BILAG 13: DATABEHANDLERAFTALE

Databehandleraftale
mellem
Aarhus Kommune, afdelingsnavn indsættes og
leverandørnavn indsættes

Det er jf. - kontrakt/driftsaftale/anden aftale + titel - aftalt, at - leverandørnavn indsættes - skal udføre følgende opgave for Aarhus Kommune: …….

Indledning
På denne baggrund indgås denne databehandleraftale mellem Aarhus Kommune som dataansvarlig og med - leverandørnavn indsættes – (herefter databehandleren) som databehandler for Aarhus Kommune, idet der jf. Persondatalovens § 42, stk. 2, skal indgås en skriftlig aftale, når Aarhus Kommune overlader en behandling af personoplysninger til en databehandler.

Der aftales herved følgende:

1. Efter instruks
Databehandleren handler alene efter instruks fra Aarhus Kommune i forbindelse med udførelse af de aftalte opgaver.

Oplysninger må ikke videregives til tredjepart eller behandles til andre formål, medmindre dette sker efter aftale med Aarhus Kommune.

2. Databeskyttelseslovgivning
Databehandleren overholder den til enhver tid gældende persondatalovgivning og herunder sikkerhedsbekendtgørelse nr. 528 af 15. juni 2000 og de sikkerhedsregler, der følger af sikkerhedsbekendtgørelsen.

2.1
Databehandleren sikrer herunder, at der er truffet de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med persondataloven eller Aarhus Kommunes IT-sikkerhedspolitik[1] (Bilag A) og herunder den offentlige standard for informationssikkerhed DS 484:2005 eller tilsvarende standard for informationssikkerhed.

Databehandleren skal ved tilbudsafgivelsen bekræfte at kunne leve op til kravene i bilag B[2]. Det skal fremhæves, at bilag B ikke er en udtømmende liste over sikkerhedskrav. Udfyldelsen af bilag B skal foretages af databehandleren og godkendes af Aarhus Kommune inden kontraktindgåelsen.

2.2
Hvis databehandleren er etableret i et andet land, skal databehandler sikre, at de ud over den danske lovgivning også lever op til dette lands databeskyttelseslovgivning.

[1] Bilag A – Aarhus Kommunes IT-sikkerhedspolitik
[2] Bilag B – Krav til databehandlere

Hvis det drejer sig om databehandling i et usikkert tredjeland[3], skal kommissionens standardkontrakt[4] indgås.

Hvis andre myndigheder fremlægger en kendelse om adgang til Aarhus Kommunes data, skal databehandler gøre indsigelse mod en kendelse og oplyse Aarhus Kommune herom.

2.3
Databehandleren skal levere en oversigt over datacentre og backup centre med præcis adresseangivelse af, hvor Aarhus Kommunes data behandles. Der sendes en ny oversigt til Aarhus Kommune ved ændringer. Der kan ikke uden forudgående aftale med Aarhus Kommune placeres data i et andet land.

2.4
Databehandleren er forpligtet til straks at give Aarhus Kommune (den kontraktansvarlige) meddelelse om driftsforstyrrelser, mistanke om brud på IT-sikkerhedsreglerne eller andre væsentlige uregelmæssigheder i forbindelse med udførelsen af opgaven.

3 Adgang til data

Ved adgang til sikrede lokaler i Aarhus Kommune, kan den enkelte kommunale afdeling udlevere et adgangskort med en personlig kode eller en nøgle mod kvittering.

Databehandleren har det ledelsesmæssige ansvar for, at databehandlerens medarbejdere overholder kommunens IT-sikkerhedsregler.

3.1
Databehandlerens medarbejdere må alene have adgang til data og/eller udføre jobs i det omfang, det er nødvendigt for udførelsen af arbejdet. Data må ikke lagres lokalt på medarbejderens udstyr.

Databehandlerens medarbejdere må ikke behandle fortrolige data uden for det aftalte driftsmiljø uden forudgående godkendelse af den pågældende afdeling[5]. Kvitteringsbilag C kan anvendes. Opbevaring af data skal ske under sikrede forhold, og sådan at der herunder alene er adgang for de involverede.

Databehandleren garanterer, at nødvendig kopiering og backup af data sker under fuldt betryggende forhold.

Efter endt brug skal udleveret datamateriale enten returneres tilstrækkeligt sikkert til Aarhus Kommune eller destrueres forsvarligt, så det ikke er muligt at genskabe dem. Eventuel destruktion skal aftales nærmere med den dataansvarlige i Aarhus Kommune.

3.2
Databehandlerens medarbejdere, som har behov for adgang til Aarhus Kommunes netværk skal forsynes med digital virksomhedssignatur (medarbejder NemID) af databehandleren. Medarbejderne skal være tilknyttet et sikkerhedsområde i Aarhus Kommunes IT-sikkerhedsorganisation.

[3] www.datatilsynet.dk – Under Erhverv, Tredjelande, Sikre tredjelande
[4] www.datatilsynet.dk – Under Erhverv, Tredjelande, Kommissionens standardkontrakt
[5] Bilag C - Kvitteringsbilag

Medarbejdere tildeles en brugerident samt en personlig og fortrolig adgangskode i h.t. gældende standarder i Aarhus Kommune. Bestilling af ny kode - ved glemt kode - skal så vidt muligt ske via Aarhus Kommunes IT-sikkerhedsorganisation.

