



KONKURRANSEGRUNNLAGETS DEL II

mobil oppvarmings og ventilasjonsløsning plasthaller væskebasert varmepumpe Akkasæter region Nord

**Avtaledokument med kontraktsbestemmelser som utfyller lov om kjøp av 13.5.1988
nr 27 (kjøpsloven)**

Vedlegg:

- Mal for endringsavtale
- Orientering til leverandører om krav til håndtering og beskyttelse av skjermingsverdig informasjon i forbindelse med anskaffelser

Dette dokumentet er kun ment som en orientering til tilbyderne, og skal således ikke fylles ut i forbindelse med tilbudsinnleveringen

AVTALEDOKUMENT TILVIRKNINGSKJØP AV VARER

1 Partene og deres representanter

| Oppdragsgiver | | |
|---|----------------|--|
| Navn: | | Organisasjonsnr: |
| Staten v/Forsvarsdepartementet v/Forsvarsbygg | | 975 950 662 |
| Adresse: | | |
| Grev Wedels plass 5, 0151 Oslo. Postboks 405 Sentrum, 0103 Oslo | | |
| Representant: | Tlf: | E-post |
| Olav Christoffer Breilid | +47 951 22 620 | Olav.Christoffer.Breilid@forsvarsbygg.no |

| Leverandøren | | |
|---------------|------|------------------|
| Navn: | | Organisasjonsnr: |
| Adresse: | | |
| Representant: | Tlf: | E-post |

Alle henvendelser knyttet til gjennomføringen av denne kontrakten skal rettes til partenes representanter. Representantene er bemyndiget til å opptre på vegne av partene i saker som angår kontrakten.

Partene er enige om at:

elektronisk kommunikasjon aksepteres

2 Kontraktsdokumenter. Tolkningsregler

Følgende dokumenter inngår som en del av denne kontrakten:

1. Dette avtaledokumentet
2. Referater og annet materiale fra forhandlinger og oppklarende drøftelser, som er godkjent av begge parter
3. Leverandørens tilbud
4. Forsvarsbyggs konkurransegrunnlag
5. Kjøpsloven

Ved motstrid gjelder dokumentene i ovennevnte rekkefølge. Dersom dette ikke løser motstridssituasjonen, skal spesielle bestemmelser gjelde foran generelle.

3 Om leveransen

3.1 Bestilt ved avtaleinngåelsen

Ved avtaleinngåelsen er følgende leveranse bestilt av oppdragsgiveren:

Se konkurransegrunnlagets del III.

3.2 Endringer av avtalen

Avtalen kan bare endres ved at begge parter undertegner en endringsavtale, jfr. mal vedlagt konkurransegrunnlagets del II. Leverandøren kan ikke påberope seg uttalelser, handlinger eller unnlatelser fra oppdragsgiverens side, herunder møtereferater og korrespondanse, som grunnlag for at avtalen er endret.

3.3 Opsjoner

Oppdragsgiver har rett, men ingen plikt, til å bestille følgende tilleggsytelser fra leverandøren:

| Beskrivelse av opsjonen | Frist for bestilling |
|---|----------------------------------|
| Opsjon på kjøp av ytterligere 10 enheter. | 24 mnd. etter kontraktsignering. |

4 Levering og tidsfrister

4.1 Levering og mottakskontroll

Leveransen(e) skal skje til følgende adresse:

Akkasæter

Når leveransen ankommer leveringsstedet, skal det holdes mottakskontroll. Med mottakskontroll menes opptelling av ytelsens bestanddeler og kontroll av dokumentasjon i henhold til avtalen. Mottakskontroll kan ikke avholdes uten oppdragsgiverens tilstedeværelse. Leverandøren skal i rimelig tid varsle oppdragsgiver om tidspunkt for mottakskontroll og dersom avtalt mottakskontroll ikke kan avholdes som planlagt. Det skal utarbeides en protokoll i forbindelse med mottakskontrollen som begge parter skal undertegne. Levering anses skjedd når mottakskontroll er foretatt og protokollen er undertegnet av begge parter.

Alt materiell og tjenester som omfattes av avtalen skal leveres DDP (Incoterms 2020) til avtalt leveringsadresse. Det vil si fritt levert.

4.2 Leverandørens tidsfrister

| Ytelse: | Frist: | Dagmulkt: (Ja, Nei eller beløp) |
|--|--------------------------------|------------------------------------|
| Hovedleveransen skal påbegynnes: | Avtales ved kontraktsinngåelse | Nei |
| Hovedleveransen skal være ferdigstilt: | Innen 15. desember 2026. | Nei |
| Opsjoner: | | |
| Frister for påbegynnelse og ferdigstilling av opsjoner avtales med valgt leverandør. | | |

5 Bestemmelser om pris

5.1 Kontraktssum

| | |
|-------------------------|------------|
| Hovedleveranse | NOK |
| Opsjonspris | NOK |
| Totalpris opsjonspriser | NOK |
| Merverdiavgift | NOK |
| Til sammen | NOK |
| Kontraktssummen | NOK |

5.2 Regulering av prisen

Prisene justeres på følgende måte:

Leverandør kan be om prisjustering av enhetsprisene for ytterligere opsjoner etter gjeldende indeksregulering.

Tidligst 12 mnd. etter tilbudsfrist.

Dersom ikke annet fremgår ovenfor, ligger prisene fast i hele kontraktsperioden.

Gis det i kontraktsperioden tilbud på tilleggsleveranser, skal prisene ikke reguleres med mindre annet avtales.

6 Betaling og fakturering

6.1 Fakturering

Fakturering skal skje når ytelsen er levert og overtatt av oppdragsgiver. Hvis ikke annet er avtalt.

6.1 Betalingsbetingelser

Betaling skal skje innen 30 dager etter at både leveransen og korrekt merket faktura med avtalte bilag er mottatt av Forsvarsbygg.

Ved delleveranser: Betaling skjer innen 30 dager etter at både delleveransen og fakturaer med avtalte bilag er mottatt.

Betaling innebærer ingen godkjenning av grunnlaget for vedkommende faktura eller frafall av mangelsinnsigelser.

Dersom oppdragsgiver ikke betaler til rett tid, skal oppdragsgiver betale forsinkelsesrente i henhold til lov om renter ved forsinket betaling m.m. av 17.12.1976 nr. 100.

6.2 Krav til fakturaene

Faktura og kreditnota skal sendes elektronisk til Forsvarsbyggs fakturamottak i samsvar med standarden Elektronisk handelsformat (EHF). Forsvarsbyggs elektroniske fakturaadresse er **975950662**. For nærmere informasjon om fremgangsmåte, se www.ehandel.no.

Alle fakturaer skal inneholde:

- Innkjøpsordrenummer, opprettes ved avtaleinngåelse. oppgis «Order reference».
- Videre skal beskrivelsesfeltet inneholde opplysninger om hvilke ytelser/leveranser fakturaen gjelder. Fakturaene skal spesifiseres og dokumenteres slik at de kan kontrolleres av oppdragsgiveren.

