

Databehandleraftale

i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger

mellem

[NAVN]

CVR: [CVR]

[ADRESSE]

[POSTNUMMER OG BY]

[LAND]

herefter "den dataansvarlige"

og

Døgndata ApS

CVR 33 77 17 97

Axel Kiers Vej 5A,

8270, Højbjerg

Danmark

herefter "databehandleren"

der hver især er en "part" og sammen udgør "parterne"

Parterne har således aftalt følgende standardkontraktbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

1. Indhold	
2. Præambel.....	3
3. Den dataansvarliges rettigheder og forpligtelser.....	3
4. Databehandleren handler efter instruks.....	4
5. Fortrolighed.....	4
6. Behandlingssikkerhed.....	4
7. Anvendelse af underdatabehandlere.....	5
8. Overførsel til tredjelande eller internationale organisationer.....	6
9. Bistand til den dataansvarlige.....	6
10. Underretning om brud på persondatasikkerheden.....	8
11. Sletning og returnering af oplysninger.....	8
12. Revision, herunder inspektion.....	8
13. Parternes aftale om andre forhold.....	9
14. Ikrafttræden og ophør.....	9
15. Kontaktpersoner hos den dataansvarlige og databehandleren.....	10
Bilag A	11
Bilag B	13
Bilag C	17
Bilag D	23

2. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.
2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).
3. I forbindelse med leveringen af licens til databehandlerens løsning(er) og service(s) behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.
10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes¹ nationale ret og disse Bestemmelser.
2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

¹ Henvisninger til "medlemsstat" i disse bestemmelser skal forstås som en henvisning til "EØS medlemsstater".

3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

4. Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.
2. Databehandleren underretter 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.

5. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.
2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

- a. pseudonymisering og kryptering af personoplysninger.
- b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester.
- c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.
- d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.
3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).
2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.
3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.
4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

6. Databehandleren skal om muligt i sin aftale med underdatabehandleren indføre den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.
7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

- a) Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.
- b) Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.
- c) Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:
 - a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
 - b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
 - c. behandle personoplysningerne i et tredjeland
- d) Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.
- e) Disse Bestemmelser skal ikke forveksles med standardkontraktbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

9. Bistand til den dataansvarlige

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

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
2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 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 unødigt 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 unødigt 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.
3. Databehandlerens forpligtelser i henhold til aftalen medfører ikke krav på særskilt betaling til databehandleren for medgået tid, medmindre medgået tid overstiger fem (5) timer.
4. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:
 - a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
 - b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
 - c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.
4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

1. Ved ophør af databehandlerens tjenester vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er slettet, medmindre den dataansvarlige instruerer databehandleren om andet, eller medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

12. Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, 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.
2. Procedurene for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft ved begge parters underskrift heraf.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.
4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.
5. Underskrift

På vegne af den dataansvarlige

Navn
Stilling
Underskrift
Dato

På vegne af databehandleren

Navn Martin Lyngby Hansen
Stilling Adm. direktør
Underskrift

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Databehandleren kan kontaktes via nedenstående kontaktperson eller ved kommunikation til personer, der normalvis kommunikerer med i aftaleforholdet mellem den dataansvarlige og databehandleren.
2. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.
3. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner. Såfremt det ikke er muligt for databehandleren at træffe den dataansvarlige ved oplyste kontaktperson, tillader den dataansvarlige at databehandleren kontakter anden person, der normalvis kommunikerer med i aftaleforholdet.

Navn Martin Lyngby Hansen
Stilling Adm. direktør
Telefonnummer 93104000
E-mail info@sofus.dk



Navn
Stilling
Telefonnummer
E-mail

3. Bilag A Oplysninger om behandlingen

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

Behandlingen af den dataansvarliges personoplysninger sker med det formål at opfylde den mellem databehandleren og den dataansvarlige indgåede aftale om databehandlerens levering af databehandlerens løsninger og services.

Formålet med databehandlerens løsning(er) og/eller service(s) er:

Dagbogsprogrammet

Dagbogsprogrammet er en digital løsning hvor Dataansvarlig kan dokumentere og håndtere skriftligt arbejde og kommunikation vedrørende børn, unge og voksne som er anbragt.

