

KVALIFIKASJONGRUNNLAG - (FOSA under EØS terskelverdi)

INNHold:

- Kvalifikasjonsgrunnlag (konkurranseregler)
- Vedlegg:
 - Etisk egenerklæring
 - Egenerklæring om russisk involvering i offentlige anskaffelser
 - Egenerklæring sikkerhetskrav
 - Forpliktelseserklæring fra støttende virksomheter
 - Erklæring om solidaransvar

Ovennevnte vedlegg skal fylles ut og returneres sammen med søknaden.

1 INNLEDNING

Forsvarsbygg inviterer leverandøren til å inngi tilbud i en konkurranse med forhandling (to trinnsprosedyre), som gjelder rammeavtale for aggregatstyringer av nye og eksisterende tavler.

Konkurransen gjelder en anskaffelse over EØS terskelverdiene fastsatt i forskrift om forsvars- og sikkerhetsanskaffelser (FOSA) § 2-2, og følger reglene i denne forskriftens del I.

Anskaffelsen er kunngjort i Doffin. I tillegg til kunngjøringen og dette kvalifikasjonsgrunnlaget vil det komplette konkurransegrunnlaget bestå av følgende dokumenter:

- Del I - Innbydelse til konkurranse
- Del II - Forsvarsbyggs kontraktsbestemmelser
- Del III - Oppdragsbeskrivelse

Konkurransegrunnlaget er anslagsvis klart for utsendelse medio august. Kun de leverandører som blir invitert til å inngi tilbud vil motta konkurransegrunnlaget. Hvilke leverandører som inviteres avhenger av besvarelsen på dette kvalifikasjonsgrunnlaget.

2 INFORMASJON

2.1 Beskrivelse av oppdraget

Oppdragsgiveren har behov for oppgraderte aggregatstyretavler av typen KFS2017 som skal leveres, monteres, testes og tilpasses radiolinjestasjoner / andre aktuelle stasjoner, som erstatning for eldre styretavler som er montert per i dag.

I dette ligger det også demontering av gamle tavler som skal erstattes med nye, samt eventuell utlegging av nytt kabelmaterieell for nye styretavler. Det skal i tillegg leveres oppgraderingspakker for et gitt omfang av tidligere leverte styretavler av typen KFS2010, med den hensikt å få oppgradert disse styretavlene til et teknisk tilsvarende nivå som nye styretavler.

Søkere må kunne håndtere leveranser av erstatning og oppgradering av eldre styretavler som er montert per i dag. Samt fremtidig service og vedlikehold Avtalen er landsdekkende.

Rammeavtalen har en estimert verdi på 25-30 millioner eks.mva. dersom alle opsjoner tas ut, og maksimal levetid for avtalen på 10 år blir gjennomført.

2.2 Informasjonsmøte

Det vil ikke bli avholdt informasjonsmøte knyttet til konkurransen.

2.3 Tilleggsopplysninger

Ugradert kommunikasjon i prosessen skal foregå via Mercell-portalen, www.mercell.no. Dette for at all kommunikasjon skal loggføres.

Når du er inne på konkurransen skal du velge fanebladet Kommunikasjon. Klikk deretter på ikonet "Ny melding" i menylinjen. Skriv inn informasjon til oppdragsgiver og trykk deretter på ikonet "Send". Oppdragsgiver mottar så meldingen din. Hvis spørsmålet angår alle tilbydere vil oppdragsgiver besvare dette anonymisert ved å gi svaret som en tilleggsinformasjon. Tilleggsinformasjon er tilgjengelig under fanebladet Kommunikasjon og deretter under fanebladet Tilleggsinformasjon. Du vil også få en e-post med en link til tilleggsinformasjonen.

3 KRAV TIL SØKNADEN

3.1 Språkkrav

Søknad med tilhørende dokumentasjon skal fortrinnsvis leveres på norsk, men annet skandinavisk språk vil også aksepteres.

3.2 Innlevering av søknaden

Søknaden skal leveres elektronisk til www.mercell.no innen søknadsfristen.

Er du ikke bruker hos Mercell, har du spørsmål knyttet til hvordan du skal laste opp søknaden din, eller hvordan du skal gi tilbud, ta kontakt med Mercell support på telefon 21 01 88 60 eller via e-post til support@mercell.com.

Ved offentlige anbud kreves det elektronisk signatur (BankID, Commfides eller Buypass), har du spørsmål vedrørende dette, vennligst kontakt Mercell support. **NB! Hvis du ikke har brukt elektronisk signatur tidligere, anbefales det å avklare bruken av dette i god tid før innleveringsfrist!** Vi gjør oppmerksom på at det kan ta noen dager å få levert elektronisk signatur. Denne prosessen bør derfor settes i gang så raskt som mulig.

Mercell anbefaler at signeringen testes med sertifikatet man har tilgjengelig snarest mulig (i god tid før tilbudsfrist). Test-funksjonaliteten ligger i påmeldings-/søknadsinnleveringsstegene.

Elektronisk signatur utenfor Norge.

Vi gjør oppmerksom på at Mercell-portalen støtter følgende elektroniske signatur fra Sverige og Danmark:

Sverige: Svensk Bank ID, Nordea

Danmark: Nem ID, TDC/OCES

Innen EU benytter Mercell en tjeneste levert av Unizeto (<http://unizeto.eu/>) gjennom en avtale med DIFI og EU prosjektet PEPPOL (www.peppol.eu). Dette støtter de fleste X.509 sertifikater.

3.3 Frist for å levere søknad

Frist for innlevering av søknad er 08.01.2026.

4 KRAV TIL LEVERANDØRENE

4.1 Kvalifikasjonskrav

Det stilles følgende krav til leverandørene som ønsker å delta i konkurransen:

Krav:	Dokumentasjon som skal leveres:
Generelle krav:	
Leverandøren skal være et lovlig registrert firma	Utenlandske leverandører må fremlegge dokumentasjon for at firmaet er lovlig registrert i sitt hjemland. Norske leverandører trenger ikke dokumentere oppfyllelse av kravet utover fremleggelse av skatte- og mva-attest, jf. nedenfor.
Krav til økonomisk/finansiell stilling:	
Leverandøren skal ha et ryddig forhold til innbetaling av skatter og avgifter (kun for norske leverandører)	' <u>Attest for skatt og merverdiavgift</u> ' (RF-1316). Attesten kan bestilles via www.altinn.no . Attesten skal ikke være eldre enn 6 måneder regnet fra tilbudsfristen.
Leverandøren skal ha økonomisk kapasitet til å gjennomføre kontrakten	Kredittvurdering av leverandøren som ikke er eldre enn 6 måneder regnet fra utløpet av søknadsfristen. Kredittvurderingen skal inneholde en vurdering av leverandørens betalingshistorikk/-pålitelighet. Resultatet av kredittvurderingen skal fremkomme som en gradert verdi (bokstaver eller tall) mot en definert skala. Dersom leverandøren, for å oppfylle kravet, viser til garantier stilt av andre foretak (f.eks morselskap) må det fremlegges tilsvarende kredittvurdering fra dette selskapet. <u>Samt:</u> Fremleggelse av regnskapstall fra siste tilgjengelig årsregnskap som viser leverandørens omsetning. (Ikke nødvendig dersom regnskapets nøkkeltall fremgår av kredittvurderingen)
Krav til tekniske og faglige kvalifikasjoner:	