Ved manglende eller feil merking vil leverandøren kunne få beskjed om at den umerkede/feilmerkede fakturaen ikke vil bli behandlet. Leverandøren plikter da å kreditere den umerkede fakturaen og utstede en ny korrekt faktura med ny fakturadato og nytt forfall.

7 Retting og omlevering (avhjelp) av mangler

Leverandøren har ikke rett til å foreta mer enn to avhjelpsforsøk av samme mangel, med mindre det foreligger særlige grunner som gjør at ytterligere avhjelp er rimelig.

8 Øvrige bestemmelser

8.1 Forsikring

Leverandøren skal inneha eller tegne ansvarsforsikring på vanlige vilkår med et forsvarlig beløp som er dekkende i forhold til det ansvar han kan komme i som følge av denne avtale. Forsikringsbevis skal forelegges oppdragsgiveren for kontroll, hvis oppdragsgiveren ber om det. Leverandøren har alene ansvaret for at forsikringen er dekkende, uavhengig av oppdragsgiverens kontroll.

8.2 Kvalitetssikring

Leverandøren skal ha et kvalitetssikringssystem som er innrettet slik at faktiske mangler, potensielle mangler og andre forhold som kan føre til utilfredsstillende kvalitet, blir oppdaget så tidlig som mulig.

Oppdragsgiver har rett til å kontrollere alle forhold ved leverandørens oppfyllelse av sine forpliktelser, slik som utvikling, konstruksjon og tilvirkning på alle trinn under avtalen. Dette gjelder også ethvert dokument eller nedtegnelse. Oppdragsgiveren skal gi leverandøren varsel i rimelig tid før kontrollen gjennomføres.

Oppdragsgiverens rett til å kontrollere etter annet ledd, er uavhengig av på hvilket sted leverandøren utfører sine forpliktelser etter avtalen. Dersom leverandøren utfører noen av sine forpliktelser etter avtalen i utlandet, har oppdragsgiveren rett til å delegere gjennomføring av kvalitetssikring til vedkommende lands militære myndighet. Oppdragsgiverens kvalitetssikring fritar ikke leverandøren for de forpliktelser han har påtatt seg i avtalen. Manglende utført kvalitetssikring medfører ingen reduksjon av oppdragsgiverens rettigheter etter avtalen.

8.3 Immaterielle rettigheter

8.3.1 Brudd på tredjemanns immaterielle rettigheter

Leverandøren skal ikke krenke patenter eller andre immaterielle rettigheter i forbindelse med oppfyllelse av avtalen. Leverandøren skal holde oppdragsgiver skadesløs for ethvert krav som følge av krenkelse av patenter eller andre immaterielle rettigheter i forbindelse med oppfyllelse av avtalen.

Oppdragsgiveren skal holde leverandøren skadesløs for ethvert krav som skyldes bruk av oppdragsgiverens tegninger, spesifikasjoner eller lisenser.

Partene skal gjensidig varsle hverandre om krav vedrørende krenking av patenter eller andre immaterielle rettigheter ved fremstilling eller bruk av leveransen.

8.3.2 Patenter og sikkerhetsbeskyttet informasjon

Dersom leverandøren ønsker å søke om patent som inneholder sikkerhetsbeskyttet informasjon, skal leverandøren fremlegge søknaden for oppdragsgiveren for skriftlig godkjenning før patentsøknaden innleveres. Oppdragsgiveren kan nekte godkjenning uten begrunnelse.

8.3.3 Bruk av dokumentasjon

Oppdragsgiver har rett til å bruke dokumentasjon, som overleveres i forbindelse med leveransen, til utdanning, bruk, kodifisering, vedlikehold og reparasjon. Oppdragsgiveren har rett til å kopiere dokumentasjonen til egen bruk.

8.4 **Rettigheter til materiell som oppdragsgiveren overlater til leverandøren og merking**

8.4.1 Rettigheter til materiell som oppdragsgiveren overlater til leverandøren

Oppdragsgiveren har eiendomsrett og alle andre rettigheter til alt materiell som oppdragsgiveren overlater til leverandøren i forbindelse med gjennomføring av avtalen. Dette gjelder også eventuelt skrap og overskuddsmateriell som stammer fra dette materialet.

8.4.2 Merking av oppdragsgiverens eiendom

Leverandøren skal merke oppdragsgiverens eiendom som er i leverandørens besittelse tydelig med "Forsvarets eiendom". Oppdragsgiverens eiendom skal oppbevares adskilt fra andre leveranser, annet materiell, annet utstyr m.v. slik at eiendommen lar seg identifisere.

8.5 **Etiske krav**

Leverandøren plikter å gjøre seg kjent med og overholde de etiske krav og retningslinjer som oppdragsgiveren har utarbeidet. De etiske kravene og retningslinjene kan leses på www.forsvarsbygg.no.

8.6 **Krav til etisk handel**

8.6.1 Ansattes rettigheter

8.6.1.1 ILOs kjernekonvensjoner

Leverandøren skal etterleve følgende grunnleggende krav:

- a) Forbud mot barnearbeid (FNs barnekonvensjon artikkel 32, ILO-konvensjoner nr. 138 og 182): Barn har rett til å bli beskyttet mot økonomisk utnyttning i arbeid, og mot å utføre arbeid som kan svekke utdannings- og utviklingsmuligheter. Minstealderen må ikke i noe tilfelle være under 15 år (14 eller 16 år i visse land). Barn under 18 år skal ikke utføre arbeid som setter helse eller sikkerhet i fare, inkludert nattarbeid. Dersom det foregår slikt barnearbeid, skal det arbeides for snarlig utfasing. Det skal samtidig legges til rette for at barna gis mulighet til livsopphold og utdanning inntil barnet ikke lenger er i skolepliktig alder.
- b) Forbud mot tvangsarbeid/slavearbeid (ILO-konvensjoner nr. 29 og 105): Det skal ikke forekomme noen form for tvangsarbeid, slavearbeid eller ufrivillig arbeid. Arbeiderne må ikke levere depositum eller identitetspapirer til arbeidsgiver, og skal være fri til å avslutte arbeidsforholdet med rimelig oppsigelsestid.
- c) Forbud mot diskriminering (ILO-konvensjoner nr. 100 og 111): Det skal ikke forekomme noen diskriminering i arbeidslivet basert på etnisk tilhørighet, religion, alder, uførhet, kjønn, ekteskapsstatus, seksuell orientering, fagforeningsmedlemskap eller politisk tilhørighet.
- d) Organisasjonsfrihet og retten til kollektive forhandlinger (ILO-konvensjoner nr. 87 og 98): Arbeiderne skal uten unntak ha rett til å slutte seg til eller etablere fagforeninger etter eget valg, og å forhandle kollektivt. Dersom disse rettigheter er begrenset eller under utvikling, skal leverandøren medvirke til at de ansatte får møte ledelsen for å diskutere lønns- og arbeidsvilkår uten at dette får negative konsekvenser for arbeiderne.

