM) er fagorgan for forebyggende sikkerhet, og sikkerhetsmyndighet etter lov om nasjonal sikkerhet (sikkerhetsloven). NSM skal gi informasjon, råd og veiledning om forebyggende sikkerhetsarbeid.

Sikkerhetsloven med tilhørende forskrifter trådte i kraft 1. januar 2019. Loven skal bidra til å forebygge, avdekke og motvirke tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser.

Sikkerhetsloven gjelder for statlige, fylkeskommunale og kommunale organer og for leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser. De enkelte departementer skal innenfor sine ansvarsområder vedta at andre virksomheter underlegges loven dersom de behandler sikkerhetsgradert informasjon eller råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner, eller driver aktivitet som har avgjørende betydning for disse funksjonene.

NSMs veiledere utdyper regelverksforståelsen, herunder den tematiske sammenhengen mellom ulike bestemmelser i sikkerhetsloven og tilhørende forskrifter. Veilederne representerer NSMs syn på hvordan lov og forskrifter er å forstå, og danner et grunnlag for virksomhetenes arbeid med å etterleve regelverket.

NSM gir i tillegg ut håndbøker og tekniske råd som gir mer utfyllende anbefalinger om hvordan lovens funksjonelle krav kan oppfylles. Håndbøkene og de tekniske rådene beskriver fremgangsmåter og prosedyrer og gir eksempler på tiltak for å hjelpe virksomhetene i regelverksanvendelsen.

Veilederen anbefales lest i sammenheng med lov og forskrift, samt NSMs øvrige relevante veiledere, håndbøker og tekniske råd.

INNHOLD

1. Innledning

1.1. Innhold i veilederen

Denne veilederen omhandler bestemmelsene om anskaffelser i sikkerhetsloven kapittel 9, virksomhetssikkerhetsforskriften og klareringsforskriften. Sikkerhetsloven har bestemmelser om sikkerhetsgraderte anskaffelser og bestemmelser om sikkerhet i anskaffelser som ikke er graderte, men av andre årsaker faller inn under lovens virkeområde. I det følgende framgår krav til sikkerhetsgraderte anskaffelser av kapittel 2, mens krav til andre anskaffelser framgår av kapittel 3, og felles krav framgår av kapittel 4.

Virksomhetssikkerhetsforskriften (forskrift om virksomheters arbeid med forebyggende sikkerhet) presiserer de rammene som sikkerhetsloven setter for virksomhetenes arbeid med forebyggende sikkerhet og forsvarlig sikkerhetsnivå.

Reglene i forskriftens kapittel om sikkerhetsgraderte anskaffelser skal bidra til at sikkerhetsnivået hos leverandørene er like godt som hos oppdragsgiverne. Klareringsforskriften (forskrift om sikkerhetsklarering og annen klarering) utfyller sikkerhetslovens regler om sikkerhetsklarering av personer, adgangsklarering av personer og leverandørklarering av virksomheter. Formålet med leverandørklarering er å forebygge bruk av leverandører hvor det er rimelig tvil om deres sikkerhetsmessige skikkethet. Veilederen gir utrykk for hvordan bestemmelsene om sikkerhetsgraderte anskaffelser skal forstås. Målgruppen for veilederen er virksomheter omfattet av sikkerhetsloven § 1-2 første ledd og § 1-3 som skal gjennomføre en anskaffelse.

Nasjonal sikkerhetsmyndighet publiserer på sine nettsider skjemaer og maler som virksomhetene kan benytte når de gjennomfører en sikkerhetsgradert anskaffelse. Det vil også bli utarbeidet en håndbok på området med nærmere prosessbeskrivelse av hvordan sikkerhetsgraderte anskaffelser kan gjennomføres.

1.2. Generelt om regler for anskaffelser

Ikke alle anskaffelser etter sikkerhetsloven er offentlige anskaffelser. Både offentlige og private virksomheter har anskaffelsesbehov og inngår kontrakter med sine leverandører. De må alle håndtere og etterleve sikkerhetslovens regler, og for offentlige oppdragsgivere må det skje parallelt med etterlevelsen av reglene for offentlige anskaffelser.

Offentlige anskaffelser er innkjøp med felleskapets midler. De skal gjennomføres på en samfunnstjenlig måte og i samsvar med grunnleggende prinsipper om konkurranse, likebehandling, forutberegnelighet, etterprøvbarhet og forholdsmessighet.

Hovedreglene følger av anskaffelsesloven (LOA) og dens fire prosedyreforskrifter: anskaffelsesforskriften (FOA), forskrift om forsvars- og sikkerhetsanskaffelser (FOSA), forsyningsforskriften og konsesjonskontraktforskriften. Digitaliseringsdirektoratet har praktiske veiledere til disse på sine nettsider, mens Nærings- og fiskeridepartementet og Forsvarsdepartementet har utarbeidet juridiske veiledere. Videre har Nærings- og fiskeridepartementet sammen med Forsvarsdepartementet gitt ut en veileder om ivaretakelse av sikkerhet i offentlige anskaffelser. Denne har som mål å synliggjøre handlingsrommet i anskaffelsesregelverket, og gjennom dette vise hvordan offentlige oppdragsgivere kan ivareta norske sikkerhetsinteresser når de gjør innkjøp.

Mange forsvars- og sikkerhetsanskaffelser gjennomføres etter forskrift om forsvars- og sikkerhetsanskaffelser (FOSA), men når forsvars- eller sikkerhetsinteresser gjør det nødvendig, kan anskaffelsene unntas fra ordinære regler med hjemmel i EØS-avtalen artikkel 123. For mange forsvarsrelaterte anskaffelser gjelder en egen instruks: anskaffelsesregelverk for forsvarssektoren (ARF).

Sikkerhetsgraderte anskaffelser må ses i sammenheng med regelverket for offentlige anskaffelser. I tilfeller der sikkerhet i anskaffelsen står sentralt vil sikkerhetslovens bestemmelser ofte virke i tillegg til den aktuelle forskriften for anskaffelsesområdet. Samtidig er det viktig å være oppmerksom på at anskaffelsesloven med forskrifter og sikkerhetsloven med forskrifter har forskjellig formål og forskjellig virkeområde. For sikkerhetsgraderte anskaffelser gjelder reglene i sikkerhetsloven og dens forskrifter, virksomhetssikkerhetsforskriften og klareringsforskriften.

2. Sikkerhetsgraderte anskaffelser

2.1. Sikkerhetsgraderte anskaffelser

Sikkerhetsloven definerer en sikkerhetsgradert anskaffelse slik:

> *§ 9-1. Sikkerhetsgradert anskaffelse*
>
> *En sikkerhetsgradert anskaffelse er en anskaffelse som innebærer at leverandøren av varen eller tjenesten kan få tilgang til eller tilvirker sikkerhetsgradert informasjon, jf. § 5-3, eller få tilgang til et skjermingsverdig objekt eller infrastruktur, jf. § 7-1.*

Med *leverandører* menes i denne sammenhengen alle tilbydere, leverandører og underleverandører i en anskaffelse. Leverandørens personell identifiseres her med leverandøren. *Sikkerhetsgradert informasjon* er informasjon som kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende. *Objekter* og *infrastruktur* er skjermingsverdige dersom det kan skade grunnleggende nasjonale funksjoner om de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse.

En anskaffelse er en sikkerhetsgradert anskaffelse når leverandøren kan få tilgang til visse skjermingsverdige verdier. Men ikke alle skjermingsverdige verdier gjør at anskaffelsen blir en sikkerhetsgradert anskaffelse. Sikkerhetsloven § 9-1 viser at anskaffelsen er en sikkerhetsgradert anskaffelse når

- leverandøren kan få tilgang til sikkerhetsgradert informasjon,
- leverandøren tilvirker sikkerhetsgradert informasjon,
- leverandøren kan få tilgang til et skjermingsverdig objekt, eller
- leverandøren kan få tilgang til skjermingsverdig infrastruktur.

Skjermingsverdige informasjonssystemer er i utgangspunktet ikke med i opplistingen i § 9-1. Anskaffelser til skjermingsverdige informasjonssystemer kan imidlertid i enkelte tilfeller være sikkerhetsgraderte anskaffelser. For det første kan et skjermingsverdig informasjonssystem utpekes som skjermingsverdig objekt eller skjermingsverdig infrastruktur. For det andre kan en anskaffelse til et skjermingsverdig informasjonssystem føre til at leverandøren får tilgang til sikkerhetsgradert informasjon via informasjonssystemet.

