

Veileder fra NSM

Veileder for ivaretagelse av sikkerhet i anskaffelser

Veileder fra NSM

Veileder for ivaretagelse av sikkerhet i anskaffelser

Versjon

1.0

Godkjent dato

03.06.2025

Dokumentnr

U-25-78

Sak

U-25/00763

Siste versjon endret

Dato: 03.06.2025

☐ Kun henvisninger/referanser ☐ Kun språklige endringer ☐ Endring i faglig innhold

Nasjonal sikkerhetsmyndighet (NSM) er sikkerhetsmyndighet etter lov om nasjonal sikkerhet (sikkerhetsloven) og fagorgan for forebyggende sikkerhet. NSM gir informasjon, råd og veiledning om forebyggende sikkerhetsarbeid og krav til tiltak.

NSM har tre kategorier av veiledere.

- Veiledere lov og forskrift
- Håndbøker
- Tekniske veiledere

Veilederne representerer NSMs syn på hvordan lover og forskrifter er å forstå. De utdyper krav og gir tekniske og prosedyremessige anbefalinger. Veiledere legges til grunn for NSMs arbeid knyttet til godkjenninger og tilsyn. NSM tilbyr også kurs på sentrale områder, både som e-læring og fysiske kurs. Mer informasjon finnes på NSMs nettsider.

Vi anbefaler at NSMs ulike veiledninger leses i sammenheng for å sikre en helhetlig tilnærming til forebyggende sikkerhetsarbeid.

Ugraderte veiledere er åpent tilgjengelige på NSMs nettsider. Graderte veiledere er tilgjengelige på graderte samhandlingsplattformer og kan formidles fra NSM iht. tjenstlige behov.

NSM oppdaterer jevnlig dokumentene. Siste versjon av ugraderte veiledere er alltid tilgjengelig på NSMs nettsider.

NSMs veiledere er dokumenter som er ment å gi støtte til offentlige og private virksomheters arbeid med forebyggende sikkerhet. Virksomheter som er omfattet av sikkerhetsloven skal ha nødvendig informasjon om hvordan de kan oppnå forsvarlig sikkerhet

NSM utgir også andre publikasjoner av mer generell karakter, som ikke har status som veiledere, eksempelvis generelle grunnprinsipper for sikkerhet og andre rådgivende dokumenter.

Vi håper veilederne gir god støtte til arbeidet med forebyggende sikkerhet og mottar gjerne tilbakemeldinger dersom det er behov for endringer eller andre veiledere.

Innhold

Innhold	3
1 Innledning	5
2 Vurdering av om en anskaffelse er sikkerhetsgradert	5
2.1 Kompetanse	6
2.2 Oppdragsgivers verdier	6
2.2.1 Fremtidige verdier	6
2.3 Leverandør	7
2.4 Tilgang til	7
3 Sikkerhetskrav i sikkerhetsgraderte anskaffelser	8
3.1 Risikovurdering	8
3.1.1 Oppdragsgivers varslingsplikt	10
3.2 Sikkerhetskrav i konkurransegrunnlaget	10
3.3 Sikkerhetsavtale	11
3.3.1 Unntak fra krav om sikkerhetsavtale	12
3.4 Leverandørklarering	12
3.4.1 Krav om leverandørklarering	13
3.4.2 Andre tilfeller hvor leverandørklarering kan være aktuelt	14
3.4.3 Leverandørklaringsprosessen	14
3.4.4 Autorisasjon	17
3.5 Oppdragsgivers oppfølging av leverandørforhold	18
3.6 Utenlandske leverandører	18
3.6.1 Sikkerhetsavtale	18
3.6.2 Leverandørklarering	19
3.6.3 Klarering og autorisering av personell	20
3.6.4 Vilkår og prosedyrer ved besøk	20
3.7 Tilbakelevering	20
3.7.1 Overføring av verdier til nye parter	20
3.8 Unntak fra sikkerhetskrav	21
4 Sikkerhet i ugraderte anskaffelser	21

4.1	Forholdet mellom sikkerhetsloven og lov om offentlige anskaffelser	21
4.2	Relevante hensyn ved planlegging og gjennomføring av anskaffelser	22
4.3	Ivaretagelse av sikkerhet i anskaffelsesprosessen	22
4.4	Sikkerhetskrav i kontrakt	23
5	Oppsummering	24

1 Innledning

Veilederen gir en innføring i krav som stilles til anskaffelser etter sikkerhetsloven. Veilederen er relevant for alle virksomheter som er underlagt sikkerhetsloven og er skrevet for fagmiljø som planlegger og gjennomfører sikkerhetsrelevante anskaffelser.

Aktuelle bestemmelser for anskaffelser etter sikkerhetsloven (sikkl) fremgår av kapittel 9 og § 1-2 annet ledd. I forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften) er det § 18 og kapittel 13 og som regulerer sikkerhet i anskaffelser og sikkerhetsgraderte anskaffelser. Klareringsforskriften kapittel 4 inneholder relevante bestemmelser for leverandørklarering. Veilederen avgrenses mot generelle anskaffelsesprosedyrer og anskaffelser som følger annen særlovgivning. I punkt 4 vil det helt kort bli redegjort for forholdet mellom sikkerhetsloven og anskaffelsesregelverket.

NSM anbefaler å se veilederen i sammenheng med annet veiledningsmateriale NSM har utarbeidet, blant annet knyttet til gjennomføring av verdi- og skadevurdering, risikostyring og personellsikkerhet. Det vil også være hensiktsmessig å se veilederen i sammenheng med de årlige trussel- og risikovurderingene som utgis av Politiets sikkerhetstjeneste, Etterretningstjenesten og NSM.

På NSM sine nettsider publiseres det skjema og maler som virksomheter kan benytte når de gjennomfører sikkerhetsgraderte anskaffelser. Det presiseres at slike skjemaer og maler bør tilpasses de konkrete anskaffelsene de benyttes i.

2 Vurdering av om en anskaffelse er sikkerhetsgradert

En sikkerhetsgradert anskaffelse er en anskaffelse hvor en leverandør av varer eller tjenester kan få tilgang til eller tilvirker sikkerhetsgradert informasjon, eller hvor leverandøren kan få tilgang til skjermingsverdig objekt eller infrastruktur.¹ Slike verdier har betydning for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser og det stilles derfor strengere krav til gjennomføringen av sikkerhetsgraderte anskaffelser enn for ordinære anskaffelser.

Formålet med reglene om sikkerhetsgraderte anskaffelser er å sikre at leverandøren eller personell fra leverandøren oppfyller de samme krav til sikkerhet som gjelder for oppdragsgiver eller oppdragsgivers personell. Oppdragsgiver er ansvarlig for å ivareta et forsvarlig sikkerhetsnivå i alle deler av egen virksomhet, også for aktivitet som utføres av andre gjennom anskaffelse av varer og tjenester. Leverandører og underleverandører til sikkerhetsgraderte anskaffelser underlegges derfor sikkerhetsloven og må overholde krav til forebyggende sikkerhetsarbeid.² Det bemerkes at krav til forsvarlig sikkerhetsnivå og aktuelle sikkerhetstiltak hos leverandøren må tilpasses ut fra faktiske behov i og krav til anskaffelsen. Det er kun de deler av sikkerhetsloven som er relevant for anskaffelsen som leverandøren må forholde seg til. Dersom leverandøren eksempelvis får tilgang til sikkerhetsgradert informasjon, må leverandøren blant annet forholde seg til krav knyttet til informasjons- og personellsikkerhet.

¹ Jf. sikkl § 9-1, jf. §§ 5-3 og 7-1.

² Jf. sikkl § 1-2 annet ledd, jf. kapittel 4.

Selv om oppdragsgiver konkluderer med at det ikke er en sikkerhetsgradert anskaffelse, er det viktig å være oppmerksom på at dette kan endre seg underveis i anskaffelsesprosessen. Anskaffelser kan være komplekse, langvarige og det kan skje endringer knyttet til verdi, sårbarhet og trussel underveis. Det må fortløpende tas stilling til endringer som kan påvirke vurderingen av hvordan anskaffelsen må gjennomføres og om regelverket for sikkerhetsgraderte anskaffelser kommer til anvendelse.

2.1 Kompetanse

En forutsetning for å gjennomføre gode og dekkende vurderinger av hvilke behov som gjør seg gjeldende i den enkelte anskaffelse og tilrettelegge prosessen best mulig, er at oppdragsgiver sikrer riktig kompetanse inn i anskaffelsesprosessene. Det kreves både kunnskap om, og kompetanse på, gjennomføring av anskaffelser og ivaretagelse av helhetlig sikkerhet. Videre er det nødvendig med avtalekompetanse for å sikre godt utarbeidede kontrakter som ivaretar sikkerhet og oppdragsgivers behov for kontroll i hele prosessen. Involvering av brukere av det som anskaffes kan også bidra positivt i arbeidet med å ivareta sikkerhetshensyn og implementere riktige sikkerhetstiltak.

2.2 Oppdragsgivers verdier

Oppdragsgiver må avklare hvilke verdier anskaffelsen kan gi tilgang til og hvilken betydning disse har for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser. Det er kun tilgang til sikkerhetsgradert informasjon, skjermingsverdig objekt og skjermingsverdig infrastruktur som kan gjøre en anskaffelse sikkerhetsgradert.

Sikkerhetsgradert informasjon er informasjon som må beskyttes fordi det kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende. Det er virksomheten som tilvirker informasjonen som er ansvarlig for å vurdere skadepotensial og sikkerhetsgradere informasjonen på riktig nivå.

Objekter og infrastruktur er skjermingsverdig dersom det kan skade grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser om de får redusert funksjonalitet eller om de blir utsatt for skadeverk, ødeleggelse eller rettstridig overtakelse. Det er ansvarlig sektordepartementet som utpeker og klassifiserer slike verdier.