8.6.2 Oppfølging

Leverandøren skal påse at ansattes rettigheter i punkt 8.6.1 etterleves i egen virksomhet og hos den eller de underleverandører som medvirker til oppfyllelse av kontrakten. På oppfordring fra oppdragsgiver skal dette dokumenteres ved:

- Egenrapportering, og/eller
- Oppfølgingssamtaler, og/eller
- En uavhengig parts kontroll av arbeidsforholdene, og/eller
- Tredjepartssertifisering som SA8000 eller tilsvarende.

Leverandøren har bevisbyrden for at de varer og materialer som leveres ikke innebærer et brudd på punkt 8.6.1 ovenfor.

8.6.3 Brudd

Brudd på punkt 8.6.1 eller 8.6.2 innebærer mislighold av kontrakten. Ved slikt mislighold plikter leverandøren å rette de påpekte manglene, uavhengig av kostnadene ved slik retting, innen en tidsfrist som oppdragsgiver bestemmer, så lenge fristen ikke er urimelig kort. Rettelsene skal dokumenteres skriftlig og på den måten oppdragsgiver bestemmer. Oppdragsgiver har rett til å holde tilbake deler av kontraktssummen, tilsvarende ca. to ganger besparelsen for leverandøren, til det er dokumentert at forholdet er rettet.

Ved manglende utbedring vil det etter oppdragsgivers skjønn kunne påløpe en bot på inntil 1 % av kontraktssummen per mislighold. Likeartede brudd anses som ett mislighold. Vesentlig mislighold av plikter som følger av punkt 8.6.1 eller 8.6.2 kan påberopes som grunnlag for heving, selv om leverandøren retter forholdet. Dersom misligholdet har skjedd hos underleverandør, herunder bemanningsselskaper, kan oppdragsgiver på samme måte kreve at leverandøren skifter ut underleverandøren. Dette skal skje uten omkostninger for oppdragsgiver. Leverandøren blir videre ansvarlig for det tap som oppdragsgiver lider som følge av mangelen. Eventuell erstatning kommer i tillegg til ovennevnte bot.

Alle avtaler leverandøren inngår for utføring av arbeid under denne kontrakten, skal inneholde tilsvarende bestemmelser som for punkt 8.6.1, 8.6.2 og 8.6.3.

8.6.4 Korrupsjonsforebygging

Leverandøren plikter å arbeide for å forhindre korrupsjon i sin virksomhet. Leverandøren må kunne vise til at de har iverksatt tiltak eller har systemer som skal forebygge korrupsjon og påvirkningshandel. Dette kan være etablering av internkontroll, utarbeidelse av etiske retningslinjer, opprettelse av varslingskanal og lignende, og som minimum går ut på å forebygge korrupsjon og påvirkningshandel.

8.6.5 Ivaretagelse av grunnleggende menneskerettigheter i leverandørkjeden

Dette kontraktskravet gjelder for leverandørene som faller inn under virkeområdet til åpenhetsloven, jf. åpenhetsloven § 2.

Leverandøren skal under hele kontraktsperioden overholde punktene i dette kontraktsvilkåret for å ivareta åpenhetslovens krav til dokumentasjon, og gjennomføring og oppfølging av aktsomhetsvurderinger. Kontraktsvilkårene bygger på FNs veiledende prinsipper for næringsliv og menneskerettigheter og OECDs retningslinjer for ansvarlig næringsliv med aktsomhetsvurderinger som metode.

Dersom leverandøren bruker underleverandører for å oppfylle denne kontrakt, er leverandøren forpliktet til å videreføre og bidra til etterlevelse av kravene i leverandørkjeden.

8.6.5.1 Retningslinjer og prosedyrer for aktsomhetsvurderinger

For å sikre etterlevelse av kravene i punkt 8.6.1.1, samt for å forebygge og håndtere eventuelle avvik fra kravene, skal leverandøren senest innen 6 måneder etter kontraktsinngåelse, ha retningslinjer og prosedyrer på plass for aktsomhetsvurdering.

Det betyr at leverandøren skal kartlegge, forebygge, begrense og gjøre rede for hvordan de håndterer risiko for negativ påvirkning på kravene i punkt 8.6.1.1, og retter opp skade. I tråd med metoden for aktsomhetsvurderinger skal interessenter, særlig berørte rettighetshavere, involveres. Alvorligst risiko, uavhengig av hvor i leverandørkjeden risikoen er, prioriteres først.

Senest innen 6 måneder etter kontraktsinngåelse, skal leverandøren ha:

- En eller flere offentlig tilgjengelige retningslinjer for ivaretagelse av grunnleggende menneskerettigheter i leverandørkjeden, vedtatt av styret. Innholdet skal som minimum omfatte en forpliktelse om å etterleve kravene i punkt 8.6.1.1, i egen virksomhet og i leverandørkjeden.
- En eller flere ansatte på ledelsesnivå som har ansvar for etterlevelse og rapportering om arbeidet med aktsomhetsvurderinger til styret.
- Prosedyrer for formidling og regelmessig oppfølging av retningslinjer og prosedyrer i egen virksomhet og i leverandørkjeden.
- Prosedyrer for å utføre regelmessige risikoanalyser i egen virksomhet og i leverandørkjeden. Det innebærer å kartlegge og vurdere risiko for brudd på kravene i punkt 8.6.1.1.
- Prosedyrer som beskriver hvilke tiltak leverandøren vil iverksette for å stanse, forebygge eller redusere negativ påvirkning og skade på kravene i punkt 8.6.1.1.

Leverandøren skal kunne vise til offentlig tilgjengelig informasjon om arbeidet med aktsomhetsvurderinger i egen virksomhet og i leverandørkjeden. Dette omfatter hvordan risiko for brudd på kravene i punkt 8.6.1.1, og eventuell skade i egen virksomhet og i leverandørkjeden, er håndtert.

Dersom leverandøren har forårsaket, eller medvirket til skade, skal leverandøren sørge for å rette opp skaden og yte erstatning til skadelidende.

8.6.5.2 Kontraktsoppfølging

Leverandøren skal sikre at kravene i punkt 8.6.1.1 samt 8.6.5.1 etterleves i egen virksomhet og i leverandørkjeden. Dersom leverandøren blir klar over forhold i strid med punkt 8.6.1.1 samt 8.6.5.1 i leverandørkjeden, skal leverandøren rapportere dette til oppdragsgiver uten ugrunnet opphold.

Oppdragsgiver kan kreve at etterlevelse dokumenteres ved hjelp av et eller flere av følgende tiltak:

- Fremviser vedtatte retningslinjer og prosedyrer, jf. punkt 8.6.1.1.
- Fremviser en oversikt over produksjonseenheter i leverandørkjeden, inkludert kontaktopplysninger, for utvalgte produkter, og/eller komponenter og/eller råvarer. Oppdragsgiver angir hvilke produkter og hvilken del av leverandørkjeden.
- Fremviser gjennomført risikoanalyse, og rapportere om oppfølging og håndtering av funnene.
- Delta i oppfølgingsamtale(r) med oppdragsgiver og eventuelt andre relevante interessenter.
- Kontroll og revisjon av kravene i punkt 8.6.1.1 samt 8.6.5.1 hos leverandøren og i leverandørkjeden.

