DATABEHANDLERAFTALE

Indholdsfortegnelse

INDHOLDSFORTEGNELSE 2

1 PARTERNE 3

2 UNDERSKRIFT 3

3 KONTAKTPERSONER 3

4 PRÆAMBEL 4

5 DEN DATAANSVARLIGES RETTIGHEDER OG FORPLIGTELSER 4

6 DATABEHANDLEREN HANDLER EFTER INSTRUKS 5

7 FORTROLIGHED 6

8 BEHANDLINGSSIKKERHED 6

9 ANVENDELSE AF UNDERDATABEHANDLERE 7

10 OVERFØRSEL TIL TREDJELANDE ELLER INTERNATIONALE ORGANISATIONER 8

11 BISTAND TIL DEN DATAANSVARLIGE 8

12 UNDERRETNING OM BRUD PÅ PERSONDATASIKKERHEDEN 9

13 SLETNING OG RETURNERING AF OPLYSNINGER 10

14 REVISION, HERUNDER INSPEKTION 11

15 PARTERNES AFTALER OM ANDRE FORHOLD 11

16 IKRAFTTRÆDEN OG OPHØR 12

BILAG A OPLYSNINGER OM BEHANDLINGEN 14

BILAG B UNDERDATABEHANDLERE 16

BILAG C INSTRUKS VEDRØRENDE BEHANDLING AF PERSONOPLYSNINGER 19

BILAG D PARTERNES REGULERING AF ANDRE FORHOLD 24

ÆNDRINGER 25

1 PARTERNE

1.1 Denne Databehandleraftale (DPA), herefter kendt som "Aftalen" er indgået mellem:

Kunden:	Leverandøren:
[Navn på virksomhed]	Intect aps.
[Adresse]	Hørkær 12A
[Post nr + by]	2730 Herlev
CVR: XXXXXX	CVR: 37035084
et selskab stiftet i henhold til lovgivningen i Danmark. herefter ”Den Dataansvarlige”	et selskab stiftet i henhold til lovgivningen i Danmark. (herefter "Databehandleren");

1.2 der hver især er en ”part” og sammen udgør ”parterne”

1.3 Har aftalt følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder.

2 UNDERSKRIFT

2.1 Aftalen underskrives af begge parter, og er bindende fra signeringsdatoen.

2.2 Dokumentet er underskrevet via ECIT Sign.

På vegne af den dataansvarlige:	På vegne af databehandleren:
Navn: [NAVN]	Navn: Frants Moraitis
Stilling: [STILLING]	Stilling: Managing Director
Telefonnummer: [+45 TELEFONNUMER]	Telefonnummer: +45 71 99 11 22
E-mail: [E-mail]	E-mail: support@intect.io Att: Managing Director

3 KONTAKTPERSONER HOS DEN DATAANSVARLIGE OG DATABEHANDLEREN

3.1 Parterne kan kontakte hinanden via nedenstående kontaktpersoner, om forhold vedrørende denne aftale.

3.2 Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

På vegne af den dataansvarlige:	På vegne af databehandleren:
Navn: [NAVN]	Navn: Signe K.
Stilling: [STILLING]	Stilling: Intect, DPO
Telefonnummer: [+45 TELEFONNUMER]	Telefonnummer: +45 71 99 11 22
E-mail: [E-mail]	E-mail: dpo@intect.io

4 PRÆAMBEL

4.1 Denne Databehandleraftale fastsætter Leverandørens (herefter "Databehandleren") rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af Kunden (herefter "den Dataansvarlige").

4.2 Denne Databehandleraftale 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).

Ydelserne:

4.3 Parterne har indgået en aftale om den Dataansvarliges **brug af Intect's Applikation**(-er) ("Tjenesterne").

4.4 I forbindelse med leveringen af Tjenesterne behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

4.5 Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem Parterne.

Bilag:

4.6 Der hører fire bilag til denne Databehandleraftale, og bilagene udgør en integreret del af denne Databehandleraftale.

Bilag A	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.
Bilag B	Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
Bilag C	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.
Bilag D	Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

Opbevaring af Databehandleraftalen

4.7 Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge Parter.

Overholdelse af gældende lov

4.8 Denne Databehandleraftale frigør ikke Databehandleren fra forpligtelser, som Databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

5 DEN DATAANSVARLIGES RETTIGHEDER OG FORPLIGTELSER

5.1 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 medlemsstaternes nationale ret og denne Databehandleraftale.

5.2 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.

