Bilag 4b – Sikkerhedskrav

**Vejledning til tilbudsgiver i forbindelse med udarbejdelse af tilbud**

*Bilaget indeholder By & Havns krav og ønsker til den udbudte opgave. Kravene er nummereret med fortløbende nummerering samt kategoriseret som enten forhandlingskrav (“K”) eller evalueringskrav (“EK”).*

*Tilbudsgiver opfordres til at nærlæse den i Bilag VII til udbudsbetingelserne beskrevne kravmetodik forud for tilbudsafgivelsen.*

*Som en del af tilbudsgivers tilbud skal tilbudsgiver udfylde dette Bilag 4b med afkrydsning af opfyldelsesgraden for evalueringskrav (“EK”).*

*Tilbudsgiver skal for hvert EK angive, om kravet er “Helt”, ”Delvist” eller “Ikke” opfyldt ud fra følgende betydning:*

*Helt = Kravet er i sin helhed opfyldt*

*Delvist = Dele af kravet opfyldes ikke*

*Ikke = Kravet opfyldes ikke.*

*Tilbudsgivers besvarelse af de enkelte “EK” skal indsættes i Bilag 4.1 ”Leverandørens løsningsbeskrivelse”.*

*Hvor tilbudsgiver angiver kravopfyldelsesgraden til "Delvist" ved et EK, skal tilbudsgiver i sin besvarelse i Bilag 4.1 angive både hvilke dele af EK’et, som ikke er opfyldt, og hvilke som er opfyldt. Det er vigtigt, at tilbudsgiver udførligt beskriver, hvilke dele af evalueringskravet, der er opfyldt henholdsvis ikke-opfyldt, idet manglende eller upræcise oplysninger vil blive tillagt negativ vægt ved tilbudsvurderingen.*

*I kravtabellerne er der i kolonnen ”Positiv vægtning i evaluering” angivet hvad der vægter positivt i tilbudsgivers besvarelse, hvilket tilbudsgiver bedes lægge vægt på i besvarelsen i Bilag 4.1. Tilbudsgiver skal være opmærksom på, at By & Havn alene er berettiget til at lægge vægt på de ved tilbuddet indkomne oplysninger, og at By & Havn vil tage alle oplysninger i tilbuddet i betragtning ved vurdering af, om et krav er opfyldt.*

*Det betyder blandt andet, at tilbudsgivers besvarelse i et Bilag vil kunne indgå ved vurderingen af, om et krav i et andet Bilag er opfyldt. Tilbudsgiver bør derfor altid sikre, at tilbudsgivers besvarelse i ét Bilag ikke fører til, at et krav må anses for ikke-opfyldt i et andet Bilag.*

*Denne vejledning og eventuel tekst angivet med kursiv i Bilaget slettes inden Kontraktens underskrivelse.*

Indholdsfortegnelse

[1. Indledning 4](#_Toc168597197)

[2. Krav til it-sikkerhed 4](#_Toc168597198)

[2.1. Driftsmæssige krav til sikkerhed 10](#_Toc168597199)

# Indledning

Dette Bilag 4b beskriver By & Havns krav til sikkerhed omkring Systemet.