Kontraktsoppfølgingen kan gjennomføres av oppdragsgiver eller av offentlig enhet som oppdragsgiver samarbeider med.

Oppdragsgiver forbeholder seg retten til å dele revisjonsrapportene med andre offentlige virksomheter, som vil omfattes av taushetsplikten.

8.6.5.3 Sanksjoner

Ved brudd på punkt 8.6.5.1, 8.6.5.2, eller om det foreligger mangler i dokumentasjonen, gjelder punkt 8.6.3 Brudd.

8.7 Skatte- og avgiftsforpliktelser

8.7.1 Oppdragsgivers rett til å innhente opplysninger fra skattemyndighetene

Før kontraktsinngåelse skal leverandøren gi oppdragsgiver en fullmakt for innhenting av opplysninger om skatt og avgift (OSA), se vedlegg til Del I - Innbydelse. Tilsvarende gjelder for underleverandør som benyttes for å oppfylle et kvalifikasjonskrav.

Fullmakten gir oppdragsgiver rett til, et ubegrenset antall ganger, å innhente taushetsbelagte opplysninger fra skattemyndighetene som er angitt i fullmakten. De rettigheter og plikter som fremgår av fullmakten, gjelder i 4 år fra signering av fullmakten. Fullmakten er generell for Forsvarsbygg, og opprettholdelse av fullmakten er vesentlig for kontraktsforholdet.

Fullmakt for innhenting av opplysninger om skatt og avgift (OSA) skal undertegnes av alle underleverandører så tidlig som mulig, dog minimum 10 dager før oppstart av underleverandørens arbeid med mindre annet skriftlig avtales med oppdragsgiver.

8.7.2 Plikt til å etterleve skatte- og avgiftslovgivningen

Leverandøren skal til enhver tid etterleve Norges skatte- og avgiftslovgivning, herunder levere skattemeldinger og a-meldinger samt betale skatt og avgift i henhold til skatteforvaltningslovens frister. Det samme gjelder underleverandører.

Oppdragsgiver kan under kontraktsperioden kreve at Leverandøren betaler utestående skatt eller avgift uten ugrunnet opphold. Dersom restansene gjelder en underleverandør kan Oppdragsgiver kreve at Leverandøren sørger for at underleverandøren betaler det utestående uten ugrunnet opphold.

Brudd på overnevnte plikter gir oppdragsgiver rett til å kreve at forholdet rettes opp, eller om nødvendig bytte ut underleverandør, innen en rimelig frist gitt ved skriftlig varsel fra oppdragsgiver.

Vesentlig mislighold av ovennevnte plikter kan påberopes av oppdragsgiver som grunnlag for heving.

Alle avtaler leverandør inngår for utføring av arbeid under denne kontrakten skal inneholde tilsvarende bestemmelse.

8.8 Varens innhold av farlige stoffer

Dersom varen inneholder farlige stoffer, dvs. stoffer som kan medføre helsefare for dem som bruker varen, fare for brann eller eksplosjon eller fare for ytre miljø, skal leverandøren levere HMS-datablad for varen.

Oppdragsgiveren ønsker å unngå varer som inneholder stoffer som står på myndighetens prioritetsliste over stoffer som skal utfases innen 2010. Leverandøren skal informere oppdragsgiveren dersom varen inneholder slike stoffer, samt om eventuelle substitusjonstiltak, jfr. produktkontrollloven § 3 a. Det samme gjelder varer med mer enn 0,1 vektprosent av stoffer på myndighetenes OBS-liste.

8.9 Reklame / informasjon

Leverandøren og dennes underleverandører forplikter seg til ikke å offentliggjøre noen form for prosjekterelatert informasjon uten på forhånd å ha innhentet skriftlig godkjenning fra oppdragsgiveren.

8.10 Eierskapskontroll

8.10.1 Oversendelse av opplysninger om eierskap

Oppdragsgiver kan, på ethvert tidspunkt i avtaleforholdet, kreve at leverandøren oversender opplysninger om eierskap til oppdragsgiver. Leverandøren skal oversende opplysningene om eierskap til oppdragsgiver uten ugrunnet opphold. Opplysningene om eierskap skal inneholde informasjon om:

- leverandørens daglige leder, administrasjon (toppleidelse/toppledergruppe) og navn på selskapets styremedlemmer inkludert varamedlemmer
- oversikt over konsernstruktur
- aksjonærer til alle selskapene som inngår i konsernstrukturen. Børsnoterte selskaper skal opplyse om minimum sine ti største aksjonærer med eierandel
- reelle rettighetshavere (direkte og indirekte eierskap) til alle selskapene som inngår i konsernstrukturen

Opplysningene om selskaper skal omfatte navn og organisasjonsnummer. Det skal opplyses om selskapenes nasjonalitet, herunder:

- hvilken stats rettsregler er lagt til grunn for selskapenes stiftelse
- adressene der selskapene har sitt forretningskontor
- adressene der den daglige ledelsen utøves dersom disse er en annen enn forretningskontor

Opplysningene om fysiske personer skal omfatte navn, adresse, fødselsnummer eller D-nummer, nasjonalitet og personlige næringsinteresser utenfor den aktuelle virksomheten. Dersom den fysiske personen ikke har norsk fødselsnummer eller D-nummer, skal meldingen i stedet opplyse om personens fødselsdato.

Leverandøren skal, uoppfordret eller dersom oppdragsgiver krever det, oppgi ytterligere opplysninger som kan ha betydning for oppdragsgivers vurdering av risiko for nasjonale sikkerhetsinteresser i eierskapet.

8.10.2 Varslingsplikt ved eierskifte av en kvalifisert eierandel

8.10.2.1 Når varslingsplikten inntreffer

Leverandøren skal uten ugrunnet opphold skriftlig varsle oppdragsgiver ved erverv av en kvalifisert eierandel i leverandøren eller i annet selskap som inngår i konsernstrukturen. Varslingsplikten inntreffer når leverandøren blir kjent med ervervet.

Med kvalifisert eierandel menes at ervervet vil føre til at erververen direkte eller indirekte samlet oppnår minst 10 prosent av aksjekapitalen, andelen eller stemmene i leverandøren eller i annet selskap som inngår i konsernstrukturen. Det samme gjelder når ervervet vil føre til at:

- a) erververens kvalifiserte eierandel økes til minst 20 prosent, en tredjedel, 50 prosent, to tredjedeler eller 90 prosent av aksjekapitalen, andelen eller stemmene i leverandøren eller i annet selskap som inngår i konsernstrukturen, eller
- b) erververen oppnår betydelig innflytelse over forvaltningen av leverandøren eller av annet selskap som inngår i konsernstrukturen på annen måte, eller
- c) erververen sammen med sine nærstående, jf. verdipapirhandelloven § 2-5, oppnår en kvalifisert eierandel eller en posisjon som nevnt i bokstav a eller b.

