Tjekliste til databehandleraftaler

Professionshøjskolen Absalon
30. januar 2019, ver 02

Skal der laves en databehandleraftale

For at man kan bestemme om der skal laves en databehandleraftale eller ej, skal det afklares om der er en dataansvarlig og en databehandler. Hver rolle har forskellige pligter og de to skal samarbejde om at sikre behandlingen af personoplysningerne.

Databeskyttelsesforordningen definerer "den dataansvarlige" som 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.

Det afgørende i afklaringen af hvem der er dataansvarlig er, hvem der faktisk afgør, hvordan oplysningerne skal behandles.

En databehandler defineres som en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på vegne af en dataansvarlig.

- En dataansvarlig kan fx være en offentlig myndighed, som er blevet pålagt en bestemt behandling af personoplysninger.
- En databehandler er kendetegnet ved at denne kun behandler personoplysningerne på vegne (efter instruks) fra en dataansvarlig. En databehandler behandler ikke personoplysningerne til egne formål og må i udgangspunktet ikke bruge oplysningerne, som databehandleren har fået overladt, til andet end at udføre opgaven for den dataansvarlige.

Hvis der skal laves en databehandleraftale

Hvis der skal laves en databehandleraftale med en ekstern leverandør, er der flere punkter du, hvor du skal være opmærksom på aftalens indhold. Der er nemlig flere emner i databehandleraftalen, hvor eksterne leverandører ofte ikke har styr på reglerne, eller har ønsker der ikke nødvendigvis er de samme som Absalons ønsker til indholdet.

Generelle ting der skal være i databehandleraftalen

- ☐ Henvisninger til lovgivning skal være til gældende lov, altså **databeskyttelsesforordningen** (*Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger*) eller **databeskyttelsesloven**, lov nr. 502 af 23/05/2018 (*Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven*).
- ☐ Henvisning til ikke længere gældende lov, skal fjernes.

- [ ] **Genstanden** for behandlingen (dvs. hvad er det, systemet eller den eksterne leverandør skal hjælpe med.)
- [ ] Typer af **personoplysninger** og kategorier af **registrerede** skal fremgå.
- [ ] **Formålet** med behandlingen og behandlingens karakter skal fremgå.
- [ ] **Varigheden** af aftalen (dvs. hvor længe den eksterne part forventes at skulle bistå. Det kan fx være et bestemt antal måneder eller år, eller det kan være "indtil videre", "indtil aftalen opsiges" osv.)

Databehandlerens forpligtelser

- [ ] Der skal være et punkt, hvoraf det fremgår, at databehandleren og enhver person, der arbejder på vegne af databehandleren, må **kun behandle personoplysninger efter dokumenterede instrukser** fra den dataansvarlige.
- [ ] Det skal fremgå at kun de medarbejdere der har behov for at tilgå oplysningerne, må tilgå oplysningerne, samt at disse skal være underlagt fortrolighed.
- [ ] Det er ikke tilladt for databehandlere at overføre personoplysninger til lokationer uden for EU, uden Absalons godkendelse.
- [ ] Databehandleren skal være forpligtiget til omgående at **underrette den dataansvarlige**, hvis en instruks efter databehandlerens mening er i strid med forordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret
- [ ] Ved databrud skal der meget gerne stå at databehandleren skal underrette den dataansvarlige uden unødig forsinkelse – hvis der sættes en timefrist skal denne ikke overskride 24 timer.
- [ ] Det skal fremgå, at databehandleren skal bistå den dataansvarlige, med opfyldelse af forpligtelser til at besvare anmodninger om udøvelse af de **registreredes rettigheder**: Indsigt, berigtigelse, sletning, begrænsning af behandling, dataportabilitet, indsigelse.
- [ ] Det skal være tydeligt at databehandleraftalen er gældende så længe databehandleren behandler den dataansvarliges personoplysninger, uanset om hovedaftalen er ophørt.
- [ ] Det skal fremgå at alle personoplysninger skal tilbageleveres eller slettes efter aftalens ophør.
- [ ] Af aftalen skal det fremgå, af databehandleren, at alle personoplysninger skal tilbageleveres og derefter slettes eller anonymiseres når hovedaftalen ophører.

Databehandlerens udgifter

- [ ] Eventuelle omkostninger ved henvendelser fra de registrerede er en del af den samlede pris, det er ikke acceptabelt, hvis databehandleren vil have dækket omkostningerne ad hoc.
- [ ] Eventuelle omkostninger ved databrud er en del af den samlede pris, det er ikke acceptabelt, hvis databehandleren vil have dækket omkostningerne ad hoc.
- [ ] Absalon vil ikke acceptere at en databehandler forsøger at begrænse eller fordele erstatningsansvaret og fordeling af bøder i aftalen, dette må reguleres af datatilsynet og domstolene.

Sikkerhed

Sikkerhedsniveauet skal bestemmes i samarbejde med den system eller processansvarlige hos Absalon, og afhænger af typen af oplysninger og behandlingens karakter. Absalon har dog nogle mindstekrav til sikkerheden hos databehandlere, som er beskrevet nedenfor.

- ☐ Databehandleren skal **implementere passende tekniske og organisatoriske foranstaltninger** for at beskytte personoplysningerne. Det skal fremgå, hvordan det gøres i praksis.
- ☐ **Adgangskontroller og -begrænsninger** skal være beskrevet.
- ☐ Vær fx opmærksom på, at **kommunikation** af følsomme og fortrolige personoplysninger skal ske over sikre forbindelser (fx ved beskyttes med kryptering).
- ☐ Databehandleren skal sørge for **løbende sikkerhedskopiering** af personoplysningerne. Kopierne skal opbevares adskilt og forsvarligt og på en måde som sikrer mulighed for at oplysningerne kan genskabes.

Underdatabehandlere

- ☐ Der skal være en liste over godkendte underdatabehandlere.
- ☐ Hvis der skal flere/nye underdatabehandlere på listen, skal disse godkendes af Absalon.
- ☐ Ved brug af underdatabehandlere skal der være indgået en underdatabehandleraftale med disse, og denne aftale skal sikre, at underdatabehandleren pålægges de samme databeskyttelsesforpligtelser og kontraktlige betingelser, som dem der er fastsat i denne aftale mellem den dataansvarlige og databehandleren
- ☐ Hvis der bruges underdatabehandlere uden for EU skal der foreligge en EC SCC aftale med disse.

Tilsyn

- ☐ Databehandleren skal stille alle de **oplysninger til rådighed** for den dataansvarlige, der er nødvendige for at påvise overholdelse af lovgivningsmæssige krav.
- ☐ Absalon skal selv kunne føre tilsyn/audit, det er ikke acceptabelt, hvis det kun er tredjeparter der kan lave tilsynet.
- ☐ Der skal ikke være udgifter for Absalon forbundet med et tilsyn/audits.
- ☐ Det er en fordel, hvis de arbejder med revisorerklæringer.
- ☐ Eventuelle udgifter til en revisorerklæring skal afholdes af databehandleren og ikke af Absalon.