2.2.1 Fremtidige verdier

Anskaffelser kan knytte seg til utvikling eller produksjon av produkter eller etablering av objekter, som man på forhånd ikke vet verdien til. Et eksempel på dette kan være oppføring av et bygg eller utvikling av et informasjonssystem som på sikt kan komme til å bli utpekt som skjermingsverdig. Det kan også tenkes tilfeller hvor det er behov for konfidensialitet i tilknytning til teknologien som er benyttet for å utvikle noe, eller hvordan noe er bygd opp. I tilfellene der det på forhånd ikke er avgjort hvilken verdi noe vil få, må anskaffelsen gjennomføres med utgangspunkt i antatt fremtidig verdi basert på vurderinger av mulig skadepotensial for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser.

Det kan være utfordrende å gjennomføre vurderinger av hvilken verdi og beskyttelsesbehov noe vil kunne komme til å få i fremtiden. Oppdragsgiver må etter beste evne gjennomføre kvalifiserte vurderinger av hvilken betydning noe som tilvirkes kan få for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser, herunder potensielt skadepotensial ved bortfall av konfidensialitet, tilgjengelighet eller integritet. Videre må oppdragsgiver må ha oversikt over

virksomhetens samlede aktiviteter og verdier, og evne å se dette i sammenheng. Hvordan lignende verdier har blitt vurdert tidligere eller hvordan tilsvarende anskaffelsesprosesser har blitt gjennomført, både internt og eksternt, kan være nyttig å se hen til. Vurderingene må inkludere tilgjengelig og oppdatert informasjon om aktuelle sårbarheter og trusler. Oppdragsgiver bør fortløpende gjennomføre vurderinger ved endringer i verdi, trussel og sårbarhet.

At endelig verdi ikke er avklart avskjærer ikke muligheten for å gjennomføre anskaffelsen som en sikkerhetsgradert anskaffelse, da sikkerhetsloven ikke stiller krav om leverandøren *skal* få tilgang til sikkerhetsgradert informasjon eller skjermingsverdig objekt eller infrastruktur. Hvilke sikkerhetstiltak som stilles til tilbydere eller valgte leverandører kan imidlertid ikke basere seg på urealistiske antagelser om at noe på sikt vil bli gradert eller klassifisert på et gitt nivå. Krav om nødvendighet og forholdsmessighet vil begrense oppdragsgivers handlingsrom. Noen sikkerhetstiltak er mer inngripende enn andre og vil kreve at oppdragsgiver er mer sikker på fremtidig verdi for å kunne iverksettes, eksempelvis leverandørklarering. Dersom det er stor usikkerhet omkring fremtidig verdi og ønskede sikkerhetskrav ikke kan implementeres i anskaffelsesprosessen, må oppdragsgiver vurdere om det kan være andre egnede tiltak som kan ivareta sikkerheten i anskaffelsen. Eksempler på dette gis i punkt 4 i veilederen.

En anskaffelse som ikke var sikkerhetsgradert ved kontraktsinngåelse, men som i ettertid endrer karakter og som medfører at leverandøren kan få tilgang til sikkerhetsgradert informasjon, skjermingsverdig objekt eller infrastruktur, må oppfylle de krav som stilles til sikkerhetsgraderte anskaffelser.

2.3 Leverandør

Leverandørbegrepet i sikkerhetsgraderte anskaffelser omfatter både hoved- og underleverandører.³ Tilbydere vil også være omfattet av begrepet dersom det skal gis tilgang til sikkerhetsgradert informasjon, skjermingsverdig objekt eller infrastruktur allerede i tilbudsfasen.

Selv om anskaffelsen innebærer at det kun er enkeltpersoner hos leverandøren som skal utføre arbeid for oppdragsgiver og få tilgang til oppdragsgivers verdier i oppdragsgivers lokaler, vil dette likevel være å anse som en sikkerhetsgradert anskaffelse. Det vises til bruk av begrepet «tjeneste» i sikkerhetsloven og at arbeidet leverandørens personell skal utføre er tjenesten som anskaffes. Leverandørens mulighet til å få tilgang til oppdragsgivers verdier gjennom egne ansatte, medfører at leverandørens personell må identifiseres med leverandøren.

Om leverandøren skal råde over sikkerhetsgraderte eller klassifiserte verdier i eller fra egne lokaler eller om det bare er personellet som får tilgang til sikkerhetsgraderte eller klassifiserte verdier i oppdragsgivers lokaler, vil ha betydning for hvilke og hvor omfattende krav sikkerhetsloven stiller til anskaffelsesprosessen. Dersom tilgang til aktuelle verdier skjer i eller fra leverandørens egne lokaler stilles det mer omfattende krav til innholdet i sikkerhetsavtalen enn om tilgangen skjer fra oppdragsgivers lokaler. Se mer om dette i punkt 3.

2.4 Tilgang til

For å avklare om anskaffelsen er en sikkerhetsgradert anskaffelse må oppdragsgiver få klarhet i om leverandøren kan få tilgang til oppdragsgivers verdier. Det er ikke et krav om at leverandøren *skal* få

³ jf. Prop 153 L (2016-2017) punkt 19.9 (merknad til § 9-1).

tilgang for at anskaffelsen omfattes av regelverket for sikkerhetsgraderte anskaffelser. Tilgang omfatter både fysisk og logisk tilgang til oppdragsgivers verdier.

En tilgang som gir leverandøren innsikt i sikkerhetsgradert informasjon medfører at anskaffelsen er sikkerhetsgradert, basert på konfidensialitetshensyn. En anskaffelse som gir tilgang som innebærer at leverandøren kan endre, ødelegge, skade eller fjerne et skjermingsverdig objekt eller infrastruktur er sikkerhetsgradert med begrunnelse i tilgjengelighets- og/eller integritetshensyn. Sonderingen mellom hvilke beskyttelseshensyn som er førende for anskaffelsen, gir seg utslag i hvilke sikkerhetskrav som må implementeres for å sikre et forsvarlig sikkerhetsnivå.

Oppdragsgiver må derfor få klarhet i hvilke tilganger leverandøren må ha for å utføre sitt oppdrag, og om disse vil kunne gi tilgang til sikkerhetsgradert informasjon, skjermingsverdig objekt eller skjermingsverdig infrastruktur. Oppdragsgiver må ha kunnskap om hvilket handlingsrom en gitt tilgang gir og hvordan denne eventuelt kan misbrukes. Et eksempel på tilgang som gir mulighet for misbruk kan være anskaffelse av komponenter til et skjermingsverdig objekt eller infrastruktur, hvor komponentene kan inneholde en bakdør som kan gi tilgang til systemet på et senere tidspunkt. Dette må også sees i sammenheng med hvilke sikkerhetstiltak som er innført hos oppdragsgiver. Dersom det i et bygg ikke er innført soneinndeling med ulike tilgangsnivåer kan tilgang til bygget gi omfattende innpass til eventuelle verdier som befinner i bygget.

Vurderingen av om en leverandør kan få tilgang til oppdragsgivers verdier må være realistisk, ikke enhver tenkt mulighet vil være tilstrekkelig. Risikoaksepten er lavere for høyt graderte eller klassifiserte verdier, sammenlignet med verdier som er gradert eller klassifisert på et lavere nivå.

3 Sikkerhetskrav i sikkerhetsgraderte anskaffelser

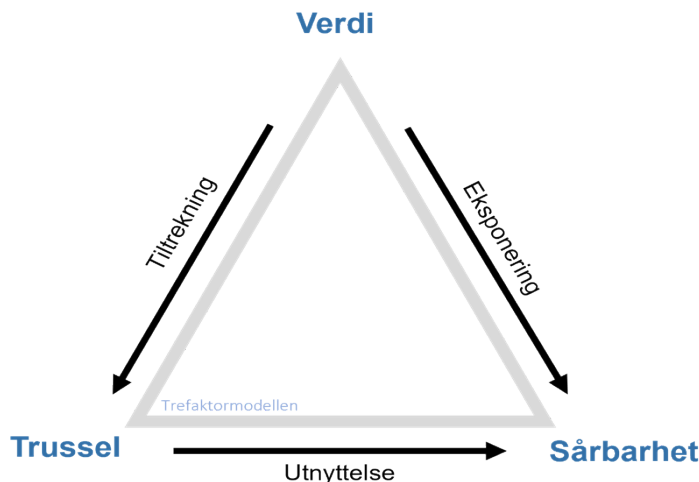
Sikkerhet skal være en integrert del av hele anskaffelsesprosessen. Kravene som stilles i forbindelse med sikkerhetsgraderte anskaffelser må sees i sammenheng med virksomheters plikt til å opprettholde et forsvarlig sikkerhetsnivå og redusere risikoen for sikkerhetstruende virksomhet. Tiltakene som skal implementeres er å anse som sikkerhetstiltak på lik linje med øvrige sikkerhetstiltak sikkerhetsloven stiller krav om.

3.1 Risikovurdering

Oppdragsgiver skal gjennomføre en risikovurdering av anskaffelsen med sikte på å avklare hvilke sikkerhetsbehov som gjør seg gjeldende og hvilke sikkerhetstiltak det er nødvendig å iverksette.⁴ Det er viktig at risikovurderingene tar for seg alle sikkerhetsrelevante forhold ved anskaffelsen. Risikovurderingen må inneholde informasjon om hvilke av oppdragsgivers verdier anskaffelsen kan gi tilgang til og hvilken betydning disse verdiene har for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser. I risikovurderingen må virksomheten også identifisere relevante trusler og avdekke mulige sårbarheter, for å avklare risiko i anskaffelsen og hvordan denne skal håndteres. Det må sikres dokumentasjon

⁴ Jf. sikkf § 4-2 første ledd, jf. 4-3 første ledd, jf. virksomhetsikkerhetsforskriften § 12, tredje ledd.

med gjennomførte risikovurderinger, slik at de er etterprøvbare både for intern og ekstern kontroll.⁵



I trefaktormodellen er risiko et forhold mellom verdi, trusler og sårbarhet. Kilde: NSM.