Sofus Match

SofusMATCH er en digital løsning for Dataansvarlig i forbindelse med systematisk at arbejde med plejefamilier/ressourcepersoner og match af udsatte børn, unge og voksne med disse.

Sofus Social

sofusSOCIAL er en digital løsning hvori Dataansvarlig kan skabe overblik over kontaktpersoner, mentorer og ressourcepersoner i disses arbejde med udsatte børn, unge og voksne og Dataansvarlig.

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

Som ejer og leverandør af løsningen behandler databehandleren ved generel drift, herunder hosting, visning, organisering, modtagelse, videresendelse, strukturering, tilpasning, implementering, søgning, processering, lagring, gendannelse, sletning, begrænsning, vedligeholdelse, udvikling, logning, support, fejlfinding og andre it-ydelser forbundet med databehandlerens løsning(er) og/eller service(s) til den dataansvarlige i henhold til den mellem parterne indgåede aftale.

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

Databehandleren behandler i udgangspunktet nedenstående kategorier af personoplysninger. Ved brug af løsningen er der dog mulighed for, at den dataansvarlige kan overlade behandling af alt slags data og personoplysninger til databehandleren, hvorfor databehandleren potentielt vil kunne behandle alle kategorier af personoplysninger.

Kategorier af personoplysninger:

Dagbogsprogrammet

Almindelige personoplysninger, jf. Databeskyttelsesforordningens artikel 4, stk. 1 og artikel 6:

- a) Kontaktoplysninger, som personnavn, e-mailadresse, organisationstilknytning, adresse, telefonnummer, fødselsdato, billede
- b) Brugeroplysninger, som brugernavn, nationalitet, brugerlokation og -adfærd,
- c) Og evt. øvrige personoplysninger, der er nødvendige for den dataansvarliges brug af databehandlerens levering af værktøjer og services.

Følsomme personoplysninger (jf. Databeskyttelsesforordningens artikel 9):

- a) Racemæssig eller etnisk oprindelse
- b) Politisk, religiøs og/eller filosofisk overbevisning
- c) Fagforeningsmæssigt tilhørsforhold
- d) Genetisk og/eller biometrisk data

- e) Helbredsoplysninger
- f) Seksuelle forhold eller seksuelle orientering

Oplysninger om enkeltpersoners rent private forhold (jf. Databeskyttelsesforordningens artikel 6 og 9):

- a) Strafbare forhold
- b) Væsentlige sociale problemer, herunder psykiske problemer

Andre rent private forhold, som ikke er nævnt ovenfor:

- a) Væsentlige økonomiske forhold

Oplysninger om CPR-nummer (jf. Databeskyttelsesforordningens artikel 87):

- a) CPR-numre.

Sofus Match

Almindelige personoplysninger, jf. Databeskyttelsesforordningens artikel 4, stk. 1 og artikel 6:

- d) Kontaktoplysninger, som personnavn, e-mailadresse, organisationstilknytning, adresse, telefonnummer, fødselsdato, billede
- e) Brugeroplysninger, som brugernavn, nationalitet, brugerlokation og -adfærd,
- f) Og evt. øvrige personoplysninger, der er nødvendige for den dataansvarliges brug af databehandlerens levering af værktøjer og services.

Følsomme personoplysninger (jf. Databeskyttelsesforordningens artikel 9):

- g) Racemæssig eller etnisk oprindelse
- h) Politisk, religiøs og/eller filosofisk overbevisning
- i) Fagforeningsmæssigt tilhørsforhold
- j) Genetisk og/eller biometrisk data
- k) Helbredsoplysninger
- l) Seksuelle forhold eller seksuelle orientering

Oplysninger om enkeltpersoners rent private forhold (jf. Databeskyttelsesforordningens artikel 6 og 9):

- c) Strafbare forhold
- d) Væsentlige sociale problemer, herunder psykiske problemer

Andre rent private forhold, som ikke er nævnt ovenfor:

- b) Væsentlige økonomiske forhold

Oplysninger om CPR-nummer (jf. Databeskyttelsesforordningens artikel 87):

- b) CPR-numre.

