Vejledning om tilsyn med databehandlere

Organisation	**Databeskyttelsesrådgiverfunktion i Den Storkøbenhavnske Digitaliseringsforening (DSD)**
Dokument navn	Vejledning om tilsyn med databehandlere v.1.0.docx
Dokument ejer	Michael Drews Olsen og Daniel Bach
Senest ændret	5. oktober 2018
Autoriseret af	
ISO 27002 reference	Leverandørforhold 15.1 og 15.2
GDPR-reference	Artikel 24 – dataansvarliges ansvar. Artikel 32 – risikovurdering og gennemførelse af passende sikkerhedsforanstaltninger. Artikel 28 databehandler

Version nr.	Dato	Revisions forfatter	Beskrivelse
1.0	5. oktober 2018	Michael Drews Olsen	Første version

Formål: Behandlingsaktiviteter, der helt eller delvis foretages af databehandlere, skal være i overensstemmelse med reglerne i persondataforordningen. Den fagansvarlige har ansvar for databehandlere og skal derfor kunne påvise, at indgåede databehandleraftaler overholdes, og at databehandleren har gennemført de aftalte tekniske og organisatoriske sikkerhedsforanstaltninger

Denne vejledning beskriver, hvordan den fagansvarlige i kommunen kan planlægge, dokumentere og udføre tilsyn med databehandlere.

Omfang: Alle kommuner i DSD, som er tilsluttet den fælles.

Ansvarsfordeling: Kommunens [fagansvarlige] har ansvar for at indgå databehandleraftale med databehandlere og føre tilsyn med, at databehandlere overholder databehandleraftalen.
Alt efter den risici, som er forbundet med behandlingsaktiviteten, planlægger og dokumenterer den [fagansvarlige] frekvensen og omfanget af tilsynet med databehandleren.

Kommunens [Sikkerhedsansvarlige] stiller de ressourcer og bistand til rådighed, som er nødvendige for at påse, om databehandlere overholder databehandleraftalerne.

Lovkrav
Det følger af persondataforordningens artikel 32, at den dataansvarlige og databehandleren gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen.

Det følger videre af persondataforordningens artikel 28, stk. 3, litra c, at det skal fremgå af en databehandleraftale, at databehandleren gennemfører de foranstaltninger, der kræves i henhold til artikel 32.

Hvad er et passende sikkerhedsniveau?
Hvilket sikkerhedsniveau, det er nødvendigt at gennemføre hos databehandleren, afhænger af de risici, der er forbundet med behandlingen af de pågældende personoplysninger. Sikkerhedsniveauet skal passe til risici, så personoplysningerne behandles med tilstrækkelig sikkerhed.

Det er den dataansvarliges ansvar, at risikovurderingen gennemføres.

Før behandlingens påbegyndelse skal der på baggrund af en risikovurdering tages stilling til, hvilke sikkerhedsforanstaltninger det er nødvendigt at gennemføre hos databehandleren med henblik på at sikre et passende sikkerhedsniveau. Risikovurderingen skal afspejles i de sikkerhedsforanstaltninger, som der beskrives i databehandleraftalen.

Hvad skal der føres tilsyn med?
Kommunens fagansvarlige sikrer, at databehandleren overholder databehandleraftalen. Det betyder, at der skal føres tilsyn med, om sikkerhedsniveauet er passende, og det vil i den forbindelse være naturligt at tage udgangspunkt i de sikkerhedsforanstaltninger, som er beskrevet i databehandleraftalen.

Frekvens og tilsynsform
For hver behandlingsaktivitet etablerer den fagansvarlige en tilsynsplan. Valget af frekvens og tilsynsform afhænger af den risici, som er forbundet med behandlingen af personoplysningerne.

Ved en behandlingsaktivitet, der har understøttende systemer med en stor dynamisk udvikling og i et miljø, hvor den benyttede infrastruktur er eksponeret for hurtigt skiftende risikoscenarier, vil der være behov for hyppigere og mere målrettet kontrol, end i et statisk et miljø hvor der en på forhånd kendt risiko.