Leverandøren skal ha svært god erfaring fra oppdrag av samme art, omfang og kompleksitet som har overføringsverdi til denne kontrakten.	Liste over relevante prosjekter utført i løpet av de fem siste årene, som gir en beskrivelse av prosjektene slik at Forsvarsbygg kan vurdere prosjektenes overføringsverdi til denne kontrakten.
Krav til inngåelse av sikkerhetsavtale med leverandøren, samt autorisasjon, og ev. sikkerhetsklarering av personell:	
<p>Det må inngås en sikkerhetsavtale med leverandøren før han får tilgang til konkurransegrunnlaget. Personell som leverandøren skal benytte til å lese konkurransegrunnlaget/utferdige tilbud må være autorisert t iht. sikkerhetsloven.</p> <p>Fristen for inngåelse av sikkerhetsavtale, samt autorisasjon av leverandørpersonell settes til 3 måneder etter at leverandøren får meddelelse om at han er kvalifisert.</p> <p>Det gjøres oppmerksom på at det er leverandørens risiko at sikkerhetsavtale, samt autorisasjon ikke oppnås innenfor tidsfristen, med mindre forsinkelsen skyldes forhold Forsvarsbygg svarer for.</p>	Kravet skal ikke dokumenteres i selve søknaden. Leverandørene som innleverer søknad vil bli kontaktet av Forsvarsbygg og informert om prosessene knyttet til inngåelse av sikkerhetsavtale, samt autorisasjon.

4.2 Krav ved samarbeidende leverandører

4.2.1 Bruk av underleverandører eller andre støttende virksomheter

Dersom leverandøren viser til dokumentasjon fra underleverandører for å dokumentere oppfyllelsen av kravene til tekniske og faglige kvalifikasjoner, eller støtter seg på andre virksomheter for oppfyllelsen av kravene til økonomisk/finansiell stilling, skal det fremlegges en forpliktelseserklæring som er undertegnet av disse støttende virksomhetene. Mal for slik erklæring er inntatt som vedlegg 4 til dette dokumentet.

4.2.2 Søknad fra leverandørgruppe - solidaransvar

Leverandører som har inngått et samarbeid, og som ønsker å gjennomføre kontrakten i fellesskap, skal levere «Erklæring om solidaransvar fra samarbeidende leverandører», se vedlegg 5. Leverandørgruppen skal levere én felles søknad/tilbud.

5 ANTALL LEVERANDØRER. UTVELGELSESKRITERIER

Forsvarsbygg har til hensikt å invitere 3 leverandører som gis anledning til å inngi tilbud, så fremt det melder seg tilstrekkelig mange kvalifiserte leverandører. Dersom antallet kvalifiserte leverandører overskrider grensen til Forsvarsbygg, vil vi velge de leverandører som best oppfyller kravene til tekniske og faglige kvalifikasjoner.

Forsvarsbygg er ikke forpliktet til å velge ut det maksimale antallet leverandører. Antallet leverandører innenfor det angitte intervallet kan begrenses på bakgrunn av en saklig og objektiv vurdering.

6 KRAV TIL HÅNDTERING AV SKJERMINGSVERDIG INFORMASJON

6.1 I konkurranseperioden

Anskaffelsen er sikkerhetsgradert. Konkurransegrunnlaget som leverandøren får utlevert inneholder informasjon som i henhold til lov om nasjonal sikkerhet (sikkerhetsloven) er sikkerhetsgradert BEGRENSET. Anskaffelsen er dermed underlagt krav gitt i, eller i medhold av, sikkerhetsloven.

Før leverandøren får utlevert informasjon gradert BEGRENSET må det inngås en sikkerhetsavtale mellom leverandøren og Forsvarsbygg. Leverandørpersonell som skal ha tilgang til informasjon sikkerhetsgradert BEGRENSET, må autoriseres for denne sikkerhetsgraden før tilgang gis.

Leverandøren vil ikke ha behov for å behandle informasjonen på et informasjonssystem i sine egne lokaler. Nasjonal Sikkerhetsmyndighet (NSM) er godkjenningmyndighet for skjermingsverdige informasjonssystemer som er angitt i virksomhetsikkerhetsforskriften § 51 første og andre ledd. Skjermingsverdig informasjonssystem som ikke er nevnt i første og andre ledd skal godkjennes av leverandøren, men oppdragsgiver skal gi tillatelse før informasjonssystemet kan tas i bruk.

For nivå BEGRENSET kreves det ikke leverandørklarering før sikkerhetsavtale inngås, med mindre dette er viktig for å oppnå forsvarlig sikkerhetsnivå. For denne anskaffelsen stille det ikke krav til at leverandør skal ha gyldig leverandørklarering i konkurransefasen.

6.2 I gjennomføringsfasen

Gjennomføringen av kontrakten er underlagt krav gitt i, eller i medhold av, sikkerhetsloven. Leverandøren kan få tilgang til sikkerhetsgradert informasjon, et skjermingsverdig objekt eller skjermingsverdig infrastruktur. Krav til beskyttelse av sikkerhetsgradert informasjon er beskrevet i vedlegg 6.

6.3 Generelle bestemmelser om sikkerhet

Av hensyn til fremdriften i anskaffelsen/kontrakten stilles det krav om at leverandørene må være norske foretak eller foretak fra stater som har virksom/gyldig sikkerhetsavtale med Norge.

Leverandørpersonell som det kreves sikkerhetsklarering for skal kun inneha norsk statsborgerskap, eller kun inneha statsborgerskap fra land som Norge har sikkerhetsmessig samarbeid med.

Leverandøren må påregne **minimum 6-9 måneders** saksbehandlingstid for personell som kun er norske statsborgere. Saksbehandlingstiden regnes fra korrekt utfylt personopplysningsblankett (POB) er mottatt av klareringsmyndigheten.

