

Journalnummer.: X-X-XX-XX-XX

DATABEHANDLERAFTALE

Vedrørende **projekt navn/titel/system/beskrivelse**



Dato XX-XX-20XX

Sagsbehandlerens navn

Tel. +45 XXXX XXXX

e-mail@e-mail.dk

For at sikre overholdelsen af de til enhver tid gældende regler om behandling af personoplysninger, herunder særligt persondataloven¹ og dertil hørende bekendtgørelser og vejledninger, har

Region

Adresse

Afdeling

CVR-nr.

(herefter den "*Dataansvarlige*")

og

Firmanavn

Adresse

Evt. underafdeling

Kontaktperson

CVR-nr.

(herefter "*Databehandleren*")

indgået nærværende databehandleraftale (herefter "*Databehandleraftalen*") som en del af aftalegrundlag af xx. xxxxxx 201x om leverance af... /samarbejde vedrørende... (herefter "*Hovedaftalen*")

hvor data fysisk behandles på følgende adresse(r), lokale(r), placering af server(e)

¹ Lov nr. 429 af 31.maj 2000 om behandling af personoplysninger med senere ændringer § 42, stk. 2 jf. § 41.

1. Databehandlerens ansvar

Databehandleren handler alene efter instruks fra den Dataansvarlige og alene i det omfang, det er nødvendigt for, at Databehandleren kan opfylde sine forpligtelser i henhold til Databehandleraftalen. Databehandleraftalen er således en del af den Dataansvarliges instruks til Databehandleren.

Databehandleren forpligter sig til, til enhver tid at overholde den danske såvel som Databehandlerens nationale lovgivningsmæssige krav vedrørende databehandling og datasikkerhed samt den Dataansvarliges informationssikkerhedspolitik med tilhørende retningslinjer i forbindelse med den databehandling, som udføres for den Dataansvarlige.

2. Databehandlerens opgave

Formålet med databehandlingen er...

Databehandlerens opgave er at hoste/supportere/drifte systemet etc... - klar beskrivelse og afgrænsning af den databehandling, der skal leveres.

Databehandlingen vil omfatte følgende kategorier af registrerede personer...

Databehandlingen vil omfatte følgende kategorier af data...

Uddybning af instruks til Databehandler - evt. henvisning til hovedkontrakt

3. Tekniske og organisatoriske sikkerhedsforanstaltninger

Databehandleren skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hædeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Databehandleren forpligter sig til at overholde de til enhver tid gældende lovgivningsmæssige krav vedrørende behandling af personoplysninger. Databehandlingen skal derfor foregå i overensstemmelse med de til enhver tid gældende regler om behandling af personoplysninger, herunder særligt persondataloven og dertil hørende bekendtgørelser² og vejledninger.

Databehandler behandler oplysninger på den Dataansvarliges vegne og handler alene efter instruks fra den Dataansvarlige jf. bilag 1. Af instruksen fremgår minimumskrav til de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger.

Databehandleren forpligter sig endvidere til at behandle personoplysningerne i overensstemmelse med den informationssikkerhedspolitik som den Dataansvarlige er underlagt jf. bilag 2.

Principperne og anbefalingerne i ISO 27001 med senere ændringer vil således på alle relevante områder skulle efterleves som ramme, i det omfang andet ikke fremgår af nærværende databehandleraftale.

² Se f.eks. Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, der behandles for den offentlige forvaltning med senere ændringer.

4. Databehandlers brug af Underdatabehandler

Databehandleren må ikke indgå aftaler med en Underdatabehandler om behandling af personoplysninger omfattet af denne databehandleraftale, med mindre den Dataansvarlige skriftligt har givet samtykke til aftaleindgåelsen. Den Dataansvarlige er berettiget til at stille vilkår for et sådant samtykke.

Databehandleren må endvidere ikke overføre eller tillade overførsel af personoplysninger til lande uden for EU og det Europæiske Økonomiske Samarbejdsområde uden den Dataansvarliges forudgående skriftlige samtykke.

Såfremt den Dataansvarlige har givet tilladelse til en overførsel af personoplysninger til lande uden for EU og det Europæiske Økonomiske Samarbejdsområde, påhviler det Databehandleren at sikre, at data ikke overføres, før der foreligger et lovligt kontraktgrundlag for overførsel af personoplysninger til de pågældende lande herunder en direkte databehandleraftale mellem den Dataansvarlige og eventuelle Underdatabehandlere beliggende i tredjelande.