Begrepene «sikkerhetsgradert informasjon» og «skjermingsverdig objekt eller infrastruktur» er sentrale i sikkerhetsloven, også utenfor reglene om sikkerhetsgraderte anskaffelser, og er definert nærmere i § 5-3 og § 7-1.

Sikkerhetsloven med forskrifter stiller krav som både virksomheten og leverandøren må forholde seg til i forbindelse med en anskaffelse. Reglene krever at leverandører som håndterer sikkerhetsgradert informasjon eller har tilgang til skjermingsverdig objekt eller infrastruktur, oppfyller kravene som stilles i sikkerhetsloven og forskriftene for å oppnå forsvarlig sikkerhet. Dette er viktig både for å sikre at sikkerhetsgradert informasjon blir håndtert på en forsvarlig måte og for å sikre at tilgang til skjermingsverdige objekter og infrastruktur ikke misbrukes på en måte som kan få alvorlige skadefølger.

Videre stiller sikkerhetsloven med forskrifter krav til blant annet risikovurdering og eventuelt varsling i anskaffelser der leverandøren får tilgang til skjermingsverdig ugradert informasjon/informasjonssystem samt der leverandør/personell kan få mulighet til å påvirke skjermingsverdig objekt, infrastruktur eller informasjonssystem.

Sikkerhetsloven legger føringer for hva som kan eller skal skje i hvilken rekkefølge og på hvilket stadium i anskaffelsesprosessen. Eksempelvis må partene inngå sikkerhetsavtale før oppdragsgiveren kan gjøre sikkerhetsgradert informasjon kjent for tilbyderen eller leverandøren. Når partene senest må inngå sikkerhetsavtalen avhenger av når i anskaffelsesprosessen oppdragsgiveren velger å gjøre sikkerhesgradert informasjon tilgjengelig. Hvilken leverandørklarering for virksomheten og hvilken sikkerhetsklarering for personellet som er nødvendig – eller om det overhodet er nødvendig med leverandørklarering og sikkerhetsklarering – avhenger av hvilken sikkerhetsgrad eller sikkerhetsklasse oppdragsgiveren har fastsatt for anskaffelsen. Sikkerhetskravene slår inn på ulike stadier, noen allerede før kontraktstildelingen, andre etterpå. Noen sikkerhetskrav er relevante bare i en kort, innledende periode, mens andre gjelder gjennom hele kontraktsperioden.

§ 1-2. Hvem loven gjelder for [andre ledd]

Loven gjelder for leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser etter kapittel 9.

Tilbydere, leverandører og underleverandører i sikkerhetsgraderte anskaffelser er i tråd med § 1-2 automatisk underlagt relevante bestemmelser i sikkerhetsloven med forskrifter, altså utover lovens kapittel 9, avgrenset til den sikkerhetsgraderte anskaffelsen. Dette medfører eksempelvis at leverandøren ikke på eget initiativ kan iverksette egne graderte anskaffelser.

2.2. Sikkerhetsavtale

Ved sikkerhetsgraderte anskaffelser skal det som hovedregel inngås en sikkerhetsavtale mellom oppdragsgiveren og leverandøren. Oppdragsgiver er den som skal gjennomføre en sikkerhetsgradert anskaffelse. Begrepet «oppdragsgiver» kan omfatte alle former for virksomhet som omfattes av sikkerhetsloven § 1-2 første ledd eller § 1-3. Ved vurderingen av om en virksomhet omfattes av loven er det uten betydning om det er et privat selskap, foretak, forvaltningsorgan, forvaltningsbedrift, et hel- eller deleid statlig selskap, statsforetak, ideell organisasjon, stiftelse eller annet. Oppdragsgiveren anskaffer varer eller tjenester fra en leverandør. Underleverandør er den som understøtter leveranser til (hoved)leverandøren, og kravet om sikkerhetsavtale kan gjelde også underleverandøren.

Sikkerhetsavtalen formaliserer sikkerhetsmessige aspekter i forbindelse med en sikkerhetsgradert anskaffelse, og skal legge til rette for at lokale forhold, praktisk gjennomføring og detaljer av betydning for sikkerheten kan reguleres tilfredsstillende.

Før en sikkerhetsgradert anskaffelse iverksettes, skal sikkerhetsavtale mellom oppdragsgiver og leverandør være inngått. Dette fremgår av sikkerhetsloven:

§ 9-2. Sikkerhetsavtale med leverandør

Før en sikkerhetsgradert anskaffelse iverksettes, skal virksomheten inngå en sikkerhetsavtale med leverandøren. Dersom en utenlandsk leverandør eller dennes personell må klareres eller gis tilgang til sikkerhetsgradert informasjon, skal sikkerhetsmyndigheten godkjenne leverandøren før det inngås en sikkerhetsavtale.

Sikkerhetsavtalen skal tydeliggjøre og konkretisere partenes plikter og ansvar etter loven. Sikkerhetsavtalen skal alltid inneholde hvilken sikkerhetsgrad anskaffelsen skal ha, jf. §§ 5-3 og 7-2, spesifisert for hver del av oppdraget, og hvordan leverandøren skal forholde seg til de av lovens krav som gjelder for anskaffelsen.

Leverandøren må selv dekke utgifter til å oppfylle krav som følger av lovens bestemmelser, hvis ikke noe annet følger av sikkerhetsavtalen.

Kongen kan gi forskrift om innholdet i en sikkerhetsavtale og om unntak fra kravet om sikkerhetsavtale.

Hvilken sikkerhetsgrad og hvilke krav som gjelder for den enkelte anskaffelsen vil avhenge av hva leverandøren får tilgang til ved anskaffelsen, jf. virksomhetssikkerhetsforskriften § 79. Det må i denne

sammenheng gjennomføres en vurdering av anskaffelsens sikkerhetsgrad og/eller -klasse, jf. sikkerhetsloven § 5-3 og § 7-2.

Dersom sikkerhetsgraden øker i løpet av anskaffelsen, kan det være nødvendig å revidere eller inngå ny sikkerhetsavtale samt foreta ny leverandørklarering.

Nærmere beskrivelse av sikkerhetsavtalens innhold følger av virksomhetssikkerhetsforskriften:

§ 80. Krav til sikkerhetsavtalen når en leverandør skal ha tilgang til sikkerhetsgradert informasjon, et skjermingsverdig objekt eller skjermingsverdig infrastruktur.

Dersom en leverandør skal ha tilgang til sikkerhetsgradert informasjon, et skjermingsverdig objekt eller skjermingsverdig infrastruktur i eller fra sine egne lokaler, skal det fremgå av sikkerhetsavtalen etter sikkerhetsloven § 9-2
a) hvilken sikkerhets- eller klassifiseringsgrad informasjonen, objektet eller infrastrukturen har
b) hvem som skal få tilgang til den sikkerhetsgraderte informasjonen eller det skjermingsverdige objektet eller infrastrukturen
c) hvordan den sikkerhetsgraderte informasjonen skal formidles mellom avtalepartene
d) hvilket informasjonssystem som skal brukes for å behandle den sikkerhetsgraderte informasjonen, eller for å få tilgang til det skjermingsverdige objektet eller infrastrukturen, og hvem som er ansvarlig for å godkjenne systemet
e) hvilke lokaler den sikkerhetsgraderte informasjonen skal behandles i
f) hvordan det skal varsles om sikkerhetstruende virksomhet og avvik fra sikkerhetskrav
g) om den sikkerhetsgraderte informasjonen skal leveres tilbake eller destrueres når oppdraget er avsluttet.

En sikkerhetsavtale kan tas inn i det ordinære avtaledokumentet for anskaffelsen.

Leverandøren er omfattet av sikkerhetslovens bestemmelser uavhengig av om det inngås en sikkerhetsavtale, men sikkerhetsavtalen tydeliggjør og operasjonaliserer de sikkerhetskrav som gjelder for den enkelte anskaffelse. Oppdragsgiver bør gjennom sikkerhetsavtalen skaffe seg adgang til å kontrollere at leverandøren etterlever gjeldende sikkerhetskrav for anskaffelsen. Avtalen skal tydeliggjøre og konkretisere partenes plikter og ansvar. Mislighold kan utløse sanksjoner som er hjemlet i sikkerhetsloven. Ofte framgår sanksjonene av avtalen. NSM anbefaler partene å benytte NSMs mal for sikkerhetsavtale.

Det følger av virksomhetssikkerhetsforskriften at det i særskilte tilfeller kan gjøres unntak fra krav om sikkerhetsavtale:

§ 81. Unntak fra krav om sikkerhetsavtale
Det kreves ikke sikkerhetsavtale etter sikkerhetsloven § 9-2 dersom leverandørens personell bare skal gis tilgang til sikkerhetsgradert informasjon, skjermingsverdige objekter eller skjermingsverdig infrastruktur under oppsyn av en representant for oppdragsgiveren.

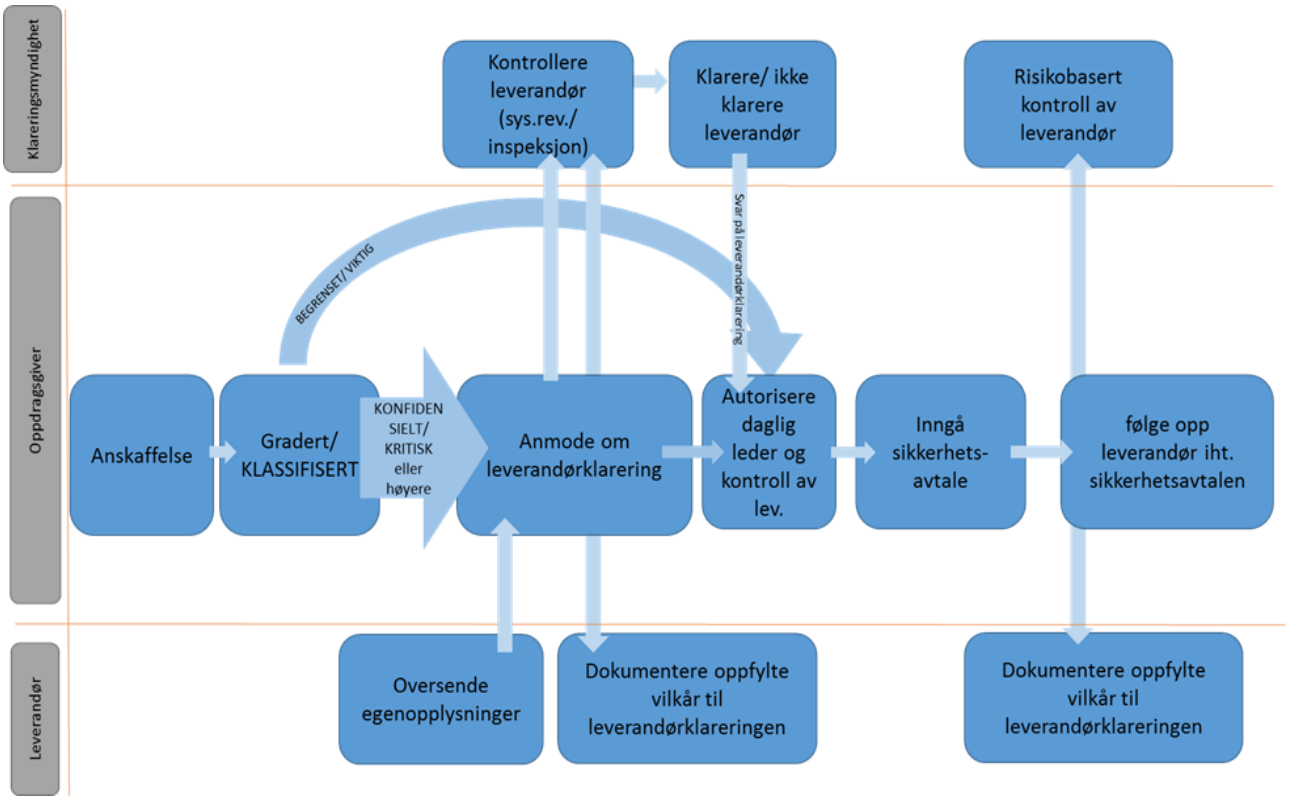
Med «oppsyn» menes at en representant for oppdragsgiveren, for eksempel en ansatt eller innleid personell, har kontroll over hvor i lokalene leverandørens personell til enhver tid oppholder seg, eller hvilke operasjoner leverandørens personell gjør i et informasjonssystem for behandling av sikkerhetsgradert informasjon.

For at oppsynet fra oppdragsgiverens representant skal gi en reell beskyttelse må representanten ha kontroll med hva leverandørens personell til enhver tid foretar seg. Dette medfører at representanten må ha tilstrekkelig kompetanse til å forstå om leverandøren vil ha mulighet til å skade objektet eller infrastrukturen, eller hente ut, endre eller slette informasjon.

Et eksempel der det ikke kreves sikkerhetsavtale kan være når leverandørens personell må ha tilgang til skjermingsverdig objekt eller infrastruktur for å utføre arbeid eller vedlikehold. Oppdragsgiver må da følge leverandørens personell og sørge for at den/disse ikke får tilgang til annet enn det som er relevant for oppdraget.

Paragrafene 80 og 81 gir ikke en uttømmende liste over mulige situasjoner og omstendigheter. Det kan derfor tenkes anskaffelser som ikke kommer inn under virksomhetssikkerhetsforskriften § 80 eller § 81, men hvor kravet om sikkerhetsavtale etter sikkerhetsloven § 9-2 likevel gjelder.

2.3. Leverandørklarering



2.3.1. Krav om leverandørklarering

Ved sikkerhetsgradert anskaffelse som medfører at leverandøren kan få tilgang til informasjon gradert KONFIDENSIELT eller høyere, eller objekt og infrastruktur klassifisert KRITISK eller høyere, skal leverandøren klareres. For nivå BEGRENSET eller VIKTIG kreves det ikke leverandørklarering med mindre dette er nødvendig for å oppnå forsvarlig sikkerhetsnivå. Oppdragsgiveren er likevel forpliktet

til å sørge for at også leverandørene på disse graderings-/klassifiseringsnivåene har tilstrekkelig risiko- og sikkerhetsforståelse, jf. sikkerhetsloven § 4-1 andre ledd.

Kravet om leverandørklarering er et eksempel på at høyere klarerings-/klassifiseringsnivå sikres med sterkere tiltak. Sikkerhetsloven § 9-3 andre ledd peker på at det ikke skal være «noen rimelig grunn til å tvile på at leverandøren er sikkerhetsmessig skikket». I dette ligger det blant annet at leverandøren skal være skikket til å bidra i, og ivareta eget ansvar i, det forebyggende sikkerhetsarbeidet.

Leverandørklarering av virksomheter etter sikkerhetsloven kan være tidkrevende og må medregnes i planleggingen av anskaffelsen.

Kravet til leverandørklarering fremgår av sikkerhetsloven:

§ 9-3. Leverandørklarering

Før en leverandør kan få tilgang til informasjon gradert KONFIDENSIELT eller høyere, skal leverandøren ha gyldig klarering for angitt sikkerhetsgrad. Leverandøren skal også klareres dersom det er nødvendig av andre grunner.

En leverandørklarering skal bare gis dersom det ikke er noen rimelig grunn til å tvile på at leverandøren er sikkerhetsmessig skikket. I vurderingen skal det bare legges vekt på forhold som kan innvirke på leverandørens evne og vilje til å gjøre forebyggende sikkerhetsarbeid etter loven. En personkontroll av personer i leverandørens styre og ledelse skal være en del av vurderingsgrunnlaget.

Leverandøren skal gi klareringsmyndigheten alle opplysninger som kan ha betydning for leverandørklareringen.

Leverandøren skal så snart som mulig orientere klareringsmyndigheten om endringer i styret eller ledelsen, endringer i eierstrukturen, flytting av lokaliteter og utstyr, åpning av gjeldsforhandling, begjæring om konkurs og annet som kan påvirke vurderingen av om leverandøren er sikkerhetsmessig skikket. Dersom det oppstår en sikkerhetsrisiko som ikke kan fjernes med forebyggende sikkerhetstiltak, kan klareringsmyndigheten inndra leverandørklareringen. Sikkerhetsgradert informasjon eller skjermingsverdige objekter eller infrastruktur kan ikke overføres til en ny eier eller inngå i bobehandling ved gjeldsforhandling eller konkurs hvis ikke klareringsmyndigheten har samtykket til det.

For øvrig gjelder reglene i kapittel 8 så langt de passer.

Kongen utpeker en klareringsmyndighet for leverandørklarering. Kongen kan gi forskrift om krav til leverandørklarering og varigheten av klareringen.

Saksbehandlingsreglene i sikkerhetsloven kapittel 8 om personellsikkerhet, herunder bestemmelsene om begrunnelse og klage i klareringssaker, gjelder «så langt de passer» for leverandørklareringer. Det er klagerett, men sammenlignet med klage etter ordinære forvaltningsrettslige regler vil klageren i klareringssaker ha noe færre rettigheter. Eksempelvis kan klareringsmyndigheten normalt ikke gi innsyn i sikkerhetsgraderte opplysninger som inngår i vurderingsgrunnlaget og begrunnelsen.

Kravet til leverandørklarering er videre presisert i virksomhetssikkerhetsforskriften:

§ 83. Krav om leverandørklarering
En leverandør til en sikkerhetsgradert anskaffelse skal ha leverandørklarering når det er nødvendig for å oppnå et forsvarlig sikkerhetsnivå under anskaffelsen. Leverandøren skal uansett ha leverandørklarering dersom den skal

a) ha tilgang til eller oppbevare informasjon gradert KONFIDENSIELT eller høyere i sine egne informasjonssystemer eller lokaler

b) ha elektronisk tilgang fra sine egne informasjonssystemer eller lokaler til objekter eller infrastruktur klassifisert KRITISK eller MEGET KRITISK

c) råde over objekter eller infrastruktur som tilhører oppdragsgiveren, og som er klassifisert KRITISK eller MEGET KRITISK.

Hvorvidt det kreves leverandørklarering for anskaffelser til skjermingsverdig objekt eller infrastruktur må avgjøres i hvert enkelt tilfelle, med mindre tilfellet faller inn under bestemmelsens bokstav a til c. I vurderingen av nødvendighetskravet i bestemmelsens første setning, skal det blant annet legges vekt på om leverandørens personell får tilgang til hele eller deler av objektet eller infrastrukturen og om dette har et høyt skadepotensial.

Eksempler:

- Leverandøren eier en lokasjon hvor det er etablert et datasenter og har mulighet til å skru av strøm eller kjøling. Dette vil kunne påvirke tilgjengeligheten og til dels integriteten til tjenesten.
- Leverandøren er et vaktselskap som har ansvaret for beskyttelsen av objekt eller infrastruktur og kan påvirke alarm, adgangskontroll og overvåkningssensorer. Dette kan påvirke objektet eller infrastrukturens tilgjengelighet og konfidensialitet.

Med «råde over» i § 83 bokstav c menes at en leverandør har objektet eller infrastrukturen under sin kontroll og kan påvirke objektet eller infrastrukturens integritet, tilgjengelighet eller konfidensialitet.

Der oppdragsgiveren og leverandøren inngår sikkerhetsavtale, men leverandøren ikke faller inn under bokstav a til c i § 83, kan en leverandørklarering likevel være nødvendig for å oppnå et forsvarlig sikkerhetsnivå. I slike saker vil først oppdragsgiveren og senere leverandørklareringsmyndigheten vurdere forholdene som er relevante i anskaffelsen i leverandørklareringen. Følgende kan være relevante forhold i vurderingen:

- Sikkerhetsgraderingen/klassifiseringen i anskaffelsen
- Kriteriene nevnt i klareringsforskriften § 33

Bestemmelsens krav om leverandørklarering gjelder også i tilbudsfasen av en anskaffelse, selv om det i tilbudsfasen ofte er utrykket tilbyder og ikke leverandør som brukes. Virksomhetssikkerhetsforskriften § 79 nevner tilbydere eksplisitt, men ofte må tilbyderne innfortolkes der hvor loven og forskriftene omtaler leverandører.

Det vil være hensiktsmessig å forsøke å begrense graderingsnivå og omfang av utlevering av gradert informasjon i en tilbudsfase, både for å ivareta fremdriften til anskaffelsen og for å ivareta prinsippet om minst mulig inngripende tiltak overfor leverandøren.

2.3.2. Forespørsel om leverandørklarering

Ved behov for leverandørklarering skal oppdragsgiveren be klareringsmyndigheten om å klarere leverandøren. Dette følger av virksomhetssikkerhetsforskriften:

> *§ 85. Forespørsel om leverandørklarering*
>
> *Oppdragsgivere skal be klareringsmyndigheten om en leverandørklarering. Forespørselen skal inneholde informasjon om det høyeste graderingsnivå i anskaffelsen, jf. § 79, og egenopplysninger fra leverandøren, jf. klareringsforskriften § 35 [§ 34 red.anm.].*

Ved forespørsel om leverandørklarering skal oppdragsgiver vurdere graderingsnivået samt oversende egenopplysninger fra leverandøren til klareringsmyndigheten. Det stilles samme sikkerhetsmessige krav til underleverandør som til hovedleverandør. Dette fremkommer av virksomhetssikkerhetsforskriften:

> *§ 79. Vurdering av graderingsnivået for ulike deler av en sikkerhetsgradert anskaffelse*
>
> *Oppdragsgiveren skal ta stilling til hva tilbydere, leverandører og underleverandører kan få tilgang til av sikkerhetsgradert informasjon, skjermingsverdige objekter eller skjermingsverdig infrastruktur i de ulike fasene av en sikkerhetsgradert anskaffelse.*

Og klareringsforskriften:

> *§ 34. Egenopplysninger fra leverandøren*
>
> *En leverandør som skal klareres, skal gi samtykke til å bli kontrollert og i skjema fastsatt av Nasjonal sikkerhetsmyndighet gi opplysninger om*
>
> *a) leverandørens navn, adresse og eierstruktur*
> *b) utenlandske eierinteresser i leverandøren*
> *c) leverandørens eierinteresser i utlandet*
> *d) navn, fødselsnummer og statsborgerskap for virksomhetens leder*
> *e) pågående oppdrag for utenlandske oppdragsgivere, med opplysninger om oppdragsgivere og hvilken andel av leverandørens omsetning oppdragene utgjør.*
>
> *Leverandøren skal sammen med skjemaet levere skisser eller tegninger over lokalene som skal brukes til behandling og oppbevaring av sikkerhetsgradert informasjon.*

Ved gjennomføringen av leverandørklarering vil klareringsmyndigheten legge til grunn det vurderingsgrunnlaget som fremgår av klareringsforskriften § 33 og kan innhente ytterligere opplysninger om leverandøren fra kilder som fremkommer i klareringsforskriften § 35.

Det bemerkes særskilt at før en leverandørklarering kan gis, skal leverandørens leder og styremedlemmer klareres for det samme nivå som det er bedt om leverandørklarering for, jf. klareringsforskriften § 33 andre ledd. En personkontroll av personer i leverandørens styre og ledelse skal være en del av vurderingsgrunnlaget, jf. sikkerhetsloven § 9-3 andre ledd tredje punktum. Der hvor et styremedlem eller virksomhetens leder ikke kan klareres, kan vedkommende gi avkall på rett til innsyn i sikkerhetsgradert informasjon eller tilgang til skjermingsverdig objekt/infrastruktur. Gitt at sikkerhetsklarering er en inngripende prosess, legger NSM til grunn at det ikke er et krav at det før

innsynsretten fraskrives må være gjennomført en klareringsprosess med et negativt utfall. Det anbefales at NSMs skjema for avkall på innsynsrett benyttes.

Leverandørklareringens varighet fremgår av klareringsforskriften:

> *§ 38. Leverandørklareringers gyldighetstid*
>
> *En leverandørklarering kan gis for inntil fem år, med mindre annet følger av avtale mellom Norge og en annen stat eller internasjonal organisasjon.*

Bestemmelsen åpner for en viss fleksibilitet i form av at leverandørklarering kan gis for inntil fem år. Kortere leverandørklarering kan gis dersom det er åpenbart at leverandørklareringen ikke vil bli benyttet i fem år, eller at leverandøren ikke ønsker å opprettholde sikkerhetstiltakene etter at oppdraget som utløser klareringsbehovet er avsluttet.

Nasjonal sikkerhetsmyndighet klarerer norske leverandører i forbindelse med sikkerhetsgraderte anskaffelser. Utenlandske leverandører klareres av myndigheten i sitt hjemland, jf. klareringsforskriften § 32. Oppdragsgiveren sender sin forespørsel om klareringsstatus eller leverandørklarering til Nasjonal sikkerhetsmyndighet, også når det gjelder en utenlandsk leverandør.

