Hvad er baggrunden for Datatilsynets standard-databehandleraftale, og hvordan skal du læse den?

Baggrunden for Datatilsynets standard-databehandleraftale

Det er Datatilsynets erfaring, at en del dataansvarlige og databehandlere har svært ved at finde ud af, hvornår man er henholdsvis dataansvarlig og databehandler, ligesom en del dataansvarlige og databehandlere har nogle udfordringer i forhold til at få indgået en databehandleraftale, der lever op databeskyttelsesforordningens minimumskrav, når man er kommet frem til, at der er tale om en databehandlerkonstruktion.

For at afhjælpe ovennævnte udfordringer har Datatilsynet i november – sammen med Justitsministeriet – offentliggjort en vejledning om dataansvarlige og databehandlere, der kan hjælpe de private virksomheder, offentlige myndigheder, fysiske personer, institutioner og andre organer, som skal vurdere, om de handler som dataansvarlig eller databehandler, når de behandler oplysninger om andre personer. Vejledningen kan ses her:

https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_om_dataansvarlige_og_databehandlere_-_endelig_version.pdf

Samtidig med offentliggørelsen af ovennævnte vejledning meddelte Datatilsynet, at tilsynet primo 2018 ville offentliggøre en standard-databehandleraftale.

Datatilsynets standard-databehandleraftale er tænkt som en hjælp til dataansvarlige og databehandlere, der skal efterleve databeskyttelsesforordningens krav om at indgå en skriftlig databehandleraftale.

Det er dog vigtigt at være opmærksom på, at standard-databehandleraftalen alene er Datatilsynets bud på, hvordan en databehandleraftale kan se ud, hvis den skal leve op til databeskyttelsesforordningens minimumskrav. Der er således ikke noget til hinder for, at man benytter en anden databehandleraftale, hvis denne også lever op til databeskyttelsesforordningens minimumskrav.

Vælger man at udarbejde en anden databehandleraftale, kan man eventuelt benytte Datatilsynets standard-databehandleraftale som en tjekliste i forhold til, om man har fået skrevet noget om alle minimumskravene i sin aftale.

Hvordan skal du læse Datatilsynets standard-databehandleraftale?

Ved Datatilsynets udarbejdelse af standard-databehandleraftalen er der – som nævnt – taget udgangspunkt i, at aftalens indhold skal leve op til de minimumskrav, som fremgår af databeskyttelsesforordningens artikel 28, stk. 3.

Det har herudover været vigtigt for tilsynet at udforme en aftale, som er praktisk anvendelig og skaber mest mulig klarhed over parternes forskellige ansvar og rolle i databehandlingen – og derigennem en bedre beskyttelse af de registrerede. Datatilsynet har således også indhentet input til standard-databehandleraftalen fra en række eksterne parter, der er vant til at arbejde med databehandleraftaler i det daglige.

Standard-databehandleraftalen er opdelt i to dele;

- **En generel del** (side 1-11), som det - udover at indsætte navnene på parterne og hovedaftalen - ikke er nødvendigt at tilrette fra aftaleforhold til aftaleforhold. Den generelle del vil derfor fungere som den dataansvarliges standardtekst.

- **En specifik del/bilagene** (side 12-20), som udfyldes særskilt fra aftaleforhold til aftaleholdhold. Denne del af aftalen vil bl.a. skulle indeholde de nærmere oplysninger om behandlingen, den aftalte behandlingssikkerhed, den dataansvarliges godkendelse af eventuelle underdatabehandlere og procedurer for tilsynet med databehandleren og eventuelle underdatabehandlere. Den specifikke del kan herudover omfatte parternes særlige aftaleretlige regulering af forholdet, herunder f.eks. aftaler om regres mellem parterne mv.

Når teksten i standard-databehandleraftalen er markeret med **fed**, indikerer dette, at teksten – efter Datatilsynets opfattelse – er afgørende for databehandleraftalens gyldighed (minimumskrav) og derfor ikke kan slettes, medmindre teksten erstattes af anden tekst med tilsvarende meningsindhold. I aftalen er felterne markeret med gul overstregning, når det er nødvendigt for aftalens gyldighed, at disse udfyldes. Det skal dog bemærkes, at de afsnit, der ikke er markeret med fed eller gul, vil være hensigtsmæssige at have med i sin aftale, idet de – efter Datatilsynets opfattelse – kan hjælpe til at dokumentere overholdelsen af andre bestemmelser i forordningen.

Minimumskrav til en databehandleraftale hvis du vælger selv at udarbejde en aftale

Som nævnt ovenfor kan en dataansvarlig og databehandler frit vælge at udarbejde deres egen databehandleraftale, når denne blot lever op til databeskyttelsesforordningens minimumskrav.

