



DET KONGELIGE
UTENRIKSDEPARTEMENT

Bilag 8
Sikkerhetsbestemmelser
kontraktsfasen for rammeavtale for
levering av datakablingstjenester
og tilhørende materiell
«Sikkerhetsavtalen»

Saksnummer: 26/06755

Avtale

er inngått mellom:

(heretter kalt Leverandøren)

og

Utenriksdepartementet (UD)

(heretter kalt Kunden)

Sted og dato:

Oslo, xx.xx.2026

Kunden

Leverandøren

Avtalen undertegnes i to eksemplarer, ett til hver part, og gjelder fra
xx.xx.2026

Alle daglige henvendelser vedrørende denne avtalen rettes til:

Hos Kunden:

Hos Leverandøren:

1. Sikkerhetsavtalens omfang og formål

Denne sikkerhetsavtalen skal regulere bestemmelser knyttet til sikkerhet etter ikrafttreden av Rammeavtale 26/06755 om levering av levering av datakablingstjenester og tilhørende materiell. Avtalen gjelder for Rammeavtalen med underliggende avropsavtaler, heretter kalt Avtalen.

Formålet med sikkerhetsavtalen er å fastsette sikkerhetskrav til graderte anskaffelser slik at UD og Leverandøren som et minimum oppfyller kravene i lov av 1. juni 2018 nummer 24, lov om nasjonal sikkerhet (sikkerhetsloven), instruks for beskyttelse av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen) av 17.mars 1972 nr. 3352 og forskrift om sikkerhetsgraderte anskaffelser av 1. juli 2001 nr 753.

2. Avtalens bestemmelser

2.1. Leverandørs ansvar for å følge krav etter sikkerhetsloven

Kunden er underlagt lov om nasjonal sikkerhet (sikkerhetsloven) og instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (Beskyttelsesinstruksen). Leverandør og eventuelle underleverandører, skal i den grad dette kreves etter lov og forskrift eller administrativ beslutning, ha godkjente systemer for produksjon, utveksling og oppbevaring av sikkerhetsgradert informasjon. Det er Kunden som avgjør gradering av informasjon og dokumentasjon.

2.2. Sikkerhetsklarering og taushetserklæring

Leverandør vil kunne få tilgang til skjermingsverdig objekt, infrastruktur, informasjon og informasjonssystem. Dette innebærer at personell fra Leverandør som skal jobbe med leveransene må gjennomgå autorisasjonssamtale hos Kunden og signere taushetserklæring.

Personell som arbeider på anleggene eller gis informasjon om anleggene skal minimum være sikkerhetsklarert for HEMMELIG. I tillegg kan Kunden kreve autorisasjon for det enkelte arbeid som skal utføres.

Leverandøren er forpliktet til å ha personell sikkerhetsklarert til HEMMELIG.

Leverandør har ansvar for å sørge for at vedkommende, og eventuelle underleverandører, til enhver tid kan stille med sikkerhetsklarert personell. Manglende sikkerhetsklarering frigjør ikke Leverandøren fra sine forpliktelser. Fra dette gjelder følgende unntak dersom Leverandøren godtgjør at han ikke har tilgjengelig sikkerhetsklarert personell i organisasjonen:

- Etter signering av Avtalen eller ved krav til økt sikkerhetsnivå, har Leverandør rett på rimelig tid til å få gjennomført sikkerhetsklarering. Det er en forutsetning at Leverandør leverer nødvendig dokumentasjon for klarering til Kunden innen fem virkedager etter signering eller varsel om heving av sikkerhetsnivå, for oversendelse til gjeldende klareringsmyndighet. Kunden har risikoen for tiden som medgår til klareringsmyndighetens saksbehandling. Leverandøren kan bare fritas dersom de det søkes om klarering for kan sikkerhetsklareres (det vil si at de oppfyller grunnleggende krav for å bli vurdert).

- Ved avgang av sikkerhetsklarert personell har Leverandør tilsvarende rett, med tilsvarende begrensninger, på tid til å sikkerhetsklarere nytt personell. Dette gjelder bare dersom Leverandøren umiddelbart etter han får vite om avgangen varsler Kunden. Videre er det et vilkår at det er satt av reservekapasitet for avgang av sikkerhetsklarert personell.

Personell som skal prosjektere installasjoner og utarbeide FDV-dokumentasjon, skal ha gjennomgått autorisasjonssamtale hos Kunden.

Leverandøren er ansvarlig for å dekke kostnader knyttet til sikkerhetsklarering og autorisasjoner for egne ansatte.

2.3. Informasjonsbehandling

2.3.1. Utlevering av informasjon

Leverandøren skal ikke utlevere eller bekjentgjøre sikkerhetsgradert informasjon eller annen taushetsbelagt informasjon til tredjepart, herunder underleverandører, konsulenter, målgrupper for markedsføring eller media uten Kundens skriftlige samtykke. Leverandøren skal ikke uten Kundens forhåndssamtykke kunngjøre sin deltakelse i en sikkerhetsgradert anskaffelse.

2.3.2. Tilvirking og behandling av gradert informasjon

Der Leverandøren tilvirker gradert informasjon anses dette som informasjon som tilvirkes på vegne av Kunden. Denne informasjon skal kun tilvirkes og behandles i Kundens lokaler og på Kundens systemer godkjent for graderingsnivået.