2.3.3. Internasjonale sikkerhetsgraderte anskaffelser

I enkelte tilfeller kan det være aktuelt å benytte en utenlandsk leverandør i en sikkerhetsgradert anskaffelse. Med utenlandsk leverandør menes en leverandør med lokaler utenfor norsk jurisdiksjon eller som driver sin virksomhet fra en annen stats jurisdiksjon.

Disse anskaffelsene er nærmere regulert i sikkerhetsloven § 9-2 første ledd andre punktum, virksomhetssikkerhetsforskriften § 84, klareringsforskriften § 32 samt i bilaterale sikkerhetsavtaler inngått mellom Norge og myndighetene i andre land.

Ønsker en virksomhet å benytte en leverandør lokalisert i et annet land, må det foreligge en godkjennelse av NSM, jf. sikkerhetslovens § 9-2 første ledd andre punktum. Virksomheten må derfor fremsende en forespørsel til NSM hvor leverandøren, og det land hvor denne er lokalisert, identifiseres. For anskaffelser som innebærer at leverandøren vil få tilgang til norsk sikkerhetsgradert informasjon/informasjonssystem, vil NSM, som hovedregel, bare kunne gi en slik godkjenning hvis det foreligger en bilateral sikkerhetsavtale mellom myndighetene i Norge og myndighetene i landet hvor leverandøren er lokalisert, jf. virksomhetssikkerhetsforskriften § 25.

I de tilfeller det kreves leverandørklarering av en leverandør lokalisert i et annet land, følger det av klareringsforskriften § 32, samt de bilaterale sikkerhetsavtalene myndighetene i Norge har inngått, at sikkerhetsmyndighetene i landet hvor leverandøren er lokalisert gjennomfører klareringsprosessen, og utsteder hva som internasjonalt betegnes som en «Facility Security Clearance». De bilaterale sikkerhetsavtalenes systematikk er at forespørsel og bekreftelse av leverandørklareringer skjer i en prosess mellom de to landenes sikkerhetsmyndigheter. Virksomheten som ønsker å benytte en

leverandør i et annet land må derfor forespørre NSM, som deretter vil videresende forespørselen til sikkerhetsmyndigheten i det aktuelle landet. Den annen stats sikkerhetsmyndighet vil gi en bekreftelse tilbake til NSM når leverandørklarering foreligger, og NSM vil deretter informere virksomheten som skal gjennomføre anskaffelsen om dette.

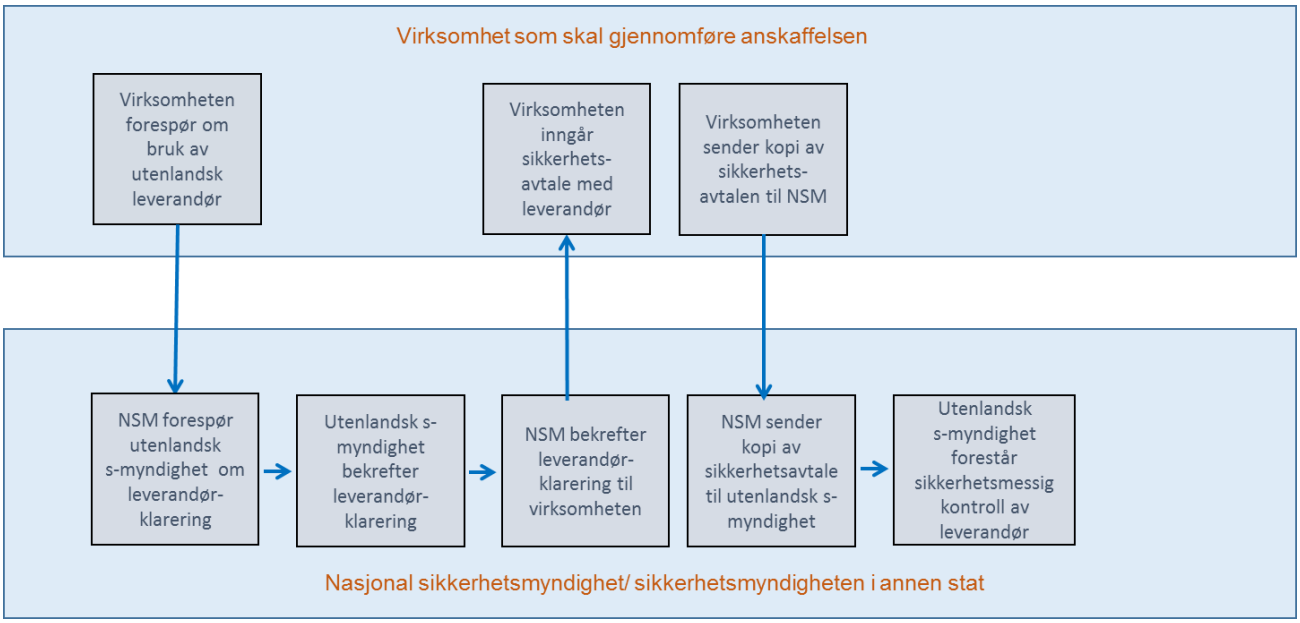
I henhold til de bilaterale sikkerhetsavtalene vil nødvendig sikkerhetsklarering av leverandørens personell bli foretatt av de kompetente myndigheter i landet hvor leverandøren er lokalisert, og sikkerhetsmyndigheten vil der dette er nødvendig bekrefte personellets klareringsstatus. Dette innebærer at det normalt ikke skal utstedes norske sikkerhetsklareringer til leverandørens personell der leverandøren er lokalisert i en annen stat. Det er imidlertid en åpning for at klareringsmyndighetene likevel kan klarere personen, jf. sikkerhetsloven § 8-7.

Sikkerhetsavtalen som blir inngått mellom den norske virksomheten som gjennomfører en sikkerhetsgradert anskaffelse og leverandøren i en annen stat forutsettes fremsendt til NSM. NSM vil i henhold til internasjonale forpliktelser etter de bilaterale sikkerhetsavtalene fremsende disse til sikkerhetsmyndigheten i landet hvor leverandøren er lokalisert, hvor de vil tjene som grunnlag for kontroll med leverandøren. Internasjonalt vil disse avtalene gjerne bli omtalt som «Security Clauses», eller i kontrakter som krever mer omfattende sikkerhetsmessige reguleringer som «Project Security Instructions» (PSI).

Der leverandørens personell har behov for å gjennomføre et besøk i Norge i forbindelse med en sikkerhetsgradert anskaffelse, må besøket gjennomføres i samsvar med virksomhetssikkerhetsforskriften § 87. Denne bestemmelsen stiller krav om at den besøkendes identitet og klarering skal kontrolleres. Utfyllende bestemmelser om gjennomføring av besøk som vil gi tilgang til sikkerhetsgradert informasjon følger av de ulike bilaterale sikkerhetsavtalene Norge har inngått. Det bærende prinsipp i disse avtalene er at besøksanmodninger (internasjonalt omtalt som «Request for Visit» (RfV)) som vil gi tilgang til sikkerhetsgradert informasjon skal fremsendes og klareres gjennom statenes respektive kompetente sikkerhetsmyndigheter, og at personellets sikkerhetsklarering bekreftes av leverandørenes sikkerhetsmyndighet som ledd i denne prosessen. I denne prosessen benyttes et internasjonalt anerkjent skjema. I Norge er utøvelsen av besøkskontrollregimet delegert til Forsvarets sikkerhetsavdeling (FSA).

I den sikkerhetsgraderte kontraktens løpetid vil sikkerhetsmyndighetene i landet hvor leverandøren er lokalisert være forpliktet til å forestå sikkerhetsmessig oppfølging og tilsyn med leverandøren. Denne oppfølgingen vil bli gjennomført i henhold til det aktuelle landets nasjonale lovgivning, og plikten følger av den bilaterale sikkerhetsavtalen mellom myndighetene i Norge og myndighetene i det aktuelle landet.

Prosessen knyttet til bruk av leverandører i et annet land kan illustreres slik:



Klareringsmyndigheten eller oppdragsgiver skal ikke føre kontroll dersom det følger av sikkerhetsavtale mellom Norge og annen stat eller internasjonal organisasjon at kontrollen skal gjennomføres av andre.

2.3.4. Kontroll av om leverandøren oppfyller sikkerhetskravene

Som hovedregel skal klareringsmyndigheten føre kontroll med om leverandøren oppfyller sikkerhetskravene som gjelder for å inneha leverandørklarering. Kontroll med leverandører av sikkerhetsgraderte anskaffelser gjøres i den hensikt å avgjøre om leverandøren er sikkerhetsmessig skikket til, som ledd i sin leveranse, å få tilgang til eller tilvirke sikkerhetsgradert informasjon eller få tilgang til skjermingsverdig objekt eller infrastruktur.