# Krav til it-sikkerhed

I skemaet nedenfor er By & Havns krav til it-sikkerhed angivet. Hvor det er relevant, er kravet listet ud fra en ISO 27001-referenceramme. Der stilles ikke krav om certificering; der er alene tale om referenceramme.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Kravtype** | **Beskrivelse** | **Kravsopfyldelsesgrad** | | | **Positiv vægtning i evaluering** |
| MK  K  EK  O | **Helt** | **Delvist** | **Ikke** |
| **(X)** | **(X)** | **(X)** |
|  | K | **IT-sikkerhed**  Leverandøren skal sikre at sikkerhedskravene i dette Bilag efterleves for alle de af By & Havns it-systemer og –services, der er omfattet af Kontrakten.  Alle krav vedr. it-sikkerhed i nærværende Bilag er inkluderet i Leverandørens vederlag for etablering og i det faste månedlige vederlag – med undtagelse af krav, hvor det specifikt angives, at leverancen er på T&M eller lignende. |  |  |  |  |
|  | K | **Informationssikkerhedspolitikker**  Leverandøren skal på baggrund af en risikovurdering udarbejde en sikkerhedspolitik, som regelmæssigt revideres, og som kan gøres tilgængelig for By & Havn.  Politikken skal tage højde for gældende lovgivning om beskyttelse af personoplysninger  Leverandøren skal udarbejde risikovurderinger for behandling af By & Havns personoplysninger hvori der tages hensyn til risici af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder. |  |  |  |  |
|  | EK | **Adgangsstyring (ISO27001 Anneks A.9)**  Leverandøren skal have en dokumenteret proces for styring af brugere, adgange og rettigheder, som omfatter såvel By & Havns brugere som egne ansatte, Tredjepartsleverandører etc. og denne proces understøtter muligheden for, at By & Havn kan kontrollere brugeradgange og -rettigheder til By & Havns systemer og data. Der skal gives mulighed for, at lave udtræk af Brugere, hvoraf deres rettigheder fremgår.  Leverandøren skal sikre, at alle brugernavne er unikke, henførbare, individuelle og at der tildeles adgange efter Least-privilege princippet.  Leverandøren skal vedligeholde og dokumentere deres passwordpolitik.  Proceduren for adgangsstyring skal sikre, at det hos Leverandøren alene er medarbejdere med et arbejdsbetinget behov, der har adgang til personoplysninger og at disse adgange løbende inddrages eller ændres ved ophør af ansættelse eller skift af arbejdsområde.  Leverandørens procedure skal indeholde en løbende kontrol af brugerrettigheder.  *Tilbudsgiver bedes i Bilag 4.1 beskrive proces for adgangs- og brugerstyring, herunder hvordan det sikres, at Brugere oprettes, slettes og at deres rettigheder løbende vurderes og tilpasse det aktuelle behov i henhold til gældende regler og politikker.* |  |  |  | *Det vægter positivt, at tilbudsgiver kan dokumentere velbeskrevne processer til adgangsstyring. Det vægter yderligere positivt, at processerne er værktøjsunderstøttede, og at der er rutinemæssige kontroller, der verificerer, at politikker for brugere og passwords overholdes, gerne understøttet af et årshjul.* |
|  | K | **Fysisk sikring og miljøsikring (ISO27001 Anneks A.11)**  Leverandøren skal etablere fysiske sikringsforanstaltninger og adgangskontrol, der sikrer at uvedkommende ikke har adgang til By & Havns driftsmiljøer.  Leverandøren skal have etableret udstyrssikkerhed, herunder sikringsforanstaltninger til beskyttelse mod miljøpåvirkninger som brand, vandskade, varme, strømafbrydelser etc. samt procedurer for opretholdelse af datasikkerhed i relation til bortskaffelse og vedligeholdelse af udstyr. |  |  |  |  |
