|  |
| --- |
| **SPØRGESKEMA TIL TILSYN MED DATABEHANDLERE** |
| *Hvis databehandleren har en certificering, som dækker IT-sikkerhed (f.eks. ISO 27001) bruges dette skema til at afdække GDPR-forpligtelser, der rækker udover IT-sikkerhed. Hvis databehandleren har givet en skriftlig status på forhold omfattet af databehandleraftalen, bruges dette skema som tjekliste til at sikre at alt er kommet med. Hvis databehandleren ikke har hverken certificering eller afgivet årlig status, bruges skemaet som skabelon for, hvilke oplysninger, man skal indhente fra databehandleren. Eventuelle spørgsmål til udfyldelsen og brugen af skemaet rettes til Nanna Jansfort på:* *nj@gapsolutions.dk* *eller 71 74 73 34* |
| **Identifikation** |
|  | Dato for udfyldelsen af skemaet: |  |
|  | Databehandlerens (virksomhedens) navn: |  |
|  | Databehandlerens CVR-nr.: |  |
|  | Kontaktperson hos databehandleren for eventuelle spørgsmål til de anførte oplysninger: |  |
|  | Kontaktpersonens virksomhed (kun relevant, hvis kp er fra ekstern virksomhed, f.eks ved ekstern DPO): |  |
|  | Kontaktpersonens kontaktoplysninger (e-mail og tlf): |  |
| **Organisatoriske sikkerhedsforanstaltninger og bistand til den dataansvarlige** |
| **NR** | **Spørgsmål** | **Svar (må meget gerne uddybes)** |
| 1.1 | Føres der en fortegnelse over behandlingsaktiviteter? |  |
| 1.2 | Findes der en ajourført, ledelsesgodkendt it-sikkerhedspolitik, persondatapolitik eller anden type retningslinje for sikkerhed og håndtering af data, som alle medarbejdere har kendskab til? |  |
| 1.3 | Bliver databehandlingsaktiviteterne risikovurderet med passende intervaller? |  |
| 1.4 | Er alle medarbejdere, der behandler personoplysninger, underlagt tavshedspligt, f.eks. i ansættelseskontrakt, særskilt aftale eller ved lov? |  |
| 1.5 | Findes der procedurer og ansvarshavende for håndtering af anmodninger fra den dataansvarlige på vegne af dennes registrerede? Indsigt, berigtigelse, dataportabilitet, sletning,osv |  |

|  |  |  |
| --- | --- | --- |
| 1.6 | Findes der procedurer og/eller ansvarshavende for underretning af den dataansvarlige i tilfælde af at dennes instruks strider imod anden lovgivning, som databehandleren er forpligtet til at efterleve? |  |
| 1.7 | Findes der procedurer og/eller ansvarshavende for underretning af den dataansvarlige i tilfælde af sikkerhedsbrud? |  |
| 1.8 | Findes der procedurer og/eller ansvarshavende for underretning af/godkendelse fra den dataansvarlige om ændringer i underdatabehandlere? |  |
| 1.9 | Findes der procedurer for at stille de nødvendige oplysninger til rådighed for at den dataansvarlige kan føre tilsyn? |  |
| 1.10 | Findes der procedurer for sletning og/eller tilbagelevering af data ved aftaleforholdets ophør? |  |
| **Fysiske og tekniske sikkerhedsforanstaltninger** |
| **NR** | **Spørgsmål** | **Svar (må meget gerne uddybes)** |
| 2.1 | Er fysisk adgang til virksomhedens lokaler adgangsreguleret? Både i og udenfor arbejdstid? |  |
| 2.2 | Er adgang til personoplysninger - både på fysisk og digital form - reguleret efter arbejdsbetinget behov? |  |
| 2.3 | Er der retningslinjer for behandling af skriftligt og printet materiale med personoplysninger? Sker destruktion på en sikker og forsvarlig måde, f.eks. opsamling eller makulering? |  |
| 2.4 | Er alle systemer med personoplysninger sikret med passende opdateret anti-virus, anti-malware, firewall etc.? |  |
| 2.5 | Er der indført retningslinjer for brugeradgange til systemer med personoplysninger, f.eks. individuelle brugerkonti m. passwords, lukning af unødvendige brugerkonti, begrænsning af rettigheder? |  |

