

**Databeskyttelses- og datasikkerhedsspørgsmål for leverandører**

GDPR pålægger Ishøj Kommune som dataansvarlig forpligtelser i forbindelse med udvælgelse og brug af databehandlere. Ishøj Kommune skal sikre, at vi kun bruger databehandlere, som giver tilstrækkelige garantier for, at de gennemfører og opretholder passende tekniske og organisatoriske foranstaltninger for at sikre, at behandlingen af personoplysninger opfylder kravene efter GDPR og sikrer beskyttelse af de registreredes rettigheder.

Udfyld venligst dette spørgeskema ved at give de krævede svar og bekræftelser.

Returner venligst det udfyldte spørgeskema tilbage til os. Skemaet skal være underskrevet af en autoriseret repræsentant for virksomheden.

|  |  |  |
| --- | --- | --- |
|  | **Databeskyttelse** | **Svar** |
|  | Hvilke personoplysninger vil I indsamle/behandle for Ishøj Kommune (f.eks. navne, e-mailadresser, IP-adresse osv.)? |  |
|  | Hvordan indsamles/modtages eller overføres personoplysningerne?  Angiv også, hvordan personoplysningerne sendes til Ishøj Kommune eller modtages fra Ishøj kommune. |  |
|  | Hvordan vil I behandle/bruge personoplysningerne? |  |
|  | Har I en databeskyttelsespolitik?  Hvis ja, skal I vedlægge en  Kopi. |  |
|  | Hvem er jeres lokale databeskyttelsestilsynsmyndighed, og hvilken databeskyttelseslovgivning håndhæver denne tilsynsmyndighed?  Er I registreret som dataansvarlig/databehandler hos denne (eller enhver anden) tilsynsmyndighed? |  |
|  | Beskriv de tekniske og organisatoriske sikkerhedsforanstaltninger, der er truffet for at beskytte de personoplysninger, I behandler på vegne af Ishøj Kommune. |  |
|  | Har I en fortegnelse over alle behandlingsaktiviteter, der foretages på vegne af en dataansvarlig, som I til enhver tid kan fremvise, hvis det er relevant? |  |
|  | Bruger I underdatabehandlere i forbindelse med behandling af personoplysninger for Ishøj Kommune?  Angiv i bekræftende fald følgende oplysninger:   * hvem er de * deres forretningsfunktion * deres adresse   Hvilke foranstaltninger gennemfører I for at:   * kontrollere underdatabehandlernes integritet samt sikkerhedsprocedurer for håndtering af personoplysninger * sikre, at underdatabehandlerne overholder gældende databeskyttelseslovgivning.   Hvordan sikrer I, at underdatabehandlerne overholder fortroligheds- og sikkerhedsprocedurer, der som minimum svarer til jeres virksomheds egne procedurer for håndtering af personoplysninger? |  |
|  | Overføres Ishøj Kommunes personoplysninger:   * mellem lokaliteter eller til ikke EU/EØS-lande dvs. usikre tredjelande som fx Indien, Ukraine eller USA   Hvis ja, har I så udarbejdet et sikkert overførselsgrundlag?  Hvis ja, hvilket grundlag?  Hvis I ikke overfører personoplysninger mellem lokaliteter eller til ikke EU/EØS-lande, hvordan kan I bekræfte og verificere dette? |  |
|  | Hvilke politikker og procedurer har I implementeret vedrørende:   * opbevaring af personoplysninger * sikker bortskaffelse af udstyr, medier, dokumenter og information.   Vedlæg venligst kopier af de relevante politikker. |  |
|  | I forbindelse med anmodning fra den registrerede om brug af rettigheder efter GDPR (indsigt, indsigelse, berigtigelse, sletning osv.), kan I i den forbindelse:   * give Ishøj Kommune oplysningerne inden for 30 dage? * Er I i stand til at give Ishøj Kommune oplysningerne i et passende format i overensstemmelse med relevant lovgivning? * Er I i stand til at slette personoplysninger efter anmodning herom fra Ishøj Kommune? |  |
|  | **Processer og kommunikation ved persondatasikkerhedsbrud** |  |
|  | Har I eller en koncern, som I er en del af, eller en underdatabehandler, som I har brugt, haft et persondatasikkerhedsbrud inden for de seneste 3 år?  I bekræftende fald skal I venligst give nærmere oplysninger herom. |  |
|  | Har I eller en koncern, som I er en del af, været genstand for undersøgelse hos en databeskyttelsestilsynsmyndighed eller en kundetvist vedrørende jeres behandling af personoplysninger inden for de sidste 3 år?  I bekræftende fald skal I venligst give nærmere oplysninger herom. |  |
|  | Har I en dokumenteret beredskabsplan/hændelsesstyrings-proces, der skal følges i tilfælde af persondatasikkerhedsbrud?  I bekræftende fald skal I vedlægge  en kopi. |  |
|  | Venligst bekræft, at I i tilfælde af et potentielt eller faktisk persondatasikkerhedsbrud vil underrette Ishøj Kommune ***så hurtigt som muligt og i alle tilfælde inden for 48 timer.*** |  |
|  | Hvem skal Ishøj Kommune kontakte i tilfælde af persondatasikkerhedsbrud?  Angiv kontaktoplysninger. |  |
|  | Angiv oplysninger om jeres forretningskontinuitet og processer samt procedurer for it-beredskab. |  |
|  | **Datasikkerhed** |  |
|  | Angiv nærmere oplysninger om eventuelle sikkerhedscertificeringer, som jeres organisation har - f.eks. ISO27001.  Hvor ofte gennemgås jeres procedurer for at bekræfte fortsat overholdelse af disse certificeringer?  Vedlæg kopier af dokumentation, der bekræfter jeres certificering. |  |
|  | Gælder disse sikkerhedsakkrediteringer for jeres ydelser for Ishøj Kommune? |  |
|  | Hvordan sikrer I, at Ishøj Kommunes data gemmes sikkert? |  |
|  | Hvordan adskilles Ishøj Kommunes data fra andre kundedata? |  |
|  | Er logisk og fysisk adskillelse på plads? |  |
|  | Hvordan gennemføres adgangskontrollen i forhold til Ishøj Kommunes data og oplysninger? |  |
|  | Er adgangen begrænset til specifikt personale? |  |
|  | Er Ishøj Kommunes data  krypteret? |  |
|  | Hvis ja, hvordan er dekrypteringsnøgler gemt og kontrolleret? |  |
|  | Hvor er data gemt/hostet? | . |
|  | Har I fortrolighedserklæringer på plads for alle jeres medarbejdere og leverandører? |  |
|  | Hvordan sikrer I, at personale, der medvirker i leveringen af ydelser til Ishøj Kommune, har den nødvendige bevidsthed om og uddannelse i databeskyttelse og datasikkerhed? |  |

**Underskrevet af:**

**For og på vegne af:**

**Stilling:**

**Dato:**