En person som har utenlandsk statsborgerskap, kan etter en konkret helhetsvurdering få klarering, dersom det ikke er rimelig grunn til å tvile på at personen er sikkerhetsmessig skikket. Det vil i vurderingen legges vekt på hjemlandets sikkerhetsmessige betydning, personens tilknytning til hjemlandet og tilknytningen til Norge. Utfallet av slike søknader er usikkert, og i alle tilfeller må det påregnes vesentlig lengre saksbehandlingstid enn for norske statsborgere.

Det gjøres oppmerksom på at det er leverandørens risiko at autorisasjon eller sikkerhetsklarering ikke oppnås. Han har også risikoen for at autorisasjon eller sikkerhetsklarering tar lengre tid enn 6 måneder med mindre forsinkelsen skyldes forhold oppdragsgiver eller norske sikkerhetsmyndigheter svarer for.

6.4 Egenerklæring om sikkerhetskrav

Leverandørene skal fylle ut og levere inn en egenerklæring om sikkerhetskrav. Egenerklæringen er inntatt som vedlegg 3 til dette kvalifikasjonsgrunnlaget.

7 ANDRE OPPLYSNINGER FOR LEVERANDØRENE

7.1 Bruk av personer med bakgrunn fra forsvarssektoren

Det skal utvises varsomhet ved bruk av tidligere forsvarsansatte i oppdrag for forsvarssektoren. Med tidligere ansatte menes her personer som har vært ansatt innenfor de siste to år regnet fra tilbudsfristens utløp.

Leverandøren skal, så langt det er mulig, unngå å benytte tidligere ansatte i forsvarssektoren i direkte kontakt med oppdragsgiver under anskaffelsesprosessen. Dersom leverandøren ikke har mulighet til å imøtekomme dette kravet skal dette opplyses om i tilbudet.

7.2 Egenerklæring om etiske og straffbare forhold

Leverandøren skal som del av tilbudet levere inn «Etisk egenerklæring». Malen vedlagt dette dokumentet skal benyttes. Erklæringen skal være undertegnet. Dersom leverandøren besvarer bekræftende på ett eller flere av punktene i egenerklæringens punkt 3, skal leverandøren i tilbudsbrevet gi en redegjørelse for forholdet/forholdene.

7.3 Behandling av personopplysninger

Ved innsendelse av søknad om kvalifisering og tilbud ber vi leverandørene påse at det ikke forekommer taushetsbelagte eller sensitive personopplysninger utover det som uttrykkelig etterspørres. Leverandøren er ansvarlig for at de har tillatelse til å formidle CV-er og andre dokumenter med personopplysninger og at vedkommende er tilstrekkelig informert om hva som deles. CV-ene skal være egnet for offentlig tilgjengeliggjøring og skal ikke inneholde flere opplysninger enn det som er nødvendig for evaluering av søknad om kvalifisering og tilbud.

For ytterligere informasjon om behandling av personopplysninger, se Forsvarsbyggs personvernerklæring på <https://www.forsvarsbygg.no/om-oss/personvernerklaering>.

8 FRIST FOR BEGJÆRING OM MIDLERTIDIG FORFØYNING

I forbindelse med eventuell senere meddelelse av beslutning om avvísning eller forkastelse av søknad om kvalifisering, kan oppdragsgiver sette en frist på 15 dager for å begjære midlertidig forføyning mot beslutningen, jf forskrift om forsvars- og sikkerhetsanskaffelser § 10-6.

9 SAMARBEID MED SKATTEETATEN – FULLMAKT TIL FORSVARSBYGG

Forsvarsbygg har inngått et samarbeid med Skatteetaten, hvor formålet er forebygging og bekjempelse av arbeidslivskriminalitet. I den forbindelse krever Forsvarsbygg at tilbyder som innstilles til kontrakt skal sende inn signert fullmakt, før kontraktsinngåelse, som gir Forsvarsbygg en utvidet rett til et ubegrenset antall ganger å innhente opplysninger om tilbyderens skatte- og avgiftsmessige forhold. Fullmakten ligger som vedlegg til Del I Innbydelse til konkurranse.

Kravet om signert fullmakt gjelder også for tilbyderens underleverandører. Tilbyderen skal kontraktsfeste signeringsplikten nedover i leverandørkjeden. Før signering av kontrakt kreves det dog kun signert fullmakt fra tilbyder, med mindre underleverandører benyttes for å oppfylle et kvalifikasjonskrav i konkurransen. I så fall skal signert fullmakt foreligge fra både tilbyder og underleverandører. Signert fullmakt fra øvrige underleverandører må imidlertid være levert og godkjent av oppdragsgiver før de kan benyttes i kontrakten/prosjektet. Dette gjelder i hele kontraktsperioden.

Forsvarsbygg gjør oppmerksom på at det kan være aktuelt å avvise den tilbyder og eventuelle underleverandører som i meddelelsesbrevet er innstilt som vinner av konkurransen, dersom det etter meddelelse, men forut for signering av kontrakt, mottas opplysninger fra Skatteetaten om manglende oppfyllelse av skatte- og avgiftsforpliktelser mv. Tildelingen kan derfor ikke anses endelig før det foreligger en vurdering av de innhentede opplysninger som ikke endrer oppdragsgivers tildelingsbeslutning. Det presiseres også at hvis det ikke mottas signert fullmakt fra tilbyder og eventuelle underleverandører som man har støttet seg på for å oppfylle kvalifikasjonskravene, vil dette anses som et vesentlig forbehold til kontrakten som vil medføre at tilbyder avvises fra konkurransen.

Kontrakten kan bli gjenstand for oppfølging gjennom hele kontraktsperioden. Oppfølgingen innebærer at tilbyder sender månedlige oversiktslister til Forsvarsbygg med fødsels- eller D-nummer på alle ansatte som utfører arbeid som ledd i oppfyllelsen av kontrakten. Listene vil kontrolleres av Skatteetaten.

10 OPPDRAGSGIVERS FORBEHOLD

Oppdragsgiver forbeholder seg retten til å avlyse konkurransen dersom det foreligger saklig grunn, for eksempel ved bortfall av planlagt finansiering eller manglende godkjenning fra politisk eller militært hold.