Efter databeskyttelsesforordningens artikel 28 er minimumskravene til en databehandleraftale følgende:

En databehandlers behandling af personoplysninger skal være reguleret af en kontrakt eller et andet retligt dokument i henhold til EU- retten eller medlemsstaternes nationale ret. Denne kontrakt skal være bindende for databehandleren med hensyn til den dataansvarlige, og kontrakten skal fastsætte genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger og kategorierne af registrerede samt den dataansvarliges forpligtelser og rettigheder.

Kontrakten eller det andet retlige dokument skal navnlig fastsætte, at databehandleren:

a) kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel af personoplysninger til et tredjeland eller en international organisation, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser

b) sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt

c) iværksætter alle foranstaltninger, som kræves i henhold til artikel 32

d) opfylder de betingelser, der er omhandlet i stk. 2 og 4, for at gøre brug af en anden databehandler

e) under hensyntagen til behandlingens karakter, så vidt muligt bistår den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder som fastlagt i kapitel III

f) bistår den dataansvarlige med at sikre overholdelse af forpligtelserne i medfør af artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren

g) efter den dataansvarliges valg sletter eller tilbageleverer alle personoplysninger til den dataansvarlige, efter at tjenesterne vedrørende behandling er ophørt, og sletter eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne

h) stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i denne artikel, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige. For så vidt angår første afsnit, litra h), underretter databehandleren omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

Overordnede krav til parterne i forbindelse med en databehandlerkonstruktion

I forbindelse med udarbejdelsen af ovennævnte vejledning om dataansvarlige og databehandlere og Datatilsynets standard-databehandleraftale er Datatilsynet endvidere blevet opmærksom på, at mange dataansvarlige og databehandlere har svært ved at overskue, hvilke overordnede krav der gælder for de respektive parter i forbindelse med anvendelsen af en databehandlerkonstruktion.

Nedenfor har Datatilsynet derfor oplistet de overordnede krav, der følger af databeskyttelsesforordningen.

Overordnede krav til en dataansvarlig i forbindelse med dennes brug af en databehandler

- Den dataansvarlige må kun benytte databehandlere, der kan stille de fornødne garantier for, at de vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

- Den dataansvarlige skal sørge for at indgå en databehandleraftale, som lever op til databeskyttelsesforordningens minimumskrav.

- Den dataansvarlige skal sørge for, at der foreligger en dokumenteret instruks, som databehandleren skal følge.

- Den dataansvarlige forbliver direkte ansvarlig for overholdelsen af databeskyttelsesforordningen, og for at kunne dokumentere overholdelsen. Hvis dette ikke er opfyldt, kan den dataansvarlige blive forpligtet til at betale erstatning eller administrative bøder, eller blive pålagt andre sanktioner.

Overordnede krav til en databehandler, som behandler oplysninger på vegne af en dataansvarlig

- Databehandleren må kun behandle personoplysningerne efter en dokumenteret instruks fra den dataansvarlige.

- Hvis databehandleren afgør formål og hjælpemidler med behandlingen (modsat kun at behandle personoplysninger efter instruks fra den dataansvarlige) vil denne kunne anses for at være dataansvarlig, og dermed blive underlagt de samme forpligtelser som den oprindelige dataansvarlige.

- Udover de kontraktuelle forpligtelser overfor den dataansvarlige er databehandleren efter databeskyttelsesforordningen direkte forpligtet til:

    - ikke at anvende en anden databehandler (underdatabehandler) uden forudgående godkendelse fra den dataansvarlige (artikel 28, stk. 2.);
    - at samarbejde med relevante tilsynsmyndigheder, for eksempel Datatilsynet (artikel 31);
    - at sikre den nødvendige behandlingssikkerhed (artikel 32);
    - at føre en fortegnelse over behandlingsaktiviteter (artikel 30, stk. 2.), medmindre databehandleren er fritaget fra kravet herom (30, stk. 5.);
    - at underrette den dataansvarlige uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden (artikel 33, stk. 2);
    - at udpege en databeskyttelsesrådgiver, såfremt databehandleren er omfattet af kravet herom (artikel 37);
    - at udpege en repræsentant i Unionen, hvis databehandleren ikke er etableret i Unionen og er omfattet af kravet herom (artikel 27).

- Hvis databehandleren ikke efterlever ovennævnte forpligtelser, eller behandler oplysninger udenfor eller modsat instruksen fra den dataansvarlige, kan databehandleren blive forpligtet til at betale erstatning eller administrative bøder, eller blive pålagt andre sanktioner.

- Hvis databehandleren bruger en anden databehandler (underdatabehandler), vil den oprindelige databehandler forblive fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.