5.3 Den Dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som Databehandleren instrueres i at foretage.

6 DATABEHANDLEREN HANDLER EFTER INSTRUKS

Behandling af personoplysninger

6.1 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.

6.2 Denne instruks skal være specificeret i denne Databehandleraftales bilag 12 A (Oplysninger om behandlingen) og bilag 12 C (Instruks vedrørende behandling af personoplysninger).

6.3 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 denne Databehandleraftale.

Instruks ved brug af Tredjeparts-app(s).

6.4 Tjenesterne er udviklet med åbent API, som gør det muligt for andre at udvikle og tilbyde apps, der kan kommunikere med Applikationen, herunder udveksle oplysninger på tværs af programmerne ("Tredjeparts-app(s)"). I det omfang den dataansvarlige vælger at installere og gøre brug af Tredjeparts-apps, der kan kommunikere med Applikationen, anses det for at udgøre en instruktion til databehandleren om, at der kan ske overførsel af de i Applikationen indtastede/indlæste og de af Applikationen generede oplysninger til sådanne Tredjeparters apps.

6.5 Den dataansvarlige accepterer desuden, at dennes Medarbejdere har mulighed for at installere og gøre brug af Tredjeparts-apps, der kan kommunikere og udveksle den enkelte Medarbejders adgang til oplysninger med Applikationen, og at sådan databehandling er omfattet af instruksen ifølge denne aftale.

Underretning ved ulovlige instrukser

6.6 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.

6.7 Hvis databehandleren er af den opfattelse, at udførelsen af instruksen fra den dataansvarlige højst sandsynlig vil være i strid med gældende lovgivning, skal databehandleren straks underrette den dataansvarlige herom. Hvis den dataansvarlige fastholder, at instruksen er i overensstemmelse med gældende lovgivning og fastholder, at instruksen skal udføres, kan databehandleren udføre instruksen uden at ifalde ansvar overfor den dataansvarlige, ligesom den dataansvarlige skal friholde databehandleren fra eventuelle tredjemands krav, herunder krav fra de registrerede, som følge af den udførte instruks.

6.8 Uanset Bestemmelse 4.8, er databehandleren ikke forpligtet til aktivt at efterprøve eller undersøge lovligheden af den dataansvarliges instrukser.

6.9 I det omfang den dataansvarlige giver instrukser til databehandleren, som efterfølgende viser sig at være ulovlige, er den dataansvarlige forpligtet til at friholde databehandleren for ethvert tab som følge heraf, herunder at friholde databehandleren for ethvert krav mod databehandleren, der følger heraf, inklusive bødekrav eller andre sanktioner, fra relevante myndigheder, samt krav fra øvrige tredjeparter, herunder de berørte datasubjekter, underdatabehandlere og databehandlerens øvrige samarbejdspartnere.

7 FORTROLIGHED

7.1 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.

7.2 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.

Påvisning af tavshedspligt for medarbejdere

7.3 Databehandleren skal efter anmodning fra den Dataansvarlige kunne påvise, at de pågældende personer, som er underlagt Databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

8 BEHANDLINGSSIKKERHED

8.1 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.

8.2 Den Dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder, som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici.

8.3 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.

Databehandlerens ansvar efter artikel 32

8.4 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.

8.5 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.

8.6 Databehandlerens bistand til den Dataansvarlige i relation til artikel 32

8.7 Derudover skal Databehandleren bistå den Dataansvarlige med vedkommendes overholdelse af den Dataansvarliges forpligtelse efter forordningens artikel 32, ved blandt andet 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.

8.8 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 denne Databehandleraftales bilag 12 C (Instruks vedrørende behandling af personoplysninger).

9 ANVENDELSE AF UNDERDATABEHANDLERE

9.1 Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2 og 4, for at gøre brug af en anden databehandler (en underdatabehandler).

Forudgående Generel godkendelse fra den Dataansvarlige

9.2 Databehandleren må ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.

9.3 Databehandleren har den Dataansvarliges **forudgående generelle godkendelse** til brug af underdatabehandlere.

9.4 Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst **to (2) ugers** varsel.

9.5 Databehandleren skal give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e).

9.6 Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B (Underdatabehandlere).

9.7 Den dataansvarlige anerkender, at databehandlerens Tjenester er standardiserede, cloud-baserede abonnementsydelser, der stilles til rådighed for et stort antal kunder, og at databehandleren derfor som udgangspunkt ikke kan imødekomme individuelle krav om fravalg af specifikke underdatabehandlere.