2.3.3. Oppbevaring av informasjon

Informasjon transporteres og oppbevares som angitt nedenfor. Ved oppbevaring av informasjon gradert HEMMELIG eller høyere skal dette avklares med dokumentutsteder i hvert enkelt tilfelle.

2.3.3.1. Oppbevaring av informasjon i Leverandørens lokaler

Etter godkjenning av Kunden, kan leverandøren få anledning til å oppbevare dokumenter eller lagringsmedium inneholdende informasjon sikkerhetsgradert BEGRENSET i avlåst rom eller nedlåst i oppbevaringsenhet i leverandørens lokaler. Kun personell som av Kunden er autorisert til dette skal ha tilgang til dokumentasjonen. Når området ikke er under oppsyn, skal dette være alarmert.

Dokument eller lagringsmedium inneholdende informasjon merket UNNTATT OFFENTLIGHET oppbevares som angitt i ovenstående punkt så langt dette lar seg gjennomføre.

Leverandøren skal ikke oppbevare informasjon gradert høyere enn BEGRENSET i egne lokaler.

2.3.3.2. Transport av sikkerhetsgradert informasjon

Det skal benyttes krav som for forsendelse av KONFIDENSIELL også for BEGRENSET, bruk av dobbel, ugjennomsiktig konvolutt av solid kvalitet, ref. Virksomhetsikkerhetsforskriften § 36. All overlevering skal skje personlig.

2.3.4. Tilbakelevering av informasjon

Leverandøren skal levere tilbake til Kunden eller destruere all sikkerhetsgradert informasjon på godkjent måte innen kontraktsforholdet opphører.

Når behovet for sikkerhetsavtalen opphører, skal leverandøren levere tilbake eller, på godkjent måte destruere sikkerhetsgradert informasjon før Kunden kan terminere sikkerhetsavtalen.

2.4. Endringer hos Leverandøren

Leverandøren skal orientere Kunden ved endring av styre, daglig leder eller virksomhetsnavn. Det samme gjelder ved endring i eierinteresser eller eierform, herunder oppdeling av virksomheten eller sammenslåing med andre virksomheter. Flytting av lokalteter skal meddeles Kunden før flyttingen finner sted.

2.5. Underleverandører

Underleverandører som benyttes i kontraktsfasen, er gjennom denne avtalen underlagt tilsvarende sikkerhetskrav som Leverandøren i kontraktsfasen. Underleverandør som leverer utstyr, er ikke omfattet av denne bestemmelsen.

Ved endringer i bruk av underleverandører skal leverandøren varsle Kunden, unntaket er hvis det åpenbart ikke vil være relevant for skjermingen av eller tilgangen

2.6. Bruk av IKT-utstyr i Kundens systemer

Det er ikke anledning for Leverandør å bruke eget IKT-utstyr ved arbeider på Kundens sikkerhetsanlegg eller andre datasystemer uten at dette er særskilt avtalt på forhånd.

Leverandøren plikter å følge Kundens retningslinjer og krav for IKT-systemer som Kunden stiller til disposisjon.

2.7. Tilgang til Kundens lokaler

Der det for avtalen eller den enkelte bestilling/avrop er formålstjenlig, leverandørens personell midlertidig eller permanent tilgang til Kundens lokaler. Leverandøren plikter å følge Kundens til enhver tid gjeldende regler og retningslinjer for slik tilgang, herunder også *Felles adgangsbestemmelser for departementene*.

2.8. Varsling

Leverandøren skal varsle Kunden om avvik fra sikkerhetskrav eller sikkerhetstruende virksomhet som kan påvirke Kunden og/eller leveransen gjennom rammeavtalen. Leverandøren må vurdere skjermingsbehovet i varselet og derav varsle via ugradert eller graderte plattformer.

- Ugradert varsling skal skje på følgende måte: E-post til daglig kontaktperson hos Kunden.
- Gradert varsling kan skje på følgende måte: E-post til daglig kontaktperson hos Kunden på plattform godkjent for BEGRENSET eller ved fysisk oppmøte hos Kunden etter avtale.

2.9. Revisjon og kontroll av sikkerhet

Representanter for Nasjonal sikkerhetsmyndighet (NSM) og Kunden har rett til å gjennomføre tilsyn av sikkerhetstilstanden innen leverandørens virksomhet i tilknytning til Avtalen. Dersom vedkommende representant fastslår sikkerhetsmessige svakheter eller sikkerhetsmessige mangler innen virksomheten, skal leverandøren gis en skriftlig melding om forholdet eller forholdene med tiltak for å bedre sikkerhetstilstanden. Ved brudd på sikkerhetsavtalen kan hele eller deler av Avtalen opphøre.

2.10. Endringer i avtalen

Forandringer i denne avtalen skal skje skriftlig og skal godkjennes av begge parter. Avtalen skal gjelde så lenge leverandøren deltar i den sikkerhetsgraderte anskaffelsen eller tilbudet. Leverandøren plikter til tilbakelevering, destruksjon iht. godkjente metoder, eller oppgivelse av råderett opphører ikke før de er gjennomført, og øvrige plikter iht. sikkerhetsavtalen opphører ikke før Kunden terminerer avtalen.

2.11. Distribusjon

Denne avtalen er utferdiget i to eksemplarer. Hver av partene beholder *ett* eksemplar. Kopi av avtalen formidles Nasjonal sikkerhetsmyndighet.