|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Compliance analyse**  **Databeskyttelsesforordningen** | | | | | |
| **Compliance område:** | **Udført af:** | | **Bemærkninger?**  (Ja/Nej) | **Hvis negativ besvarelse, hvilke samt eventuelle tiltag?** | |
| **a) Ekstern compliance** *(databehandler, underdatabehandler samt tredjemænd)* | | | | | |
| a.1.  Er der et samarbejde med en ekstern fysisk- eller juridisk person, der indeholder behandling af personoplysninger, hvor der ikke er indgået en skriftlig databehandleraftale? |  | |  |  | |
| a.2.  Såfremt der benyttes databehandler: Er databehandlerens tekniske og organisatoriske foranstaltninger kontrolleret i den seneste periode? |  | |  |  | |
| a.3.  Såfremt der anvendes underdatabehandler: Er underdatabehandlerens tekniske og organisatoriske foranstaltninger kontrolleret i den seneste periode samt foreligger der en skriftlig databehandleraftale mellem databehandleren og underdatabehandleren? |  | |  |  | |
| a.4.  Er personoplysninger kommet tredjemand til hænde via en utilsigtet hændelse, fx tyveri, hacking eller direkte overførsel? |  | |  |  | |
| **b) Ekstern compliance i forhold til børn/forældre samt samarbejdspartnere** | | | | | |
| b.1.  Er der konstateret nogen behandling af personoplysninger, der ikke har et lovligt grundlag ifølge artikel 6, stk. 1, litra a-f, fx samtykke, kontrakt eller lignende? |  | |  |  | |
| b.2.  Er der nogle kategorier af registrerede (forældre/børn og samarbejdspartnere), der ikke har modtaget oplysningsskrivelsen efter artikel 13? |  | |  |  | |
| b.3.  Har en eller flere kategorier af registrerede (forældre/børn og samarbejdspartnere) udøvet sine rettigheder efter Databeskyttelsesforordningen inden for den seneste periode? |  | |  |  | |
| b.4.  I bekræftende fald på spørgsmål b.3.: Er Databeskyttelsesforordningens krav til reaktionstid m.v. blevet overholdt i forbindelse med svar på den pågældendes anmodning? |  | |  |  | |
| b.5.  Er personoplysningerne i den seneste periode gennemgået med henblik på, at afklare om nogle oplysninger bør slettes, da de ikke længere er nødvendige for behandlingen? I bekræftende fald, er personlysningerne blevet slettet? |  | |  |  | |
| **c) Intern compliance i forhold til de ansatte** | | | | | |
| c.1.  Er der nogen ansatte, der ikke har givet samtykke til behandling af deres personoplysninger, fx samtykke til offentliggørelse af deres billede? |  | |  |  | |
| c.2.  Er der nogen ansatte, der ikke er blevet underrettet om deres rettigheder angående behandlingen af deres personoplysninger efter artikel 13 samt eventuel orientering om videoovervågning? |  | |  |  | |
| c.3.  Er nogen af de ansatte blev trænet i Databeskyttelsesret inden for den seneste periode? |  | |  |  | |
| **d) Intern compliance i forhold til fortegnelsen** | | | | | |
| d.1.  Er fortegnelsens formkrav, altså at fortegnelsen skal foreligge skriftligt og elektronisk overholdt? | |  | | |  |
| d.2.  Er fortegnelsen blevet ajourført inden for de seneste 6 mdr.? | |  | | |  |
| d.3.  Er der registreret nogle ændringer? | |  | | |  |
| **e)** **Intern compliance i forhold til princippet om god databehandlingsskik, om formålsbestemthed, herunder finalité, om dataminimering, om rigtighed samt om opbevaringsbegrænsning** | | | | | |
| e.1.  Er der blevet foretaget en stikprøvekontrol indenfor de seneste 6 mdr., der har til formål at belyse om de førnævnte principper overholdes? | |  | | |  |
| e.2.  I bekræftende fald på spg. e.1: Har stikprøvekontrollen udvist nogle brud på principperne? | |  | | |  |
| e.3.  I bekræftende fald på spg. e.2.: Er der implementeret fremtidige procedurer, der skal imødegå det påviste brud på principperne? | |  | | |  |
| **f) Intern compliance i forhold til passende tekniske og organisatoriske foranstaltninger** | | | | | |
| f.1.  Er IT blevet løbende opdateret, dvs. opdatering af fx firewall og antivirus? |  | |  |  | |
| f.2.  Bliver adgangskoderne løbende skiftet og overholder disse formkravene i den interne persondatapolitik? |  | |  |  | |
| f.3.  Har der været et IT sikkerhedsbrud i den seneste periode? |  | |  |  | |
| f.4.  I bekræftende fald på spørgsmål f.3., er der så sket behørig underretning til henholdsvis Datatilsyn samt berørte registrerede, fx ansatte eller forældre/børn? |  | |  |  | |
| f.5.  I bekræftende fald på spørgsmål f.3., hvordan sikres, at det pågældende brud ikke sker igen? |  | |  |  | |
| f.6.  Er samtlige fysiske og elektroniske arkiver, der indeholder personoplysninger afspærret for uautoriseret personale samt offentligheden, medmindre der er givet samtykke til andet? |  | |  |  | |
| f.7.  Har der været et sikkerhedsbrud af fysiske arkiver af personoplysningerne i den seneste periode? |  | |  |  | |
| f.8.  I bekræftende fald på spørgsmål f.7., er der så sket behørig underretning til henholdsvis Datatilsyn samt berørte registrerede? |  | |  |  | |
| f.9.  I bekræftende fald på spørgsmål f.7., hvordan sikres, at det pågældende brud ikke sker igen? |  | |  |  | |
| f.10.  Er der uautoriseret personale, der kan tilgå personoplysningerne fysisk eller elektronisk? |  | |  |  | |
| f.11.  I bekræftende fald på spørgsmål f.10., har det uautoriserede personale tilgået personoplysningerne i den seneste periode? |  | |  |  | |
| f.12.  I bekræftende fald på spørgsmål f.10., hvordan sikres det fremadrettet, at det uautoriserede personale afskæres fra, at have mulighed for, at tilgå personoplysningerne? |  | |  |  | |
| f.13.  Er der nogen medarbejdere, der har ubegrænset adgang til personoplysninger, som ikke er pålagt tavshedspligt? |  | |  |  | |
| f.14.  Hvis der benyttes mobilt udstyr, overholder disse enheder den vedtagne politik, såsom anvendelse af kryptering samt lås på arbejdstelefoner? |  | |  |  | |
| f.15.  Hvis der er fremsendt følsomme personoplysninger pr. mail i perioden, er oplysningerne fremsendt via sikker mail? |  | |  |  | |
| f.16.  Har der været benyttet hjemmearbejdspladser i perioden, hvor benyttelsen har været i strid med den vedtagne politik? |  | |  |  | |