Retningslinjer for tilsyn med databehandlere

Når der er indgået en databehandleraftale med den leverandør, følger en række afledte opgaver, herunder pligten til at foretage en risikovurdering og føre tilsyn med databehandleren.

I persondataforordningens artikel 5 listes syv principper for hvordan man bør behandle persondata. Jf. princip nr. 7 ”Ansvarlighed” skal den dataansvarlige kunne påvise, at alle principper efterleves ved de behandlinger, der foretages. Denne dokumentationsforpligtelse løftes b.la. gennem fortegnelser og ved tilsyn med databehandler.

# Tilsyn med databehandlere

Planlægningen af tilsyn med databehandlere starter ved indgåelsen af databehandleraftalen, hvor frekvens og tilsynsform besluttes med udgangspunkt i risikovurderingen.

Tilsynet med databehandlere kan foretages enten via indhentelse af en revisionserklæring eller via et spørgeskema.

Upåagtet om der anvendes en revisorerklæring eller et spørgeskema er formålet med tilsynet at give Ishøj Kommune sikkerhed for, at databehandlere lever op til kravene i GDPR, som de har forpligtiget sig til ved indgåelse af databehandleraftalen.

Tilsynet kan ofte med fordel kombineres med det faglige tilsyn af leverandøren.

Frekvensen af tilsyn og formen herfor, afhænger af en konkret risikovurdering af den enkelte databehandler. Jo større risiko, des oftere bør tilsyn føres, og dette bør eventuelt ske ved fysisk tilsyn.

## Fælles tilsyn via Den Storkøbenhavnske Digitaliseringsforening (DSD)

Nogle tilsyn vil blive foretaget i regi af Den Storkøbenhavnske Digitaliseringsforening (DSD), hvor Ishøj Kommune er medlem. DSD har en ressource ansat til at føre tilsyn med de systemer, som er fælles eller udbredt blandt foreningens medlemskommuner.

## Frekvens og tilsynsform

Frekvensen af, hvor ofte der skal foretages tilsyn med databehandleren, og hvilken tilsynsform der anvendes, afhænger af risikovurderingen. Jo større mængder af følsomme data leverandøren

behandler, jo mere omfattende skal tilsynet være.

## Valg af frekvens

Hvis risikoen er høj, kan det være nødvendigt at foretage tilsyn med databehandleren halvårligt eller årligt. Hvis risikoen er lav, kan du som dataansvarlig nøjedes med at påse din databehandlers behandlingssikkerhed med en lavere frekvens. Datatilsynet kommer dog ikke med nærmere præcisering af, hvad "lavere frekvens" indebærer.

## Valg af tilsynsform

Alt efter den identificerede risiko kan tilsynet af databehandlere foretages som et fysisk besøg eller som en skriftlig informationsindsamling.

Hvis risikoen for de registreredes rettigheder vurderes høj, kan det være nødvendigt at foretage fysisk tilsyn med databehandleren. Momenter i risikovurderingen, som kan tale for et fysisk tilsyn, er blandt andet delegation og brug af administrative rettigheder, adgangen til persondata, pålagte sletteregler m.fl.

Tilsynet kan foretages enten via indhentelse af en revisionserklæring eller via et spørgeskema.

En revisionserklæring (eksempelvis ISAE 3000 eller ISAE 3402) er udarbejdet af en uvildig tredjepart og anvendes ofte til større leverandører eller leverandører, der behandler følsomme oplysninger.

Et spørgeskema udsendes af dataansvarlig og anvendes ofte til mindre leverandører, der ikke behandler følsomme eller store mængder af oplysninger.

Upåagtet om der anvendes en revisorerklæring eller et spørgeskema er formålet med tilsynet at give Ishøj Kommune sikkerhed for, at databehandlere lever op til kravene i GDPR, som de har forpligtiget sig til ved indgåelse af databehandleraftalen.

I udgangspunktet kan opstilles følgende vejledning for frekvens og tilsynsform:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Leverandørtype** | **Risiko-vurdering** | **Frekvens** | **IT-**  **revisorerklæring** | **Fysisk tilsyn** | **Interview/**  **spørgeskema** |
| Hostingfirma, større IT-leverandører, databehandlingsbureauer o.l | Grøn | Hvert 3. år\*\* | Nej\* | Hvis en  risikovurdering  siger det. | Ja |
| Gul | Årlig | Ja | Hvis det ikke er muligt at få revisorerklæring | Hvis det ikke er muligt at få revisorerklæring |
| Rød | halvårligt | Ja | Hvis det ikke er muligt at få revisorerklæring | Hvis det ikke er muligt at få revisorerklæring |
| Leverandør der behandler få mængder af personoplysninger | Grøn | Hvert 3. år\*\* | Nej\* | Hvis en  risikovurdering  siger det. | Ja |
| Gul | Årlig | Nej\* | Hvis en  risikovurdering  siger det. | Ja |
| Rød | halvårligt | Ja | Hvis det ikke er muligt at få revisorerklæring | Hvis det ikke er muligt at få revisorerklæring |

\*) Hvis leverandøren selv tilbyder den, så vælg den!

\*\*) Følger anbefalingerne fra Den Storkøbenhavnske Digitaliseringsforening (DSD) som Ishøj Kommune er en del af

DIGIT kan hjælpe med at vurdere passende frekvens og tilsynsform.

# Løbende tilsyn med databehandlere

For nogle Centre er der indgået mange databehandleraftaler med hver deres beslutning om nødvendige proces. For at sikre overblik anbefales det, at der føres et årshjul med alle tilsyn, så overblikket holdes og tidsplanen for tilsyn kan dokumenteres ved besøg af datatilsynet.

KITOS indeholder modulet ”Databehandling” der med fordel kan anvendes til at holde det nødvendige overblik og foretage registreringer. Se retningslinje for IT-registreringspraksis bilag B, som indeholder en oversigt over felter i KITOS modulet ”Databehandling”.

Tilsyn for et kalenderår, skal være afsluttet og dokumenteret inden udgangen af december, så et sammendrag kan komme med i den årlige ledelsesrapportering om informationssikkerhed.