11 SØKNADENS INNHOLD OG ORGANISERING

Forsvarsbygg ber om at søknaden inneholder følgende dokumentasjon:

(Leverandørene bes bruke tabellen nedenfor som sjekkliste)

Nr:	Hva skal leveres?	Sett kryss
1.	Søknadsbrev	
	Søknadsbrevet. Avvik og forbehold av enhver art i forhold til konkurransegrunnlaget skal klart, utvetydig og uttømmende fremgå av søknadsbrevet.	
2.	Dokumentasjon på kvalifikasjonskravene (se del I punkt 4.1)	
	Attest for skatt og merverdiavgift	
	Kredittvurdering	
	Regnskapstall fra siste tilgjengelig årsregnskap som viser leverandørens omsetning. (Ikke nødvendig dersom regnskapets nøkkeltall fremgår av kredittvurderingen)	
	Referanseprosjekter	
	Forpliktelseserklæring fra støttende virksomheter (hvis aktuelt) Er vedlagt dette dokumentet	
	Erklæring om solidaransvar (hvis aktuelt). Er vedlagt dette dokumentet	
3.	Øvrige dokumenter	
	Forpliktelseserklæring fra støttende virksomheter - Kvalifikasjonskrav. Se vedlegg 4	
	Erklæring om solidaransvar fra samarbeidende virksomheter. Se vedlegg 5	
	Eventuelle øvrige dokumenter	

Det er ønskelig at leverandøren organiserer sin søknad ut fra rekkefølgen angitt ovenfor.

Er det usikkerhet knyttet til hva som skal leveres inn må leverandøren selv kontakten Forsvarsbygg gjennom Mercell i god tid før tilbudsfristens utløp.

Blir leverandøren oppmerksom på at konkurransegrunnlaget inneholder feil, uklarheter, ufullstendigheter mv, plikter han snarest mulig å varsle oppdragsgiveren om dette slik at slike forhold kan rettes opp før tilbudene sendes inn.

VEDLEGG 6

Orientering til leverandører om krav til håndtering og beskyttelse av skjermingsverdig informasjon i forbindelse med anskaffelser

Innholdsfortegnelse

1.	Innledning.....	2
1.1.	Formål.....	2
1.2.	Definisjoner.....	2
1.3.	Sikkerhet i anskaffelser.....	2
1.4.	Hjemmel.....	3
1.4.1.	Forholdet til regelverket om offentlige anskaffelser.....	3
1.5.	Generelle krav til forebyggende sikkerhetsarbeid.....	3
1.5.1.	Styringssystem for sikkerhet.....	3
1.5.2.	Leverandørens ansvar.....	3
1.5.3.	Krav om forsvarlig sikkerhetsnivå.....	3
1.5.4.	Utgifter til oppfyllelse av sikkerhetskrav.....	3
1.5.5.	Brudd på sikkerhetskrav.....	3
2.	Anskaffelser på skjermingsverdig ugradert nivå.....	4
2.1.	Veiledere.....	4
3.	Sikkerhetsgraderte anskaffelser.....	4
4.	Sikkerhetsgraderte anskaffelser på BEGRENSET nivå.....	4
4.1.	Forsvarlig sikkerhetsnivå for informasjon som er gradert BEGRENSET.....	4
4.2.	Inngåelse av sikkerhetsavtale på BEGRENSET nivå.....	4
4.2.1.	Autorisasjon.....	5
4.2.2.	Autorisasjon av utenlandsk statsborger.....	5
4.2.3.	Godkjenning av skjermingsverdige informasjonssystem.....	5
4.2.4.	Unntak fra krav om sikkerhetsavtale.....	6
4.2.5.	Innholdet i sikkerhetsavtalen.....	6
4.2.6.	Brudd på sikkerhetskrav.....	7
4.2.7.	Ytterligere sikkerhetskrav.....	7
4.2.8.	NSMs veiledere og håndbøker.....	7
5.	Sikkerhetsgraderte anskaffelser på KONFIDENSIELT nivå eller høyere.....	7
5.1.	Forsvarlig sikkerhetsnivå for informasjon som er gradert KONFIDENSIELT eller høyere.....	7
5.1.1.	Soneinndeling for informasjon gradert KONFIDENSIELT eller høyere.....	7
5.1.2.	Godkjenning av skjermingsverdig informasjonssystem.....	8
5.1.3.	Leverandørklarering.....	8
5.1.4.	Sikkerhetsklarering og autorisasjon av leverandørpersonell.....	8
5.2.	Inngåelse av sikkerhetsavtale på KONFIDENSIELT nivå eller høyere.....	9
5.2.1.	Brudd på sikkerhetskrav.....	9
5.2.2.	Ytterligere krav.....	9
5.2.3.	NSMs veiledere og håndbøker.....	9

1. Innledning

1.1. Formål

Formålet med denne orienteringen er å bidra til å gjøre leverandører av varer og tjenester til Forsvarsbygg (oppdragsgiver) oppmerksom på sikkerhetskrav som kan gjøres gjeldende i anskaffelsesprosessen.

1.2. Definisjoner

Sikkerhetsgradert anskaffelse: anskaffelse som innebærer at leverandøren av varen eller tjenesten kan få tilgang til skjermingsverdig informasjon eller informasjonssystemer som behandler slik informasjon, eller kan få tilgang til skjermingsverdig objekt eller skjermingsverdig infrastruktur.

Forebyggende sikkerhetstjeneste: planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende tiltak mot sikkerhetstruende virksomhet og følger av slik virksomhet.

Sikkerhetstruende virksomhet: tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser, eksempelvis forberedelse til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandlinger, samt medvirkning til slik virksomhet.

Skjermingsverdig informasjon: Samlebetegnelse som benyttes om all informasjon som skal beskyttes etter sikkerhetsloven. Informasjonen kan være sikkerhetsgradert eller ugradert.

Ugradert skjermingsverdig informasjon: informasjon som har betydning for grunnleggende nasjonale funksjoner, men som ikke er sikkerhetsgradert. Informasjonen er skjermingsverdig ut ifra en integritets- og tilgjengelighetsvurdering, dvs. at den kan skade nasjonale sikkerhetsinteresser dersom den går tapt eller blir endret (integritet), eller gjort utilgjengelig (tilgjengelighet).

Sikkerhetsgradert skjermingsverdig informasjon: informasjon som er merket med sikkerhetsgrad (BEGRENSET, KONFIDENSIELT, HEMMELIG eller STRENGT HEMMELIG). Informasjonen er skjermingsverdig ut ifra en integritets-, tilgjengelighets- og konfidensialitetsvurdering, dvs. den kan skade nasjonale sikkerhetsinteresser om den går tapt eller blir endret (integritet), gjort utilgjengelig (tilgjengelighet) eller blir kjent for uvedkommende (konfidensialitet).

Skjermingsverdig objekt og skjermingsverdig infrastruktur: eiendom og infrastruktur som er utpekt og klassifisert av et departement eller Nasjonal sikkerhetsmyndighet (NSM), fordi det kan skade grunnleggende nasjonale funksjoner om objektene eller infrastrukturen får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse.