Sofus Social

Almindelige personoplysninger, jf. Databeskyttelsesforordningens artikel 4, stk. 1 og artikel 6:

- g) Kontaktoplysninger, som personnavn, e-mailadresse, organisationstilknytning, adresse, telefonnummer, fødselsdato, billede
- h) Brugeroplysninger, som brugernavn, nationalitet, brugerlokation og -adfærd,
- i) Og evt. øvrige personoplysninger, der er nødvendige for den dataansvarliges brug af databehandlerens levering af værktøjer og services.

Følsomme personoplysninger (jf. Databeskyttelsesforordningens artikel 9):

- m) Racemæssig eller etnisk oprindelse
- n) Politisk, religiøs og/eller filosofisk overbevisning
- o) Fagforeningsmæssigt tilhørsforhold

- p) Genetisk og/eller biometrisk data
- q) Helbredsoplysninger
- r) Seksuelle forhold eller seksuelle orientering

Oplysninger om enkeltpersoners rent private forhold (jf. Databeskyttelsesforordningens artikel 6 og 9):

- e) Strafbare forhold
- f) Væsentlige sociale problemer, herunder psykiske problemer

Andre rent private forhold, som ikke er nævnt ovenfor:

- c) Væsentlige økonomiske forhold

Oplysninger om CPR-nummer (jf. Databeskyttelsesforordningens artikel 87):

- c) CPR-numre.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Databehandleren behandler i udgangspunktet nedenstående kategorier af registrerede. Ved brug af løsningen er der dog mulighed for, at den dataansvarlige kan overlade behandling af alt slags data og personoplysninger til databehandleren, hvorfor databehandleren potentielt vil kunne behandle personoplysninger om flere kategorier af registrerede.

Kategorier af registrerede:

Dagbogsprogrammet

- a) Anbragte børn, unge og voksne
- b) Borgere med relation til anbragte borgere, f.eks. mor/far/væрге
- c) Medarbejdere hos Dataansvarlige

Sofus Match

- a) Plejefamilier
- b) Anbragte børn, unge og voksne
- c) Medarbejdere hos Dataansvarlig

Sofus Social

- a) Ressourcepersoner knyttet til den Dataansvarlige
- b) Anbragte børn, unge og voksne
- c) Medarbejdere hos Dataansvarlige

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

Behandlingen er ikke tidsbegrænset og varer, indtil abonnementsaftalen mellem parterne om levering af databehandlerens værktøjer til den dataansvarlige, opsiges eller ophæves af en af parterne.

4.

5. Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

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

Dagbogsprogrammet

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Hetzner Online GmbH	DE812871812	Industriestr. 25, 91710 Gunzenhausen, Tyskland	Hetzner anvendes til hosting af Døgndata applikationer og støttesystemer, samt backup.
Heysender ApS	31282322	Jens Baggesens Vej 47, 8200 Aarhus N, Danmark	Heysender anvendes som service for udsendelse af e-mails.
Scaleway S.A.S.	FR35433115904	8 rue de la Ville l'Evêque, 75008 Paris, Frankrig	Scaleway anvendes til hosting af Døgndata applikationer og støttesystemer, samt backup.
Compaya A/S	31375428	Palægade 4, 2. tv., 1261 København K, Danmark	Compaya anvendes som service for udsendelse af SMS'er.

Sofus Match

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Hetzner Online GmbH	DE812871812	Industriestr. 25, 91710 Gunzenhausen, Tyskland	Hetzner anvendes til hosting af Døgndata applikationer og støttesystemer, samt backup.
Heysender ApS	31282322	Jens Baggesens Vej 47, 8200 Aarhus N, Danmark	Heysender anvendes som service for udsendelse af e-mails.
Scaleway S.A.S.	FR35433115904	8 rue de la Ville l'Evêque, 75008 Paris, Frankrig	Scaleway anvendes til hosting af Døgndata applikationer og støttesystemer, samt backup.
Compaya A/S	31375428	Palægade 4, 2. tv., 1261 København K, Danmark	Heysender anvendes som service for udsendelse af SMS'er.

Sofus Social

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Hetzner Online GmbH	DE812871812	Industriestr. 25, 91710 Gunzenhausen, Tyskland	Hetzner anvendes til hosting af Døgndata applikationer og støttesystemer, samt backup.
Heysender ApS	31282322	Jens Baggesens Vej 47, 8200 Aarhus N, Danmark	Heysender anvendes som service for udsendelse af e-mails.
Scaleway S.A.S.	FR35433115904	8 rue de la Ville l'Evêque, 75008 Paris, Frankrig	Scaleway anvendes til hosting af Døgndata applikationer og støttesystemer, samt backup.
Compaya A/S	31375428	Palægade 4, 2. tv., 1261 København K, Danmark	Heysender anvendes som service for udsendelse af SMS'er.

Ved Bestemmelsernes 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.

Databehandleren skal opretholde en gældende liste over underdatabehandlere på databehandlerens hjemmeside, som udgør gældende bilag B. Underdatabehandleraftalerne rekvireres via hjemmesiden eller ved skriftlig anmodning til databehandleren.

B.2. Varsel for godkendelse af underdatabehandlere

Databehandlerens underretning om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere skal være den dataansvarlige i hænde minimum 30 dage, før anvendelsen eller ændringen skal træde i kraft, så vidt dette umiddelbart er muligt jf. kontraktsbestemmelse 7, 7.3.

Uanset ovenstående accepterer den dataansvarlige, at der kan være særlige tilfælde, hvor der kan opstå et konkret behov for, at ændringen vedrørende tilføjelse eller erstatning af underdatabehandlere sker med kortere varsel eller straks. I sådanne tilfælde vil databehandleren underrette den dataansvarlige om ændringen snarest muligt.

Såfremt den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give databehandleren meddelelse herom inden ændringens varslede virkningstidspunkt. Den dataansvarlige kan alene gøre indsigelse, hvis den dataansvarlige har rimelige, konkrete årsager hertil.

Ved den dataansvarliges indsigelse accepterer den dataansvarlige samtidig, at databehandleren kan være forhindret i at levere hele eller dele af de aftalte tjenester. Sådant manglende opfyldelse kan ikke tilskrives databehandlerens misligholdelse. Databehandleren opretholder sit krav på betaling for sådanne ydelser, uanset de ikke kan leveres til den dataansvarlige.

Hvor det er særligt aftalt, at databehandleren ikke må gøre brug af underdatabehandlere uden den dataansvarliges forudgående tilladelse, accepterer den dataansvarlige, at dette kan medføre, at databehandleren kan blive afskåret fra at opfylde tjenesterne. Hvis den dataansvarlige har afslået, at der foretages ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere, vil manglende levering af tjenester derfor ikke anses for en misligholdelse af parternes aftale vedrørende levering af tjenesterne, som kan tilskrives databehandleren i de tilfælde, hvor den manglende opfyldelse kan henføres til en underdatabehandlers forhold.

6. 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:

generel drift, herunder hosting, visning, organisering, modtagelse, videresendelse, strukturering, tilpasning, implementering, søgning, processering, lagring, gendannelse, sletning, begrænsning, vedligeholdelse, udvikling, logning, support, fejlfinding og andre it-ydelser forbundet med databehandlerens løsning(er) og/eller service(s) til den dataansvarlige i henhold til den mellem parterne indgåede aftale.

Dagbogsprogrammet

Databehandleren stiller Dagbogsprogrammet til rådighed for den Dataansvarlige. Som led i dette lagrer og behandler Databehandleren personoplysningerne. Dagbogsprogrammet er et værktøj målrettet Dataansvarliges arbejde med anbragte børn, unge og voksne.

Sofus Match

Databehandleren stiller sofusMATCH til rådighed for den Dataansvarlige. Som led i dette lagrer og behandler Databehandleren personoplysninger. sofusMATCH er et værktøj rettet mod Dataansvarliges arbejde med social udsatte borgere – primært børn og unge, samt de plejefamilier/ressourcepersoner borgere måtte være eller kan knyttes til.

Sofus Social

Databehandleren stiller sofusSOCIAL til rådighed for den Dataansvarlige. Som led i dette lagrer og behandler Databehandleren personoplysninger. sofusSOCIAL er et værktøj rettet mod Dataansvarliges arbejde med socialt udsatte borgere – primært børn, unge og voksne, samt de ressourcepersoner borgere måtte være eller kan knyttes til.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Databehandlerens løsninger og services omfatter som udgangspunkt behandling af personoplysninger som omfattet af Databeskyttelsesforordningens forskellige kategorier af personoplysninger som anført i bilag A. Derfor har databehandleren valgt at implementere et generelt højt sikkerhedsniveau afspejlende, at der kan ske behandling heraf. 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:

Informationssikkerhed

Databehandleren har implementeret politikker, kontroller og processer, som dækker de nedenfor beskrevne informationssikkerhedsområder:

Fortrolighed: Sikre at uautoriserede personer ikke kan få adgang til data, som kan misbruges til skade for databehandlerens kunder, forretningsforbindelser og ansatte.

Integritet: Sikre at systemer indeholder akkurat og komplet information.

Tilgængelighed: Sikre at relevant information og relevante systemer er tilgængelige og stabile.

Instruks

Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.

Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra den dataansvarlige.

Fysisk sikring og miljøsikring

Databehandleren skal opretholde fysiske sikringsforanstaltninger til sikring af lokaliteter, som anvendes til behandling af personoplysninger, herunder opbevaring af personoplysninger omfattet af Databehandleraftalen mod uvedkommendes adgang og manipulation.

Skal have passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang til lokaler, hvor der behandles persondata. Databehandleren skal desuden, hvor det er nødvendigt, evaluere og forbedre effektiviteten af sådanne forholdsregler

Sikrer at niveauet for den fysiske sikkerhed til enhver tid være afstemt med det aktuelle trusselbillede samt den følsomhed og mængde af persondata som databehandleraftalen omfatter

Kommunikationsforbindelser og kryptering

Databehandleren har passende tekniske foranstaltninger til at beskytte systemer og netværk, herunder beskytte data under transmission og adgang via internettet, samt til at begrænse risikoen for uautoriseret adgang og/eller installering af skadelig kode.

Databehandleren anvender passende krypteringsteknologier og andre tilsvarende foranstaltninger i overensstemmelse med kravene i lovgivningen, godkendte standarder for kryptering af klassificeret information samt god databehandlingskik.

I det omfang det er et krav i medfør af gældende national og international lovgivning, standarder vedrørende kryptering af klassificeret information eller god databehandlingskik anvender databehandler krypteringsteknologier og andre tilsvarende foranstaltninger.

Transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af kryptering. Teknologiske løsninger til kryptering er tilgængelige og aktiveret. Firewall tillader kun krypteret datatrafik. Der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme.

Firewall eller lignende tekniske foranstaltninger

Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en VPN. Der skal foreligge administrativ adgang til at vedligeholde firewall-konfiguration og -regelsæt.

Antivirus

Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres

Sikkerhedskopiering

Databehandler skal have interne beredskabsprocedurer, der sikrer genetablering af services uden ugrundet ophold i tilfælde af driftsafbrydelser i henhold til hovedaftalen. Databehandleren sikrer daglig backup.

Sikkerhedskopiering af konfigurationsfiler og data skal finde sted i et ubrudt forløb, så at relevant data kan reetableres. Sikkerhedskopierne opbevares således, at de ikke hændeligt eller ulovligt (eks. ved brand, oversvømmelse, uheld, tyveri eller lignende) tilintetgøres, fortabes, forringes, kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

Sikkerhedskopierne skal opbevares fysisk adskilt fra primære data og i et sikkerhedsgodkendt datacenter.

Anvendelse af hjemme/fjernarbejdspladser

Såfremt der foretages databehandling fra ad hoc og/eller hjemmearbejdspladser, sikre Databehandleren at disse lever op til de sikkerhedsmæssige krav i denne Databehandleraftale med bilag og lovgivning i øvrigt.

Databehandler skal blandt andet opfylde følgende:

- At deres anvendes krypteret forbindelse mellem ad hoc arbejdspladsen og Databehandlerens/Dataansvarliges netværk
- Databehandlerens har en intern instruks til egne medarbejdere vedrørende ad hoc og hjemmearbejdspladser

Derudover skal Databehandleren, hvis det er teknisk muligt anvende 2-faktor-autentifikation.

Instruktion af medarbejdere

Databehandleren sikrer at ansatte til stadighed er bekendt med og har tilstrækkelig uddannelse og instruktion om databehandlingens formål, politikker, arbejdsgange og om deres tavshedspligt.

Der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.

Informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler.

Der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse

Medarbejdere har underskrevet en fortrolighedsaftale. Medarbejdere er blevet introduceret til:

- Informationssikkerhedspolitikken.
- Procedurer vedrørende databehandling, samt anden relevant information

Der foreligger procedurer, der sikrer, at fratrådte medarbejders rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon osv. inddrages. Fratrådte medarbejders rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.

Der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Ansættelseskontrakten indeholder retningslinjer for, at medarbejdere er underlagt tavshedspligt efter ophørt samarbejde.

Databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.

Der foreligger dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.

Bortskaffelse af udstyr

Databehandleren har formelle processer med henblik på at sikre, at der sker en effektiv sletning af personoplysninger inden bortskaffelse af elektronisk udstyr.

Logning

1. Sikrer logning på alle miljøer, hvor personoplysninger behandles.
2. Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder.
3. Ændringer i logopsætninger, herunder deaktivering af logning.
4. Ændringer i systemrettigheder til brugere.
5. Sikrer, at sikkerhedsloggens omfang er defineret ud fra en af Databehandleren udført risikovurdering
6. Sikrer, at der er plads nok til at sikkerhedsloggene kan gemmes for perioden
7. Sikrer, at der gennemføres løbende stikprøvekontroller, af, at sikkerhedsloggene indeholder det forventede
8. Afvejer sikkerhedsloggens slettefrister imellem muligheden for at analysere cyberangreb, understøtte efterforskning og hensynet til beskyttelses af fysiske personers rettigheder og frihedsrettigheder.
9. Sikrer opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod sletning og manipulation.

C.3 Bistand til den dataansvarlige

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

Registreredes rettigheder, jf. pkt. 9.1.

- Databehandleren skal bistå med at iagttage de registreredes rettigheder ved bl.a. at kunne give indsigt i, slette, begrænse og berigtige oplysninger, og sørge for at dette også sker hos underdatabehandlerne.
- Databehandleren skal bistå med at opfylde de registreredes rettigheder uden unødigt forsinkelse
- Databehandleren skal have udarbejdet en procedure for, hvordan de behandler anmodninger fra en registreret om deres rettigheder.

Brud og hændelser, jf. pkt. 9.2.

Informationer som skal sendes:

- Fakta om det konstaterede brud (tid, sted, årsag).
- Hvornår bruddet startede, hvornår det blev opdaget og hvornår bruddet er standset.
- Karakteren af bruddet på persondatasikkerheden, herunder om der er sket brud på fortrolighed, integritet og tilgængelighed.
- Kategorierne og det omtrentlige antal berørte registrerede, hvis det er muligt.
- Kategorierne af personoplysninger, hvis det er muligt.
- Navn og kontaktoplysninger til kontaktpunkt, hvor yderligere oplysninger kan indhentes.
- Beskrivelse af de sandsynlige konsekvenser af bruddet.
- Beskrivelse af foranstaltninger der er truffet, eller foreslås truffet som led i håndteringen af bruddet og dets mulige skadevirkninger.

C.4 Opbevaringsperiode/sletterutine

Personoplysninger opbevares i perioden for parternes aftale om databehandlerens levering af databehandlerens løsning(er) og/eller service(s) til den dataansvarlige, eller i henhold til særskilt skriftlig aftale, hvorefter de slettes hos databehandleren.

Ved ophør skal databehandleren således enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

C.5 Lokaltet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end de, som følger af nærværende databehandleraftale og de adresser som fremgår af anvendte underdatabehandlere, samt underdatabehandlere i yderligere led, som nærmere beskrevet i gældende bilag B.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler, medmindre en sådan overførsel sker til en af de autoriseret underdatabehandlere nævnt i bilag B. Overførselsgrundlag anvendes i henhold til Databeskyttelsesforordningens Kapitel V om overførsler af personoplysninger til tredjelande eller internationale organisationer. De specifikke overførselsgrundlag følger af gældende bilag B.

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

Databehandleren skal inden for en periode af 12 måneder for egen regning indhente en ISAE 3000 revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Revisorerklæringen vil være tilgængelig for den dataansvarlige på databehandlerens hjemmeside.

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

Baseret på resultaterne af erklæring, 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 disse Bestemmelser.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover, mod betaling, adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

Databehandleren skal for egen regning gennemføre passende tilsyn med underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

Dokumentation for sådanne inspektioner fremsendes ved anmodning herom til den dataansvarlige til orientering.