Databehandleren skal i sin aftale med Underdatabehandleren sikre sig, at Underdatabehandleren som minimum kan opfylde de forpligtelser, som Databehandleren har påtaget sig ved denne databehandleraftale, for så vidt angår den behandling af personoplysninger, der varetages af Underdatabehandleren.

Databehandleren indestår for kontraktmæssigheden og lovligheden af Underdatabehandlerens behandling af personoplysninger. Det forhold, at Databehandler indgår aftale med en Underdatabehandler, fritager ikke Databehandleren for pligten til at efterleve nærværende Databehandleraftale.

Ved ophør af en aftale med en Underdatabehandler om behandling af personoplysninger omfattet af denne Databehandleraftale, skal Databehandleren give den Dataansvarlige meddelelse herom. Databehandleren skal i den forbindelse sikre, at Underdatabehandleren sletter data behørigt i overensstemmelse med punkt 9.

Såfremt Databehandleren anvender Underdatabehandler, skal oplysninger om denne fremgå af punkt 15.

5. Ad hoc arbejdspladser

I det omfang, databehandlingen sker fra ad hoc arbejdspladser (fjernarbejdspladser eller hjemmearbejdspladser) skal dette beskrives i punkt 15.

Såfremt Databehandleren foretager databehandling fra ad hoc arbejdspladser, skal Databehandleren sikre, at disse lever op til de sikkerhedsmæssige krav i denne Databehandleraftale med bilag samt Datatilsynets IT-sikkerhedstekster herom.

Databehandleren skal blandt andet opfylde og dokumentere følgende:

- Beskrivelse af anvendt krypteret forbindelse mellem ad hoc arbejdspladsen og Databehandlerens/Dataansvarliges netværk
- Anvendelse af 2-faktor-autentifikation

- Databehandlers interne instruks til egne medarbejdere vedrørende ad hoc arbejdspladser

6. Tilsynsmyndigheder, audits og revisionserklæringer

Databehandleren skal på den Dataansvarliges anmodning give den Dataansvarlige tilstrækkelige oplysninger til at denne kan påse, at de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger m.v. er truffet. Endvidere skal Databehandleren kunne dokumentere, at identificerede sårbarheder bliver imødegået ud fra en risikobaseret vurdering.

I tilfælde af, at den Dataansvarlige og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en fysisk inspektion (audit) af de foranstaltninger, som Databehandler foretager i medfør af Databehandleraftalen, forpligter Databehandleren sig til - med et rimeligt varsel - at stille tid og ressourcer til rådighed herfor. Databehandleren forpligter sig på samme måde til at sikre, at sådanne audits også kan gennemføres hos dennes Underdatabehandlere.

Som supplement eller alternativ til de ovenfor nævnte audits kan der indgås aftale om, at Databehandler og eventuelle Underdatabehandlere for egen regning sørger for, at en uafhængig ekspert årligt udarbejder en revisionserklæring på grundlag af en anerkendt standard angående Databehandlerens overholdelse af kravene til sikkerhedsforanstaltninger fastsat i Databehandleraftalen. Erklæringen skal være formuleret konkret i forhold til den opgave, som Databehandleren løser for den Dataansvarlige. En aftale herom kan fremgå af punkt 15.

7. Underretningspligt og assistance

Databehandleren forpligter sig til straks og skriftligt at orientere den Dataansvarlige om enhver afvigelse fra kravene i databehandleraftalen, f.eks.:

- ved enhver fravigelse fra givne instrukser
- ved enhver afvigelse fra det aftalte om tilgængelighed
- ved planlagte releases, opgraderinger, tests mv.
- ved enhver mistanke om brud på fortroligheden
- ved enhver mistanke om misbrug, fortabelse og forringelse af data
- ved enhver hændelig eller uautoriseret videregivelse af eller adgang til personoplysningerne behandlet efter denne databehandleraftale

Databehandleren og dennes eventuelle Underdatabehandlere skal straks assistere den Dataansvarlige med håndteringen af enhver henvendelse fra en registreret, herunder anmodning om indsigt, berigtigelse, blokering eller sletning, hvis de relevante personoplysninger behandles af Databehandleren.

Databehandleren og dennes eventuelle Underdatabehandlere skal assistere den Dataansvarlige med at overholde øvrige forpligtelser, der måtte påhvile den Dataansvarlige efter gældende ret, hvor assistance er forudsat, samt hvor assistance er nødvendig for, at den Dataansvarlige kan overholde sine forpligtelser.