Skjermingsverdig informasjonssystem: informasjonssystem som behandler skjermingsverdig informasjon, eller som har avgjørende betydning for grunnleggende nasjonale funksjoner.

Skjermingsverdig verdi: skjermingsverdig objekt, infrastruktur, informasjon eller informasjonssystem.

Grunnleggende nasjonale funksjoner: tjenester, produksjon, og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.

Styringssystem for sikkerhet: styringssystem som utgjør rammen for hvordan leverandøren oppfyller kravene til forebyggende sikkerhet. Styringssystemet for sikkerhet skal sikre at sikkerhetsarbeidet planlegges, gjennomføres og kontinuerlig utvikles på en systematisk måte og helhetlig måte.

1.3. Sikkerhet i anskaffelser

Ved anskaffelse av varer og tjenester skal oppdragsgiver ta stilling til hva leverandører (omfatter også tilbydere og underleverandører) kan få tilgang til av skjermingsverdig informasjon, skjermingsverdige objekter eller skjermingsverdig infrastruktur i de ulike fasene av en anskaffelse.

I konkurransegrunnlaget kan det bli stilt krav om at leverandøren må være i stand til å til å håndtere og beskytte skjermingsverdig informasjon i sine egne lokaler, eller oppfylle krav som stilles for tilgang til

skjermingsverdig informasjon, skjermingsverdig objekt eller skjermingsverdig infrastruktur hos oppdragsgiver. I den forbindelse vil oppdragsgiver gi råd og veiledning om forebyggende sikkerhetstjeneste.

1.4. Hjemmel

Lov om nasjonal sikkerhet av 1. juni 2018 nr. 24 (sikkerhetsloven) gjelder for statlige, fylkeskommunale og kommunale organer, samt leverandører av varer og tjenester i forbindelse med anskaffelser etter loven.

Sentrale forskrifter som er hjemlet i sikkerhetsloven:

- Forskrift om virksomheters arbeid med forebyggende sikkerhet av 20. desember 2018 nr. 2053 (virksomhetsikkerhetsforskriften)
- Forskrift om sikkerhetsklarering og annen klarering av 20. desember 2018 nr. 2054 (klareringsforskriften)

1.4.1. Forholdet til regelverket om offentlige anskaffelser

Reglene om sikkerhetsgraderte anskaffelser kommer i tillegg til reglene som gjelder for offentlige anskaffelser (anskaffelsesloven) med tilhørende forskrifter.

1.5. Generelle krav til forebyggende sikkerhetsarbeid

1.5.1. Styringssystem for sikkerhet

Leverandører som omfattes av sikkerhetsloven og skal oppbevare, behandle eller tilvirke sikkerhetsgradert informasjon i sine egne lokaler, skal etablere et styringssystem for sikkerhet. Systemet skal sikre at leverandøren oppfyller kravene gitt i eller med hjemmel i sikkerhetsloven.

1.5.2. Leverandørens ansvar

Leverandøren eller personell fra leverandøren skal oppfylle de samme krav til sikkerhet som gjelder for oppdragsgiver. Kravene til leverandøren vil avhenge av hva leverandøren får tilgang til, og hvordan denne tilgangen gis.

Leverandørens leder har ansvaret for det forebyggende sikkerhetsarbeidet innen sitt ansvars- og myndighetsområde, herunder underlagte virksomheter. Det kreves at sikkerhetsarbeidet utøves på en proaktiv og systematisk måte.

1.5.3. Krav om forsvarlig sikkerhetsnivå

Det stilles funksjonelle krav til håndtering av risiko knyttet til skjermingsverdig informasjon. Funksjonelle krav innebærer at det stilles krav om hva sikkerhetstiltakene i virksomhetene skal oppnå, ikke hvordan kravene oppnås. Det er derfor, med visse unntak, ikke avgjørende hvilke sikkerhetstiltak som velges, så lenge de valgte tiltakene gjør at det oppnås et forsvarlig sikkerhetsnivå. Det legges således opp til at leverandøren kan velge å kombinere fysiske, elektroniske, menneskelige og organisatoriske tiltak, så lenge virksomheten har et forsvarlig sikkerhetsnivå.

Leverandøren skal identifisere, analysere og evaluere risiko for at kravet om forsvarlig sikkerhetsnivået ikke kan oppfylles. På bakgrunn av risikovurderingen skal leverandøren gjennomføre de forebyggende sikkerhetstiltakene som er nødvendig for å oppnå et forsvarlig sikkerhetsnivå.

Leverandøren skal dokumentere at han på en tilfredsstillende måte både har vurdert og håndtert risiko og hvilke sikkerhetstiltak som er etablert.

1.5.4. Utgifter til oppfyllelse av sikkerhetskrav

Leverandøren må selv dekke utgifter til å oppfylle krav som følger av lovens bestemmelser, hvis ikke noe annet følger av avtalen, sikkerhetsavtalen med Forsvarsbygg (oppdragsgiver) eller forskrifter (se sikkerhetsloven § 9-2 tredje ledd og klareringsforskriften § 31).

1.5.5. Brudd på sikkerhetskrav

Overtredelse av sikkerhetsbestemmelser, forsettlig eller uaktsomt, kan anses som brudd på leverandørens kontraktsforpliktelser.

2. Anskaffelser på skjermingsverdig ugradert nivå

Ved håndtering av risiko knyttet til skjermingsverdig ugradert informasjon skal det etableres forebyggende sikkerhetstiltak som et minimum sørger for at informasjonen ikke kan gå tapt, endres eller gjøres utilgjengelig med enkle midler. Ved valg av sikkerhetstiltak skal leverandøren se behovet for å beskytte informasjonens integritet og tilgjengelighet i sammenheng og veie hensynene mot hverandre.

2.1. Veiledere

For virksomheter som skal ha tilgang til skjermingsverdig ugradert informasjon vil NSMs Håndbok i beskyttelse av skjermingsverdig ugradert informasjon være relevant å benytte i det forebyggende sikkerhetsarbeidet, se <https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/>

3. Sikkerhetsgraderte anskaffelser

I sikkerhetsloven kapittel 9 og virksomhetsikkerhetsforskriften kapittel 13 stilles det særskilte krav til oppdragsgiver og leverandører i forbindelse med sikkerhetsgraderte anskaffelser.

Skal leverandøren oppbevare, behandle eller tilvirke sikkerhetsgradert informasjon i sine egne lokaler, eller gis tilgang til skjermingsverdig objekt eller infrastruktur fra sine egne lokaler, må leverandøren oppfylle de krav som sikkerhetsloven med forskrifter stiller til virksomheter med tilsvarende mulighet til å råde over samme informasjon, objekt eller infrastruktur. Det understrekes at underleverandører med samme tilgang også må oppfylle kravene i sikkerhetsloven med forskrifter.