|  |  |  |
| --- | --- | --- |
| 2.6 | Tages der back-up af alle personoplysninger, der behandles på vegne af den dataansvarlige? |  |
| 2.7 | Er netværk, faste og trådløse, sikret med passende adgangskontrol? Evt. opdelt i internt netværk, gæstenetværk etc.? |  |
| 2.8 | Hvis relevant: Bliver systemer I selv udvikler og leverer vedligeholdt løbende i forhold til seneste viden om cybersikkerhed? |  |
| **Underleverandører/underdatabehandlere** |
| **NR** | **Spørgsmål** | **Svar (må meget gerne uddybes)** |
| 3.1 | Anvendes underleverandører til behandling af personoplysninger på den dataansvarliges vegne, f.eks. distributør, marketing, serverhosting, el.lign.? Hvis nej, spring sektion 3 over. |  |
| 3.2 | Findes der en liste over samtlige underdatabehandlere? |  |
| 3.3 | Er der en skriftlig aftale med underdatabehandlere om overholdelse af reglerne i databehandleraftalen med den dataansvarlige? |  |
| 3.4 | Føres der kontrol med underdatabehandlere, f.eks ved indhentning af ISAE-erklæringer eller ISO-certifikater? Hvor ofte? |  |
| 3.5 | Er en eller flere underdatabehandlere placeret i usikre tredjelande? Hvis ja, hvordan sikres det, at de også lever op til kravene til sikkerhed i behandlingen? |  |
| **Kontroller/stikprøver** |
| **NR** | **Spørgsmål** | **Svar (må meget gerne uddybes)** |
| 4.1 | Føres der kontrol med at brugeradgange og -rettigheder er tildelt korrekt? Hvor ofte? |  |
| 4.2 | Føres der kontrol med at henvendelser fra den dataansvarlige bliver besvaret indenfor den aftalte frist? Hvor ofte? |  |

|  |  |  |
| --- | --- | --- |
| 4.3 | Føres der kontrol med, at alle hændelser, som den dataansvarlige skal informeres om også er blevet viderebragt indenfor den aftale frist? Hvor ofte? |  |
| 4.4 | Overvåges systemer i form af systemlog? Hvor ofte gennemgås loggen for tegn på fejl, nedbrud el. sikkerhedsbrud? |  |
| 4.5 | Sikres det, at systemer/data kan gendannes fra back-up? Hvor ofte? |  |
| 4.6 | Sikres det, at relevante medarbejderes viden om databeskyttelse og fortrolighed holdes opdateret, f.eks. med awarenesstræning el. uddannelse? Hvordan og hvor ofte? |  |
| **Siden sidste tilsyn el. siden indgåelse af databehandleraftale** |
| **NR** | **Spørgsmål** | **Svar (må meget gerne uddybes)** |
| 5.1 | Er der kommet nye underdatabehandlere til siden sidste tilsyn? Hvis der ikke er ført tilsyn før, er der da sket ændringer siden indgåelsen af databehandleraftalen? |  |
| 5.2 | Er der sket ændringer i behandling eller procedurer, som kan have betydning for den dataansvarliges benyttelse og/eller vurdering af ydelsen? |  |
| 5.3 | Har der været nedbrud, driftsforstyrrelser, sikkerhedsbrud eller andre sikkerhedshændelser siden sidste tilsyn? |  |
| 5.4 | Redegør for eventuelle andre forhold vedrørende IT- anvendelse eller det interne kontrolmiljø, som kan være afbetydning for vurderingen af databehandlingen. |  |