8.10.2.2 Varslets innhold

Varslet skal inneholde opplysninger om:

- organisasjonsnummeret til selskapet ervervet gjelder
- erververens navn, nasjonalitet, adresse og organisasjonsnummer, eventuelt fødselsnummer eller D-nummer. Dersom den fysiske personen ikke har norsk fødselsnummer eller D-nummer, skal meldingen i stedet opplyse om personens fødselsdato. Det skal også opplyses om organisasjonsnummeret til selskapet ervervet gjelder.
- erververens eierandel etter at ervervet er gjennomført

8.10.3 Oversendelse av opplysninger om erverver

På oppdragsgivers forespørsel skal leverandøren uten ugrunnet opphold oversende opplysninger om erververen ved eierskifte av en kvalifisert eierandel i leverandøren eller i annet selskap som inngår i konsernstrukturen.

Oppdragsgiver kan be om tilsvarende opplysninger som fremgår av punktet over om «Oversendelse av opplysninger om eierskap» for erververen.

8.10.4 Varslingsplikt ved andre endringer

Leverandøren skal uten ugrunnet opphold skriftlig varsle oppdragsgiver ved endringer i styret eller ledelsen i leverandøren eller i annet selskap som inngår i konsernstrukturen, eller om andre forhold som kan ha betydning for oppdragsgivers vurdering av risiko for nasjonale sikkerhetsinteresser. Varslingsplikten inntreffer når leverandøren blir kjent med endringen.

8.10.5 Underleverandører

Alle avtaler leverandøren inngår for utføring av arbeid under denne kontrakten skal inneholde tilsvarende bestemmelser som hele punktet om eierskapskontroll. Oppdragsgiver kan, på ethvert tidspunkt i avtaleforholdet, kreve at leverandøren oversender opplysninger om underleverandøren til oppdragsgiver. Leverandøren skal varsle oppdragsgiver ved endringer hos underleverandøren.

8.10.6 Sanksjoner

Dersom leverandøren ikke overholder fristene for oversendelse av opplysninger om eierskap, eller dersom opplysningene som oversendes er mangelfulle, kan oppdragsgiver med rimelig varsel stanse arbeidene for leverandørens regning og risiko.

Oppdragsgiver har rett til å, uten forutgående varsel, stanse arbeidene for leverandørens regning og risiko eller heve kontrakten dersom risiko for nasjonale sikkerhetsinteresser ikke kan utelukkes etter oppdragsgivers skjønnsmessige vurdering.

Oppdragsgiver kan gi leverandøren mulighet til å rette forholdet slik at risiko for nasjonale sikkerhetsinteresser kan utelukkes eller reduseres til et akseptabelt nivå etter oppdragsgivers skjønnsmessige vurdering.

Oppdragsgiver kan kreve bytte av underleverandør på leverandørens regning og risiko dersom risiko for nasjonale sikkerhetsinteresser ikke kan utelukkes eller reduseres til et akseptabelt nivå etter oppdragsgivers skjønnsmessige vurdering.

8.11 Sikkerhet

Dersom oppdraget innebærer at leverandøren får tilgang til eller tilvirker skjermingsverdig informasjon, eller får tilgang til et skjermingsverdig objekt eller infrastruktur, plikter leverandøren å ivareta krav gitt i, eller i medhold av, lov om nasjonal sikkerhet av 1. juni 2018 nr. 24 (sikkerhetsloven) med forskrifter.

Leverandøren er ansvarlig for å påse at sikkerhetsbestemmelser etterleves i egen virksomhet og hos underleverandør som medvirker i anskaffelsen. Overtredelse av sikkerhetskrav vil kunne anses som vesentlig mislighold av leverandørens kontraktsforpliktelser.

Leverandøren må selv dekke utgifter til å oppfylle krav som følger av sikkerhetsloven med forskrifter, hvis ikke noe annet følger av avtalen, sikkerhetsavtalen eller forskrift (se forskrift om sikkerhetsklarering og annen klarering av 20. desember 2018 (klareringsforskriften) § 31).

Forsvarsbygg har etter sikkerhetsloven § 4-1 annet ledd et ansvar for å påse at leverandøren har tilstrekkelig risiko- og sikkerhetsforståelse. Det innebærer at Forsvarsbygg som ledd i oppfølgingen av at leverandøren oppfylder sine kontraktsforpliktelser vil kunne kontrollere at kravet til forsvarlig sikkerhetsnivå er oppfylt. Leverandøren skal legge til rette for at Forsvarsbygg kan gjennomføre slik kontroll.

8.11.1 Oppdrag underlagt sikkerhetsrestriksjoner

Velg et element.

Det stilles krav om at leverandøren må være et norsk foretak eller foretak fra stat som Norge har et sikkerhetspolitisk samarbeid med.

8.11.2 Leverandørens behov for tilganger til skjermingsverdige verdier

Oppdragsgiveren har tatt stilling til hva leverandøren kan få tilgang til av skjermingsverdig informasjon, informasjonssystemer, objekter eller infrastruktur (skjermingsverdige verdier).

Velg et element.

Krav til beskyttelse av skjermingsverdig informasjon er gitt i vedlegg 2.

Velg et element.

8.11.3 Tilgang til skjermingsverdig informasjon i leverandørens egne lokaler

Leverandøren Velg et element.

Leverandøren Velg et element.

Informasjonssystem hos leverandør som skal behandle skjermingsverdig informasjon skal godkjennes før det tas i bruk.

Informasjonssystem hos leverandøren Velg et element. være tilknyttet skjermingsverdig objekt eller infrastruktur.

8.11.4 Tilgang til skjermingsverdige verdier hos oppdragsgiveren

Leverandøren vil ha behov for tilgang til skjermingsverdig informasjon (i papirform eller elektronisk) hos oppdragsgiveren Velg et element. av representant for oppdragsgiveren. Informasjonen vil være Velg et element..

Leverandøren vil ha behov for fysisk tilgang til skjermingsverdig objekt eller infrastruktur Velg et element. av representant for oppdragsgiveren.

8.11.5 Avtale om håndtering og beskyttelse av ugradert skjermingsverdig informasjon og skjermingsverdig ugradert informasjonssystem

Før leverandøren får tilgang til ugradert skjermingsverdig informasjon eller skjermingsverdig ugradert informasjonssystem, må leverandøren inngå en avtale med oppdragsgiveren. I avtalen fastsettes det hvordan leverandøren skal forholde seg til de kravene som gjelder for anskaffelsen.

For denne kontrakten gis det Velg et element.

8.11.6 Krav til sikkerhetsavtale mellom oppdragsgiveren og leverandør, og eventuell leverandørklarer

Før leverandøren gis tilgang til skjermingsverdige verdier er det Velg et element.

8.11.7 Krav til autorisasjon, og eventuell sikkerhetsklarer

Før leverandørens personell gis tilgang til skjermingsverdige verdier er det krav til Velg et element.

Nærmere informasjon om autorisasjon og eventuell sikkerhetsklarer knyttet til gjennomføring av kontrakten vil bli gitt ved henvendelse til oppdragsgiveren.

8.12 Reklamasjonsfrist

Følgende er et tillegg til kjøpsloven § 32 nr 2: For leveranser som ved vanlig bruk er ment å vare vesentlig lengre enn to år, er fristen for å reklamere fem år.

8.13 Avbestilling

Oppdragsgiver har rett til å avbestille hele eller deler av leveransen. Avbestilling skal skje skriftlig i så god tid som mulig.

Ved avbestillingen har leverandøren krav på slikt oppgjør:

- a) For ytelser som er levert betales avtalt pris.
- b) For utførte arbeider knyttet til ytelser som ikke er levert, betales en forholdsmessig andel av avtalt pris. Resultatet av disse arbeidene skal leveres til oppdragsgiver når endelig oppgjør er fastsatt.
- c) Betaling for dokumentert tap som leverandøren er påført som følge av oppsigelsen, herunder tapt fortjeneste. Tapsdekningen er begrenset til 5 % av de avbestilte ytelsenes verdi.

9 Øvrige kontraktsvilkår

Kontrakten reguleres av lov om kjøp av 13. mai 1988 nr 27 (kjøpsloven).

Leverandøren kan ikke gjøre gjeldende vilkår som er ugunstigere for Forsvarsbygg enn det som følger av kjøpsloven.

10 Signaturer

Avtalen skal signeres elektronisk. Signatur vil fremkomme av egen signaturfil opprettet i Mercellportalen.

Avtaler over kr 100.000 ekskl. mva. skal signeres av både fagteknisk og merkantilt ansvarlig hos Forsvarsbygg, og er først gyldig inngått når begge signaturer foreligger. Forsvarsbygg ved direktør Forsvarsbygg eller direktør anskaffelser kan ensidig godkjenne avtalen ved manglende signatur.

Leverandøren skal uten ugrunnet opphold varsle Forsvarsbygg etter at han blir eller burde ha blitt oppmerksom på at ikke begge ansvarlige hos Forsvarsbygg har signert. Varselet sendes til anskaffelser@forsvarsbygg.no.

Vedlegg

- 1. Mal for endringsavtale**
- 2. Orientering til leverandører om krav til håndtering og beskyttelse av skjermingsverdig informasjon i forbindelse med anskaffelser**

**FORSVARSBYGG****ENDRINGSAVTALE**

| | | | | | |
|------------|--|--------------|--|-------------------|--|
| Leveranse | | Kontraktsnr: | | Endringsavtale nr | |
| Leverandør | | Saksnr: | | Dato: | |
| | | | | Side: | |

PARTENE ER ENIGE OM FØLGENDE ENDRINGSAVTALE:

Ved underskrift av begge parter gjelder dette dokumentet som endringsavtale. Leverandøren har ingen rett til å utføre endringene før underskrifter foreligger.

For Forsvarsbygg

Sted/dato _____

Signatur _____

For leverandøren

Sted/dato _____

Signatur _____

Vedlegg 2 - Orientering til leverandører om krav til håndtering og beskyttelse av sikkerhetsgradert informasjon i leverandørens egne lokaler

Innhold

| | |
|---|---|
| Innhold..... | 1 |
| 1. Innledning..... | 2 |
| 1.1. Formål..... | 2 |
| 1.2. Definisjoner..... | 2 |
| 1.3. Sikkerhet i anskaffelser..... | 2 |
| 1.4. Hjemmel..... | 3 |
| 1.4.1. Sikkerhetsloven med forskrifter..... | 3 |
| 1.4.2. 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..... | 4 |
| 1.5.5. Brudd på sikkerhetskrav..... | 4 |
| 2. Sikkerhetsgraderte anskaffelser på BEGRENSET nivå..... | 4 |
| 2.1. Forsvarlig sikkerhetsnivå for informasjon som er gradert BEGRENSET..... | 4 |
| 2.2. Inngåelse av sikkerhetsavtale på BEGRENSET nivå..... | 4 |
| 2.2.1. Autorisasjon..... | 5 |
| 2.2.2. Autorisasjon av utenlandsk statsborger..... | 5 |
| 2.2.3. Godkjenning av skjermingsverdig informasjonssystem..... | 6 |
| 2.2.4. Unntak fra krav om sikkerhetsavtale..... | 6 |
| 2.2.5. Brudd på sikkerhetskrav..... | 6 |
| 3. Sikkerhetsgraderte anskaffelser på KONFIDENSIELT nivå..... | 7 |
| 3.1. Forsvarlig sikkerhetsnivå for informasjon som er gradert KONFIDENSIELT..... | 7 |
| 3.1.1. Soneinndeling for informasjon gradert KONFIDENSIELT..... | 7 |
| 3.1.2. Godkjenning av skjermingsverdig informasjonssystem..... | 7 |
| 3.1.3. Leverandørklarering..... | 7 |
| 3.1.4. Sikkerhetsklarering og autorisasjon av leverandørpersonell..... | 7 |
| 3.1.5. Sikkerhetsklarering og autorisasjon av leverandørpersonell med utenlandsk statsborgerskap..... | 8 |
| 3.2. Inngåelse av sikkerhetsavtale på KONFIDENSIELT nivå..... | 8 |
| 3.2.1. Brudd på sikkerhetskrav..... | 8 |

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 skal oppbevare, behandle eller tilvirke sikkerhetsgradert informasjon i sine egne lokaler.

1.2. Definisjoner

Sikkerhetsgradert anskaffelse: anskaffelse som innebærer at leverandøren av varen eller tjenesten kan få tilgang til sikkerhetsgradert informasjon eller informasjonssystemer som behandler slik informasjon (skjermingsverdig informasjonssystem), 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 terrorhandling, samt medvirkning til slik virksomhet.

Sikkerhetsgradert informasjon: informasjon som er merket med sikkerhetsgrad (BEGRENSET, KONFIDENSIELT, HEMMELIG eller STRENGT HEMMELIG).

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 rettstridig overtakelse.

Nasjonale sikkerhetsinteresser: landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser knyttet til

- a) de øverste statsorganers virksomhet, sikkerhet og handlefrihet
- b) forsvar og beredskap
- c) forholdet til andre stater og internasjonale organisasjoner
- d) økonomisk stabilitet
- e) samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet

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 og deres personell (omfatter også tilbydere, underleverandører) kan få tilgang til av sikkerhetsgradert informasjon, skjermingsverdige objekter eller skjermingsverdig infrastruktur (skjermingsverdige verdier) 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 sikkerhetsgradert informasjon i sine egne lokaler. I den forbindelse vil oppdragsgiver gi råd og veiledning om hvordan den forebyggende sikkerhetstjenesten skal praktiseres for å gi et forsvarlig sikkerhetsnivå.

1.4. Hjemmel

1.4.1. Sikkerhetsloven med forskrifter

Lov om nasjonal sikkerhet av 1. juni 2018 nr. 24 (sikkerhetsloven, heretter forkortet sl.) 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, heretter forkortet vsf.)
- Forskrift om sikkerhetsklarering og annen klarering av 20. desember 2018 nr. 2054 (klareringsforskriften, heretter forkortet kf)

1.4.2. 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.

