Dokumentdato: 23. januar 2020
Dokumentansvarlig: KRR

Anvisning vedrørende databehandlere

1. Indhold

2. Introduktion

Denne institutionelle anvisning definerer håndteringen af databehandleraftaler på DMJX. Selvom begreberne "databehandlere" og "databehandleraftaler" ikke er nye og ukendte i dansk ret og EU-ret, så er håndteringen af databehandlere særligt kommet helt frem i bevidstheden og højt på prioriteringslisten pga. Persondataforordningens skærpede sanktionsniveau.

Målet med anvisningen er både at definere håndteringen af databehandlersituationerne på DMJX, men også at skabe klarhed. Derfor vil anvisningen blive opdateret løbende.

3. Målgruppe

De primære målgrupper for anvisningen er forskere og medarbejdere der skal benytte databehandlere til at indsamle, behandle og opbevare persondata.

Afklar 'konstruktionen'

Det er vigtigt at afklare 'konstruktionen' omkring en databehandlingssituation. Det er nemlig vigtigt at finde ud af præcis *om der reelt behandles persondata, hvem der har ansvaret, hvem der skal udføre behandlingen osv*. Disse forhold gennemgås i de følgende underafsnit.

3.1 Behandles der persondata?

Nogle gange ser vi databehandleraftaler på områder, hvor der behandles anonymiseret data. Det giver ikke juridisk mening, at have databehandleraftaler, når der ikke behandles persondata. En databehandleraftale forudsætter at der selvfølgelig behandles persondata. Nogle gange står DMJX (og dermed ledere eller medarbejdere) i det valg, at det godt kan reducere behandlingen af persondata til kun at være behandling af (ikke-personhenførbart/anonymiseret) data. I så fald, så finder de persondataretlige regler ikke anvendelse.

3.2 Hvem er dataansvarlig?

En dataansvarlig er man, når man *fastsætter formål og hjælpemidlerne til behandling af persondata* (jf. GDPR artikel 4, nr. 7). Databehandler er man, når man *behandler data på den dataansvarliges vegne* (jf. GDPR artikel 4, nr. 8). Det ses ofte, at man anvender disse to begreber forkert – og forkerte anvendelser har store følgevirkninger. Derfor er det vigtigt, at få kategoriseret relationerne korrekt.

DMJX er som oftest (og som hovedregel) den juridiske enhed, der er dataansvarlig for de persondata, der behandles i DMJX-regi. Men i nogle situationer behandler DMJX persondata på andres vegne – og optræder dermed som 'databehandler' i forhold til disse. Dette kan fx være aktuelt når DMJX udfører evalueringer for andre organiationer eller virksomeheder.

Bemærk, begreberne "dataansvarlig" og "databehandler" er juridiske begreber – og ikke må forstås rent sprogligt. Det juriske begreb "databehandler" kunne, hvis man kun forstår det sprogligt, virke som om at det udtryk for "den, der behandler persondata". Dette er ikke juridisk korrekt. Behandling af persondata kan både foretages af den dataansvarlige (dvs. personer hos den dataansvarlige) eller hos en databehandler (dvs. personer hos databehandleren).

Som ansat i DMJX er du altså ikke "databehandler" (som juridisk begreb) fordi du *behandler* persondata.

Som ansat i DMJX er du (for det arbejde du udfører for DMJX) "en del af den datasvarlige/databehandleren". Det betyder, at går der noget galt med persondata i dit arbejde ved DMJX, så er DMJX – og ikke dig – dataansvarlig herfor. Skulle det ske, at der kommer påtaler, kritik eller bøder for håndteringen af persondata, så er det altså DMJX, som juridisk person disse bliver givet til.

Særligt om fælles dataansvar

Det er også en mulighed at flere dataansvarlige går sammen om et dataansvar. "Hvis to eller flere dataansvarlige i fællesskab fastlægger formålene med og hjælpemidlerne til behandling, er de fælles dataansvarlige.", jf. GDPR artikel 26, stk. 1, 1. punktum. I så fald skal der indgås en aftale om

fælles dataansvar. I dette tilfælde skal Datatilsynets skabelon til aftale om fælles dataansvar bruges. I så fald skal du inddrage DPO eller GDPR-konsulenten.

3.3 Hvem er ”databehandler”?

En databehandler er typisk en virksomhed, som leverer en tjenesteydelse for en anden (dataansvarlig) virksomhed – og denne tjenesteydelse omhandler behandling af persondata.

I nogle situationer kan der opstå tvivl om hvorvidt den leverende virksomhed reelt er ”databehandler” i juridiske forstand. Nogle gange er den persondatabehandling, der foregår hos den leverende virksomhed så begrænset, at man juridisk ikke anser den leverende virksomhed som ”databehandler”, men selvstændigt dataansvarlig. Det gør ’konstruktionen’ markant lettere.