Anskaffelser kan være komplekse, langvarige og det kan skje endringer knyttet til verdi, sårbarhet og trussel underveis. Det må fortløpende tas stilling til endringer som kan påvirke vurderingen av beskyttelsesbehovet og aktuelle sikkerhetstiltak, og om det er behov for gjennomføring av en ny risikovurdering.

I forkant av at leverandør velges til en anskaffelse må oppdragsgiver avklare om bruk av den konkrete leverandøren kan komme i konflikt med oppdragsgivers plikt til å ivareta et forsvarlig sikkerhetsnivå i anskaffelsen. Det må sees i sammenheng sikkerhetskravene som er oppstilt for anskaffelsen. Videre må oppdragsgiver se hen til tidligere og fremtidige leveranser, og den samlede informasjonsmengden en leverandør kan bli sittende med. Dersom samme virksomhet benyttes som leverandør i flere anskaffelser, kan leverandøren få en oversikt over oppdragsgivers verdier som samlet sett innebærer at anskaffelsen må gjennomføres som en sikkerhetsgradert anskaffelse.

Omfattende bruk av enkeltleverandører eller bruk av leverandører fra samme land eller områder kan i tillegg medføre avhengigheter som kan være uheldig i et sikkerhet- og beredskapsperspektiv. Det vises blant annet til risikoen for at noen aktører kan få stor innflytelse over eller omfattende innsikt i norske verdikjeder. For virksomheter som har sentrale roller i og som må opprettholde leveranser i alle deler av krisespennet, er det spesielt viktig å være oppmerksom på hvilke avhengighetsforhold man har til hvilke aktører. Det er uheldig om man gjør seg helt avhengig av leveranser fra virksomheter eller nasjoner som det er risiko for at kan bli utilgjengelig ved en eskalering i krisespennet eller andre geopolitiske endringer. Nasjonal sikkerhet skal ivaretas i fred, krise og krig. For å redusere risikoen for at man gjør seg for avhengig av enkeltaktører eller at uønskede aktører får innpass i leverandørkjeder, er det viktig at oppdragsgiver har god oversikt over anskaffelser i sin virksomhet og hvilke leverandører de benytter i ulike prosesser. Det omfatter også oversikt over bruk av underleverandører og leverandørkjeden i sin helhet. I sikkerhetsgraderte anskaffelser er oppdragsgiver pålagt å holde slik oversikt.⁶

⁵ Se gjerne hen til anerkjente standarder for gjennomføring av risikovurderinger.

⁶ Jf. virksomhetsikkerhetsforskriften § 86.

3.1.1 Oppdragsgivers varslingsplikt

Risikovurderingen av anskaffelsen kan danne grunnlag for varsling ved risiko for at oppdragsgivers verdier kan bli brukt til sikkerhetstruende virksomhet. Dersom en anskaffelse kan gi leverandøren eller personell hos leverandøren mulighet til å påvirke skjermingsverdig informasjonssystem, objekt eller infrastruktur, må oppdragsgiver ta stilling til om det medfører en ikke ubetydelig risiko for at verdien kan bli rammet av eller brukt til sikkerhetstruende virksomhet.⁷ Plikten til å gjennomføre risikovurdering og eventuell varslingsplikt gjelder ikke utelukkende i sikkerhetsgraderte anskaffelser, men også anskaffelser til skjermingsverdige informasjonssystemer.

Varsling og involvering av myndighetene er ment for spesielle situasjoner hvor risikoen vurderes å være på et nivå utover det som er normalt. I normaltillfeller skal oppdragsgiver selv, ved risikohåndtering og iverksettelse av risikoreduserende tiltak, fjerne eller redusere risikoen til et akseptabelt nivå.

Varselet skal inneholde all informasjon som er relevant for å kunne ta stilling til risikoen forbundet med anskaffelsen.⁸ Varsel skal sendes til ansvarlig sektordepartement, eller NSM dersom virksomheten ikke er underlagt noe departement. Oppdragsgiver skal innen 60 dager fra varselet er mottatt få orientering om anskaffelsen kan gjennomføres eller om saken må behandles av Kongen i statsråd.

3.2 Sikkerhetskrav i konkurransegrunnlaget

Konkurransegrunnlaget bør utarbeides med utgangspunkt i gjennomført risikovurdering og de sikkerhetshensyn som gjør seg gjeldende. Selv om leverandører til sikkerhetsgraderte anskaffelser underlegges sikkerhetsloven og plikter å overholde krav til forebyggende sikkerhetsarbeid, kan det være hensiktsmessig at det tas inn informasjon om dette i konkurransegrunnlaget for å tydeliggjøre rammene for anskaffelsen.

Videre anbefales det at konkurransegrunnlaget inneholder informasjon om spesifikke sikkerhetskrav og -kriterier som gjelder for den konkrete anskaffelsen, såfremt det er informasjon som kan deles. Krav kan knytte seg til tiltak for informasjons-, informasjonssystems-, objekt-, infrastruktur- eller personellsikkerhet. I en sikkerhetsgradert anskaffelse skal det som hovedregel inngås en sikkerhetsavtale mellom oppdragsgiver og leverandør, og da bør det fremgå av konkurransegrunnlaget at det vil stilles krav til inngåelse av en slik avtale. Det vises også til de særskilte krav som gjelder for å kunne godkjenne utenlandske leverandører, herunder at NSM må godkjenne disse før det kan inngås en sikkerhetsavtale.⁹

Dersom det etter regelverket stilles krav om at personell og/eller leverandøren må klareres, bør det informeres om i konkurransegrunnlaget da det ikke er gitt at det vil være mulig å oppfylle for alle leverandører.

Der det fremtidige beskyttelsesbehovet ikke er endelig avklart, bør det tas forbehold om at det kan bli aktuelt å stille ytterligere krav til sikkerhet og hvilke tiltak det kan omfatte.

⁷ Jf. sikkerhetsloven § 9-4, jf. presisering i virksomhetsikkerhetsforskriften § 18 første ledd.

⁸ Se virksomhetsikkerhetsforskriften § 19 første ledd.

⁹ Se sikkerhetsloven § 9-2 første ledd, annet punktum.

Oppdragsgiver bør unngå å inkludere sikkerhetsgradert informasjon i konkurransegrunnlaget, da tilbydere må autoriseres og eventuelt klareres for å få tilgang til informasjonen. I tillegg vil dette medføre at oppdragsgiver som hovedregel må inngå en sikkerhetsavtale med leverandør allerede på dette tidspunktet i anskaffelsen. For å unngå unødig spredning av sikkerhetsgradert informasjon og iverksettelse av inngripende og potensielt tidkrevende klareringsprosesser, bør oppdragsgiver derfor være restriktiv med deling av sikkerhetsgradert informasjon på dette stadiet i anskaffelsesprosessen. Dersom det likevel er nødvendig å dele sikkerhetsgradert informasjon bør tilgang primært gis i oppdragsgivers lokaler, for å begrense behovet for å gjennomføre leverandørklareringer og eventuelle investeringer i sikkerhetstiltak for virksomhetene på dette stadiet.

3.3 Sikkerhetsavtale

Sikkerhetsavtale skal som hovedregel inngås i alle sikkerhetsgraderte anskaffelser.¹⁰ Det gjelder også sikkerhetsgraderte anskaffelser hvor både oppdragsgiver og leverandør er offentlige virksomheter. Formålet med en sikkerhetsavtale er å tydeliggjøre og konkretisere krav sikkerhetsloven og tilhørende forskrifter stiller til oppdragsgiver og leverandør for å ivareta et forsvarlig sikkerhetsnivå i anskaffelsen. I tillegg skal avtalen sikre en omforent forståelse av roller og ansvar i det forebyggende sikkerhetsarbeidet.

Sikkerhetsavtalen skal inngås før leverandøren får tilgang til sikkerhetsgradert informasjon eller utpekte og klassifiserte verdier. Dersom man underveis i anskaffelsesprosessen ser at det er behov for mer eller mindre omfattende sikkerhetskrav, må sikkerhetsavtalen oppdateres slik at den reflekterer de til enhver tid gjeldende krav for anskaffelsen. Sikkerhetsavtalen skal også oppdateres dersom det skjer andre endringer av betydning for ivaretagelse av et forsvarlig sikkerhetsnivå. Behovet for fortløpende vurdering av risiko gjør seg dermed gjeldende før, under og etter at kontrakt er inngått. Kontrakten mellom oppdragsgiver og leverandør bør derfor regulere hvilket handlingsrom oppdragsgiver har til å gjøre endringer i sikkerhetskrav og hvem som skal bære ansvaret for tilleggskostnader som følge av endrede sikkerhetskrav.

Omfanget av sikkerhetsavtalen må ta utgangspunkt i hva som skal anskaffes, hvem som kan få tilgang til oppdragsgivers verdier og hvor tilgangen skal skje fra.¹¹ Sikkerhetsavtalen skal alltid inneholde informasjon om hvilken sikkerhetsgrad anskaffelsen skal ha, spesifisert for hver del av oppdraget, og hvordan leverandøren skal forholde seg til de av lovens krav som gjelder for anskaffelsen. I anskaffelser hvor personell fra leverandøren kun får tilgang til aktuelle verdier hos oppdragsgiver, vil det være hensiktsmessig å innta informasjon om hvilket personell som skal klareres, for hva og hvordan disse skal følges opp. Oppdragsgiver må vurdere konkret hva det er behov for å regulere i sikkerhetsavtalen, og om det er nødvendig å innta elementer utover det som regelverket oppstiller krav om for å oppnå formålet med inngåelse av en sikkerhetsavtale.

For å sikre oppdragsgiver nødvendig oversikt over leverandørkjeden og involverte aktører, kan det være hensiktsmessig at det i sikkerhetsavtalen inkluderes varslingsplikt ved endringer i eierskap og eierskapsstruktur hos leverandøren. Det vises til at leverandører til sikkerhetsgraderte anskaffelser uten leverandørklarering ikke er pålagt noen slik varslingsplikt i regelverket.

¹⁰ Jf. sikkf § 9-2 første ledd.