Dette reguleres i klareringsforskriften:

§ 36. Kontroll av om leverandøren oppfyller sikkerhetskravene

Før leverandøren kan klareres, skal klareringsmyndigheten kontrollere at leverandøren oppfyller kravene til sikkerhetsstyring og beskyttelse av skjermingsverdige verdier i sikkerhetsloven og virksomhetsikkerhetsforskriften som gjelder for anskaffelsen. Dersom leverandøren ikke oppfyller kravene til sikkerhetsstyring eller ikke har gjennomført tilstrekkelige sikkerhetstiltak, skal en leverandørklarering ikke gis eller gis på vilkår.

Klareringsmyndigheten skal kontrollere leverandøren på nytt dersom det i klareringens gyldighetstid er nødvendig ut fra en risikovurdering, er nødvendig som ledd i en reklarering eller dersom leverandøren selv ber om det. Er det gjennomført tilsyn med leverandøren, skal klareringsmyndigheten innhente en rapport fra tilsynsmyndigheten om tilsynet.

Leverandøren skal motta skriftlig varsel før klareringsmyndigheten gjennomfører en stedlig kontroll. Kontrollen kan likevel gjennomføres uten varsel dersom det av sikkerhetshensyn er nødvendig å

gjennomføre kontrollen uten at leverandøren varsles. Klareringsmyndigheten skal utarbeide en rapport fra kontrollen.

Kontrollen etter første og andre ledd kan etter avtale med klareringsmyndigheten gjennomføres av oppdragsgiveren.

Dersom det følger av sikkerhetsavtale mellom Norge og annen stat eller internasjonal organisasjon at kontrollen skal gjennomføres av andre, jf. virksomhetsikkerhetsforskriften § 84 andre ledd, skal klareringsmyndigheten be myndighetene i staten om å gjennomføre kontrollen.

Kontroll etter § 36 første og andre ledd kan avtales gjennomført av oppdragsgiver, jf. klareringsforskriften § 36 fjerde ledd. Dersom en slik fullmakt gis, er det en forutsetning at oppdragsgiveren har tilstrekkelig fagkompetanse. Ytterligere kriterier for gjennomføring av kontroll, etter avtale mellom NSM og oppdragsgiver, vil bli fastsatt under avtaleinngåelsen.

Dersom leverandøren ikke oppfyller kravene til sikkerhetsstyring eller ikke har gjennomført tilstrekkelige sikkerhetstiltak, kan leverandørklarering gis på vilkår, jf. § 36 første ledd. For at klarering på vilkår skal kunne gis, må det foreligge en risikovurdering foretatt av klareringsmyndigheten. I utgangspunktet er dette en snever unntaksbestemmelse og utfallet av risikovurderingen vil stå sentralt i vurderingen av om leverandørklarering på vilkår kan gis. Eksempelvis kan leverandørklarering gis på vilkår dersom leverandøren har iverksatt en prosess for sikring av objekt eller infrastruktur, kompenserende tiltak er på plass, og det vurderes at leverandøren ellers er sikkerhetsmessig skikket.

2.3.5. Tilbakekall av leverandørklarering

Tilbakekall av leverandørklarering er hjemlet i klareringsforskriften:

§ 37 Tilbakekall av leverandørklarering

Dersom leverandøren ikke retter brudd på kravene fastsatt i eller med hjemmel i sikkerhetsloven innen en fastsatt frist, kan leverandørklareringen kalles tilbake. Er et brudd vesentlig, kan klareringsmyndigheten tilbakekalle leverandørklareringen uten at det settes en frist.

Brudd på relevante bestemmelser som avdekkes som følge av kontroll eller med bakgrunn i informasjon som tilfaller oppdragsgiver eller klareringsmyndighet, kan medføre bortfall av leverandørklarering. Avdekkede forhold vil være gjenstand for en risikovurdering for å avgjøre om brudd på den relevante bestemmelsen er å anse som vesentlig og om hvorvidt leverandørklareringen skal tilbakekalles.

2.4. Oversikt over sikkerhetsgraderte anskaffelser

Oppdragsgiveren har en plikt til å holde oversikt over sikkerhetsgraderte anskaffelser og skal i henhold til virksomhetssikkerhetsforskriften § 86 første ledd bokstav a–e sende oversikt over egne anskaffelser til Nasjonal sikkerhetsmyndighet årlig. Oversikten skal sendes i løpet av januar påfølgende år. Kopi av inngåtte og terminerte sikkerhetsavtaler innrapporteres fortløpende til NSM.

§ 86. Oversikt over sikkerhetsgraderte anskaffelser

Oppdragsgivere skal føre en årlig oversikt over sikkerhetsgraderte anskaffelser til sin virksomhet. Oversikten skal inneholde informasjon om
a) hva anskaffelsene gjelder
b) leverandørenes navn, adresse, organisasjonsnummer eller tilsvarende nummer, og nasjonalitet
c) hvilken sikkerhetsgrad informasjon som leverandørene skal få, eller har fått, tilgang til
d) det høyeste klassifiseringsnivået til objekter eller infrastruktur som leverandørene skal få, eller har fått, tilgang til
e) hvor lang tid anskaffelsene tok.

Oversikten skal årlig sendes til klareringsmyndigheten.

Forsvarsdepartementet kan gjøre unntak fra kravet i andre ledd dersom virksomheten har et særlig behov for å skjerme opplysningene av hensyn til sin operative virksomhet.

3. Ugraderte anskaffelser til skjermingsverdige, ugraderte verdier

3.1. Avtale om sikkerhet i anskaffelsen

Ved ugraderte anskaffelser til skjermingsverdige, ugraderte verdier skal partene inngå en avtale som beskrevet i virksomhetssikkerhetsforskriften § 18 annet ledd. Avtalen skal forplikte leverandøren til å følge de samme kravene for beskyttelse av de skjermingsverdige verdiene som gjelder for oppdragsgiveren. Avtalen må også gi oppdragsgiveren mulighet til å undersøke om leverandøren oppfyller kravene til beskyttelse.

Bestemmelsen kan minne om kravet til sikkerhetsavtale i sikkerhetsloven § 9-2, men gjelder for anskaffelser som ikke er sikkerhetsgraderte. Avtalen kan inngås som et selvstendig dokument eller integreres i leveranseavtalen mellom virksomheten og leverandøren. Avtalen vil ha vesentlige likhetstrekk med en sikkerhetsavtale og skal konkretisere hvordan partene skal beskytte de skjermingsverdige, ugraderte verdiene i den enkelte ugraderte anskaffelsen. Nasjonal sikkerhetsmyndighet anbefaler at virksomhetene ser hen til malene for sikkerhetsavtaler når de skal inngå avtale etter § 18 annet ledd.

4. Felles regler for anskaffelser etter sikkerhetsloven

4.1. Varslingsplikt ved «ikke ubetydelig risiko»

Både sikkerhetsgraderte anskaffelser og anskaffelser til skjermingsverdige, ugraderte verdier er underlagt en varslingsplikt hvis anskaffelsen utgjør en «ikke ubetydelig risiko» for sikkerhetstruende virksomhet. Kapitlene nedenfor gir en nærmere forklaring av plikten til å vurdere risiko, plikten til å identifisere risikoreduserende tiltak og til slutt selve varslingsplikten.

Departementene ønsker å få kjennskap til risikofylte anskaffelser på et så tidlig tidspunkt som mulig. Oppdragsgiveren vil selv ha ansvaret for å vurdere risiko ved anskaffelsen, og for å iverksette risikoreduserende tiltak. Oppdragsgiverens håndtering vil være det primære, og det vil kun i noen få saker være aktuelt å varsle myndighetene.

Uavhengig av om anskaffelsen er sikkerhetsgradert eller ikke, kan bestemmelsen i sikkerhetsloven § 9-4 komme til anvendelse. Den sikkerhetsmessige risikoen ved en anskaffelse kan være høy i begge kategorier av anskaffelser. I sikkerhetsgraderte anskaffelser vil sikkerhetslovens krav til anskaffelsene normalt gi oppdragsgiveren de nødvendige tiltakene for å redusere risikoen. Likevel kan risikovurderingen etter sikkerhetsloven § 9-4 indentifisere ytterligere tiltak for å oppnå «ubetydelig risiko».