8. Aftalens ikrafttræden og varighed

Databehandleraftalen træder i kraft samtidig med indgåelsen af Hovedaftalen som anført på side 1.

Databehandleraftalen ophører, når al behandling af personoplysninger i henhold til Hovedaftalen er ophørt og Databehandleren har slettet data, jf. punkt 9.

9. Håndtering af data efter aftalens ophør

Databehandleren og dennes eventuelle Underdatabehandlere forpligter sig til at tilbagelevere og/eller slette personoplysninger, når databehandlingen i henhold til aftale med den Dataansvarlige ophører. Den Dataansvarlige skal oplyse Databehandleren om det tidspunkt, hvor databehandlingen skal ophøre. Det påhviler herefter Databehandleren at tilbagelevere og/eller slette personoplysningerne på det oplyste tidspunkt.

Sletning må ikke ske, før den Dataansvarlige skriftligt har godkendt den påtænkte fremgangsmåde for sletning.

Såfremt den Dataansvarlige ikke finder metoden tilstrækkelig sikker og i overensstemmelse med gældende regler om behandling af personoplysninger, skal den Dataansvarlige meddele Databehandleren hvilken metode, der kan anvendes i stedet. Der henvises til Datatilsynets it-sikkerhedstekst ST3 fra 2014 med eventuelle opdateringer.

Når sletningen er foretaget, skal Databehandleren fremsende en skriftlig erklæring på, at data er slettet som aftalt, inklusiv en beskrivelse af den anvendte metode.

Såfremt Databehandler eller dennes Underdatabehandlere i forbindelse med konkurs el.lign. ophører med at behandle personoplysninger for den Dataansvarlige, skal alle personoplysningerne straks leveres tilbage til den Dataansvarlige på en måde, der gør det muligt for den Dataansvarlige at anvende disse fremadrettet. Herefter er Databehandler, dennes konkursbo el.lign. forpligtet til effektivt at slette oplysningerne fra egne systemer i overensstemmelse med ovenstående.

10. Tavshedspligt og fortrolighed

Databehandlerens ansatte, samarbejdspartnere, eksterne konsulenter og vikarer mfl. vil i forbindelse med behandlingen af fortrolige oplysninger være omfattet af de regler om tavshedspligt, som gælder for ansatte i den offentlige forvaltning. Der henvises til forvaltningslovens § 27 og straffelovens §§ 152-152 f.

Det påhviler Databehandler og dennes Underdatabehandlere at informere egne ansatte, samarbejdspartnere, eksterne konsulenter og vikarer mfl. om udstrækningen af tavshedspligten og om konsekvenserne ved en eventuel overtrædelse.

Databehandleren skal holde personoplysningerne fortrolige, og er således alene berettiget til at anvende personoplysningerne som led i opfyldelsen af sine forpligtelser i henhold til denne databehandleraftale og instruks.

Databehandleren påtager sig endvidere at begrænse adgangen til personoplysningerne til de medarbejdere, for hvem det er nødvendigt at behandle personoplysninger for at kunne opfylde Databehandlerens forpligtelser over for den Dataansvarlige.

Databehandlerens forpligtelser om tavshedspligt og fortrolighed gælder også efter aftalens ophør.

11. Overdragelse

Databehandleren må ikke overdrage sine rettigheder og forpligtelser i henhold til denne databehandleraftale uden den Dataansvarliges forudgående samtykke.

12. Misligholdelse

Det betragtes som væsentlig misligholdelse af Hovedaftalen som anført på side 1, såfremt Databehandler ikke overholder forpligtelserne i Databehandleraftalen, de til enhver tid gældende lovgivningsmæssige krav og kravene i de dokumenter, der fremgår af Databehandleraftalens bilag. Den Dataansvarlige er i så fald berettiget til uden varsel at opsige samtlige gældende aftaler om databehandling, som udføres for denne.

Uanset ophævelse/opsigelse af aftalen er Databehandleren dog forpligtet til at levere databehandling i henhold til Hovedaftalen og denne Databehandleraftale indtil databehandling er sikret hos anden databehandler.

Databehandleren skal levere relevant ophørsassistance til den Dataansvarlige. Dette inkluderer men er ikke begrænset til Hovedaftalen, som nævnt på side 1 og samtlige andre aftaler indgået med samme Databehandler og/eller Underdatabehandler vedrørende behandling af samme data.

