

AFTALEBILAG 2

MILITÆR SIKKERHED OG INFORMATIONSSIKKERHED

Nærværende dokument er et bilag til Rammeaftalen, som indeholder særlige krav til militær sikkerhed og informationssikkerhed, som Rådgiver skal overholde i relation til Rammeaftalen.

De i Rammeaftalen indeholdte definitioner finder også anvendelse i nærværende dokument.

1. MILITÆR SIKKERHED

Rådgiver skal overholde Forsvarets bestemmelser for den militære sikkerhedstjeneste, FKOBST 358-1, jf. fe-ddis.dk.

1.1 Sikkerhedsgodkendelse

Relevante medarbejdere, herunder eventuelle underrådgiveres medarbejdere, skal opnå og opretholde sikkerhedsgodkendelse til niveauet "FORTROLIGT" af Forsvarets Efterretningstjeneste (FE), jf. cirkulære 2014-12-17 nr. 10338 vedrørende sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO, EU og WEU, og andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelses interesse.

Det er tillige et krav, at Rådgivers virksomhed sikkerhedsgodkendes.

De nærmere retningslinjer for opnåelse og ansøgning af sikkerhedsgodkendelse fremgår af Aftalebilag 1 - Procedure for sikkerhedsgodkendelse og www.fe-ddis.dk.

Der kan i Rammeaftalens løbetid opstå behov for rådgivningsydelser i forbindelse med Honorarafteraler, hvor kravene til sikkerhedsgodkendelse er skærpede. Skærpede sikkerhedskrav, herunder krav om sikkerhedsgodkendelse til et højere niveau, vil fremgå af den konkrete Honoraraftale med bilag.

Umiddelbart efter at Ejendomsstyrelsen har meddelt tildelingsbeslutning af Rammeaftalen, skal Rådgiver iværksætte sikkerhedsgodkendelse af relevante medarbejdere. Rådgiver skal sikre, at tilstrækkelige medarbejdere er sikkerhedsgodkendt i henhold til nærværende bestemmelse i hele Rammeaftalens løbetid, således Ejendomsstyrelsen til stadighed kan få løst rådgivningsopgaver.

Såfremt sikkerhedsgodkendelse ikke kan opnås for en konkret medarbejder, er Rådgiver forpligtet til at udskifte medarbejderen på Rammeaftalen. Udskiftning af medarbejdere skal ske i henhold til Rammeaftalens afsnit 15.

Personer med behov for adgang til sikrede, kontrollerede og overvågede områder i forbindelse med en opgave skal være sikkerhedsgodkendt i forhold til aktuel klassifikation, før arbejdet kan påbegyndes. Den fremmødte medarbejder skal kunne identificere sig med billedlegitimation. Rådgivers medarbejder skal ved ankomst til et etablisement henvende sig ved Hovedvagten eller lokal DESK (reception) med henblik på eventuel udlevering af gæstekort og kontrol af sikkerhedsgodkendelse, såfremt dette kræves.

Der kan i aftaleperioden forekomme ændringer i Forsvarets Efterretningstjenestes krav vedrørende niveau for sikkerhedsgodkendelse af personer, der færdes på Ejendomsstyrelsens område.

Det påhviler Rådgiveren at sørge for, at eventuelle underrådgivere er sikkerhedsgodkendte forinden disse anvendes. Ejendomsstyrelsen kompenserer ikke for spildtid på baggrund af dette.

Kan fornøden sikkerhedsgodkendelse ikke opnås eller opretholdes for virksomheden og/eller det relevante antal medarbejdere, er Ejendomsstyrelsen berettiget til at bringe Rammeaftalen til ophør.

Udgifter forbundet med sikkerhedsgodkendelse er Ejendomsstyrelsen uvedkommende.

1.2 Lokale forhold

Rådgivers medarbejdere skal modtage sikkerhedsbriefing fra den lokale sikkerhedsofficer forud for adgang til Forsvarsministeriets etableringer. Kontaktoplysninger på den lokale sikkerhedsofficer kan fås af den medarbejder hos Ejendomsstyrelsen, der er angivet som kontaktperson på Honoraraftalen.

Rådgiveren og dennes medarbejdere samt eventuelle underrådgivere er forpligtet til at imødekomme alle anvisninger om forhold vedrørende den militære sikkerhed, som Rådgiveren modtager.