4. Sikkerhetsgraderte anskaffelser på BEGRENSET nivå

4.1. Forsvarlig sikkerhetsnivå for informasjon som er gradert BEGRENSET

For beskyttelse av informasjon gradert BEGRENSET, er kravet til forsvarlig sikkerhetsnivå oppfylt dersom informasjonen med enkle midler ikke kan bli kjent for uautoriserte personer. Dette kravet kommer i tillegg til ovennevnte krav som gjelder for beskyttelse av skjermingsverdig ugradert informasjon. Ved valg av sikkerhetstiltak skal leverandøren se behovet for å beskytte informasjonens konfidensialitet, integritet og tilgjengelighet i sammenheng og veie hensynene mot hverandre.

Generelle krav som gjelder vurdering og håndtering av risiko og iverksettelse av forebyggende sikkerhetstiltak, er gitt i virksomhetsikkerhetsforskriften kapittel 3 og 7.

4.2. Inngåelse av sikkerhetsavtale på BEGRENSET nivå

Sikkerhetsavtale mellom oppdragsgiver og leverandøren skal inngås før leverandøren kan oppbevare, behandle eller tilvirke informasjon gradert BEGRENSET i sine egne lokaler. Sikkerhetsavtale skal også inngås dersom leverandøren kan gis tilgang til skjermingsverdig objekt eller infrastruktur i eller fra sine egne lokaler.

Før sikkerhetsavtalen kan inngås må leverandøren dokumentere at han oppfyller krav som sikkerhetsloven og virksomhetsikkerhetsforskriften stiller til et forsvarlig sikkerhetsnivå for sikkerhetsgrad BEGRENSET.

Følgende dokumenter må utarbeides:

- Beskrivelse av virksomhetens styringssystem for sikkerhet og bekreftelse på at styringssystemet er implementert, jf. sikkerhetsloven § 4.1 og virksomhetsikkerhetsforskriften § 3
- Styringsdokument for det forebyggende sikkerhetsarbeidet, jf. virksomhetsikkerhetsforskriften § 4
- Sikkerhetsmål, jf. virksomhetsikkerhetsforskriften § 5
- Beskrivelse av roller og ansvar i den lokale sikkerhetsorganisasjonen, jf. virksomhetsikkerhetsforskriften § 6
- Bekreftelse på at personellet i den lokale sikkerhetsorganisasjonen og personellet som skal håndtere sikkerhetsgradert informasjon i forbindelse med anskaffelsen har tilstrekkelig kompetanse om forebyggende sikkerhetstjeneste og kjenner til relevante sikkerhetstrusler og sikkerhetsbestemmelser, jf. sikkerhetsloven § 4-1 andre ledd og virksomhetsikkerhetsforskriften § 7
- Risikovurdering og risikohåndtering. Kopi av lokal risikovurdering må sendes inn, jf. sikkerhetsloven §§ 4-2 og 4-4 og virksomhetsikkerhetsforskriften §§ 12 og 13.

- Beskrivelse av lokalt etablerte sikkerhetstiltak (grunnsikringstiltak) og planlagte påbyggingstiltak samt tegning/skisse av lokalene hvor sikkerhetsgradert informasjon skal oppbevares og behandles, jf. sikkerhetsloven § 4-4 og virksomhetsikkerhetsforskriften §§ 14 og 15.

4.2.1. Autorisasjon

Leverandørens daglig leder skal autoriseres av oppdragsgiver før sikkerhetsavtale inngås. Daglig leder er autorisasjonsansvarlig og har ansvaret for at eget personell som skal ha tilgang til informasjon gradert BEGRENSET, som oppbevares i leverandørens egne lokaler, er autorisert før tilgang gis. Det skal gjennomføres en autorisasjonssamtale før det gis autorisasjon. Krav til autorisasjonssamtalens innhold er gitt i virksomhetsikkerhetsforskriften § 68 andre ledd.

Daglig leder er også ansvarlig for sikkerhetsmessig ledelse og kontroll av eget personell som er autorisert.

Informasjon som inneholder personopplysninger i saker om autorisasjon, personkontroll eller klarering, skal merkes PERSONKONTROLL. Kravet gjelder ikke meldinger om at det er gitt en autorisasjon eller klarering eller meldinger om andre autorisasjons- eller klareringsavgjørelser til personen som avgjørelsen gjelder.

Den autorisasjonsansvarlige skal bestemme hvem i virksomheten som kan få tilgang til opplysninger merket PERSONKONTROLL. Slike opplysninger skal lagres atskilt fra andre opplysninger i virksomheten, og de skal bare være tilgjengelige for det utpekte personellet. Når virksomheten utveksler opplysninger merket PERSONKONTROLL, skal det gjøres på en slik måte at uvedkommende ikke får tilgang til opplysningene.

Den som skal autoriseres skal signere en taushetserklæring på blankett fastsatt av NSM før det gis autorisasjon.

4.2.2. Autorisasjon av utenlandsk statsborger

Før en utenlandsk statsborger som ikke har klarering, kan autoriseres for informasjon gradert BEGRENSET, skal den autorisasjonsansvarlige vurdere om personens tilknytning til hjemlandet og hjemlandets sikkerhetsmessige betydning utgjør en uakseptabel risiko. Den autorisasjonsansvarlige kan be klareringsmyndigheten om en vurdering av hjemlandets sikkerhetsmessige betydning.

Dersom en utenlandsk statsborger kommer fra en stat som Politiets sikkerhetstjeneste (PST) mener utgjør en høy sikkerhetsrisiko for Norge, se PSTs årlige nasjonale trusselvurdering, må den autorisasjonsansvarlige innhente samtykke fra en klareringsmyndighet før den utenlandske statsborgeren kan autoriseres for BEGRENSET. Dette kravet gjelder også for personer som har dobbelt statsborgerskap (hvorav det ene er norsk), er statsløse eller har uavklart statsborgerskap.

Det gjøres oppmerksom på at det er leverandørens risiko at autorisasjon ikke oppnås. Han har også risikoen for at autorisasjon tar uforholdsmessig lang tid, med mindre forsinkelsen skyldes forhold oppdragsgiver svarer for.

4.2.3. Godkjenning av skjermingsverdige informasjonssystem

NSM er godkjenningsmyndighet for skjermingsverdige informasjonssystemer som er angitt i virksomhetsikkerhetsforskriften § 51 første og andre ledd. Skjermingsverdige informasjonssystemer som ikke er nevnt i første og andre ledd skal godkjennes av leverandøren, men oppdragsgiver skal gi tillatelse før informasjonssystemet kan tas i bruk.

