# Arbejdsgang for gennemførelse af tilsyn med databehandlere

Som systemejer er man dataansvarlig og dermed ansvarlig for at der gennemføres tilsyn med databehandlere og handles på eventuelle bekymringer.

Gennemførelsen af tilsyn afhænger af de beslutninger der er er truffet ifm. indgåelsen af databehandleraftalen. Nedenfor er skitseret processen for de forskellige tilsynsformer:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Fysisk besøg med revisorerklæring** | **Fysisk besøg med spørgeskema** | **Skriftlig informationsindsamling** | **Tilsyn via DSD** |
| **Hvem gennemfører tilsynet** | Tredjepart | Dataansvarlig | Dataansvarlig | DSD |
| **Forberedelse** | Du skal som dataansvarlig indhente revisorerklæringen hos leverandøren.  Såfremt databehandler benytter underdatabehandlere skal du huske i samme ombæring at bede om revisorerklæringer på disse, eller få dokumentation/garanti fra leverandøren om, at der er foretaget tilsyn på anden vis. | Du skal som dataansvarlig varsle tilsynet overfor leverandøren i passende tid og orientere omkring de emner du ønsker at have fokus på.  Du skal lave en plan for de områder du ønsker at tilse og fremsende denne til databehandler. | Du skal som dataansvarlig fremsende spørgeskemaet til gennemførelse af tilsyn til databehandleren.  Såfremt databehandler benytter underdatabehandlere skal du huske i samme ombæring at bede om revisorerklæringer på disse, eller få dokumentation/garanti fra leverandøren om, at der er foretaget tilsyn på anden vis. | DIGIT modtager resultatet af tilsynet fra DSD og videresender denne til evt. bemærkninger til dataansvarlig. |
| **Gennemførelse** | Når du har modtaget revisorerklæringen, skal du gennemgå den grundigt, særligt med fokus på om revisor har påpeget forhold der bør  løftes overfor databehandleren.  Herefter skal du vurdere om der er forhold du ønsker afklaret hos databehandleren og indhente disse til brug for den samlede afgørelse.  Inddrag DIGIT og Jura efter behov. | Det fysiske tilsyn begynder allerede på parkeringspladsen. Her kan det være, at du ikke kan undgå at se at der ligger fortrolige data på forsædet af en bil, det kan være du overhører medarbejdere tale om personfølsomme oplysninger mens du går forbi eller det kan være at du kan gå uhindret ind i bygningen og færdes frit i kontormiljøer med fortrolige data. Møder du forhold som disse bør du i samtalen drøfte dem med databehandleren.  Mødet tager udgangspunkt i den fremsendte agenda, men kan udvides hvis du i samtalen vurderer at der er andre relevante emner som bør drøftes i relation til tilsynet.  Bed altid om at få en rundvisning så du kan se hvordan de behandler fysiske produkter med fortrolige data.  Hvis databehandler benytter underdatabehandlere skal du huske at bede om revisorerklæringer eller få dokumentation/garanti fra leverandøren om, at de har foretaget tilsyn med underdatabehandleren.  Afslut mødet med en aftale omkring videre proces, herunder hvis I har aftalt opfølgning på forhold og evt. genbesøg i forbindelse med dette tilsyn. | Når du som dataansvarlig modtager spørgeskemaet retur, skal du gennemgå det grundigt og vurderer om der er forhold der giver anledning til at indhente yderligere oplysninger hos databehandleren.  Inddrag DIGIT og DPO efter behov. | Som dataansvarlig skal du gennemgå tilsynsrapporten fremsendt af DIGIT.  Hvis du har opklarende spørgsmål, rettes disse til DSD og/eller DPO. |
| **Afgørelse om evt. handling** | På baggrund af materialet skal du som dataansvarlig træffe afgørelse om hvordan der skal reageres på tilsynet. Det kan eks. være:   * Tilsynet er tilfredsstillende, så der foretages ikke yderligere. * Der er kritiske opmærksomhedspunkter, der kræver en forklaring fra leverandørens side. * Kommunen vil stille krav om ændringer til leverandøren, der efterfølgende skal dokumenteres. * Kommunen må opsige samarbejdet på baggrund af tilsynet.   Du kan eventuelt søge råd og vejledning hos DIGIT eller DPO ved tvivlsspørgsmål.  Du skal beskrive grundigt hvilke udfordringer du ses, hvilke foranstaltninger du foreslår, dialogen med databehandler samt de konkrete aftaler du indgår med, databehandler omkring foranstaltninger og opfølgning. | | | |
| **Dokumentation**  ***erklæring om tilsyn med databehandlere*** | Som dataansvarlig skal du udfylde dokumentet *erklæring om tilsyn med databehandlere,* der udgør dokumentation for, at tilsynet er udført. Dokumentet kan tilgås via følgende link: [Procedurer, retningslinjer og skabeloner | Uglen (ishoj.dk)](https://uglen.ishoj.dk/procedurer-retningslinjer-og-skabeloner).  Herefter skal du journalisere al materialet i IT-systemets SBSYS-sag, i samme mappe som databehandleraftalen er journaliseret i. Materialet kan omfatte:   * Erklæring om tilsyn med databehandlere * Revisorerklæringen * Rapport fra fælles DSD-tilsyn * Yderligere materiale tilsendt fra databehandler * Dokumentation fra fysisk tilsyn * Spørgeskemabesvarelse * Aftalte foranstaltninger * Aftale om opfølgning   Datatilsynet gennemfører løbende kontrol af Kommunernes tilsyn med databehandlere. Datatilsynet kan komme anmeldt eller uanmeldt. Særligt ved de uanmeldte besøg er det væsentligt at dokumentationskravet er overholdt, så dokumentation let kan fremsøges i SBSYS. | | | |
| **Opfølgning på iværksatte foranstaltninger** | Er der indgået aftale med databehandler omkring foranstaltninger er det vigtigt at der sker en opfølgning og at resultatet heraf dokumenteres i sagen.  Du skal som dataansvarlig sikre, at de besluttede foranstaltninger iværksætter og at du går gennemført den besluttede/aftalte opfølgning på tilsynet med databehandleren. Husk løbende at journaliserer eventuel yderligere dokumentation på sagen; svar på opfølgning mv. | | | |
| **Registrering i KITOS, journalisering i SBSYS og Afslutning** | Når du er tilfreds med de iværksatte foranstaltninger, kan du afslutte sagen.  Du skal registrere tilsynet i KITOS for den konkrete databehandleraftale. Under fanen ”Tilsyn” skal du oprette det gennemførte tilsyn og udfylde de obligatoriske felter med resultatet. Tilsynet kan efter oprettelse rettes eller slettes. Der kan oprettes flere tilsyn, så det fulde billede skabes.  Du skal journalisere tilsynsrapporten samt øvrige dokumenter omkring tilsynet på den sag i SBSYS, hvor øvrige dokumenter vedr. IT-systemet er journaliseret. Opret en ny mappe til tilsynet. | | | |