Rådgiver gøres opmærksom på, at informationer omkring de fysiske forhold af visse tekniske installationer er klassificerede, og at disse informationer derfor ikke må behandles på internetforbudne systemer. Omfanget af disse informationer og tekniske installationer vil blive fastlagt i Honoraraftalen.

Rådgiver gøres opmærksom på, at det, som udgangspunkt, er forbudt at fotografere på Forsvarsministeriets etableringer. Hvis det i forbindelse med udførelsen af en Honoraraftale er nødvendigt at fotografere, skal tilladelse hertil indhentes hos den lokale sikkerhedsofficer.

1.3 Fysisk dokument- og udstyrshåndtering

Fysisk håndtering af klassificeret materiale må alene ske af medarbejdere, der er sikkerhedsgodkendt til relevant niveau og i henhold til "need to know"-princippet.

Klassificerede medier, eksempelvis papirdokumenter, USB-nøgler og computere, som udleveres til Rådgiver, skal opbevares i et aflåst skab i et aflåst rum, når dette ikke bruges.

1.4 Underretning

Den lokale sikkerhedsofficer skal straks underrettes, såfremt Rådgiver konstaterer eller har mistanke om, at der er sket brud på forhold vedrørende den militære sikkerhed.

2. INFORMATIONSSIKKERHED

2.1 Krav til informationssikkerhed

Ejendomsstyrelsen er som offentlig myndighed underlagt krav om brug af ISO/IEC 27001 til behandling af oplysninger og data, jf. Regeringens National strategi for cyber- og informationssikkerhed.

Niveau for informationssikkerhed fastsættes konkret i hver Honoraraftale. Hvis andet ikke fremgår af den konkrete Honoraraftale, vil de krav, som fremgår af Aftalebilag 2.2 - Informationssikkerhed (Niveau Grøn), være gældende for Honoraraftalen.

Det kan imidlertid i den konkrete honoraraftale fastsættes, at der skal gælde andre krav til informationssikkerhed, hvilket eksempelvis kan være, men ikke begrænset hertil, de krav, der fremgår af Aftalebilag 2.1 - Informationssikkerhed (Niveau Hvid) eller Aftalebilag 2.3 - Informationssikkerhed (Niveau Gul).

Det forventes, at Aftalebilag 2.1 - Informationssikkerhed (Niveau Hvid) vil være gældende for de fleste Honoraraftaler.

Ejendomsstyrelsen forbeholder sig retten til løbende at foretage ændringer i de krav, som Ejendomsstyrelsen stiller til informationssikkerhed. Dette kan eksempelvis være tilfældet, såfremt Ejendomsstyrelsen bliver pålagt at efterleve strengere krav af en overordnet myndighed, som følge af lovkrav eller som følge af den generelle udvikling på området for informationssikkerhed, herunder også persondatabeskyttelse.

Hvis der i Rameaftalens løbetid opstår behov for at stille andre krav til informationssikkerhed, end de krav der er oplyst i henholdsvis Aftalebilag 2.1 - Informationssikkerhed (Niveau Hvid), 2.2 - Informationssikkerhed (Niveau Grøn) eller Aftalebilag 2.3 - Informationssikkerhed (Niveau Gul), vil disse krav som udgangspunkt være baseret på ISO/IEC 27001 og/eller FKOBS 358-1.

2.2 Persondatabeskyttelse (GDPR)

Såfremt Rådgiveren i forbindelse med udførelse af en Honoraraftale skal behandle personoplysninger på vegne af Ejendomsstyrelsen, er Rådgiveren til enhver tid forpligtet til at sikre, at gældende lovgivning overholdes.

Såfremt Rådgiver skal behandle personoplysninger på vegne af Ejendomsstyrelsen, skal databehandlersaftale indgås mellem Parterne. Databehandlersaftalen vedlægges Honoraraftalen som et bilag. Det forventes, at databehandlersaftalen vil være baseret på Datatilsynets til enhver tid gældende skabelon med Ejendomsstyrelsens tilpasninger. Datatilsynets skabelon til databehandlersaftale kan findes på <https://www.datatilsynet.dk/hvad-siger-reglerne/grundlaeggende-begreber-/dataansvarlig-og-databehandler>.

2.3 Underretning

Ejendomsstyrelsens kontaktperson, jf. Rammeaftalens afsnit **Error! Reference source not found.**, en udpeget kontaktperson fra Ejendomsstyrelsen angivet i den konkrete Honoraragtale eller Ejendomsstyrelsens Servicecenter skal straks underrettes, såfremt Rådgiver konstaterer eller har mistanke om, at der er sket brud på forhold vedrørende informationssikkerhed.