Som udgangspunkt kan tilsynsplanen etableres som følger:

Behandlingsaktivitet med lav risiko –			
Frekvens	Årligt eller eventuelt med lavere frekvens afhængig af risiko	Andet år	Tredje år
Tilsynstype	Compliance evalueres igennem spørge-skema/erklæringer	Skriftlig compliance atte-station	Skriftlig compliance attesta-tion
Cyklus gentages	î----------ĵ		

Behandlingsaktivitet med middel risiko		
Frekvens	Første år	Andet år
Tilsynstype	Compliance evalueres igennem erklæringer	Skriftlig compliance attestation
Cyklus gentages	↑----------	----------↵

Behandlingsaktivitet med høj risiko / dynamiske systemer	
Frekvens	Halvårligt eller årligt afhængig af risiko
Tilsynstype	Fysisk tilsyn eller compliances evalueres igennem erklæringer afhængig af risiko

Tilsynsplanen indskrives typisk i fagcenterets årshjul, således at den fagansvarlige kan overskue og sikre at der udføres tilsyn med databehandlere.

Der kan henvises til Datatilsynets vejledende tekst om tilsyn med databehandlere og underdatabehandler, som bl.a. indeholder en beskrivelse af momenter, der kan tale for fysisk tilsyn.

Sikkerhedshændelser
Hvis en databehandler, har haft sikkerhedsbrud, skal tilsynsplanen revideres. Sikkerhedsbrud kan opdeles i 2 kategorier:

- Sikkerhedsbrud uden alvorlig konsekvens for de registrerede
- Brud med alvorlig konsekvens for de registrerede, og anmeldelse til datatilsynet

Hvis en databehandler i kalenderåret, har haft et eller flere alvorlige sikkerhedsbrud, der indebærer anmeldelse til datatilsynet, skal den fagansvarlige gennemføre fuldt tilsyn (svarende til første års tilsyn) med databehandleren, indtil det kan påvises, at de relevante mangler er afhjulpet. Dette gælder for alle behandlingsaktiviteter uanset risikoniveauet for de registrerede.

Hvem påser behandlingssikkerheden hos databehandleren?
Den fagansvarlige har ansvaret for at føre tilsyn med databehandleren, men den fagansvarlige har ikke altid den nødvendige ekspertise til at påse, om databehandlere overholder de sikkerhedsforanstaltninger, der er aftalt i databehandleraftalen. Derfor bistår kommunens sikkerhedsansvarlige med nødvendig ekspertise og ressourcer fra sikkerhed eller IT-afdelingen. I nogle tilfælde, hvor flere kommuner bruger de samme databehandlere og løsninger, er der mulighed for, at et udført tilsyn kan bruges i flere DSD-kommuner.

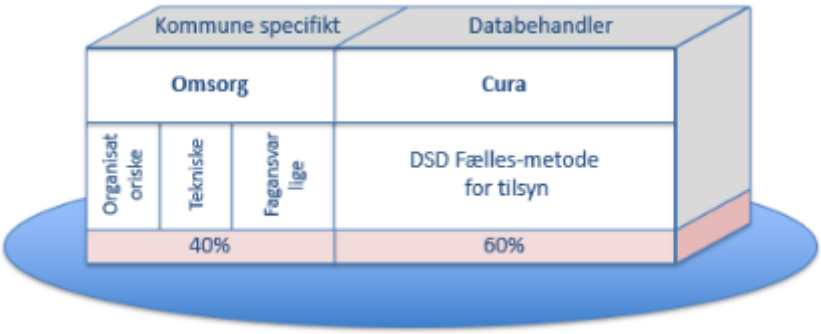
Tilsynsrapport
Med henblik på at den fagansvarlige kan påvise, at der er udført tilsyn med databehandlere, anbefales det at udarbejde en rapport med følgende struktur og indhold:

- Navnet, stilling, arbejdsgiver på forfatter af tilsynsrapporten
- Dato for evalueringen
- Behandlingsområdet for behandlingen i kommunen
- Kategorier af personoplysninger
- Identiteten af leverandøren/databehandleren
- Behandlingen (service) der føres tilsyn med, skal utvetydigt identificeres.

