Vejledning for leverandører

Vejledning til udfyldelse af DBS-skabelon til databehandleraftale

Alle overskrifter fra aftalen og bilag er taget med i denne vejledning for fuldstændighedens skyld. Der vil således være overskrifter, der ikke indeholder vejledningstekst.
I skabelonen til databehandleraftalen findes der følgende markeringer:

GUL – Angiver de obligatoriske felter, hvor der skal angives oplysninger, at der skal foretages et valg eller at der kan foretages en tilpasning af teksten.

Grøn – Viser at der er tale om et valgfrit element som kan anvendes, hvis dette findes relevant.

Tekst – Forslag til en standardtekst, som kan anvendes i forbindelse med udfyldelse af databehandleraftalen.

Opbygning af DBS-skabelonen

Skabelon er delt op på følgende måde:

- Aftaletekst
- Bilag A – Oplysninger om behandlingen
- Bilag B – Underdatabehandlere
- Bilag C – Instruks vedrørende behandlingen af personoplysninger
- Bilag D – Parternes regulering af andre forhold
- Bilag E – Databehandlerkæden

Aftalen

2. Præambel

Der skal indsættes et navn på den tjeneste, behandling eller det it-system, som behandlingen vedrører.
Herudover skal det angives hvor mange bilag, der bruges. Der er tilføjet et enkelt bilag i forhold til Datatilsynets standardkontraktbestemmelser, som giver mulighed for at angive databehandlerkæden. Denne mulighed er valgt, idet dette kan være et krav i forhold til brug af cloud-udbydere, jf. datatilsynets vejledning om cloud.

3. Den dataansvarliges rettigheder og forpligtelser

4. Databehandleren handler efter instruks

Datatilsynet opfordrer i deres standardskabelon til, at parterne forudser og overvejer konsekvenser, der kan følge af en potentiel ulovlig instruks, som den dataansvarlige har givet, og regulerer dette i en aftale mellem parterne. Det er valgt ikke at beskrive konsekvenserne yderligere, idet det vurderes, at en detailregulering ikke vil give parterne mulighed for at løse problemstillingen på den mest smidige måde. Informerer databehandleren den dataansvarlige om, at denne vurderer, at der foreligger en ulovlig instruks, skal den dataansvarlige selvfølgelig handle på denne information.

5. Fortrolighed

6. Behandlingssikkerhed

7. Anvendelse af underdatabehandlere

Pkt. 7.2.
Datatilsynet lægger op til, at der kan vælges mellem en forudgående specifik godkendelse af underdatabehandlere [valg 1] eller en forudgående generel godkendelse af underdatabehandlere [valg 2].

Hyppige skift af underdatabehandlere gør, at en forudgående generel godkendelse er lettere at administrere både for leverandører og kommuner, idet der ikke skal ske en godkendelse i alle tilfælde af skift af underdatabehandlere. Specifikke godkendelser af alle underdatabehandlere vil medføre en opgave i kommunerne med at få fremsendt de specifikke godkendelser. Hvis dette ikke sker rettidigt, så kan der opstå udfordringer hos leverandørerne med, at de ikke kan tage en ny underdatabehandler i brug, fordi en enkelt kommune ikke rettidigt har godkendt underdatabehandleren. Der kan være en risiko for afledte omkostninger for kommunerne i forbindelse med, at leverandøren skal have flere underleverandører til levere den samme ydelse.

Hvor der anvendes cloudløsninger, så kan det være særligt vanskeligt at håndtere de specifikke godkendelser, idet der kan ske mange og hyppige udskiftninger af underdatabehandlere.

Der er valgt at standardudfyldelse af pkt. 7.2. skal være en "forudgående generel skriftlig godkendelse".

Databehandleren vil være forpligtet til at pålægge sine databehandlere de samme krav, som er aftalt i denne databehandleraftale. Det vil derfor også fortsat være mulighed for at gøre indsigelse imod skiftet af underdatabehandler, hvis anvendelsen af den konkrete underdatabehandler findes problematisk.