Under utførelse av anskaffelsen på en av Forsvarsbyggs eller Forsvarets lokasjoner, er oppdragsgivers styringssystem for sikkerhet gjeldende.

1.5.2. Leverandørens ansvar

Sikkerhetskravene som gjøres gjeldende for leverandøren vil avhenge av hva leverandøren og dennes personell får tilgang til, og hvordan denne tilgangen gis.

Leverandørens daglige leder har ansvaret for det forebyggende sikkerhetsarbeidet innen sitt ansvars- og myndighetsområde, herunder underlagte virksomheter.

1.5.3. Krav om forsvarlig sikkerhetsnivå

Det stilles funksjonelle krav til håndtering av risiko knyttet til sikkerhetsgradert 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.

NSM har publisert veiledere som gir anbefalinger om hvordan lov og forskrifter er å forstå, og danner et grunnlag for virksomhetenes arbeid med å etterleve regelverket. NSM har i tillegg publisert håndbøker og tekniske råd som gir mer utfyllende anbefalinger om hvordan lovens funksjonelle krav kan oppfylles. Håndbøkene og de tekniske rådene beskriver fremgangsmåter, prosedyrer og gir eksempler på tiltak for å hjelpe virksomhetene i regelverksanvendelsen, se www.nsm.no.

Det kan være behov for veiledere som er sikkerhetsgradert eller er unntatt offentlighet. Forsvarsbygg vil fremskaffe slike veiledere ved behov. Dette er spesielt aktuelt på KONFIDENSIELT nivå.

1.5.4. Utgifter til oppfyllelse av sikkerhetskrav

Leverandøren må selv dekke utgifter til å oppfylle krav som følger av sikkerhetsloven med forskrifter, hvis ikke noe annet følger av avtalen eller sikkerhetsavtalen med forskrifter (se særlig kf. § 31).

1.5.5. Brudd på sikkerhetskrav

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

2. Sikkerhetsgraderte anskaffelser på BEGRENSET nivå

2.1. 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, gå tapt eller endres eller gjøres utilgjengelig. Ved valg av sikkerhetstiltak skal leverandøren se behovet for å beskytte informasjonens konfidensialitet, integritet og tilgjengelighet i sammenheng og veie hensynene mot hverandre, jf. vsf. § 39.

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

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

Følgende dokumenter må utarbeides av leverandøren og sendes til oppdragsgiver:

- Beskrivelse av virksomhetens styringssystem for sikkerhet og bekreftelse på at styringssystemet er implementert, jf. sl. § 4.1 og vsf. § 3.
- Styringsdokument for det forebyggende sikkerhetsarbeidet, jf. vsf. § 4.
- Sikkerhetsmål, jf. vsf. § 5.
- Beskrivelse av roller og ansvar i den lokale sikkerhetsorganisasjonen, jf. vsf. § 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, jf. sl. § 4-1 andre ledd og vsf. § 7.
- Risikovurdering og beskrivelse av hvordan risiko håndteres, jf. sl. §§ 4-2 og 4-4, samt vsf. §§ 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. sl. § 4-4, samt vsf. §§ 14 og 15. Ved etablering av fysiske sikkerhetstiltak oppfordres leverandøren til å følge Nasjonalt kompetansesenter for sikring av bygg (NKS) sine anbefalte metoder for sikring av informasjon gradert BEGRENSET, jf. Sikringshåndboka – Håndbok i sikring av eiendom, bygg og anlegg mot terror, sabotasje og spionasje og annen kriminalitet (2022 eller nyere utgave).
- Beskrivelse av skjermingsverdig informasjonssystem, jf. sl. § 6-1 og vsf. kapittel 7.

Kravene i virksomhetsikkerhetsforskriften og anbefalingene i Sikringshåndboka som gjelder beskyttelse av informasjon er minimumskrav. For å styrke beskyttelsen av informasjon gradert BEGRENSET har oppdragsgiver besluttet at leverandører som har behov for å oppbevare, behandle eller tilvirke informasjon gradert BEGRENSET skal etablere følgende sikkerhetstiltak utover minimumskravene:

- Leverandøren skal etablere et rom innenfor en kontrollert sone, jf. vsf. § 39. Det skal være et fysisk skille mellom kontrollert sone og rommet. Det fysiske skillet vil normalt bestå av gulv, tak, vegger, vinduer og dør. Da det ikke skal være mulig å ta seg inn i rommet uten at det kan oppdages, skal denne avgrensningen være hel. Dette innebærer blant annet at vegger skal gå over nedsenket himling og under hevet gulv (datagulv). Der dette ikke er praktisk

gjennomførbart kan vegg over himling og under gulv erstattes med gitter eller lignende. Konstruksjonen skal være slik at bygningselementer ikke enkelt kan fjernes for så å bli satt tilbake på plass uten at det settes visuelle spor. I tillegg til den fysiske konstruksjonen skal rommet sikres mot innsyn, også fra kontrollert sone, for å oppnå en god beskyttelse mot tilgang til sikkerhetsgradert informasjon fra uautoriserte og besøkende.

- For å hindre uautorisert adgang til skal det monteres FG-godkjent lås på dør til det aktuelle rommet. Døren skal være låst og dokumenter og lagringsmedier med informasjon som er gradert BEGRENSET skal være nedlåst i en oppbevaringsenhet godkjent for KONFIDENSIELT (K-skap) når autorisert personell ikke er til stede.
- Dersom leverandøren på et senere tidspunkt vil kunne få behov for å oppbevare, behandle eller tilvirke informasjon gradert KONFIDENSIELT i sine egne lokaler, anbefales det at leverandøren før etablering av rom godkjent for BEGRENSET tar i betraktning de krav som gjelder for beskyttelse av informasjon gradert KONFIDENSIELT, se punktene 3.1 og 3.2, jf. vsf, kapittel 6 og 7 og spesielt kravene for skjerming mot Tempest.

2.2.1. Autorisasjon

Leverandørens daglige leder skal autoriseres av oppdragsgiver før sikkerhetsavtale inngås. Leverandørens daglige leder er leverandørens autorisasjonsansvarlige. Vedkommende 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 vsf, § 68 andre ledd. NSM har publisert en Håndbok i autorisasjon og autorisasjonssamtale som kan være et nyttig hjelpemiddel.

Informasjon som inneholder personopplysninger i saker om autorisasjon, skal merkes PERSONKONTROLL. Kravet gjelder ikke meldinger om at det er gitt en autorisasjon eller meldinger om andre autorisasjonsavgjørelser 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.

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

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.

2.2.2. 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 klareringsmyndigheten (Forsvarets sikkerhetsavdeling (FSA)) 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.

2.2.3. Godkjenning av skjermingsverdig informasjonssystem

Ved behov kan det etableres et skjermingsverdig informasjonssystem hos leverandøren for å behandle sikkerhetsgradert informasjon. For å kunne behandle sikkerhetsgradert informasjon på nivå BEGRENSET hos leverandøren, må leverandøren etablere og drifte et skjermingsverdig informasjonssystem. Informasjonssystemet skal godkjennes i henhold til vsf. §§ 50-53.