Leverandøren skal sørge for et forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer. I virksomhetsikkerhetsforskriften § 49 stilles det funksjonelle krav for skjermingsverdig informasjonssystemer. Ved å følge NSMs og Forsvarsbyggs veiledere for godkjenning av informasjonssystemer anses kravene § 49 som ivarettatt.

Leverandøren må ha en sikkerhetsavtale for angjeldende anskaffelse før skjermingsverdig informasjonssystem kan installeres og tas i bruk.

Følgende dokumentasjon må utarbeides i forbindelse med godkjenning av skjermingsverdige informasjonssystemer:

- Systembeskrivelse
- Brukerinstruks
- Driftsinstruks

- Beredskapsplan
- Konfigurasjonsoversikt
- Nettverkstegning dersom lokalt lukket nettverk
- Godkjenningsskriv

Oppdragsgiver har maler for hver av de ovennevnte dokumenter.

4.2.4. Unntak fra krav om sikkerhetsavtale

Det kreves ikke sikkerhetsavtale dersom leverandørens personell bare skal gis tilgang til sikkerhetsgradert informasjon, skjermingsverdige objekter eller infrastruktur under oppsyn av en representant for oppdragsgiver. I «Veiledning for sikkerhetsgraderte anskaffelser» klargjøres det for hva som menes med «oppsyn».

For å oppnå et forsvarlig sikkerhetsnivå under anskaffelsen kan oppdragsgiver, med bakgrunn i risikovurdering, beslutte at sikkerhetsavtale skal inngås selv om kravet til oppsyn er oppfylt.

4.2.5. Innholdet i sikkerhetsavtalen

Sikkerhetsavtalen skal tydeliggjøre og konkretisere partenes plikter og ansvar etter sikkerhetsloven med forskrifter. Sikkerhetsavtale skal inngås for hver enkelt sikkerhetsgradert anskaffelse.

I virksomhetsikkerhetsforskriften § 80 stilles det krav til innholdet i sikkerhetsavtalen.

Ved inngåelse av sikkerhetsavtale på BEGRENSET nivå vil oppdragsgiver stille krav om at leverandøren forplikter seg til å:

- vedlikeholde styringssystemet for sikkerhet
- regelmessig gjennomføre vurdering av risiko og håndtere risiko
- påse at sikkerhetstiltak (fysiske, elektroniske, menneskelige og organisatoriske) for sikkerhetsgradert informasjon og informasjonssystemer som skal behandle slik informasjon, er tilpasset aktuell risiko og oppfyller kravet til forsvarlig sikkerhetsnivå
- påse at eget personell, før de gis tilgang til sikkerhetsgradert informasjon og skjermingsverdige informasjonssystemer, har gjennomført grunnleggende opplæring i sikkerhet
- gjøre styringsdokument for sikkerhet og relevante sikkerhetsinstrukser for rutiner og prosedyrer kjent og tilgjengelig for eget personell
- oppfylle kravene for autorisasjonssamtale og autorisasjon av eget personell som har tjenstlig behov for tilgang til sikkerhetsgradert informasjon og skjermingsverdig informasjonssystem som leverandøren har i sine egne lokaler
- ivareta sikkerhetsmessig ledelse og kontroll av eget personell som er autorisert
- orientere oppdragsgiver om forhold som kan ha betydning for leverandørens leders sikkerhetsmessige skikkethet
- overholde taushetsplikten også etter at anskaffelsen er avsluttet
- løpende kontrollere at sikkerhetstiltak fungerer etter sin hensikt og at sikkerhetsbestemmelser følges
- håndtere og rapportere avvik fra sikkerhetskrav/sikkerhetsbrudd til oppdragsgiver
- påse at sikkerhetsgradert informasjon ikke utleveres til tredjepart uten at samtykke fra oppdragsgiver på forhånd foreligger
- ikke offentliggjøre deltakelse i sikkerhetsgradert anskaffelse på Internett eller i markedsføring
- orientere oppdragsgiver om forhold som er av sikkerhetsmessig betydning, herunder endring av foretaksnavn, skifte av daglig leder, flytting/ombygging av lokaler, åpning av gjeldsforhandlinger, begjæring om konkurs og annet som kan påvirke leverandørens sikkerhetsmessige skikkethet
- legge til rette for at oppdragsgiver kan gi råd og veiledning om forebyggende sikkerhetstjeneste
- legge til rette for at oppdragsgiver kan kontrollere at leverandøren oppfyller kontraktsforpliktelser knyttet til forebyggende sikkerhetstjeneste
- legge til rette for at NSM eller sektormyndighet med tilsynsansvar kan kontrollere sikkerhetstilstanden hos leverandøren

4.2.6. Brudd på sikkerhetskrav

Dersom leverandøren ikke retter brudd på kravene fastsatt i eller med hjemmel i sikkerhetsloven innen en fastsatt frist, kan oppdragsgiver si opp sikkerhetsavtalen. Er et brudd vesentlig, kan oppdragsgiver si opp sikkerhetsavtalen uten at det settes en frist.

4.2.7. Ytterligere sikkerhetskrav

Det understrekes at ovennevnte krav ikke er uttømmende. I enkelte anskaffelser kan det, med bakgrunn i økt risiko knyttet til verdier, trusler eller sårbarheter bli stilt ytterligere krav til sikkerhet, jf. generelle krav til beskyttelse av skjermingsverdige verdier i virksomhetsikkerhetsforskriften kapittel 3.

4.2.8. NSMs veiledere og håndbøker

For leverandører med sikkerhetsavtale på BEGRENSET nivå vil NSMs veiledninger og håndbøker være relevante å benytte i det forebyggende sikkerhetsarbeidet, se <https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/>

5. Sikkerhetsgraderte anskaffelser på KONFIDENSIELT nivå eller høyere

5.1. Forsvarlig sikkerhetsnivå for informasjon som er gradert KONFIDENSIELT eller høyere

Virksomhetsikkerhetsforskriften kapittel 6 fastsetter krav til beskyttelse av informasjon gradert KONFIDENSIELT eller høyere.

Kravene til sikkerhetsdokumentasjon og håndtering og beskyttelse av informasjon gradert KONFIDENSIELT eller høyere kommer i tillegg til kravene som gjelder for ugradert skjermingsverdig informasjon og informasjon gradert BEGRENSET.

5.1.1. Soneinndeling for informasjon gradert KONFIDENSIELT eller høyere

For å beskytte sikkerhetsgraderte informasjon og informasjonssystem gradert KONFIDENSIELT eller høyere, skal det etableres en kontrollert og beskyttet sone. Dersom leverandøren har et område med direkte tilgang til informasjon gradert KONFIDENSIELT eller høyere, for eksempel arkivrom eller serverrom, skal det etableres en sperret sone rundt dette området.