7. Bilag D Parternes regulering af andre forhold

D.1 Ansvar og misligholdelse

En eventuel misligholdelse af Bestemmelserne reguleres og behandles i overensstemmelse med parternes aftale vedrørende levering af tjenesterne.

I tilfælde hvor databehandleren har udredt beløb til registrerede i overensstemmelse med Databeskyttelsesforordningens artikel 82 eller erstatningsansvarsloven § 26, har databehandleren fuld regres mod den dataansvarlige for det udredte beløb, som beløbsmæssigt overstiger den aftalte ansvarsbegrænsning i parternes aftale vedrørende levering af tjenesterne.

Parterne har hermed aftalemæssigt fraveget Databeskyttelsesforordningens artikel 82, stk. 5, og erstatningsansvarsloven § 26.

Uanset databeskyttelsesforordningen art 82, stk. 5 kan en part, der har udredt erstatningsbeløb til en skadelidt, der ikke svarer til fuld erstatning, gøre regres efter princippet i art. 82, stk. 5.

I forhold til anden godtgørelse for ikke-økonomiske tab til de registrerede skal princippet i art. 82 ligeledes finde anvendelse, for så vidt angår den interne endelige ansvarsfordeling mellem databehandleren og den dataansvarlige.

Parterne kan ikke gøre regres eller erstatningskrav gældende overfor den anden part for bøder eller anden straf, der er pålagt i medfør af databeskyttelsesloven § 41 samt for bødeforelæg accepteret efter databeskyttelsesloven § 42.

D.2 Konsekvenser af den dataansvarliges ulovlige instruks

Den dataansvarlige er bekendt med, at databehandleren er afhængig af den dataansvarliges anvisninger om, i hvilket omfang databehandleren er berettiget til at anvende og behandle personoplysningerne på den dataansvarliges vegne. Databehandleren hæfter derfor ikke for krav, som udspringer af databehandlerens handlinger eller undladelser, i det omfang disse handlinger eller undladelser er en direkte databehandlingsaktivitet udøvet i overensstemmelse med den dataansvarliges instrukser, medmindre det kan fastslås, at databehandleren havde kendskab til behandlingens manglende lovlighed.

D.3 Anvendelse af underdatabehandler, som leverer på standardvilkår

Uanset kontraktbestemmelse 7 skal det understreges, at hvis databehandleren anvender en underdatabehandler, som leverer sine ydelser på egne vilkår, som databehandleren ikke har mulighed for at aftale fravigelser til, gælder underdatabehandlerens vilkår for de behandlingsaktiviteter, der overlades til udførelse hos sådan underdatabehandler. Hvor der sker behandling på en underdatabehandlerens vilkår, er dette angivet ved den relevante underdatabehandler på oversigten over underdatabehandlere. Ved Bestemmelserne giver den dataansvarlige sin accept af og instruks om, at sådanne konkrete behandlingsaktiviteter sker på underdatabehandlerens vilkår.

D.4 Sletning og returnering af oplysninger

Det er mellem parterne aftalt, at den dataansvarlige instruerer om databehandlerens sletning og returnering af personoplysninger i forbindelse med Bestemmelsernes ophør.

Den dataansvarlige skal, senest 30 dage efter at behandlingen af personoplysninger er ophørt, meddele databehandleren, hvorvidt alle personoplysninger skal slettes eller tilbageleveres til den dataansvarlige. I det tilfælde hvor personoplysninger skal tilbageleveres til den dataansvarlige, skal databehandleren ligeledes slette eventuelle kopier. Databehandleren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever meddelelsen fra den dataansvarlige.

Såfremt databehandleren ikke har modtaget meddelelse fra den dataansvarlige, inden 30 dage efter behandlingen af personoplysninger er ophørt, fremsender databehandleren en rykker til den dataansvarlige. Hvis den dataansvarlige herefter ikke meddeler databehandleren, hvorvidt alle personoplysninger skal slettes eller tilbageleveres til den dataansvarlige, er databehandleren uden yderligere varsel berettiget til at slette personoplysninger.

Databehandleren er berettiget til vederlag for dennes behandlingsaktiviteter frem til det tidspunkt, hvor den dataansvarlige meddeler databehandleren, hvorvidt alle personoplysninger skal slettes eller tilbageleveres til den dataansvarlige.