Hvordan aktørene, i første rekke oppdragsgiveren, skal håndtere den sikkerhetsmessige risikoen ved anskaffelser til skjermingsverdig informasjonssystem, objekt eller infrastruktur, forklares nærmere i de neste kapitlene og er illustrert i figuren under:

§ 9-4. Varslingsplikt og myndighet til å fatte vedtak ved anskaffelser til skjermingsverdig informasjonssystem, objekt eller infrastruktur.

Ved anskaffelser til skjermingsverdig informasjonssystem, objekt eller infrastruktur skal virksomheten vurdere om anskaffelsen kan innebære en ikke ubetydelig risiko for at informasjonssystemet, objektet eller infrastrukturen kan bli rammet av eller brukt til sikkerhetstruende virksomhet. Plikten til å foreta en slik vurdering gjelder ikke dersom anskaffelsen åpenbart ikke innebærer noen slik risiko.

Virksomheten skal varsle departementet dersom vurderingen viser at anskaffelsen innebærer risiko som nevnt i første ledd. Virksomheter som ikke er underlagt noe departement, skal varsle sikkerhetsmyndigheten. Varslingsplikten gjelder uten hinder av taushetsplikt. Plikten gjelder ikke dersom virksomheten selv iverksetter tiltak som fjerner risikoen eller gjør den ubetydelig.

Departementet som mottar et varsel etter andre ledd, kan be relevante organer uttale seg om risikoen ved anskaffelsen og om leverandørens sikkerhetsmessige pålitelighet.

Dersom anskaffelsen til et skjermingsverdig informasjonssystem, objekt eller infrastruktur kan innebære en ikke ubetydelig risiko som nevnt i første ledd, kan Kongen i statsråd fatte vedtak om at anskaffelsen ikke skal gjennomføres, eller om at det skal settes vilkår for den. Dette gjelder også dersom det er inngått avtale om anskaffelsen. Dersom det ikke fattes vedtak etter første punktum, skal departementet orientere virksomheten om det. Et vedtak etter første punktum er et særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Kongen i statsråd kan gi forskrift om varslingsplikten og om myndigheten til å fatte vedtak.

4.1.1. Plikten til å vurdere risiko

Oppdragsgiveren har plikt til å vurdere risiko ved anskaffelser til skjermingsverdig informasjonssystem, objekt eller infrastruktur. Plikten følger av sikkerhetsloven § 9-4 første ledd, og vurderingstemaet er «om anskaffelsen kan innebære en ikke ubetydelig risiko for at informasjonssystemet, objektet eller infrastrukturen kan bli rammet av eller brukt til sikkerhetstruende virksomhet». Regelen er gjentatt i virksomhetssikkerhetsforskriften § 18 første ledd, men er der avgrenset til risiko for påvirkning fra leverandøren selv eller dennes personell.

Reglene om risikovurdering, risikoreduserende tiltak og varslingsplikt i sikkerhetsloven § 9-4 har likhetstrekk med reglene om risikovurdering, risikoreduserende tiltak og varslingsplikt i sikkerhetslovens kapittel 4, men formålet er forskjellig. Formålet med reglene i § 9-4 er å forebygge at anskaffelser fører til at skjermingsverdige verdier blir rammet av eller brukt til sikkerhetstruende virksomhet. Formålet med reglene i lovens kapittel 4 er å sikre et forsvarlig sikkerhetsnivå.

Risikovurdering krever både kompetanse og kunnskap. Oppdragsgivernes forutsetninger for å kunne vurdere risiko varierer. Den som eier et skjermingsverdig informasjonssystem, objekt eller infrastruktur, må kunne forventes å ha inngående kunnskap om informasjonssystemets, objektets eller infrastrukturens funksjon og betydning for samfunnet. Kunnskap om potensielle sårbarheter ved informasjonssystemet, objektet eller infrastrukturen må også kunne forventes. Slik tar risikovurderingen hensyn til særtrekk ved både oppdragsgiverens virksomhet og den konkrete anskaffelsen. Men kunnskap om mulige trusler og trusselaktører kan trolig ikke forventes i samme

grad hos alle oppdragsgivere. Mange oppdragsgivere vil i sine risikovurderinger derfor måtte fokusere på sårbarheter og mulige konsekvenser av sikkerhetstruende virksomhet og ikke på trusler.

En risikovurdering vil være en sammensatt vurdering som i tillegg til sårbarhet og konsekvenser også omfatter sannsynlighet. Sannsynligheten for at sikkerhetstruende virksomhet inntreffer vil være ett blant flere momenter i risikovurderingen, og må ses i sammenheng med de mulige konsekvensene av den sikkerhetstruende virksomheten. Det er viktig å være oppmerksom på at dersom konsekvensene av sikkerhetstruende virksomhet er alvorlige, kan risikoen være høy selv om sannsynligheten er lav. Og motsatt kan stor sannsynlighet tilsi høy risiko, selv om konsekvensene antas å være mindre alvorlige. Formuleringen «ikke ubetydelig risiko» angir ingen høy terskel, men innebærer at varslingsplikten oppstår i situasjoner hvor risikovurderingen tilsier risiko ut over det normale, altså en risiko som er høyere enn den «ubetydelige» risiko som normalt aksepteres i andre situasjoner og andre anskaffelser.

Risikoen for å «bli rammet av eller brukt til sikkerhetstruende virksomhet» omfatter både det å gjennomføre sikkerhetstruende virksomhet under anskaffelsen og det å tilrettelegge for at sikkerhetstruende virksomhet kan gjennomføres på et senere tidspunkt. Et eksempel på sistnevnte kategori er å programmere inn en bakdør i et datasystem som kan utnyttes i ettertid.

Eksempler der disse bestemmelsene kommer til anvendelse og risiko må vurderes, kan være ved leveranse av hardware til kritisk infrastruktur, kjølings- og ventilasjonsarbeider til et serverrom eller anskaffelse av et styringssystem som i seg selv ikke er sikkerhetsgradert.

4.1.2. Risikoreduserende tiltak

Når utfallet av oppdragsgiverens risikovurdering er at oppdragsgiveren konkluderer med at det totalt sett foreligger en risiko, og denne er mer enn ubetydelig, bør virksomheten identifisere og iverksette risikoreduserende tiltak. Dersom oppdragsgiveren gjennom risikoreduserende tiltak får redusert risiko til et ubetydelig nivå, kan oppdragsgiveren gjennomføre anskaffelsen uten å involvere det relevante sektordepartementet.

Risikoreduserende tiltak kan iverksettes hos oppdragsgiveren uavhengig av anskaffelsesprosedyren eller gjennomføres av partene i fellesskap som en del av anskaffelsen. Tiltakene kan være administrative, fysiske, menneskelige eller tekniske barrierer, eller de kan være av en annen art. Eksempler er oppsyn med leverandørens personell for å sikre at de ikke gjennom oppdraget kan utføre skade, tiltrodd tredjeparts kontroll av anskaffede komponenter, bruk av flere leverandører fra forskjellige land for å sikre at ikke en enkelt trusselaktør alene kan påføre skade samt tiltak for skadebegrensning og gjenoppretning.

Oppdragsgiveren har ingen plikt til å iverksette risikoreduserende tiltak, men plikten til å varsle sektordepartementet består så lenge risikoen er «ikke ubetydelig». Oppdragsgiveren har med andre ord valget mellom å redusere risikoen til «ubetydelig» eller å varsle departementet. Det er likevel forutsatt i lovbestemmelsens forarbeider at oppdragsgiveren bør forsøke risikoreduserende tiltak først og at varsel til departementet skal være et sekundært virkemiddel, forbeholdt spesielle situasjoner.

Dersom oppdragsgiveren har iverksatt risikoreduserende tiltak og konkludert med at anskaffelsen kan gjennomføres uten å varsle det ansvarlige sektordepartementet eller Nasjonal sikkerhetsmyndighet, anbefaler NSM likevel at oppdragsgiveren informerer den relevante tilsynsmyndigheten om anskaffelsens eksistens og om hvilke vurderinger som er gjort.

4.1.3. Krav til varsel etter § 9-4

Virksomheten skal varsle sitt ansvarlige departement dersom risikovurderingen viser at anskaffelsen innebærer en «ikke ubetydelig risiko» for sikkerhetstruende virksomhet i en forestående eller pågående anskaffelse.

Når en oppdragsgiver varsler departementet om en slik risiko, bør departementet normalt innhente rådgivende uttalelser fra relevante organer. I sikkerhetslovens forarbeider nevnes Politiets sikkerhetstjeneste, Etterretningstjenesten og Nasjonal sikkerhetsmyndighet som aktuelle organer.