En kontrollert sone skal være et tydelig avgrenset område der leverandøren skal kunne ha kontroll med personer, kjøretøy og annen aktivitet. Ved særlig høy risiko skal adgang og ferdsel kontrolleres med en fysisk avgrensning.

En beskyttet sone skal ha en fysisk avgrensning der sikkerhetstruende virksomhet skal kunne oppdages. I en beskyttet sone skal dokumenter og lagringsmedier med informasjon som er gradert KONFIDENSIELT eller høyere lagres i oppbevaringsenhet godkjent av NSM.

Dokumenter og lagringsmedier med informasjon som er gradert KONFIDENSIELT, skal bare oppbevares og behandles i en beskyttet sone eller sperret sone. Typiske sperrede soner vil være arkiver og dokumenthvelv, operasjonsrom, kommunikasjons- og serverrom eller lokaler der det lages sikkerhetsgraderte produkter. Dette er altså spesialrom hvor sikkerhetsgradert informasjon er åpent eller lett tilgjengelig for den som har adgang.

Personer som skal gis permanent adgang til en beskyttet eller sperret sone, skal være sikkerhetsklarert og autorisert. Det skal være kontroll med adgangen.

5.1.1.1. Balansert sikring

Verken virksomhetsikkerhetsforskriften eller NSMs veiledninger gir konkrete føringer om hvilke sikkerhetstiltak som til enhver tid er tilstrekkelig for å oppnå et forsvarlig sikkerhetsnivå. Dette må fremkomme i en risikovurdering som gjennomføres av den enkelte virksomhet.

For å redusere risiko for innbrudd kan kravet om forsvarlig sikkerhetsnivå langt på vei oppnås gjennom balansert sikring. Med balansert sikring menes at det er balanse mellom fysiske sikkerhetstiltak, deteksjonstiltak, og reaksjonstid. Balansert sikring oppnås når tiden det tar å bryte seg gjennom de ulike fysiske barrierene er lengre enn summen av tiden det tar å detektere og varsle innbruddet, og den tiden det tar før reaksjonsstyrken (vekter, politi etc.) kan være på lokasjonen.

Dersom balansert sikring ikke kan oppnås skal oppdragsgiver ta stilling til om det er nødvendig å forsterke de eksisterende fysiske sikringstiltakene (grunnsikringstiltak) eller etablere ytterligere tiltak (påbyggingstiltak) for å redusere restrisiko til et akseptabelt nivå.

5.1.2. Godkjenning av skjermingsverdig informasjonssystem

NSM er godkjenningsmyndighet for skjermingsverdige informasjonssystemer som er angitt i virksomhets sikkerhetsforskriften § 51 første og andre ledd. Skjermingsverdige informasjonssystemer som ikke er nevnt i første og andre ledd skal godkjennes av leverandøren, men oppdragsgiver skal gi tillatelse før informasjonssystemet kan tas i bruk.

Leverandøren skal sørge for et forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer. I virksomhets sikkerhetsforskriften § 49 stilles det funksjonelle krav for skjermingsverdig informasjonssystemer. Ved å følge NSMs og Forsvarsbyggs veiledere for godkjenning av informasjonssystemer anses kravene § 49 som ivarettatt.

Leverandøren må ha en leverandørklarering og sikkerhetsavtale for angjeldende anskaffelse før skjermingsverdig informasjonssystem kan installeres og tas i bruk.

Tempestrisikovurdering må utarbeides i tillegg til dokumentasjonen som er aktuell for skjermingsverdig informasjonssystem på BEGRENSET nivå. Oppdragsgiver kan fremskaffe mal for Tempestrisikovurdering.

5.1.3 Leverandørklarering

En leverandør til en sikkerhetsgradert anskaffelse skal ha en leverandørklarering når det er nødvendig for å oppnå et forsvarlig sikkerhetsnivå under anskaffelsen. Leverandørklarering gis av NSM.

Leverandør som skal oppbevare, behandle eller tilvirke informasjon gradert KONFIDENSIELT eller høyere i egne lokaler, skal uansett ha leverandørklarering før sikkerhetsavtale kan inngås med oppdragsgiver.

Før leverandørklarering kan gis skal NSM kontrollere at leverandøren oppfyller kravene i sikkerhetsloven, virksomhets sikkerhetsforskriften og klareringsforskriften.

5.1.4 Sikkerhetsklarering og autorisasjon av leverandørpersonell

Leverandørpersonell som har behov for tilgang til informasjon som er sikkerhetsgradert KONFIDENSIELT eller høyere skal ha gyldig sikkerhetsklarering for angjeldende sikkerhetsgrad. Kravet som sikkerhetsklarering gjelder også for leverandørpersonell som har behov for tilgang til skjermingsverdig objekt eller skjermingsverdig infrastruktur.

Før leverandørklarering kan gis skal leverandørens leder og styremedlemmer sikkerhetsklarerer for det samme nivå som det er anmodet om leverandørklarering for. Dersom leverandørens leder eller et styremedlem ikke kan sikkerhetsklarerer, må vedkommende skriftlig gi avkall på innsyn i den sikkerhetsgraderte anskaffelsen.

Leverandøren må påregne minimum tre måneders saksbehandlingstid for sikkerhetsklarering av personell som kun er norske statsborgere. Saksbehandlingstiden regnes fra korrekt utfylt personopplysningsblankett (POB) er mottatt av klareringsmyndigheten.

En person som har utenlandsk statsborgerskap, kan etter en konkret helhetsvurdering få sikkerhetsklarering, dersom det ikke er rimelig grunn til å tvile på at personen er sikkerhetsmessig skikket. I tillegg til forholdene som er nevnt i sikkerhetsloven § 8-4 skal det i vurderingen legges vekt på hjemlandets sikkerhetsmessige betydning, personens tilknytning til hjemlandet og tilknytningen til Norge. Utfallet av slike søknader er usikkert, og i alle tilfeller må det påregnes vesentlig lengre saksbehandlingstid enn for norske statsborgere.

Leverandørens leder skal autoriseres av oppdragsgiver før sikkerhetsgradert informasjon utleveres til eller tilvirkes i leverandørens egne lokaler.

Leverandørens leder skal sørge for at eget personell, som har behov for tilgang til informasjon gradert KONFIDENSIELT eller høyere som er i leverandørens besittelse, har gyldig sikkerhetsklarering for angjeldende sikkerhetsgrad før autorisasjon gis.