Databehandleren forpligter sig til at friholde og forsvare den Dataansvarlige imod alle krav, retskrav og ethvert ansvar, tab, bøder, omkostninger og udgifter forbundet derved som følge af Databehandlerens overtrædelse af databehandleraftalen eller gældende ret, begået af Databehandleren, Databehandlerens ansatte, Underdatabehandlere eller repræsentanter i forbindelse med levering af persondatabehandlingen, gennemførelse af aftalen eller som i øvrigt aftalt mellem parterne.

Databehandleren kan ved misligholdelse af Databehandleraftalen ifalde bod, såfremt der i Hovedaftalen er fastsat vilkår herom. Henvielse til vilkår om bod kan fremgå nærmere af punkt 15.

13. Lovvalg og værneting

Denne Databehandleraftale inklusiv ethvert spørgsmål om Databehandleraftalens gyldighed er undergivet dansk ret.

Forhandling

Såfremt der opstår en uoverensstemmelse mellem Parterne i forbindelse med Databehandleraftalen, skal Parterne med en positiv, samarbejdende og ansvarlig holdning søge at indlede forhandlinger med henblik på at løse tvisten.

Såfremt en løsning ikke kan opnås ved forhandling, må tvisten løses i det valgte konfliktløsningsorgan, jf. nedenfor.

Eventuelt:

Mediation

Enhver tvist, som måtte opstå i forbindelse med denne Databehandlersaftale, skal søges løst ved mediation i overensstemmelse med Danske IT-advokater(DITA)s mediationsprocedure (www.danske-it-advokater.dk). En Part er uberettiget til at søge tvisten løst ved voldgift, før Parterne har søgt tvisten løst ved mediation. Som minimum har en Part pligt til at deltage i det første møde, som mediator indkalder til. En Part er dog berettiget til at indlede voldgiftssag, såfremt en udsættelse deraf kan føre til retsfortabelse f.eks. på grund af forældelse.

Eventuelt:

Vejledende ekspertudtalelse

En Part er ind til eventuel indledning af voldgiftssag berettiget til at få en juridisk/teknisk udtalelse om den pågældende tvist udarbejdet efter de gældende regler herfor vedtaget af bestyrelsen for Danske IT-Advokater, Dansk ITs fagudvalg, IT-Branchens juridiske udvalg og Voldgiftsinstituttets bestyrelse.

Enten:

Voldgift

Hvis enighed ikke kan opnås via forhandling eller på anden vis, skal tvisten løses ved voldgift. Tvisten skal løses ved Voldgiftsinstituttet - The Danish Institute of Arbitration efter de af instituttet vedtagne regler herom, som er gældende ved indledningen af voldgiftssagen.

Eller:

Domstolsbehandling

Hvis enighed ikke kan opnås via forhandling eller på anden vis, skal tvisten løses ved de danske domstole.

14. Genforhandling

Databehandlersaftalen kan af hver af parterne kræves genforhandlet i anledning af ændret lovgivning herunder ikrafttrædelsen af EU-forordningen om persondatabeskyttelse³.

15. Ændringer til punkterne 3-12

Hvis det er tvingende nødvendigt at ændre punkterne 3-12, skal ændringerne beskrives her

Hvis der anvendes Underdatabehandler jf. punkt 4, skal følgende oplysninger fremgå her:

Virksomhedens navn

Adresse

CVR-nr.

Ansvarlig hos Underdatabehandleren

Kontaktperson hos Underdatabehandleren

Beskrivelse af den databehandling som Underdatabehandleren deltager i.

³ Forslag til Europaparlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse).

16. Bilag

Bilag 1: Databehandlerinstruks

Bilag 2: Dataansvarliges informationssikkerhedspolitik

Eventuelle yderligere bilag

17. Øvrige henvisninger

- Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer
- Bekendtgørelse nr. 528 af 15. juni 2000 vedrørende sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning
- Vejledning til sikkerhedsbekendtgørelsen
- Datatilsynets it-sikkerhedstekst ST3
- ISO 27001, ISMS - Ledelsessystem for informationssikkerhed

18. Underskrifter

På vegne af den Dataansvarlige:

Navn: Kenneth Becker

Stilling: CISO

Adresse: Skottenborg 26, 8800 Viborg

Dato:

Underskrift:

Den Dataansvarliges projektansvarlige/systemejers kontaktperson:

Navn:

Stilling:

Dato:

Underskrift:

På vegne af Databehandleren:

Navn:

Stilling:

Adresse:

Dato:

Underskrift: