Datatilsynets standard databehandleraftale
Aftalen kan og bør tilpasses de konkrete behandlingsaktiviteter.

Nedenfor er indsat bilag A-C fra databehandleraftalen udfyldt til eksempel:

Bilag A Oplysninger om behandlingen

[BEMÆRK: I TILFÆLDE AF FLERE BEHANDLINGSAKTIVITETER, SKAL DISSE OPLYSNINGER FREMGÅ FOR HVER ENKELT BEHANDLINGSAKTIVITET]

A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

[Eksempel: Databehandleren leverer et system til tidsregistrering af medarbejdernes arbejdstid fordelt på de sager, som medarbejderen arbejder på.]

A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

[Eksempel: Den dataansvarliges medarbejdere indtaster deres daglige arbejdstid i systemet med angivelse af de klientrelaterede og administrative sager (identificeret ved sagsnumre), som medarbejderen arbejder på. Systemet registrerer og optæller den enkelte medarbejders arbejdstid på sagerne.]

A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

[Eksempel: Navn, titel, arbejdstid, oplysninger om arbejdsopgave]

A.4. Behandlingen omfatter følgende kategorier af registrerede

[Eksempel: Medarbejdere]

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter databehandleraftalens ikrafttræden. Behandlingen har følgende varighed

[Eksempel: Behandlingens varighed løber i aftaleperioden mellem dataansvarlig og databehandler.]

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved databehandleraftalens ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere:

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING

[Alternativt til ovenstående skema:[1]

Der udfyldes ét bilag pr. underdatabehandler.

Underdatabehandler	
Virksomhedens fulde navn	
CVR-nummer (eller tilsvarende)	
Virksomhedens adresse (inkl. land)	
Øvrige adresser hvorfra der behandles personoplysninger	
Kontaktperson hos underdatabehandler	
Har databehandleren en aftale med underdatabehandleren, som opfylder kravene i databehandleraftalen?	

[1] For at få flere oplysninger om underdatabehandleren og dennes opgaver, kan man vælge at få databehandleren til at udfylde et lidt mere omfattende skema. Dette kan gøre det nemmere for den dataansvarlige at få de relevante og nødvendige oplysninger til at foretage en vurdering/risikovurdering af databehandlingen

Databehandling(er), som underdatabehandler deltager i	
Kategorier af personoplysninger som underdatabehandler behandler	

Overførsel af personoplysninger til tredjelande	
Foretager underdatabehandleren behandling af personoplysninger i et tredjeland?	
Hvis ja, angiv samtlige tredjelande	
Hvis ja, angiv overførselsgrundlaget (fx en EU-standardkontrakt eller Binding Corporate Rules)	
Såfremt overførselsgrundlaget er en EU standardkontrakt, angiv hvilken overførselsmodel, der anvendes	[fx databehandler til databehandler]

Såfremt ovenstående skema ikke ønskes, skal det fjernes fra bilaget]

Ved databehandleraftalens ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

B.2. Varsel for godkendelse af underdatabehandlere

[Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal

indgive anmodningen om en specifik godkendelse senest 3 måneder, inden databehandleren ønsker at tage den nye underdatabehandler i anvendelse. Orientering skal ske via revidering af dette bilag B og sendes til x@advokatfirma.dk]

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

[Eksempel: Databehandlingen består i, at databehandleren på baggrund af medarbejdernes indtastninger registrerer den daglige arbejdstid.]

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

[BESKRIV ELEMENTERNE, SOM ER AFGØRENDE FOR SIKKERHEDSNIVEAUET - UNDER HENSYNTAGEN TIL BEHANDLINGENS KARAKTER, OMFANG, SAMMEHÆNG OG FORMÅL SAMT RISICIENE AF VARIERENDE SANDDSYNLIGHED OG ALVOR FOR FYSISKE PERSONERS RETTIGHEDER OG FRIHEDSRETTIGHEDER]

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

Den dataansvarlig skal altid konkret forholde sig til hvilke tekniske og organisatoriske sikkerhedsforanstaltninger der skal implementeres med henblik på at etablere et passende sikkerhedsniveau.