4 Tavshedspligt

Databehandleren forpligter sig over for uvedkommende til at hemmeligholde alle oplysninger modtaget fra og om Aarhus Kommune, som databehandleren får kendskab til i forbindelse med udførelsen af arbejdet for Aarhus Kommune.

4.1

Databehandleren sikrer, at deres medarbejdere, der får adgang til oplysninger fra Aarhus Kommune har underskrevet en tavshedserklæring om, at de har tavshedspligt over for uvedkommende med hensyn til deres adgang til kunders/samarbejdspartneres data. Tavshedspligten er gældende såvel under ansættelsen som efter ansættelsens ophør.

Databehandler skal levere en kopi af disse erklæringer efter anmodning fra Aarhus Kommune.

4.2

Ved indgåelse af aftalen vedlægges et bilag D med en oversigt over de tilknyttede medarbejdere[6], der skal have adgang til Aarhus Kommunes lokaliteter/netværk. Leverandøren er forpligtet til at løbende at tilmelde nye medarbejdere og afmelde medarbejdere, der ikke længere har behov for adgang, til kontraktholder hos Aarhus Kommune.

5. Underdatabehandlere (underleverandører)

Hvis databehandleren anvender underdatabehandlere er det databehandlerens ansvar, at underdatabehandleren efterlever databehandleraftalen, idet aftalen også gælder for disse. Databehandleren skal informere Aarhus Kommune om evt. underdatabehandlere samt sikre, at også deres underdatabehandleres medarbejdere har underskrevet en tavshedserklæring.
Efter anmodning fra Aarhus Kommune skal databehandler levere en kopi af underdatabehandleraftalen.

6 Tilsyn

Aarhus Kommune fører tilsyn med, at databehandleren har truffet de fornødne sikkerhedsforanstaltninger. Dette kan ske ved et besøg hos databehandleren og/eller hos evt. underdatabehandlere. Aarhus Kommune kan også lade andre (f.eks. revisor) gennemføre tilsyn.

Aarhus Kommune er til enhver tid berettiget til at gennemføre yderligere kontrolforanstaltninger, herunder at begrænse databehandlers adgangsmuligheder til Aarhus Kommunes netværk og data.

Databehandleren skal på Aarhus Kommunes anmodning, give Aarhus Kommune tilstrækkelige oplysninger til, at denne kan påse, at de krævede tekniske og organisatoriske sikkerhedsforanstaltninger er truffet.

6.1

Hvis det fremgår af kontrakten, skal der ved underskrift af databehandleraftalen leveres den seneste revisorerklæring, og herunder evt. baggrundsmateriale til erklæringen. Herefter leveres en årlig revisorerklæring, der

[6] Bilag D – Oversigt over tilknyttede medarbejdere

er udarbejdet i overensstemmelse med de gældende branchestandarder på området (f.eks. ISAE 3000 vedrørende overholdelse af persondataloven). Dette gælder også for evt. underdatabehandlere.

7. Øvrige forhold

Hvis Aarhus Kommune oplyser, at der foretages videoovervågning i de lokaliteter, hvor databehandlerens medarbejdere færdes hos Aarhus Kommune, skal databehandleren sikre, at deres medarbejdere samt underdatabehandleres medarbejdere gøres bekendt med dette.

Databehandleren skal endvidere informere de pågældende medarbejdere om, at der sker registrering (logning) af alle anvendelser af fortrolige personoplysninger samt registrering af afviste adgangsforsøg i kommunens IT-systemer. De pågældende medarbejdere skal herunder gøres bekendt med, at der foretages kontrol med alle anvendelser af systemer med fortrolige personoplysninger. Loggen gemmes i 6 måneder, hvorefter den slettes.

8. Overtrædelse af databehandleraftalen

Parternes erstatningspligt efter dansk rets almindelige regler skal være reguleret i kontrakten.

9. Databehandleraftalens ophør

Aftalen kan genforhandles, hvis der sker ændring af det i punkt 2 anførte juridiske grundlag for aftalen.

9.1

Databehandleraftalen træder ud af funktion, når det samarbejde, der er en forudsætning for aftalen, ikke længere er gældende.

9.2

Tavshedspligten for databehandleren/underdatabehandlere og deres medarbejdere ophører ikke, selv om databehandleraftalen træder ud af kraft.

9.3.

Databehandleren må kun behandle personoplysninger, som Aarhus Kommune er ansvarlig for, så længe det er nødvendigt for udførelse af den aftalte opgave.

9.4.

Ved ophør skal det aftales med Aarhus Kommune, at data skal leveres tilbage til Aarhus Kommune eller der skal ske uoprettelig sletning punkt 3.1.

For leverandørnavn indsættes	Aarhus Kommune,
Dato: / - 201_	Dato: / - 201_

_____	_____
(Underskrift)	(Underskrift)

Bilagsoversigt:
Bilag 13A – Aarhus Kommunes IT-sikkerhedspolitik
Bilag 13B – Krav til databehandlere
Bilag 13C – Kvitteringsbilag
Bilag 13D – Oversigt over tilknyttede medarbejdere