I vsf. § 49 stilles det funksjonelle krav for skjermingsverdige informasjonssystemer. Ved å følge NSMs veiledere for godkjenning av informasjonssystemer anses kravene i vsf. § 49 som ivaretatt.

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

Leverandøren må utarbeide følgende dokumentasjon i forbindelse med godkjenning av skjermingsverdige informasjonssystem:

- Brukerinstruks
- Driftsinstruks
- Beredskapsplan
- Konfigurasjonsoversikt
- Medieregister
- Risikovurdering
- Søknad om godkjenning av informasjonssystem

Oppdragsgiver har maler for hver av de ovennevnte dokumenter.

Kostnader knyttet til anskaffelse og godkjenning av skjermingsverdig informasjonssystem som skal brukes til å behandle informasjon sikkerhetsgradert BEGRENSET:

- Leverandøren skal dekke kostnaden med godkjenningen.
- Standard IT-maskinvare kan benyttes, men det skal kjøpes inn via sikre leverandørkjeder. Forsvarets godkjente produktliste (GPL) inneholder produkter fra sikre leverandørkjeder.
- Informasjonssystemet skal aldri kobles til internett eller andre nettverk. Lisensiering av programvare kan være en utfordring, fordi stadig flere programvareleverandører krever at deres programvare er tilkoblet internett slik at gyldig lisens kan registreres. Løsninger på disse utfordringer kan medføre ekstra kostnader.
- Leverandøren må sette av tid til installasjon og godkjenning av informasjonssystemet samt utarbeidelse av dokumentasjon og instruks.
- Leverandøren må sette av tid og ressurser med tilstrekkelig IT-kompetanse til løpende drift av informasjonssystemet slik at forsvarlig sikkerhetsnivå opprettholdes i hele levetiden til informasjonssystemet.
- NSMs grunnprinsipper for IKT-sikkerhet kan gi nyttig veiledning til dette arbeidet.

2.2.4. 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, jf. vsf. § 81. I NSMs Veileder i anskaffelser etter sikkerhetsloven redegjøres 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.

2.2.5. 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.

3. Sikkerhetsgraderte anskaffelser på KONFIDENSIELT nivå

3.1. Forsvarlig sikkerhetsnivå for informasjon som er gradert KONFIDENSIELT

Vsf. kapittel 6 fastsetter krav til beskyttelse av informasjon gradert KONFIDENSIELT.

Kravene som gjelder på BEGRENSET nivå, vil også gjelde for KONFIDENSIELT nivå.

3.1.1. Soneinndeling for informasjon gradert KONFIDENSIELT

For å beskytte skjermingsverdig informasjonssystem og informasjon gradert KONFIDENSIELT eller høyere, skal det etableres en kontrollert og beskyttet sone. Dersom leverandøren har behov for et eget rom med direkte tilgang til informasjon gradert KONFIDENSIELT, skal det etableres en sperret sone, jf. vsf. kapittel 6, NSMs Veileder i fysisk sikkerhet og Sikringshåndboka.

3.1.2. Godkjenning av skjermingsverdig informasjonssystem

Ved behov skal leverandøren etablere et skjermingsverdig informasjonssystem for behandling av informasjon gradert KONFIDENSIELT. Informasjonssystemet skal godkjennes i henhold til vsf. §§ 50-53.

Elektronisk utstyr avgir stråling som medfører at informasjon kan avleses på avstand uten at noen oppdager det. I vsf. §34 er det krav om at uautoriserte personer ikke kan få tilgang til informasjon gradert KONFIDENSIELT eller høyere, uten at virksomheten oppdager det. Tempestrisikovurdering må derfor utarbeides i tillegg til dokumentasjonen som er aktuell for skjermingsverdig informasjonssystem på BEGRENSET nivå. Oppdragsgiver kan fremskaffe mal for Tempestrisikovurdering.

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.

Kostnader knyttet til anskaffelse og godkjenning av skjermingsverdig informasjonssystem som skal brukes til å behandle informasjon sikkerhetsgradert KONFIDENSIELT:

- Virksomheten skal dekke kostnaden med godkjenningen.
- Tempestrisikovurdering avgjør om Tempestgodkjent IT-maskinvare må benyttes. Forsvarsbyggs leverandører må normalt benytte Tempestgodkjent maskinvare i informasjonssystemer på KONFIDENSIELT nivå. Prisen på Tempestgodkjent maskinvare kan være 30-50% høyere enn standard maskinvare og leveringstiden kan være flere uker.
- Informasjonssystemets avstand til områder som er utenfor leverandørens kontroll har betydning for hvilke Tempesttiltak som er nødvendig, og dermed også kostnader. Bestemmelser om avstander og tiltak er sikkerhetsgradert, og informasjon kan bare utleveres til leverandøren ved behov.
- Leverandøren må sette av tid til etablering av informasjonssystemet samt utarbeidelse av dokumentasjon og instruks. Det er flere krav på KONFIDENSIELT nivå og dette kan medføre flere instruks og dokumentasjon.

3.1.3. Leverandørklarering

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

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

3.1.4. 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 om sikkerhetsklarering gjelder også for leverandørpersonell som har behov for tilgang til skjermingsverdig objekt eller skjermingsverdig infrastruktur.

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

Informasjon som inneholder personopplysninger i saker om autorisasjon, personkontroll eller sikkerhetsklarering, skal merkes PERSONKONTROLL. Kravet gjelder ikke meldinger om at det er gitt en autorisasjon eller sikkerhetsklarering eller meldinger om andre autorisasjons- eller sikkerhetsklaringsavgjørelser til personen som avgjørelsen gjelder. For tilgang til opplysninger merket PERSONKONTROLL, se punkt 2.2.1.

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

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

Det gjøres oppmerksom på at det er leverandørens risiko at autorisasjon eller sikkerhetsklarering ikke oppnås.

3.1.5. Sikkerhetsklarering og autorisasjon av leverandørpersonell med utenlandsk statsborgerskap

En person som har utenlandsk statsborgerskap, kan etter en konkret helhetsvurdering bli sikkerhetsklarert, 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.

3.2. Inngåelse av sikkerhetsavtale på KONFIDENSIELT nivå

Sikkerhetsavtale mellom oppdragsgiver og leverandøren skal inngås før leverandøren kan oppbevare, behandle eller tilvirke informasjon gradert KONFIDENSIELT i 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 KONFIDENSIELT.

3.2.1. Brudd på sikkerhetskrav

Dersom leverandøren ikke retter brudd på kravene fastsatt i eller med hjemmel i sikkerhetsloven innen en fastsatt frist, kan leverandørklarering kalles tilbake av NSM. Er et brudd vesentlig, kan NSM tilbakekalle leverandørklareringen uten at det settes en frist. Dersom leverandørklareringen kalles tilbake, vil sikkerhetsavtalen sies opp.