[Eksempel:[2]

C.2.1. Operationel sikkerhed

Databehandleren skal sikre;

(a) at det nødvendige og tilstrækkelige sikkerhedsniveau vedligeholdes og opretholdes, samt at eventuelle ændringer i databehandlerens sikkerhedsforanstaltninger relevante for personoplysningerne logges og dokumenteres,
(b) at ændringer og vedligeholdelse af databehandlerens sikkerhedsforanstaltninger så vidt muligt ikke påvirker den dataansvarliges forretning, herunder men ikke begrænset til it-systemer, netværk, forbindelser og svartider,
(c) at databehandlerens eventuelle testmiljøer er tilstrækkeligt afgrænset og i øvrigt sikret mod uautoriseret adgang,
(d) at databehandlerens it-systemer og netværk er tilstrækkeligt sikret mod hacking og anden uautoriseret adgang,

[2] Det er vigtigt, at der tages stilling til hvilke sikkerhedsforanstaltninger, der er relevante i det konkrete tilfælde. Se til inspiration Datatilsynets katalog over sikkerhedsforanstaltninger: Katalog over foranstaltninger (datatilsynet.dk)

(e) at databehandleren gennemfører kontroller for at opdage og forhindre svindel, malware mv., og
(f) at dennes interne operationelle sikkerhedsprocedurer og -manualer følges.

C2.2 Fysisk sikkerhed
Databehandleren skal sikre sine fysiske lokaliteter, servere mv. mod uautoriseret adgang.

Databehandleren skal have interne sikkerhedsprocedurer der ved fjernelse, afhændelse eller genbrug af hardware sikrer, at den dataansvarliges personoplysninger ikke kompromitteres.

C2.3 Backup
Databehandleren skal foretage backup af personoplysningerne samt teknisk test af backup, i det omfang backup er en del af [Kontrakten/Hovedaftalen], eller på anden vis er aftalt mellem parterne.

Såfremt det er en del af [Kontrakten/Hovedaftalen], eller hvis det på anden vis er aftalt mellem parterne, vil databehandleren herefter én gang i døgnet tage en backup af den dataansvarliges oplysninger. Backup-overførslen skal være krypteret. Backup skal opbevares i et aflåst område i en anden bygning, end hvor produktionsserveren fysisk er placeret. Backup gemmes i henhold til den i [Kontrakten/Hovedaftalen] definerede periode eller en anden periode aftalt mellem parterne.

Databehandleren stiller en erklæring om backup og teknisk test af backup til rådighed for den dataansvarlige.

C2.4 Adgang til personoplysninger
Databehandleren skal sikre, at kun relevante medarbejdere har adgang til de behandlede personoplysninger.

Databehandleren skal efter den dataansvarliges anmodning på ethvert tidspunkt kunne afgive en erklæring om hvilke personer, som har haft adgang til personoplysningerne på vegne af databehandleren.

Databehandleren skal sikre, at enhver person, der udfører arbejde for databehandleren og får adgang til personoplysningerne, kun behandler sådanne oplysninger efter den dataansvarliges instruks, medmindre behandlingen er påkrævet i henhold til EU-lovgivningen eller EØS-medlemsstaternes nationale lovgivning.

Databehandleren skal sikre, at enhver person, der udfører arbejde for databehandleren og får adgang til personoplysningerne har oparbejdet tilstrækkeligt kendskab til korrekt håndtering af personoplysninger, er underlagt tavshedspligt, og at de pågældende medarbejdere er bekendt med de aftalte sikkerhedskrav.

C2.6 Logning
Databehandleren foretager logning i overensstemmelse med lovgivningen og gældende branchestandarder.

Der skal foretages logning af alle afviste adgangsforsøg. Hvis der inden for en periode på 24 timer er registreret højst 3 på hinanden følgende afviste adgangsforsøg fra samme bruger, skal der blokeres for yderligere forsøg. Adgangen må først åbnes, når årsagen er klarlagt og dokumenteret.

Der skal foretages maskinel logning af alle anvendelser af personoplysninger. Loggen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrører eller det anvendte søgekriterium.

Den dataansvarlige kan på anmodning få de relevante logs udleveret fra databehandleren.

Log opbevares i 6 måneder.]

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med pkt. 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

[Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

a) oplysningspligten ved indsamling af personoplysninger hos den registrerede
b) oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
c) indsigtsretten
d) retten til berigtigelse
e) retten til sletning ("retten til at blive glemt")
f) retten til begrænsning af behandling
g) underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
h) retten til dataportabilitet
i) retten til indsigelse
j) retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til pkt. 6.3, bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

a. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

b. den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.]

C.4 Opbevaringsperiode/sletterutine

[BESKRIV EVENTUEL OPBEVARINGSPERIODE/SLETTERUTINE FOR DATABEHANDLEREN][3]

"Eksempel: Personoplysninger opbevares i [ANGIV TIDSPERIODE], hvorefter de slettes hos databehandleren.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med pkt. 11.1, medmindre den dataansvarlige – efter underskriften af denne databehandleraftale – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne."

C.5 Lokalitet for behandling

Behandling af de af databehandleraftalen omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

[ANGIV, HVOR BEHANDLINGEN FINDER STED] [ANGIV, HVILKEN DATABEHANDLER ELLER UNDERDATABEHANDLER, DER ANVENDER ADRESSEN]

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande[4]

[BESKRIV INSTRUKSEN VEDRØRENDE OVERFØRSEL AF PERSONOPLYSNINGER TIL TREDJELANDE ELLER INTERNATIONALE ORGANISATIONER]

[ANGIV GRUNDLAGET FOR OVERFØRSLEN SOM OMHANDLET I DATABESKYTTELSESFORORDNINGENS KAPITEL V][5]

Hvis den dataansvarlige ikke i denne databehandleraftale eller senere giver en dokumenteret instruks vedrørende overførsels af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af denne databehandleraftale at foretage sådanne overførsler.

[3] Det er den dataansvarlige, som fastsætter slettefristen.
[4] Lande udenfor EU/EØS, som ikke sikrer et tilstrækkeligt beskyttelsesniveau.
[5] Fx EU-standardkontrakt eller Binding Corporate Rules.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

[Eksempel: Databehandleren udfører regelmæssig egenkontrol af interne politikker, procedure og tekniske kontroller. Herudover indhentes ISAE3000 erklæring fra ekstern IT-leverandør som fremsendes til den dataansvarlige uden unødig forsinkelse.][6]

C.8 [HVIS RELEVANT] Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere
[Eksempel: Databehandleren skal en gang årligt indhente en erklæring/certifikat fra uafhængig tredjepart eller egen inspektion vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og bestemmelserne i denne databehandleraftale.

Der er enighed mellem parterne om, at følgende typer af erklæringer kan bruges:

- ISEA3000
- ISO27701
- Egen kontrol

Erklæring/egenkontrol fremsendes uden unødig forsinkelse til den dataansvarlige til orientering såfremt der findes anmærkninger til kontrollen.

Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny erklæring for egen regning under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæringen, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og bestemmelserne i denne databehandleraftale. Såfremt disse foranstaltninger ikke er lovpligtige og har en omkostning for databehandleren, vil denne omkostning videreføres til den dataansvarlige.]

[6] Der skal med udgangspunkt i Datatilsynets vejledning om tilsyn af databehandlere fastsættes en relevant tilsynsmetode: Datatilsynet_Vejledning om tilsyn med databehandlere_oktober-2021.pdf