Eksempelvis er tømrerfirmaer, rengøringsfirmaer, el-installationsfirmaer ikke databehandlere fordi de alene har kontaktoplysninger og navne på nogen, de skal levere noget til. At behandle personoplysninger er slet ikke deres kerneopgave – og derfor er de ikke databehandlere for nogen – men tømrervirksomheden er selvstændigt dataansvarlige for de kontaktoplysninger de håndterer.

Omvendt er leverandører af it-løsninger databehandler overfor DMJX, når der i systemet behandles persondata. I sådanne tilfælde skal der indgås en databehandleraftale.

Særligt om ’ikke-databehandlere”

I nogle situationer er det ikke nødvendigt med en databehandleraftale selvom man eksempelvis viser persondata til en udenforstående. Dette kunne fx være en DMJX-forsker, der får besøg af en forsker fra et universitet – og den forbindelse vil have noget sparring på dataanalysen. Her er formålet at vise dataanalysen – og som noget sekundært kan universitetskollegaen se pseudonymer på personerne. Dette kan fint klares med en kort fortrolighedsaftale. Se afsnit 5 om fortrolighedserklæringer.

3.4 Er du i tvivl om konstruktionen?

Søg gerne rådgivning hos DMJX’s GDPR team på dpo@dmjx.dk, hvis du er i tvivl om noget af ovenstående. Eftersom forholdene ofte er komplekse, så kan et telefonmøde eller møde ofte være den nemmeste og hurtigste måde at få afklaret det hele på.

4. Betingelser, der skal opfyldes vedr. databehandleraftalen

Der er en række formelle betingelser, der skal opfyldes for korrekt håndtering af databehandleraftaler i DMJX

1. Databehandleraftalen skal være skriftlig og bør så vidt muligt tage udgangspunkt i datatilsynets standard-databehandleraftaleskabelon.
2. Indgåelsen af databehandleraftalen følger det sædvanlige ledelseshierarki, men databehandleraftalen skal forud for indgåelsen til anmærkningsfri gennemgang hos DPO’en eller GDPR-konsulenten.

3. Den indgåede databehandleraftale skal journaliseres
4. Der skal føres kontrol på databehandleraftalen

Disse er uddybet i det følgende.

4.1 Databehandleraftalen skal være skriftlig

I de fleste tilfælde bør Datatilsynets standard-skabelon anvendes. Den findes både på dansk og engelsk. Se www.datailsynet.dk > Generelt om databeskyttelse > Vejledninger > Skabeloner.

Anvendelse af Datatilsynets skabelon har den fordel, at vi er sikker på at databehandleraftalen kommer omkring de krav, som GDPR artikel 28 foreskriver – og desuden har databehandleraftalen den fordel, at den er kendt af mange andre samt at Datatilsynet ikke vil have behov for nærlæsning i tilfælde af et kontrolbesøg.

Vær særligt opmærksom på følgende forhold i Datatilsynets skabelon:

- Vedr. punkt 10.2: Det er vigtigt, at databehandleren giver DMJX besked senest efter 36 timer at databehandleren er blevet bekendt med bruddet på persondatasikkerheden – ellers så kan DMJX ikke nå at indrapportere det indenfor de 72 timer (fra det tidspunkt hvor databehandleren fik kendskab til bruddet på persondatasikkerheden).
- Det er i bilagene, at der er meget vigtige forhold, der skal reguleres (udfyldes). Bilag A er næsten identisk med din fortegnelse.

4.2 Databehandleraftalen indgås lokalt, men skal til forudgående gennemtjek hos DPO'en eller GDPR-konsulenten

Databehandleraftaler indgås det relevante sted i ledelseshierarkiet. Men forud for at databehandleraftalen indgås, så er det et institutionelt krav, at databehandleraftalen skal den igennem rådgivning hos DPO'en eller GDPR-konsulenten forud for indgåelsen.

4.3 Databehandleraftalen skal journaliseres i GDPR-sagsstrukturen

Den indgåede databehandleraftale skal journaliseres

4.4 Kontrollen skal foregå lokalt

De databehandleraftaler, der indgås skal også kontrolleres samme sted, som de er indgået. En dataansvarlig (i dette tilfælde DMJX) skal føre kontrol baseret på den risikovurdering, der foreligger.

5. Fortrolighedserklæringer

Vurderer du at der kan anvendes en fortrolighedserklæring, så skal følgende betingelser opfyldes:

1. Persondata skal være sekundær/perifer
2. Få grønt lys til brug af fortrolighedserklæringen af enten DPO eller GDPR-konsulenten
3. Brug DMJX-skabelonen ”Skabelon til fortrolighedserklæringer”.
4. De udfyldte fortrolighedserklæringer skal journaliseres
5. Særligt vedr. forsknings- og udviklingsprojekter

6. Supplerende materiale

Datatilsynet vejledning om dataansvarlige og databehandlere: se www.datatilsynet.dk > Generelt om databeskyttelse > Vejledninger > Dataansvarlige og databehandlere

Datatilsynet vejledning om dataansvarlige og databehandlere: se www.datatilsynet.dk > Generelt om databeskyttelse > Vejledninger > Skabelon om fælles dataansvar.