¹¹ Jf. sikkf § 9-2 annet ledd for minimumskrav til innholdet i sikkerhetsavtalen og virksomhetsikkerhetsforskriften § 80 for krav i de tilfeller hvor leverandøren skal få tilgang fra egne lokaler.

Dersom underleverandører har behov for tilgang til sikkerhetsgradert informasjon, skjermingsverdig objekt eller infrastruktur, må oppdragsgiver inngå sikkerhetsavtale med hver enkelt av disse. Hovedleverandør har ikke anledning til å gi tilgang til slike verdier uten at det er godkjent av oppdragsgiver. Hovedleverandøren må derfor holde oppdragsgiver fortløpende orientert om endringer knyttet til bruk av underleverandører. Det bør inntas krav om dette i sikkerhetsavtalen mellom oppdragsgiver og leverandør.

En sikkerhetsavtale må ikke utformes som et selvstendig avtaledokument og kan inntas i det ordinære avtaledokumentet for anskaffelsen, dersom det er hensiktsmessig.

3.3.1 Unntak fra krav om sikkerhetsavtale

Dersom leverandørens personell kun får tilgang til sikkerhetsgradert informasjon, skjermingsverdige objekter eller infrastruktur under oppsyn av en representant fra oppdragsgiver, kreves det ikke sikkerhetsavtale. I slike tilfeller kan det inntas en bestemmelse i kontrakten med leverandøren som beskriver ordningen.¹²

At personell skal holdes «under oppsyn» kan skje både ved fysisk og logisk kontroll. Som eksempler nevnes ledsagelse, tilgangsbegrensninger og/eller overvåkning i virksomhetens informasjonssystemer.¹³ At personellet holdes under oppsyn innebærer at oppdragsgiver til enhver tid må ha kontroll med hvor leverandørens personell befinner seg og/eller hva disse gjør. En tilfredsstillende kontroll forutsetter at de som gjennomfører denne har tilstrekkelig kompetanse til å forstå hvordan gitt tilgang skal brukes og avdekke om det skjer avvik fra dette. All tilgang som kan misbrukes på en måte som kan skade grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser bør kunne kontrolleres av oppdragsgiver. Dersom dette er en risiko ved anskaffelsen må oppdragsgiver sikre nødvendig grad av oppsyn med leverandørens arbeidsutførelse. Terskelen er derfor høy for å gjøre unntak fra kravet om sikkerhetsavtale.

At personellet må holdes under oppsyn gjelder uavhengig av om de aktuelle personene er klarert og autorisert for tilgang på aktuelle nivåer. Skal personellet ha selvstendig tilgang er det krav om at det inngås en sikkerhetsavtale.

Det kan være hensiktsmessig å konkretisere de sikkerhetsmessige aspektene ved anskaffelsen i kontrakten med leverandøren, selv om det er anledning til å gjøre unntak fra kravet om sikkerhetsavtale. Det sentrale er at alle parter er omforent om og kjent med hvordan anskaffelsen skal utføres i tråd med aktuelle sikkerhetskrav.

3.4 Leverandørklarering

Leverandørklarering er et tiltak som kun kan benyttes i sikkerhetsgraderte anskaffelser. Det er et inngripende tiltak og skal kun benyttes når regelverket sier det er nødvendig for å oppnå et forsvarlig sikkerhetsnivå.

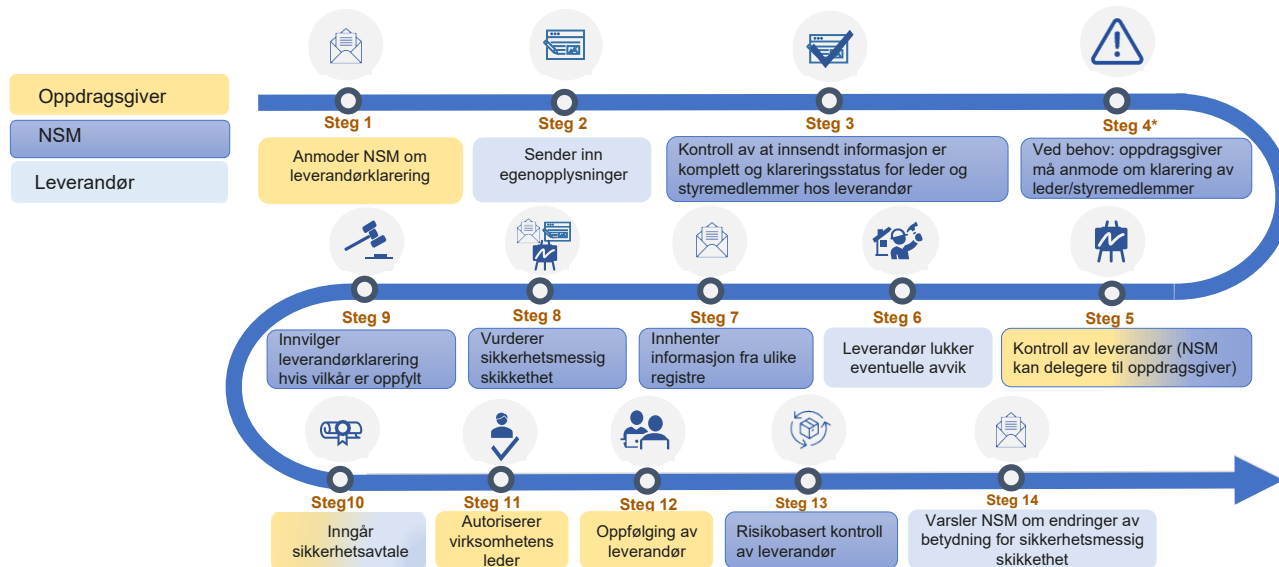
Formålet med leverandørklarering er å sikre kontroll med og tillit til leverandører av varer eller tjenester som kan ha betydning for nasjonal sikkerhet. Både leverandøren og personer i dennes styre og ledelse skal klareres, som et ledd i vurderingen av om leverandøren er sikkerhetsmessig

¹² Jf. virksomhets sikkerhetsforskriften § 81 og Prop. 153 L, punkt 13.4.3, side 142.

¹³ Jf. høringsnotat til forslag til forskrifter til ny sikkerhetslov (02.07.2018), punkt 7.11.3.

skikket til å få tilgang til sikkerhetsgradert informasjon eller skjermingsverdig objekt eller infrastruktur.¹⁴

Leverandørklaringsprosess: norske leverandører



*Den videre prosessen forutsetter at nødvendige klareringer gis

Figuren illustrerer gangen i en sikkerhetsgradert anskaffelse hvor leverandøren skal klareres. Kilde: NSM.

3.4.1 Krav om leverandørklarering

I følgende tilfeller er det nødvendig med leverandørklarering:¹⁵

- Leverandøren skal ha tilgang til eller oppbevare informasjon gradert KONFIDENSIELT eller høyere i egne informasjonssystemer eller lokaler.
- Leverandøren skal ha elektronisk tilgang til objekt eller infrastruktur klassifisert KRITISK eller MEGET KRITISK fra egne informasjonssystemer eller lokaler.
- Leverandøren skal råde over objekter eller infrastruktur som tilhører oppdragsgiver, og som er klassifisert KRITISK eller MEGET KRITISK.

Begrepet «råde over» skal forstås som de tilfeller hvor leverandøren har objektet eller infrastrukturen i sin besittelse, og omfatter både fysisk og elektronisk rådighet.¹⁶ I tilfeller hvor leverandøren har «elektronisk tilgang» fra egne informasjonssystemer eller lokaler, kan leverandøren i noen tilfeller også «råde over» objektet eller infrastrukturen. Hvorvidt tilgangen faller inn under andre eller tredje kulepunkt er imidlertid ikke avgjørende for om det kreves leverandørklarering.

¹⁴ Se sikk § 9-3 jf. klareringsforskriften kapittel 4

¹⁵ Jf. sikk § 9-3 første ledd, jf. virksomhetssikkerhetsforskriften § 83.

¹⁶ Jf. høringsnotat til forslag til forskrifter til ny sikkerhetslov (02.07.2018), punkt 7.11.5.

Virksomheter underlagt loven som følge av at de er offentlige organer eller fordi det er fattet vedtak om at loven skal gjelde for dem,¹⁷ skal ikke leverandørklareres når de er leverandører til sikkerhetsgraderte anskaffelser. I disse tilfellene er det kun behov for sikkerhetsavtale.

3.4.2 Andre tilfeller hvor leverandørklarering kan være aktuelt

Utover de opplistede tilfellene hvor det kreves leverandørklarering, må det vurderes konkret om tiltaket er nødvendig. I vurderingen vil det være relevant å se hen til hvilke verdier anskaffelsen knytter seg til, verdienes betydning for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser, hvem som får tilgang og hvor tilgangen skjer fra. Under følger eksempler på tilfeller hvor leverandørklarering *kan* være nødvendig for å ivareta et forsvarlig sikkerhetsnivå i anskaffelsen:

- I anskaffelser hvor endelig verdi ikke er avklart, eller det er sannsynlig at skadepotensialet ved bortfall i fremtiden vil øke (se punkt 2.2.1). Terskelen vil imidlertid være høy i slike tilfeller og det vil stilles strenge krav til nødvendigheten av tiltaket.
- I tilfeller hvor tilgang til verdier bare skjer hos oppdragsgiver kan det være behov for leverandørklarering om verdiene er høyt gradert eller klassifisert og har et særlig beskyttelsesbehov.
- Dersom en leverandør benyttes inn i flere sikkerhetsgraderte anskaffelser kan den totale oversikten leverandøren får over skjermingsverdige verdier bli svært omfattende. Mengden informasjon kan tilsa at det er behov for en større grad av kontroll med leverandøren og dens sikkerhetsmessige skikkethet.
- Det kan videre være behov for leverandørklarering ved tilgang til objekter og infrastruktur klassifisert på lavere nivå (VIKTIG). Som eksempel vises det til objekter og infrastruktur som i utgangspunktet har stor betydning for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser, men som er klassifisert på et lavere nivå grunnet høy grad av redundans og/eller reparasjonskapasitet eller lignende forhold.
- For objekter eller infrastrukturer med tilsvarende eller lignende funksjonalitet med store likheter knyttet til sårbarheter, beskyttelsesbehov og innførte sikkerhetstiltak. Tilgang til eller informasjon om et objekt eller en infrastruktur kan da gi tilgang til eller informasjon om lignende objekter eller infrastrukturer. Det bør tas stilling til hvilken oversikt og hvilke tilganger leverandøren i realiteten får. Dette punktet kan gjerne sees i sammenheng med forrige punkt.

3.4.3 Leverandørklaringsprosessen

Leverandørklarering skal være innvilget før det gis tilgang til sikkerhetsgradert informasjon, skjermingsverdig objekt eller infrastruktur, uavhengig av når i anskaffelsesprosessen behovet oppstår.

Bestemmelsene om personellsikkerhet i sikkerhetsloven kapittel 8 gjelder så langt de passer for leverandørklaringsprosessen.¹⁸ Det er i all hovedsak bestemmelsene om klage og begrunnelse som vil få tilsvarende anvendelse.¹⁹

¹⁷ Jf. sikk1 § 1-3

¹⁸ Jf. sikk1 § 9-3 femte ledd.

¹⁹ Se Prop. 153 L (2016-2017), punkt 19.9 (merknaad til § 9-3).

3.4.3.1 Anmodning om leverandørklarering

NSM er klareringsmyndighet for leverandørklareringer og skal føre register over innvilgede klareringer.²⁰

Det er oppdragsgiver som skal anmode NSM om leverandørklarering, ettersom oppdragsgiver har oversikt over og kan begrunne hvorfor det er et behov for klarering.²¹ Klareringsforespørsler skal avslås dersom det ikke foreligger et faktisk behov, da det ikke unødig skal iverksettes sikkerhetstiltak som griper inn i virksomhetens og enkeltpersoners rettsfære.²²

Forespørselen skal inneholde informasjon om det høyeste graderings- eller klassifiseringsnivået i anskaffelsen, leverandørens samtykke til at NSM gjennomfører kontroll, og opplysninger fra leverandøren knyttet til egen virksomhet.²³

Oppdragsgiver må i forespørselen angi hva leverandøren og dets personell kan få tilgang til av verdier. Dette får betydning for omfanget av personkontrollen øverste ledelse og personellet skal gjennom. For tilgang til objekter og infrastruktur som er utpekt og klassifisert som skjermingsverdige objekter, er det adgangsklarering som skal benyttes.²⁴ For tilgang til informasjon som er sikkerhetsgradert KONFIDENSIELT eller høyere skal sikkerhetsklarering benyttes. En sikkerhetsklarering for KONFIDENSIELT eller høyere vil også gi adgang til skjermingsverdige objekter og infrastrukturer på alle klassifiseringsnivåer.²⁵

3.4.3.2 Sikkerhetsklarering av virksomhetens leder og styremedlemmer

Styret og leder hos leverandøren skal klareres på det samme nivået som det er bedt om leverandørklarering for.²⁶ Kravet begrunnes i nevnte personer sin innflytelse over og tilganger i virksomheten. Krav om klarering av virksomhetens leder vil som utgangspunkt gjelde daglig leder. Daglig leder vil normalt vil være ansvarlig for virksomhetens sikkerhetsstyringssystem og beskyttelse av verdier virksomheten råder over, og kan derfor tilegne seg tilgang til disse. Hva gjelder styremedlemmer, må disse ha innsyn i virksomhetens informasjon for å kunne ivareta sitt ansvar. Det innebærer at de kan få tilgang til sikkerhetsgradert informasjon eller skjermingsverdig objekt eller infrastruktur. Personkontrollen av virksomhetens leder og styremedlemmer skal derfor inngå i vurderingsgrunnlaget for om det skal gis leverandørklarering.²⁷

Om noen i virksomhetens styre eller dennes leder ikke kan klareres, eksempelvis som følge av manglende tilknytning til Norge, kan leverandørklarering likevel gis dersom vedkommende gir avkall på retten til innsyn.²⁸ Det må likevel være tilstrekkelig antall sikkerhetsklarerte styremedlemmer til at styret er beslutningsdyktig. Dette vil legge begrensinger på hvor mange styremedlemmer som kan gi avkall på retten til innsyn.

NSM må få informasjon om hvordan leverandøren sikrer at avkallet er reelt og at aktuelle personer ikke vil få tilgang til sikkerhetsgradert informasjon, skjermingsverdig objekt eller infrastruktur. Som

²⁰ Jf. klareringsforskriften § 32 og klareringsforskriften § 39.

²¹ Jf. virksomhetsikkerhetsforskriften § 85 og klareringsforskriften § 3 annet ledd.

²² Jf. sikkl §§ 8-2 første ledd og 8-3 første ledd, jf. klareringsforskriften § 4

²³ Se klareringsforskriften § 34 og skjemaer til bruk ved leverandørklarering på NSM sin nettside.

²⁴ Jf. sikkl § 8-3 første ledd, jf. § 7-1 første og annet ledd.

²⁵ Jf. klareringsforskriften § 16.

²⁶ Jf. klareringsforskriften § 33 annet ledd.

²⁷ Jf. sikkl § 9-3 annet ledd.

²⁸ Jf. klareringsforskriften § 33 tredje ledd.

klareringsmyndighet er det NSM som avgjør om avkall på retten til innsyn gir mulighet til innvilgelse av leverandørklarering.

3.4.3.3 *Kontroll av leverandør*

Før en leverandør kan klareres, skal NSM kontrollere at leverandøren oppfyller de krav til sikkerhetsstyring og beskyttelse av skjermingsverdige verdier som er relevante for den konkrete anskaffelsen.²⁹ Kontrollen kan skje ved innhenting av dokumentasjon, stedlig revisjon eller ved inspeksjoner. Det skal være notoritet med gjennomførte kontroller, i form av at det utarbeides en rapport.

Etter avtale med NSM kan kontrollen gjennomføres av oppdragsgiver. Oppdragsgiver må i slike tilfeller utarbeide en rapport fra kontrollen som vil inngå i klareringsmyndighetens vurdering av om leverandørklarering skal gis.

Dersom det i klareringsperiodens gyldighetstid skjer endringer eller det fremkommer opplysninger av betydning for vurderingen av om leverandøren er sikkerhetsmessig skikket, skal det gjennomføres ny kontroll med leverandøren. Det kan oppstå situasjoner som endrer klareringsmyndighetens tidligere vurdering av om leverandøren er sikkerhetsmessig skikket til å inneha leverandørklarering. Leverandøren skal skriftlig varsles om at det skal gjennomføres kontroll, såfremt det ikke er nødvendig å unnlate varsel av sikkerhetshensyn.

3.4.3.4 *Vurderingsgrunnlag*

Innvilgelse av leverandørklarering forutsetter at det ikke er noen rimelig grunn til å betvile leverandørens sikkerhetsmessige skikkethet. I vurderingen er det kun forhold som kan innvirke på leverandørens evne og vilje til å gjøre forebyggende sikkerhetsarbeid som skal vektlegges. Leverandøren må derfor oppfylle relevante krav i sikkerhetsloven og virksomhetsikkerhetsforskriften før en leverandørklarering kan innvilges.³⁰

NSM må ha nødvendig grad av tillit til at virksomheten som klareres vil opptre i henhold til sikkerhetslovens krav. Det sentrale i vurderingen av leverandørens sikkerhetsmessige skikkethet er at det ikke foreligger forhold som gir grunn til å tro at leverandøren vil kunne opptre i strid med nasjonale sikkerhetsinteresser. For å kunne foreta en kvalifisert vurdering av dette er NSM avhengig av et godt informasjonsgrunnlag. Som ledd i informasjonsinnhenting skal leverandøren selv gi informasjon om egen virksomhet, i tillegg til at NSM kan innhente informasjon fra relevante registre.³¹ Kontrollrapporter skal inngå i vurderingsgrunnlaget, se punkt 3.5.3.3. Hvis det er gjennomført tilsyn etter sikkerhetsloven med leverandøren, vil det være relevant å innhente tilsynsrapporten.

Informasjon om økonomiske forhold, tilknytning til andre stater og virksomhetens eventuelle straffehistorikk er eksempler på forhold som kan være relevant i vurderingen av sikkerhetsmessig skikkethet. Økonomiske utfordringer kan føre til at man lar seg friste til å handle i strid med nasjonale sikkerhetsinteresser, dersom det medfører økonomisk vinning. Slike utfordringer kan også gi indikasjoner på en virksomhets evne og vilje til å ivareta sine forpliktelser. Dersom det foreligger tilknytning til andre stater må det blant annet tas stilling til om tilknytningen er av en slik art at det foreligger en risiko for at virksomheten kan havne i en lojalitetskonflikt, eller være sårbar for press, fristelser eller forledelser. Det kan også sees hen til relevante forhold ved leverandørens

²⁹ Jf. klareringsforskriften § 36.

³⁰ Jf. klareringsforskriften § 33 første ledd.

³¹ Jf. klareringsforskriften §§ 34 og 35.

ledelse og styre, siden de vil kunne påvirke virksomhetens evne og vilje til å utføre forebyggende sikkerhetsarbeid. Alle relevante forhold skal vurderes, både de som taler for og imot at klarering gis.

Kommer NSM frem til at det er grunn til å betvile leverandørens sikkerhetsmessige skikkethet eller at leverandøren ikke oppfyller nødvendige krav, skal ikke klarering gis. I slike tilfeller vil hensynet til nasjonal sikkerhet veie tyngre enn hensynet til oppdragsgiver og leverandøren, og deres behov for at leverandøren klareres. En klarering kan gis på vilkår dersom det kan redusere risikoen til et akseptabelt nivå.

Ved en reklarering må NSM på ny ta stilling til om leverandøren er sikkerhetsmessig skikket, basert på et oppdatert informasjonsgrunnlag og ny kontroll av virksomheten.

3.4.3.5 Leverandørklareringstidens gyldighetstid og endringer i klareringstidens gyldighet

Leverandørklareringer kan vare i inntil fem år, men kan også gis for en kortere tidsperiode dersom det på klareringstidspunktet er klart at det ikke er behov for en varighet på fem år.³²

Leverandørklarerte virksomheter plikter å orientere NSM om endringer som kan påvirke vurderingen av om leverandøren er sikkerhetsmessig skikket.³³ Det stilles krav om at det varsles om endringer i styret eller ledelsen, endringer i eierstrukturen, flytting av lokaliteter og utstyr, åpning av gjeldsforhandlinger, begjæring om konkurs og annet relevante forhold.

Dersom det i klareringstidens gyldighetstid oppstår en sikkerhetsrisiko som ikke kan fjernes eller det oppdages avvik fra gjeldende sikkerhetskrav, kan klareringen tilbakekalles.³⁴ Som utgangspunkt skal det fastsettes en rimelig frist for retting før en klarering tilbakekalles. Hva som er en rimelig frist må ta utgangspunkt i en konkret vurdering av forholdets alvorlighetsgrad og konsekvensene opp mot nasjonale sikkerhetsinteresser. Avvik som er av en slik karakter at det umiddelbart kan få negative konsekvenser for nasjonale sikkerhetsinteresser, kan gi grunnlag for å tilbakekalle leverandørklareringen uten at det er gitt forutgående frist. Et eksempel på dette kan være tilfeller hvor leverandøren gir tilgang til sikkerhetsgradert informasjon eller skjermingsverdige objekter, uten at det føres kontroll med om de som har fått tilgang har nødvendig klarering og/eller autorisasjon.

3.4.4 Autorisasjon

I tillegg til gyldig klarering, må de som skal gis tilgang til sikkerhetsgradert informasjon, skjermingsverdige objekter eller infrastruktur være autorisert.³⁵ Virksomhetens leder er autorisasjonsansvarlig og har ansvar for sikkerhetsmessig ledelse og kontroll av autoriserte personer. For leverandører til sikkerhetsgraderte anskaffelser vil virksomhetens leder være daglig leder eller den med tilsvarende innflytelse over virksomhetens drift.³⁶

I sikkerhetsgraderte anskaffelser er det oppdragsgiver som skal autorisere autorisasjonsansvarlig hos leverandøren.³⁷ Dette begrunnes i at det er oppdragsgiver som eier aktuelle verdier og har ansvar for å ivareta et forsvarlig sikkerhetsnivå for verdiene. Personell hos leverandøren som kun får tilgang til sikkerhetsgradert informasjon, skjermingsverdig objekt eller infrastruktur hos oppdragsgiver, skal derfor også autoriseres av oppdragsgiver. I de tilfeller hvor tilgangen skjer fra leverandørens egne informasjonssystemer eller lokaler, eller leverandøren råder over verdiene i

³² Jf. klareringsforskriften § 38.

³³ Jf. sikkl § 9-3 fjerde ledd.

³⁴ Jf. sikkerhetsloven § 9-3 fjerde ledd, jf. klareringsforskriften § 37.

³⁵ Jf. sikkl § 8-1 første ledd, jf. § 8-9.

³⁶ Se høringsnotat til forslag til forskrifter til ny sikkerhetslov (02.07.2018), punkt 8.5.3.

³⁷ Jf. virksomhetsikkerhetsforskriften § 69.

egne lokaler, er det autorisasjonsansvarlig hos leverandøren som skal autorisere leverandørens personell.

Dersom oppdragsgiver er utenlandsk, er NSM ansvarlig for å autorisere autorisasjonsansvarlig hos den norske leverandøren.

3.5 Oppdragsgivers oppfølging av leverandørforhold

Selv om leverandøren har et selvstendig ansvar for iverksetting av nødvendige sikkerhetstiltak, har oppdragsgiver et sikkerhetsmessig oppfølgingsansvar overfor leverandøren. Oppdragsgiver skal forsikre seg om at leverandøren har nødvendig risiko- og sikkerhetsforståelse og at leverandøren oppfyller krav til forebyggende sikkerhetsarbeid som er nødvendig i den konkrete anskaffelsen.³⁸ Det er viktig at oppdragsgiver etablerer gode mekanismer for å følge opp leverandører de benytter i sin virksomhet, slik at de får informasjon om endringer eller hendelser som kan ha påvirkning på vurderingen av risiko og hvilke sikkerhetstiltak som er nødvendig.

Oppdragsgiver skal ha oversikt over alle sikkerhetsgraderte anskaffelser de gjennomfører, og hvilke leverandører og underleverandører de benytter seg av i sikkerhetsgraderte anskaffelser. Oversikten over pågående sikkerhetsgraderte anskaffelser skal årlig oversendes til NSM som er ansvarlig for å føre register over sikkerhetsgraderte anskaffelser. Med hensynvisning til NSM sitt ansvar for å gjennomføre tilsyn med leverandører til sikkerhetsgraderte anskaffelser er det viktig at oppdragsgivere overholder plikten til å føre oversikt og formidle denne til NSM.³⁹ I tillegg til den årlige oversikten er det ønskelig at virksomheter holder NSM fortløpende oppdatert om leverandører de benytter i sikkerhetsgraderte anskaffelser og nivå på anskaffelsen, slik at NSM til enhver tid har oversikt over hvilke virksomheter som er underlagt sikkerhetsloven som leverandører.

3.6 Utenlandske leverandører

Leverandører som driver virksomheten fra et annet land og under et annet lands jurisdiksjon er å anse som utenlandsk i forbindelse med sikkerhetsgraderte anskaffelser. Norge har en rekke multi- og bilaterale sikkerhetsavtaler med andre land. Disse regulerer hvordan sikkerhetsgradert informasjon som utveksles over landegrensene skal behandles og etablerer en gjensidig plikt til å beskytte sikkerhetsgradert informasjon som utveksles og/eller tilvirkes. Dette gjør det mulig for norske oppdragsgivere å benytte seg av utenlandske leverandører. En forutsetning for å kunne benytte en utenlandsk leverandør i en sikkerhetsgradert anskaffelse er at det foreligger en slik bi- eller multilateral avtale mellom norske myndigheter og myndighetene i landet leverandøren holder til i eller driver fra.⁴⁰

All kommunikasjon med utenlandske sikkerhetsmyndigheter i forbindelse med sikkerhetsgraderte anskaffelser skal gå via NSM.

3.6.1 Sikkerhetsavtale

Dersom en utenlandsk leverandør eller leverandørens personell skal få tilgang til sikkerhetsgradert informasjon eller det er nødvendig med klarering av leverandør og/eller personellet, skal NSM

³⁸ Jf. sikk § 4-1 annet ledd og Prop. 153 L (2016-2017), punkt 19.4 (merknad til § 4-1).

³⁹ jf. Jf. klareringsforskriften § 39 annet ledd og virksomhetsikkerhetsforskriften § 88.

⁴⁰ Jf. virksomhetsikkerhetsforskriften §§ 25 og 84.

godkjenne leverandøren før det inngås en sikkerhetsavtale.⁴¹ Oppdragsgiver må derfor fremsende en forespørsel til NSM med navn på leverandøren og landet denne er lokalisert i fremkommer.

Dersom NSM godkjenner den utenlandske leverandøren og det inngås en sikkerhetsavtale mellom oppdragsgiver og leverandøren, skal oppdragsgiver sende kopi av sikkerhetsavtalen til NSM. NSM vil fremsende denne til sikkerhetsmyndigheten i landet hvor leverandøren er lokalisert, hvor den kan tjene som grunnlag for kontroll med leverandøren. Internasjonalt vil disse avtalene gjerne bli omtalt som *Security Clauses*, *Security Aspect letter (SAL)* eller *Project Security Instructions (PSI)*.

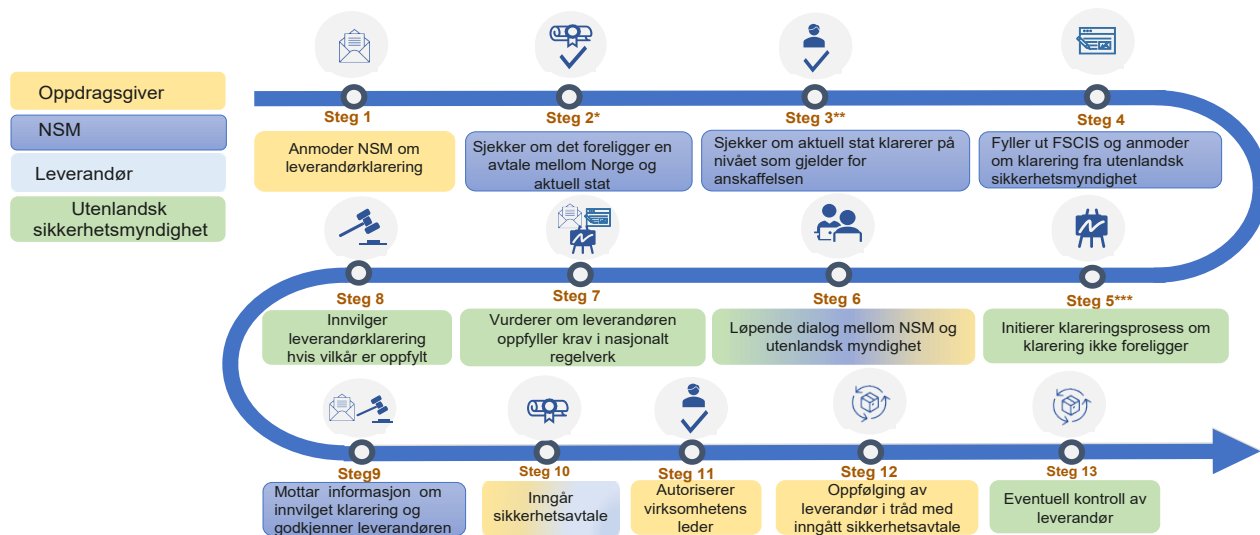
3.6.2 Leverandørklarering

Hvis leverandøren ikke har leverandørklarering og dette er et krav i anskaffelsen, er det myndighetene i hjemstaten som skal klarere leverandøren.⁴² Internasjonalt betegnes leverandørklarering som *Facility Security Clearance (FSC)*. Oppdragsgiver må sende anmodning om leverandørklarering til NSM, som videresender anmodningen til sikkerhetsmyndigheten i leverandørens hjemstat.⁴³ Den annen stats sikkerhetsmyndighet vil gi en bekreftelse tilbake til NSM om, eller når, en leverandørklarering foreligger, og NSM vil deretter informere oppdragsgiver om dette.

I den sikkerhetsgraderte anskaffelsens løpetid vil sikkerhetsmyndigheten i landet hvor leverandøren er lokalisert være forpliktet til å forestå sikkerhetsmessig oppfølging og tilsyn med leverandøren, i henhold til det aktuelle landets nasjonale lovgivning. Dette har Norge akseptert gjennom de bi- og multilaterale sikkerhetsavtalene.

Dersom andre lands sikkerhetsmyndigheter eller internasjonale organisasjoner forespør hvorvidt en norsk leverandør har leverandørklarering, er det kun NSM som kan utlevere slik informasjon.⁴⁴

Leverandørklaringsprosess: utenlandske leverandører



*Den videre prosessen forutsetter at det foreligger en bi- eller multilateral avtale mellom Norge og staten leverandøren holder til i

** Dersom aktuell stat ikke klarer på aktuelt nivå er det NSM som godkjenner leverandøren

*** Hvis gyldig klarering allerede foreligger godkjenner NSM den utenlandske leverandøren

Figuren illustrerer gangen i en sikkerhetsgradert anskaffelse hvor en utenlandsk leverandør skal klareres. Kilde: NSM.

⁴¹ Jf. sikk § 9-2 første ledd.

⁴² Jf. klareringsforskriften § 32.

⁴³ Facility Security Clearance Information Sheet (FSCIS)

⁴⁴ Jf. klareringsforskriften § 40.

3.6.3 Klarering og autorisering av personell

Klarering av leverandørens personell gjennomføres av myndighetene i hjemstaten, som bekrefter personelletts klareringsstatus til NSM. Som hovedregel skal det derfor ikke utstedes norske sikkerhetsklareringer til personell hos utenlandske leverandører.

Det stilles heller ikke krav om autorisasjon av autorisasjonsansvarlig eller personell hos utenlandsk leverandør som har utenlandsk sikkerhetsklarering. Dette følger av de bi- eller multilaterale avtalene, hvor man anerkjenner det andre landets nasjonale lovgivning for beskyttelse av sikkerhetsgradert informasjon. Det anbefales imidlertid at oppdragsgiver i sikkerhetsavtale med utenlandsk leverandør sikrer seg mulighet til å få oversikt over hvilket personell hos leverandøren som får tilgang til norsk sikkerhetsgradert informasjon.

3.6.4 Vilkår og prosedyrer ved besøk

Ved besøk fra en utenlandsk leverandør, skal besøket gjennomføres i tråd med besøksprosedyrene i aktuell bi- eller multilaterale avtale.⁴⁵ De besøkendes identitet og klarering skal kontrolleres og verifiseres i forkant av besøket.

Utfyllende bestemmelser om gjennomføring av besøk, hvor de besøkende vil få tilgang til sikkerhetsgradert informasjon, følger av de bi- eller multilaterale avtalene. Det bærende prinsipp i disse avtalene er at besøksanmodninger, «Request for Visit», skal fremsendes og godkjennes av statenes respektive sikkerhetsmyndigheter. Som ledd i denne prosessen vil de besøkendes sikkerhetsklarering bekreftes av sikkerhetsmyndigheten i staten leverandøren holder til i. I Norge er utøvelsen av besøkskontrollregimet delegert til Forsvarets sikkerhetsavdeling (FSA).

3.7 Tilbakelevering

Ved avslutning av samarbeid med hoved- og underleverandører, grunnet endt kontraktsforhold eller brudd på gjeldende sikkerhetskrav som medfører tilbakekall av leverandørklarering, skal utlevert sikkerhetsgradert informasjon tilbake til oppdragsgiver.⁴⁶ Det gjelder også dersom det er utlevert sikkerhetsgradert informasjon til tilbydere som ikke får tildelt oppdraget.

Tilganger til skjermingsverdige objekter og infrastruktur må også tilbakekalles, det gjelder både for elektroniske og fysiske tilganger.

Oppdragsgivers ansvar for å sikre tilbakelevering og tilbakekall understreker viktigheten av at oppdragsgiver har nødvendig oversikt og kontroll med hoved- og underleverandører i sikkerhetsgraderte anskaffelser.

3.7.1 Overføring av verdier til nye parter

Det er ikke anledning til å overføre sikkerhetsgradert informasjon, skjermingsverdig objekt eller infrastruktur til ny eier av en leverandørvirksomhet, uten samtykke fra NSM.⁴⁷ Verdiene kan heller ikke inngå i bobehandling ved gjeldsforhandling eller konkurs uten slikt samtykke. Leverandørens tilgang til nevnte verdier er gitt på bakgrunn av at virksomheten er vurdert som sikkerhetsmessig skikket og at den oppfyller krav til forebyggende sikkerhetsarbeid. Eierskifte eller bobehandling

⁴⁵ Jf. virksomhets sikkerhetsforskriften § 87.

⁴⁶ Jf. virksomhets sikkerhetsforskriften § 82.

⁴⁷ Jf. sikk1 9-3 fjerde ledd.

innebærer at andre aktører trer inn, og forutsetningen for tidligere gitt tilgang vil ikke lengre være tilstede, herunder at nødvendige klareringer ikke lengre foreligger.

3.8 Unntak fra sikkerhetskrav

Det kan gjøres unntak fra enkelte av kravene som stilles til sikkerhetsgraderte anskaffelser, dersom det blir «uforholdsmessig byrdefullt» for virksomheten å oppfylle.⁴⁸ Terskelen for å gjøre unntak er høy, både med henvisning til ordlyden og at lovgiver har vurdert sikkerhetstiltakene som nødvendig for å kunne ivareta et forsvarlig sikkerhetsnivå. Unntak kan være aktuelt dersom oppfyllelse av krav vil føre til at virksomheten ikke kan fungere slik den skal. Unntak skal være godt begrunnet i hensynet til virksomhetens aktivitet, og kompenserende tiltak må ha vært vurdert.⁴⁹

Det kan gjøres unntak fra følgende krav som gjelder for sikkerhetsgraderte anskaffelser:

- inngåelse av sikkerhetsavtale, jf. virksomhetsikkerhetsforskriften § 80 først ledd.
- leverandørklarering for elektronisk tilgang fra egne lokaler til objekter eller infrastruktur klassifisert KRITISK eller MEGET KRITISK, jf. virksomhetsikkerhetsforskriften § 83, bokstav b.
- leverandørklarering for å råde over objekter eller infrastruktur som tilhører oppdragsgiver, og som er klassifisert KRITISK eller MEGET KRITISK, jf. virksomhetsikkerhetsforskriften § 83, bokstav c.
- krav til bi- eller multilateral avtale mellom Norge og annen stat, ved bruk av utenlandske leverandører eller leverandører med lokaler utenfor norsk jurisdiksjon, jf. virksomhetsikkerhetsforskriften § 84.

Det er NSM som kan gjøre unntak fra kravene. Der det er utpekt sektormyndighet med tilsynsansvar vil de ha myndighet til å gjøre unntak fra kravene. Derimot er det kun NSM som kan gjøre unntak for krav som gjelder for beskyttelse av sikkerhetsgradert informasjon.⁵⁰

4 Sikkerhet i ugraderte anskaffelser

4.1 Forholdet mellom sikkerhetsloven og lov om offentlige anskaffelser

For offentlige og enkelte private virksomheter, vil sikkerhetslovens regler om sikkerhet i anskaffelser komme i tillegg til reglene som gjelder for offentlige anskaffelser.⁵¹ Anskaffelsesregelverket gir oppdragsgiver et stort handlingsrom for å tilpasse anskaffelsesprosessen ut i fra de faktiske behov, blant annet til å stille krav og kriterier som ivaretar sikkerhets- og beredskapshensyn.⁵² Utnyttelse av handlingsrommet i anskaffelsesregelverket forutsetter imidlertid at oppdragsgiver er kjent med mulighetene til å tilpasse anskaffelsen etter de faktiske behov, og evner å benytte seg av disse.

⁴⁸ Jf. virksomhetsikkerhetsforskriften § 20 første ledd.

⁴⁹ Jf. Prop. 153 L (2016-2017), punkt 10.5.2.2.

⁵⁰ Jf. virksomhetsikkerhetsforskriften § 20 annet ledd.

⁵¹ Jf. Lov om offentlige anskaffelser (LOA) § 2.

⁵² Se NOU 2024:9 del II for en gjennomgang av handlingsrommet i anskaffelsesregelverket, særlig punkt 4.5, side 108-111. Se også Veileder om ivaretagelse av sikkerhet i offentlige anskaffelser, utarbeidet av Forsvarsdepartementet og Nærings- og fiskeridepartementet.

4.2 Relevante hensyn ved planlegging og gjennomføring av anskaffelser

Med utgangspunkt i gjennomført risikovurdering må oppdragsgiver ta stilling til hvordan sikkerheshensyn skal vektes i en anskaffelse. Oppdragsgiver har et skjønn hva gjelder utforming av tildelingskriteriene og hvordan disse skal vektlegges i anskaffelsesprosessen.

Ved behov for langsiktig robusthet kan det være lite hensiktsmessig med et stort fokus på kortsiktige konsekvenser for virksomheten, eksempelvis i form av kostnad. Vektlegging av pris fremfor sikkerhet i en anskaffelsesprosess kan utgjøre en sårbarhet som kan utnyttes av trusselaktører, fordi det øker risikoen for at mindre virksomheter med nasjonal produksjon kan prises ut av konkurransen til fordel for større virksomheter med produksjon i lavkostlandsland. Det er også kjent at enkelte stater subsidierer næringslivsaktører slik at de kan vinne anbudskonkurranser i vestlige land og slik få innpass i verdikjeder. Dette kan ha betydning for nasjonal beredskap, men også by på sikkerhetsmessige utfordringer dersom produksjonslandet utgjør en risiko for nasjonal sikkerhet.

Endringer i sikkerhets- og geopolitiske forhold kan påvirke vurderingen av hvilke verdier som er viktig å beskytte, hvordan man skal gå frem for å beskytte disse og hvem vi ønsker å samhandle med. Et endret situasjonsbilde har blant annet ført til et økt behov for kontroll med teknologi, infrastruktur og innsatsfaktorer av stor betydning innenfor nasjonal sikkerhet og samfunnssikkerhet. Internasjonale spenninger påvirker også hva trusselaktører er interessert i og hvordan de går frem for å oppnå sine mål. De senere år har man sett en økende grad av tilstedeværelse fra enkeltaktører og -land inn i norske og europeiske verdikjeder, som både kan gi innsikt i informasjon om, og mulighet for å påvirke, verdier av nasjonal betydning.⁵³ Det kan være enklere å skaffe seg tilgang til verdier gjennom underleverandører som kan ha et lavere sikkerhetsnivå enn oppdragsgiver og hovedleverandør. I større anskaffelser med lange og kompliserte leverandørkjeder kan det også være enklere å skjule egen identitet og faktisk agenda.

4.3 Ivaretagelse av sikkerhet i anskaffelsesprosessen

For virksomheter som er underlagt sikkerhetsloven skal forebyggende sikkerhetsarbeid være en del av virksomhetens styringssystem, og det skal iverksettes tiltak som er nødvendig for å gi et forsvarlig sikkerhetsnivå. Kravet til forsvarlig sikkerhetsnivå gjelder for alle virksomhetens aktiviteter, også i anskaffelser. Det omfatter både sikkerhetsgraderte og ugraderte anskaffelser, selv om det i de ugraderte anskaffelsene kan variere hvor fremtredende sikkerhetsaspektet er. Selv om det er en ugradert anskaffelse kan det være nyttig å se hen til regelverket for sikkerhetsgraderte anskaffelser for veiledning knyttet til hva som må sikres og hvordan dette kan gjøres. Deler av det som tidligere er gjennomgått i veilederen vil derfor ha relevans i ugraderte anskaffelser hvor oppdragsgiver er underlagt sikkerhetsloven, se spesielt kapittel 3.1 om risikovurdering, 3.2 om sikkerhet i konkurransegrunnlaget og 3.5 oppfølging av leverandørforhold.

Det er viktig at oppdragsgiver gjennomfører gode og dekkende vurderinger av hvilke behov som gjør seg gjeldende, og hvordan disse skal ivaretas. Oppdragsgiver må også avklare hvilke regelverk og krav som gjelder i den konkrete anskaffelsen, og hvilket handlingsrom man har for å ta hensyn til og stille krav til sikkerhet. En tidlig avklaring vil gjøre samkjøring med annet regelverk enklere og lette arbeidet med å implementere nødvendige sikkerhetstiltak på riktig sted i prosessen.

⁵³ Se blant annet de åpne risiko og trusselvurderingene fra EOS-tjenestene fra de siste årene.

Hvilke tiltak oppdragiver kan iverksette for å sikre et forsvarlig sikkerhetsnivå i anskaffelsen beror på en konkret og helhetlig vurdering av hvilke behov som gjør seg gjeldende, hvilke tiltak som er nødvendige, og om disse er forholdsmessige.

For virksomheter som er underlagt sikkerhetsloven vil det være relevant å vurdere behov for nasjonal kontroll og autonomi, sett i lys av virksomhetens rolle i de ulike deler av krisespekteret, ved planlegging av anskaffelser. Eksempler på aktuelle tiltak for å ivareta sikkerhetshensyn i anskaffelser:

- oppdeling av større kontrakter og begrensninger på antall delkontrakter en leverandør kan tildeles for å unngå avhengighet til enkeltleverandører og fordele risiko
- sikre redundante løsninger for varer og tjenester virksomheten er avhengig av
- begrensninger på antall ledd i leverandørkjeder for å bedre oppdragsgivers mulighet til å ha oversikt over og kontroll med leverandører

Fordeling av anskaffelser på et større antall aktører bidrar til at flere virksomheter får økt kunnskap og kompetanse. Det kan spille positivt inn på konkurransedyktigheten til mindre og gjerne lokale virksomheter, som igjen kan øke nasjonal redundans på kapasitet og kompetanse. Tiltak for å unngå konsentrasjonsrisiko blant leverandører kan også redusere risiko for at enkeltaktører blir sittende med en omfattende og potensiell sensitiv verdioversikt. Tiltak for å sikre oversikt og kontroll med leverandørkjeder gir bedre forutsetninger for å hindre uønskede aktører innpass i leverandørkjeder og reduserer risiko for utilsiktet avhengighetskonsentrasjon.

I konkurransegrunnlaget kan oppdragsgiver stille krav og kriterier som tilbydere må kunne innfri for å bli valgt som leverandør i anskaffelsen. Det kan blant annet knytte seg til:

- krav om formell kompetanse, sertifisering, erfaring fra lignende arbeid eller nærmere angitte kvalifikasjoner for å sikre at leverandør har nødvendig risiko- og sikkerhetsforståelse
- krav til adgangs- og tilgangskontroll for å redusere risiko for uønsket tilgang til oppdragsgivers verdier
- krav til håndtering av informasjon for å sikre konfidensialitet for sensitiv informasjon

Leverandører fra enkelte land er underlagt lovbestemmelser som pålegger dem et utstrakt samarbeid med eget lands myndigheter, blant annet knyttet til deling av informasjon. Muligheten for at leverandøren kan bli pålagt å dele informasjon de får tilgang til i en anskaffelse kan komme i konflikt med lovpålagt plikt for oppdragsgiver til å beskytte taushetsbelagt informasjon.

4.4 Sikkerhetskrav i kontrakt

Selv om det ikke er krav om inngåelse av sikkerhetsavtale utenfor sikkerhetsgraderte anskaffelser, bør sikkerhetskrav være en sentral del av kontrakten. Det vil bidra til å sikre en omforent forståelse av rammene for anskaffelsen og ansvarsfordelingen mellom oppdragsgiver og leverandør.

Ved inngåelse av kontrakt bør oppdragsgivers mulighet for kontroll og tilgang til nødvendig informasjon reguleres. Informasjon om endringer i hoved- eller underleverandørers eierstruktur vil her være relevant, da helt eller delvis oppkjøp av en leverandør kan få betydning for risikovurderingen av anskaffelsen. Av informasjon som kan få slik betydning, vises det blant annet til

informasjon om at ny/nye eiere har tilknytning til andre stater eller organisasjoner med ulovlig formål, om de har en historikk med økonomisk mislighold eller annet som kan gi grunn til bekymring for ivaretagelse av sikkerhet i anskaffelsen. Det er derfor relevant å regulere hvordan partene skal forholde seg i slike situasjoner, herunder mulighet for avvikling av kontraktsforholdet.

Ved potensiale for at anskaffelsen på et senere tidspunkt kan bli mer sikkerhetssensitiv, er det hensiktsmessig at det orienteres om hvilke krav en leverandør i så tilfelle kan bli forpliktet til å innfri. Kontrakten mellom oppdragsgiver og leverandør bør derfor regulere hvilket handlingsrom oppdragsgiver har til å gjøre endringer i sikkerhetskrav og hvem som skal bære ansvaret for tilleggskostnader som følge av endrede sikkerhetskrav.

Anskaffelser som kan gi leverandøren tilgang til skjermingsverdige informasjonssystemer eller skjermingsverdig ugradert informasjon er ikke å anse som sikkerhetsgraderte anskaffelser. I slike anskaffelser stilles det likevel krav om at oppdragsgiver og leverandør skal inngå en avtale hvor relevante sikkerhetskrav til anskaffelsen fremkommer⁵⁴. Ved utarbeidelse av en slik avtale kan det være hensiktsmessig å se hen til hvilke krav som stilles til innhold i en sikkerhetsavtale.

5 Oppsummering

Det er viktig at oppdragsgiver tidlig avklarer hvilke behov som gjør seg gjeldende for anskaffelsen og tilpasser anskaffelsesprosessen etter dette, uavhengig av om anskaffelsen er sikkerhetsgradert eller ikke.

Oppdragsgiver må sikre riktig kompetanse inn i anskaffelsesprosessene slik at alle relevante behov og hensyn ivaretas, herunder til det som skal anskaffes, prosess og sikkerhet.

Gjennomføring av gode risikovurderinger forutsetter at oppdragsgiver har kjennskap til virksomhetens verdier og sårbarheter, og at man innhenter nødvendig informasjon om trusler som er relevant for egen virksomhet og den enkelte anskaffelse.

Hensynet til sikkerhet må vektlegges riktig, slik at det ikke tilsidesettes for mindre tungtveiende hensyn ved utforming av anskaffelsesprosessen og ved valg av leverandør.

Oppdragsgiver må sørge for ivaretagelse av et forsvarlig sikkerhetsnivå både før, under og etter kontraktsinngåelse. Det innebærer blant annet etablering av mekanismer som sikrer nødvendig oppfølging av leverandører og underleverandører, kontroll med gitte tilganger til oppdragsgivers verdier, og håndtering av sikkerhetstruende hendelser. Oppdragsgiver må ta høyde for at situasjonsbildet er dynamisk og at endringer kan føre til behov for nye risikovurderinger og tiltak.

⁵⁴ Jf. virksomhetsikkerhetsforskriften § 18 annet ledd.

NSM

Nasjonal sikkerhetsmyndighet

Postboks 814

1306 Sandvika

postmottak@nsm.no

nsm.no