Der henvises i øvrigt til Rådgivers underretningsforpligtelse, der er angivet i det relevante informationssikkerhedsbilag, der er gældende for den konkrete Honoraragtale.

3. STAND-ALONE ARBEJDSSTATIONER

Ejendomsstyrelsen er underlagt CIR1H nr. 10338 af 17. december 2014 om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssige beskyttelsesinteresse i øvrigt.

Indeholder en konkret opgave materiale til niveauet "TIL TJENESTEBRUG", skal Rådgiveren arbejde på stand-alone arbejdsstationer. Kravene til en stand-alone arbejdsstation er:

- Rådgiver skal være sikkerhedsgodkendt til niveauet "TIL TJENESTEBRUG"
- Den fysiske adgang til stand-alone arbejdsstationen skal være sikret i henhold til FKOBST 358-1, kapitel 7 og godkendt i forbindelse med Rådgiverens virksomhedssikkerhedsgodkendelse.
- Løsningens design skal kunne dokumenteres, og designet skal godkendes af Forsvarets Efterretningstjeneste i forbindelse med virksomhedssikkerhedsgodkendelse eller af Ejendomsstyrelsens sikkerhedsorganisation.
- IT hardware og operativsystem til stand-alone arbejdsstation skal godkendes af Ejendomsstyrelsen.
- IT software til stand-alone arbejdsstationen kan leveres af Rådgiver.

Derudover skal Rådgiver sikre følgende i forbindelse med anvendelse af stand-alone arbejdsstationen:

- USB-nøgler til overførsel af data og software til og fra stand-alone arbejdsstationen skal være udleveret af Forsvaret.
- Medarbejdere skal som minimum være sikkerhedsgodkendt til niveauet "TIL TJENESTEBRUG" før medarbejdere kan få adgang til stand-alone arbejdsstationen.
- Der skal være unikke og identificerbare brugerlogins til stand-alone arbejdsstationen.
- Der skal være en styret godkendelsesproces for oprettelse af brugeradgange til stand-alone arbejdsstationen.
- Der skal være implementeret logning af bruger- og systemadministratorers aktiviteter på stand-alone arbejdsstationen.
- Stand-alone arbejdsstationen må ikke på noget tidspunkt være forbundet til andre netværk.
- Materiale og data klassificeret til niveauet "TIL TJENESTEBRUG" må ikke overføres til andre netværk af Rådgiver.

- Stand-alone arbejdsstationen skal være beskyttet af et opdateret antivirus-/antimalware-system.
- Der skal være implementeret passende back up af stand-alone arbejdsstationen.
- Rådgiver skal planlægge egenkontrol af efterlevelse af de beskrevne sikkerhedskrav.

Derudover gælder følgende i forbindelse med stand-alone arbejdsstationer:

- Forsvarets Efterretningstjeneste og Ejendomsstyrelsens sikkerhedsorganisation har til enhver tid ret til at kontrollere Rådgiverens efterlevelse af de sikkerhedsmæssige krav til stand-alone arbejdsstationen.
- Eventuelt hardware udleveret af Forsvaret til løsningen må ikke anvendes til andre formål og skal tilbageleveres ved Rammeaftalens ophør, eller når det vurderes, at Rådgiver ikke har behov for hardwaren længere.
- Software, filer og data udleveret af Forsvaret til stand-alone arbejdsstationen må ikke anvendes til andre formål af Rådgiver.
- Filer og data udarbejdet eller generet af Rådgiver til Forsvaret på stand-alone arbejdsstationen må ikke anvendes til andre formål end beskrevet i den konkrete Honoraraftale.

Stand-alone arbejdsstationen skal godkendes af Forsvarets Efterretningstjeneste, eventuelt som led i sikkerhedsgodkendelse af Rådgiverens virksomhed, eller Ejendomsstyrelsens sikkerhedsorganisation, før stand-alone arbejdsstationen kan anvendes. Det bemærkes, at stand-alone arbejdsstationen i alle tilfælde skal godkendes eksplicit.

Indeholder en konkret opgave materiale klassificeret til et højere niveau end "TIL TJENESTE-BRUG", vil de konkrete sikkerhedskrav fremgå af den konkrete Honoraraftale.