Pkt. 7.3.
Der er valgt et varsel for underretning på mindst 30 dage inden anvendelse af den pågældende underdatabehandler. Det vurderes, at denne frist giver den dataansvarlige en mulighed for at gøre indsigelse mod sådanne ændringer jf. Databeskyttelsesforordningens art. 28, stk. 2. Et længere varsel giver i de fleste tilfælde ikke den dataansvarlige flere handlemuligheder, idet indsigelsesmuligheden gør det muligt at komme med saglige indvendinger imod anvendelse af en konkret underdatabehandler, hvilket vil afskære leverandøren fra at anvende den konkrete underdatabehandler.
Længere varsel i forhold til konkrete databehandlere kan angives i bilag B.

8. Overførsel til tredjelande eller internationale organisationer

I bilag D.1 er indsat bestemmelser om oplysning af databehandlerkæden og databehandlerens koncerndiagram med henblik på at kunne kontrollere muligheden for eventuelle overførsler til ikke sikre tredjelande. Dette er særligt et krav i forbindelse med anvendelse af cloudløsninger, jf. datatilsynets vejledning om cloud.

Databehandlerens beskrivelse af databehandlerkæden og koncerndiagram kan vælges vedlagt som bilag E.

I tilfælde af at der anvendes databehandlere eller underdatabehandlere i tredjelande, hvor man er afhængige af overførselsgrundlag, så bør man overveje en exitstrategi for, hvordan man kan flytte eller ophøre med behandlingen i tilfælde af, at overførselsgrundlaget ikke længere er tilstrækkeligt, eller at der opstår andre trusler mod behandlingssikkerheden, som gør, at behandlingen ikke kan fortsætte.

9. Bistand til den dataansvarlige

10. Underretning om brud på persondatasikkerheden

Pkt. 10.2.
Bestemmelsen i art. 33, stk. 2 har følgende ordlyd "Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden". Der er tale om en absolut regel, som databehandleren skal efterleve i alle tilfælde. I Datatilsynets standardskabelon anbefales det at fastsætte underretningsfristen i timer. Der er valgt en frist på 24 timer, idet det vurderes at denne frist giver både databehandleren og den dataansvarlige et tilstrækkeligt råderum.

Der skal kun ske underretning af den dataansvarlige indenfor denne frist. Der skal ikke nødvendigvis kunne gives en fuldstændig redegørelse for alle forhold omkring bruddet.

Fristen løber fra databehandleren er "blevet opmærksom på, at der er sket brud på person-datasikkerheden".

11. Sletning og returnering af oplysninger

Der kan her vælges mellem at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlige, at oplysningerne er slettet (valg 1) eller at tilbagelevere alle personoplysninger og slette eksisterende kopier (Valg 2).

Der er valgfrihed mellem de to muligheder for at give kommunerne mest fleksibilitet, og give mulighed for at vælge det, som giver mening i forhold til den enkelte behandling.

Pkt. 11.1.
I tilfælde af tilbagelevering, så bør det fremgå af hovedaftalen hvilket format, personoplysningerne skal tilbageleveres i.

Pkt. 11.2.
Der kan her indskrives krav i kontrakten om efterlevelse af arkivloven, samt at udlevering af data skal ske i standardformater for at kunne afleveres til arkiv.

12. Revision, herunder inspektion

Procedurerne for revision og tilsyn er nærmere beskrevet i bilag C.7 og C.8.

13 Parternes aftale om andre forhold

I bilag D er indsat en valgfri bestemmelse, som giver mulighed for at angive databehandlerkæden og databehandlerens koncerndiagram.

14 Ikrafttræden og ophør

15. Kontaktpersoner hos den dataansvarlige og databehandleren

I forhold til datatilsynets standardkontraktbestemmelser er der tilføjet mulighed for at indskrive kontakt hos den dataansvarlige ved sikkerhedsbrud.