Etter at nødvendig informasjon er samlet inn, kan departementet avgjøre saken i dialog med den aktuelle virksomheten. Ett mulig utfall på dette stadiet er at oppdragsgiveren og departementet i fellesskap identifiserer risikoreduserende tiltak som løser saken.

Kommer departementet til at anskaffelsen ikke bør gjennomføres eller at det bør stilles nærmere vilkår for gjennomførelsen, fremmer departementet saken for Kongen i statsråd. For å muliggjøre en forsvarlig risikovurdering i den videre saksbehandlingen, skal varselet inneholde den informasjonen som er angitt i virksomhetssikkerhetsforskriften § 19 første ledd.

§ 19. Varslingsplikt om anskaffelser til skjermingsverdig informasjonssystem, objekt og infrastruktur

Et varsel etter sikkerhetsloven § 9-4 skal opplyse om følgende:
a) hva anskaffelsen gjelder
b) leverandørens navn, adresse, organisasjonsnummer, nasjonalitet, styremedlemmer og eiere
c) hvordan oppdragsgiveren vurderer risikoen for at skjermingsverdige verdier kan bli rammet av sikkerhetstruende virksomhet ved anskaffelsen
d) hvordan oppdragsgiveren vil håndtere risikoen
e) om det vil gjenstå en ikke ubetydelig risiko også etter at tiltak er iverksatt
f) om anskaffelsen likevel bør gjennomføres
g) andre forhold som oppdragsgiveren antar kan ha betydning for vurderingen av risikoen forbundet med anskaffelsen.

Med anskaffelse i sikkerhetsloven § 9-4 menes også tilleggsanskaffelser og kontrakter som tildeles under en rammeavtale.

Departementet skal innen 60 arbeidsdager orientere oppdragsgiveren om anskaffelsen kan gjennomføres, eller om at saken skal behandles av Kongen i statsråd. Fristen regnes fra det tidspunktet departementet har mottatt varselet. Har departementet innen 50 arbeidsdager framsatt et skriftlig krav om ytterligere opplysninger, avbrytes fristen inntil dette svaret er mottatt.

Varslingsplikten gjelder uavhengig av andre former for lovbestemt varslingsplikt, siden disse oftest vil ha et annet formål enn sikkerhetslovens. Varslingsplikten gjelder uten hinder av lovbestemt taushetsplikt.

Et varsel etter § 9-4 vil føre til at anskaffelsen tar lengre tid enn ellers. Saksbehandling hos Kongen i statsråd kan medføre ytterligere tidsbruk og involverer flere aktører. Både av hensyn til sikkerheten i anskaffelsen og av hensyn til aktørenes ressursbruk, vil det oftest være en fordel om risikoen avklares før oppdragsgiveren kunngjør anskaffelsen. Dersom det ikke er mulig, bør oppdragsgiveren orientere om en mulig varslingsprosedyre ved kunngjøringen eller for øvrig så snart som mulig. Mest mulig informasjon tidligst mulig vil kunne redusere usikkerheten for aktørene. Samtidig kan det tenkes tilfeller der trusselbildet brått endres, slik at varslingsplikt oppstår og varsel kan gis først underveis i anskaffelsesprosedyren.

Sikkerhetslovens forarbeider presiserer at et vedtak fra Kongen i statsråd må være innrettet på en slik måte at lovens formål ivaretas. For eksempel innebærer formålsbegrensningen at det ikke er hjemmel til å gripe inn ved risiko for industrispionasje som kun er egnet til å skade en enkeltbedrifts forretningsvirksomhet. For øvrig kan Kongen i statsråd i prinsippet fatte alle typer vedtak. Den mest inngripende typen vedtak vil være å stanse en anskaffelse eller å forby bruk av visse leverandører. En mindre inngripende type vedtak er å stille vilkår om å iverksette risikoreduserende tiltak.

Et eventuelt vedtak fra Kongen i statsråd som stiller vilkår eller nekter anskaffelsen gjennomført, kan etter omstendighetene medføre erstatningskrav fra tilbydere eller leverandører.

4.2. Oppdragsgivers oppfølging av leverandør

Leverandøren er selv ansvarlig for det forebyggende sikkerhetsarbeidet, jf. sikkerhetsloven § 4-1 første ledd. I tillegg har oppdragsgiveren etter sikkerhetsloven § 4-1 andre ledd et ansvar for å påse at leverandøren har tilstrekkelig risiko- og sikkerhetsforståelse. En naturlig konsekvens av dette vil være at oppdragsgiveren må føre kontroll med at leverandøren følger opp kravene i sikkerhetsavtalen, uavhengig av klareringsmyndighetens kontroll eller tilsynsmyndighetens tilsyn. En slik kontrollmulighet bør avtalefestes i sikkerhetsavtalen mellom partene. Dette er ikke kontrollmyndighet som beskrevet i klareringsforskriften § 36, men å anse som en andrepartskontroll på linje med annen kontraktsoppfølging av leverandøren, for eksempel knyttet til pris eller kvalitet. Konsekvensen av at leverandøren ikke oppfyller kravene til avtalen bør avtalefestes, men kan ikke knyttes til sikkerhetslovens tvangsmidler eller tilbakekall av leverandørklarering.

§ 4-1. Sikkerhetsstyring

Virksomhetens leder har ansvar for det forebyggende sikkerhetsarbeidet. Forebyggende sikkerhetsarbeid skal være en del av virksomhetens styringssystem. Sikkerhetstilstanden i virksomheten skal regelmessig kontrolleres.

Virksomheten skal sørge for at ansatte, leverandører og oppdragstakere har tilstrekkelig risiko- og sikkerhetsforståelse. For leverandører til sikkerhetsgraderte anskaffelser gjelder kapittel 9.

Kongen kan gi forskrift om sikkerhetsstyring.

Oppdragsgivers forpliktelser etter sikkerhetslovens §4-1 innebærer blant annet at oppdragsgiveren skal gi råd og veiledning, gjennomføre autorisasjonssamtaler, påse at det er gjennomført

personellklareringer på riktig nivå og at godkjenninger av informasjonssystemer er foretatt der loven krever dette.

Leverandører til sikkerhetsgraderte anskaffelser har et selvstendig ansvar for det forebyggende sikkerhetsarbeidet i forbindelse med den konkrete anskaffelsen, herunder en plikt til å sørge for opplæring av eget personell. Dette gjelder for alle graderings-/klassifiseringsnivåer, også for sikkerhetsgraderte anskaffelser for nivå BEGRENSET/VIKTIG hvor det ikke er krav til leverandørklareringer.

Informasjon av betydning for leverandørklareringen må sendes tilsynsmyndigheten. Virksomhetens (både oppdragsgivers og leverandørs) plikt til å varsle tilsynsmyndigheten følger av sikkerhetsloven § 4-5.

Videre har oppdragsgiver ansvar for å anmode klareringsmyndigheten om klarering av leverandørens personell, jf. virksomhetssikkerhetsforskriften § 69:

§ 69. Autorisasjon av autorisasjonsansvarlig og personell hos leverandøren

Oppdragsgiveren skal autorisere den autorisasjonsansvarlige hos leverandøren og personell hos leverandøren som bare får tilgang til skjermingsverdig informasjon, skjermingsverdige objekter eller skjermingsverdig infrastruktur hos oppdragsgiveren.

Oppdragsgiveren skal anmode om klarering av leverandørens personell i den utstrekning dette er nødvendig for den sikkerhetsgraderte anskaffelsen, samt gjennomføre autorisasjon av leverandørens personell. Forespørsel om klarering sendes klareringsmyndigheten.

4.3. Tilsyn

Nasjonal sikkerhetsmyndighet og utvalgte sektortilsyn er tilsynsmyndigheter for leverandører til sikkerhetsgraderte anskaffelser. Dette er hjemlet i virksomhetssikkerhetsforskriften:

§ 88. Tilsynsmyndighet for leverandører til sikkerhetsgraderte anskaffelser

Nasjonal sikkerhetsmyndighet fører tilsyn med leverandører til sikkerhetsgraderte anskaffelser som har lokaler innenfor norsk jurisdiksjon, med mindre noe annet er avtalt med en sektormyndighet med tilsynsansvar.

Nasjonal sikkerhetsmyndighet

Postboks 814
1306 Sandvika

postmottak@nsm.no
www.nsm.no