- Materialet der ligger til grund for tilsynet skal identificeres og hvis muligt vedlægges som bilag
    - Fysisk tilsyn
    - Revisionsrapport (Revisor navn, type og perioden for tilsynet)
    - Certificerings type og relevant SOA (type og perioden for certificeringen)
    - Spørgeskema (Navn og Version)
    - Attestation fra leverandøren
- Underdatabehandlere - databehandleren påviser og dokumentere
    - Ændringer i underdatabehandlere involveret i behandlingen
    - Dokumentation af tilsyn med underdatabehandleren
- Eventuelle overførsler til tredjeland dokumenteres
- Revisors uvildig konklusion på afvigelser
- Eventuel mangler der skal afhjælpes samt dato
- Dato for næste tilsyn

Fælles DSD tilsynsrapport

For at kommuner i DSD kan genbruge tilsynsrapporter af fællesdatabehandlere, skal tilsynsrapporten redigeres i en standardstruktur som beskrevet ovenfor. Med andre ord er det ikke muligt at genbruge en tilsynsrapport, hvis metoden ikke er standardiseret. Tilsynsrapporten skal udformes således, at en fagansvarlig, uanset hvilken kommune denne arbejder i, kan forstå hvad der er kontrolleret, og hvorvidt der er afvigelser der skal undersøgers yderligere. Der skal også tages højde for, at databehandleraftaler kan være forskellige imellem DSD-kommuner. Hver enkelt kommune skal derfor sikre, at den fælles tilsynsrapport er fyldestgørende jf. databehandleraftalen. I tilfælde af mangler i tilsynsrapporten, skal den enkelte kommune derfor udføre supplerende kontroller.



Figuren viser eksempel på elementer der kan indgå i en fælles tilsynsrapport

Journalisering og dokumentation

En leverandør har typisk en kontrakt med kommunen samt en databehandleraftale, som er journaliseret i kommunens sagsbehandlingssystem. Det er hensigtsmæssigt at journalisere tilsynsplanen, tilsynsrapporten og relevante bilag i det samme system, hvormed den fagansvarlige kan påvise, at tilsynet med databehandleren er udført.

Definitioner:

»dataansvarlig«: en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger. I DSD-kommuner kalder vi denne rolle for [Fagansvarlig].

»fagansvarlig«: en fagansvarlig har ledelsesansvaret for et område, et center, eller en forvaltning i kommunen. En fagansvarlig har det overordnende ledelsesansvar for behandlingsaktiviteter (behandlingen af personoplysninger) inden for det pågældende område, center eller forvaltning. En fagansvarlig refererer til den administrative direktion i kommunen.

»databehandler«: en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne

»sikkerhedsansvarlig«: en sikkerhedsansvarlig kan være en it-chef med ledelsesansvar for it-sikkerheden og/eller it-driften i kommunen. En sikkerhedsansvarlig kan også være en digitaliseringschef med ledelsesansvar for digitalisering eller it i kommunen. En sikkerhedsansvarlig kan have ledelsesansvar for tværgående opgaver vedrørende it, digitalisering eller GDPR. En sikkerhedsansvarlig samarbejder med fagansvarlige i centre eller forvaltninger og refererer til den administrative direktion i kommunen.

»sikkerhedskoordinator«: en sikkerhedskoordinator er en medarbejder, som er blevet udpeget til at varetage rollen som kommunens primære kontaktperson til DPO'en. Sikkerhedskoordinatoren deltager i regelmæssige møder med andre DSD-kommuner, som er tilsluttet den fælles DPO-funktion, med henblik på at harmonisere tilgangen til sikkerhed og compliance. Sikkerhedskoordinatoren har et tæt samarbejde med kommunens sikkerhedsansvarlige.

»fagcentre«: en Kommune er opdelt i forskellige enheder med fokus på et specifikt pligtområde. Disse enheder kaldes også fagcentre, afdelinger, forvaltninger eller centre. Et fagcenter har en eller flere [fagansvarlig], der bærer rollen som dataansvarlige.

Officielle kilder:

Datatilsynet: vejledende tekst om tilsyn med databehandlere og underdatabehandlere.pdf
Persondataforordningen - Link