|  | K | **Driftssikkerhed**  Leverandøren skal have dokumenterede og vedligeholdte driftsprocedurer.  Leverandøren skal opretholde passende sikringsforanstaltninger mod cyber-angreb og skadelig kode.  Leverandøren skal have effektive processer og løsninger til logning og systemovervågning.  Leverandøren skal have dokumenterede processer for sårbarhedsstyring, herunder for sikkerhedsopdatering (patch management), hærdning og sikkerhedstest. |  |  |  |  |
|  | K | **Leverandørforhold (ISO27001 Anneks A.15)**  Leverandøren skal underlægge eventuelle Tredjepartsleverandører samme krav til it-sikkerhed, som gælder for Leverandøren.  Leverandøren skal ved anvendelse af eventuelle underdatabehandlere sikre, at der indgås en databehandleraftale, der pålægger underdatabehandleren de samme databeskyttelsesforpligtelser som er underlagt leverandøren fra By & Havn.  Leverandøren er ansvarlig for i overensstemmelse med databeskyttelsesforordningens krav om ansvarlighed at føre tilsyn med sine underdatabehandlere. |  |  |  |  |
|  | K | **Styring af informationssikkerhedsbrud**  Leverandøren skal have en dokumenteret proces for hændelsesstyring og skal uden unødigt ophold orientere By & Havn om eventuelle sikkerhedshændelser og sørge for, at By & Havn holdes informeret om den løbende håndtering af sikkerhedshændelserne.  Leverandøren skal udarbejde en skriftlig procedure for håndtering af brud på persondatasikkerheden, der sikrer, at Leverandøren, efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden uden unødig forsinkelse underretter By & Havn.  Ved brud på persondatasikkerheden, skal Leverandøren dokumentere og rapportere de faktiske omstændigheder ved bruddet herunder:   * En beskrivelse af bruddet, herunder antal af berørte registrerede samt typerne af personoplysninger * Tidsrummet for bruddet * Konsekvenserne af bruddet   De foranstaltninger der er truffet for at standse bruddet. |  |  |  |  |
|  | K | **Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring**  Leverandøren skal have dokumenterede, gennemtænkte og velafprøvede planer for disaster recovery og business continuity.  Leverandøren afvikler den tilbudte løsning i et driftsmiljø med et tilpas niveau af redundans for optimal driftssikkerhed i overensstemmelse med By & Havns krav til servicemål. |  |  |  |  |
|  | K | **Overensstemmelse (ISO27701 Anneks A.18)**  Leverandøren skal overholde relevant lovgivning herunder Persondataloven, Persondataforordningen og Sikkerhedsbekendtgørelsen. |  |  |  |  |
|  | K | **It-revisionserklæring (generelle it-kontroller)**  It-revisionserklæring (generelle it-kontroller)  Leverandøren skal, uden yderligere vederlag, årligt fremsende en ISAE3402 type-2 eller tilsvarende revisionserklæring rettet mod Leverandørens generelle it-kontroller.  Erklæringen skal første gang foreligge senest 3 måneder efter indgåelse af Kontrakt. |  |  |  |  |
|  | K | **It-revisorerklæring (kontroller relateret til Leverandørens behandling og beskyttelse af personoplysninger)**  Leverandøren skal, uden yderligere vederlag, årligt fremsende en ISAE 3000 type 2 eller tilsvarende revisionserklæring, rettet mod Leverandørens behandling og beskyttelse af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, herunder overholdelse af den indgåede databehandleraftale.  Erklæringen skal første gang foreligge senest 12 måneder efter indgåelse af kontrakt. |  |  |  |  |

## Driftsmæssige krav til sikkerhed

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Kravtype** | **Beskrivelse** | **Kravsopfyldelsesgrad** | | | **Positiv vægtning i evaluering** |
| MK  K  EK  O | **Helt** | **Delvist** | **Ikke** |
| **(X)** | **(X)** | **(X)** |
|  | K | **Sikkerhedsrutiner**  Leverandøren skal etablere rutiner, der sikrer opdatering og vedligehold af alle infrastrukturkomponenter (herunder servere og slutbrugerenheder), platforms- og applikationsservices som Leverandøren er ansvarlig for med henblik på at sikre, at sikkerheds- og tilgængelighedskrav bliver opfyldt. Disse opdateringer skal altid være underlagt ændringskontrol. |  |  |  |  |
|  | K | **Procedurer for logning og monitorering**  Leverandøren skal sikre procedurer for logning og monitorering, således at overvågning, undersøgelser og analyser foretages rettidigt og efter hensigten. Leverandøren skal følge op på logs, og der skal etableres mulighed for proaktivt at følge op på misbrug og fejlhændelser i Systemet. |  |  |  |  |
|  | K | **Håndtering af sikkerhedshændelser**  Konstaterer Leverandøren et brud på sikkerheden, som har en væsentlig indvirkning på Systemet, skal Leverandøren hurtigst muligt efter at være blevet opmærksomme på forholdet underrette By & Havn telefonisk og via e-mail og oplyse om de tiltag, der er foretaget for at begrænse og/eller løse hændelsen.  Leverandøren skal i denne forbindelse sikre, at relevante tredjeparter informeres og eventuelt involveres i sikkerhedshændelsen, samt at den til enhver tid gældende lovgivning mht. anmeldelse til myndighed kan overholdes. |  |  |  |  |
|  | K | **Security awareness**  Leverandøren skal have en proces der sikrer, at deres personale løbende bliver trænet i security awareness. |  |  |  |  |
|  | K | **Fysisk placering af data**  Leverandøren skal sikre, at By & Havn altid har en opdateret oversigt over på hvilke fysiske adresser (datacentre) By & Havns persondata findes på. |  |  |  |  |
|  | K | **Datatransmission mellem datacentre**  Leverandøren skal sikre, at der anvendes en anerkendt kryptering ved transmission over internettet (f.eks. ifm. med backup) af By & Havns data mellem Leverandørens datacentre. |  |  |  |  |
|  | K | **Løbende hærdning af it-miljøet**  Leverandøren skal sikre en løbende hærdning af alle komponenter i By & Havns it-infrastruktur. Dvs. at konfigurationer af f.eks. operativsystemer, it-sikkerhedsprodukter, gruppepolitikker (Group Policies i Active Directory) og firmware i hardware løbende tilpasses ift. det aktuelle trusselsbillede og producenternes anbefalinger. Desuden skal services, IP-porte, konti og adgangsrettigheder der ikke anvendes lukkes/fjernes. |  |  |  |  |
|  | K | **Adgang til data**  By & Havns systemer og data er fortrolige. Leverandøren skal sikre, at kun de af By & Havn autoriserede personer kan få adgang til By & Havns systemer og data (logisk sikring). Dette gælder også medarbejdere hos Leverandøren. |  |  |  |  |
|  | K | **Adskillelse af By & Havns data**  By & Havns systemer og data skal være adskilt fra Leverandørens øvrige kunders it-miljøer (som minimum logisk adskillelse såfremt Leverandøren anvender shared/delt infrastruktur, hvor flere af Leverandørens kunder placeres på samme fysiske it-infrastruktur). |  |  |  |  |
|  | K | **Funktionsadskillelse**  Leverandøren skal til enhver tid sikre, at der opretholdes funktionsadskillelse i forhold til medarbejdernes håndtering af By & Havns systemer og data. |  |  |  |  |
|  | K | **Månedlig it-sikkerhedsrapportering**  Leverandøren skal som del af den månedlige driftsrapportering afrapportere på hændelser og forhold af betydning for it-sikkerheden:   * Log over sikkerhedshændelser (konstaterede brud på sikkerheden) * Anbefalinger fra Leverandøren vedr. it-sikkerhedsmæssige tiltag f.eks. begrænsning af privilegerede rettigheder, opgradering eller udskiftning af produkter etc. |  |  |  |  |
|  | K | **Sletning af data og kassation**  Leverandøren skal sikre tilstrækkelig sletning af By & Havns data ved udskiftning eller kassation af alle former for databærende medier f.eks. men ikke begrænset til diske i storage-systemer, By & Havns arbejdsstationer, printere og backupmedier. |  |  |  |  |
|  | K | **It-sikkerhedsforanstaltninger og software**  Leverandøren skal sørge for, at sikkerhedsforanstaltningerne i By & Havns it-miljøer (herunder alle servere) opdateres og vedligeholdes i overensstemmelse med god og anerkendt praksis på området. Dette gælder bl.a.:   * Perimetersikkerhed (fx firewall) * Antivirus * IDS/IPS * Web content filter / SWG |  |  |  |  |
|  | K | **Fornødne garantier**  I overensstemmelse med databeskyttelsesforordningens artikel 28, stk. 1 benytter den dataansvarlige (By & Havn) udelukkende databehandlere (Leverandøren), der kan stille fornødne garantier for, at de vil gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre , at behandling opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.  Garantier kan eksempelvis omfatte et eller flere af følgende dokumenter:   * ISAE-3000 eller tilsvarende erklæring * ISAE 3402 eller tilsvarende erklæring * ISO 27001 eller tilsvarende certificering * Dokumentation for overførselsgrundlag til tredjelande. * Oplysning om informationssikkerhedspolitikker, risikovurderinger og beredskabsplaner m.v. * Oplysning om indførte specifikke tekniske og organisatoriske sikkerhedsforanstaltninger. |  |  |  |  |
|  | K | **Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger**  Leverandøren skal tilrettelægge arbejdet med implementering af tekniske og organisatoriske foranstaltninger efter principperne om databeskyttelse gennem design og – standardindstillinger som beskrevet i databeskyttelsesforordningens artikel 25. |  |  |  |  |
|  | K | **Databehandleraftale**  Leverandøren skal i overensstemmelse med databeskyttelsesforordningens artikel 28, stk.3 indgå en databehandleraftale med By & Havn. Databehandleraftalen baseres på skabelon udarbejdet af Datatilsynet, tilpasset til By & Havns krav.  Bilag til databehandleraftalen udarbejdes endeligt  ved indgåelse af Kontrakten.  Udkast til databehandleraftalen vedhæftes som Bilag 12 og krav, der pålægges i denne databehandleraftale skal opfyldes af Leverandøren. |  |  |  |  |
|  | K | **Fortegnelse**  Leverandøren skal i overensstemmelse med databeskyttelsesforordningens artikel 30, stk.2 føre fortegnelser over alle kategorier af behandlingsaktiviteter, der foretages på vegne af By & Havn. |  |  |  |  |
|  | K | **Brud på persondatasikkerheden**  Leverandøren skal i forbindelse med styring af informationssikkerhedsbrud sikre, at brud på persondatasikkerheden kategoriseres for at sikre rettidig orientering til By & Havn, og at medarbejdere er i stand til at identificere, om der er tale om brud på persondatasikkerheden.  Leverandøren skal ligeledes sikre, at Leverandørernes medarbejdere vil være i stand til at vejlede By & Havns medarbejdere, der kontakter supporten i forbindelse med brud på persondatasikkerheden. |  |  |  |  |
|  | K | **Fortroligheds- og hemmeligholdelsesaftaler**  Leverandøren skal sikre, at personer, der har adgang til personoplysninger er underlagt en fortrolighedsforpligtelse. Leverandøren skal i fortrolighedsaftalen specificere hvor længe forpligtelserne bør overholdes. |  |  |  |  |
|  | K | **Overførsel af personoplysninger til tredjepart**  Leverandøren må ikke overlade behandling af personoplysninger til tredjepart, uden By & Havns forudgående skriftlige samtykke jf. Bilag 12 afsnit 38. |  |  |  |  |
|  | K | **Specifikke forhold relateret til Schrems II**  Leverandøren skal på By & Havns opfordring kunne redegøre for, om der i forbindelse med behandling af personoplysninger benyttes Tredjepartsleverandører, som er underlagt lovgivning i tredjelande, som kan påtvinge Leverandøren at udlevere personoplysninger om borgere i EU hostet på servere indenfor EU/EØS (F.eks. Microsoft, Google, Amazon). |  |  |  |  |
|  | K | **Specifikke forhold relateret til Schrems II**  Leverandøren skal på By & Havns opfordring kunne redegøre for, hvilke overvejelser der er gjort i forbindelse med konsekvenserne af Schrems II, herunder hvilke overførselsgrundlag der påtænkes anvendt som alternativ til Privacy Shield.  Derudover skal Leverandøren på By & Havns opfordring kunne redegøre for, hvilke overvejelser der er gjort i forbindelse med anvendelse af Standard Contractual Clauses som overførselsgrundlag og de krav der følger af Schrems II om tilvejebringelse af et beskyttelsesniveau, der er ”essentially equivalent” med beskyttelsen i EU, herunder overvejelser om ”supplerende foranstaltninger” til opnåelse af dette. |  |  |  |  |
|  | EK | **Efterlevelse af sikkerhedsstandarder**  Leverandøren skal i videst muligt omfang basere deres sikkerhedsstrategi, sikkerhedsprocesser og sikkerhedssystemer på anerkendte sikkerhedsstandarder.  *Tilbudsgiver bedes i Bilag 4.1 beskrive hvilke sikkerhedsstandarder tilbudsgiver efterlever. Det gælder både sikkerhedsstandarder nævnt i dette Bilag samt evt. andre standarder, der er relevante.* |  |  |  | *Det vægter positivt, at tilbudsgiver efterlever relevante sikkerhedsstandarder og har en proces for sikring af, at de løbende efterlever nye versioner af disse sikkerhedsstandarder.* |
|  | EK | **Overordnet beskrivelse af den samlede sikkerhedsløsning**  Leverandøren skal som en del af den tilbudte løsning levere en sammenhængende sikkerhedsløsning, der med stor sandsynlighed sikrer By & Havn imod uønsket indtrængen samt data og produktionstab.  *Tilbudsgiver bedes i Bilag 4.1 overordnet beskrive den samlede sikkerhedsløsning og hvordan den tilvejebringer stor sandsynlighed for, at By & Havn vil kunne modstå angreb, og hvordan tilbudsgiveren overordnet vil sikre, at systemer og data kan genskabes i tilfælde af f.eks. et vellykket ransomware angreb.* |  |  |  | *Det vægter positivt, at tilbudsgiver tilbyder en robust og sammenhængende sikkerhedsløsning, der giver By & Havn stor sikkerhed i forhold til uønsket indtrængen og tab af data, samt sikrer, at systemer og data kan genskabes efter et evt. vellykket ransomware angreb.* |