9.8 Såfremt den dataansvarlige har indsigelser mod tilføjelsen af en ny underdatabehandler, forpligter databehandleren sig til at vurdere indsigelsen loyalt og i god tro og undersøge, om der findes rimelige tekniske eller forretningsmæssige alternativer. Hvis det ikke er muligt at imødekomme indsigelsen, er den dataansvarlige berettiget til at opsige abonnementsaftalen med øjeblikkelig virkning. Ingen af parterne har krav mod hinanden i anledning heraf.

Brug af global leverandør

9.9 Hvis en global leverandør, såsom Microsoft, Google eller amazone, anvendes som underdatabehandler, accepterer den dataansvarlige, at det er den globale leverandørs til enhver tid gældende vilkår der er aftalt mellem parterne, som er grundlag for den globale leverandørs behandling af den dataansvarliges data, herunder i relation til krav til inspektion, audit, kontrol og dokumentation samt ansvar.

9.10 Link til de seneste vilkår for disse underdatabehandlere findes på den globale leverandørs hjemmeside.

Forpligtelser for underdatabehandlere

9.11 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 denne Databehandleraftale, 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 denne Databehandleraftale og databeskyttelsesforordningen.

9.12 Databehandleren er ansvarlig for at kræve, at underdatabehandleren som minimum overholder Databehandlerens forpligtelser efter denne Databehandleraftale og databeskyttelsesforordningen.

9.13 Der skal være indgået en Databehandleraftale (DPA) med alle relevante underleverandører, der præciserer deres forpligtelser og ansvar i henhold til databeskyttelseslovgivningen.

9.14 Databehandleren skal implementere en proces, der sikrer, at alle leverandører og underdatabehandlere fortsat overholder aftalens krav.

9.15 En tilsynsplan skal udarbejdes for at sikre, at relevante underdatabehandlere er underlagt passende overvågning.

Fremsendelse af underdatabehandleraftale og eventuelle ændringer

9.16 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 denne Databehandleraftale, er pålagt underdatabehandleren.

9.17 Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den Dataansvarlige.

10 OVERFØRSEL TIL TREDJELANDE ELLER INTERNATIONALE ORGANISATIONER

Overførsel af oplysninger

10.1 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.

Overførsel af oplysninger i henhold til EU-ret eller medlemsstaternes nationale ret

10.2 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.

10.3 Uden dokumenteret instruks fra den Dataansvarlige kan Databehandleren således ikke inden for rammerne af denne databehandleraftale:

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.

10.4 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 denne Databehandleraftales bilag C.

10.5 Denne Databehandleraftale skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og denne Databehandleraftale kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

11 BISTAND TIL DEN DATAANSVARLIGE

Forpligtelse til at bistå med at besvare anmodninger om udøvelsen af rettigheder

11.1 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.

11.2 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.

11.3 Såfremt den dataansvarlige ønsker databehandlerens bistand til de ydelser, der er beskrevet under Bestemmelse 11.2 (c), (d) og (e), stiller databehandleren sig til rådighed herfor. I det omfang bistanden går ud over, hvad der med rimelighed kan anses for sædvanligt og forventeligt, er databehandleren berettiget til at kræve et rimeligt vederlag herfor. Vederlaget fastsættes på baggrund af den tid, der medgår, og i overensstemmelse med de til enhver tid gældende timesatser, som fremgår af databehandlerens Generelle Vilkår og Betingelser.

Forpligtelse til at bistå med passende foranstaltninger

11.4 I tillæg til Databehandlerens forpligtelse til at bistå den Dataansvarlige i henhold til bestemmelse i punkt 8.7 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 **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 **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.

Angivelse af de fornødne tekniske og organisatoriske foranstaltninger

11.5 Parterne skal i denne Databehandleraftales bilag C (Instruks vedrørende behandling af personoplysninger) angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed

12 UNDERRETNING OM BRUD PÅ PERSONDATASIKKERHEDEN

12.1 Databehandleren underretter uden unødig forsinkelse den Dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

Tidspunkt for underretning

12.2 Databehandlerens underretning til den Dataansvarlige skal om muligt ske senest **48 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.

Bistand ved anmeldelse af brud på persondatasikkerheden

12.3 I overensstemmelse med bestemmelse i punkt 11.4, litra 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.

12.4 Parterne skal angive i bilag C (Instruks vedrørende behandling af personoplysninger), 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.

13 SLETNING OG RETURNERING AF OPLYSNINGER

Sletning eller tilbagelevering

13.1 Ved ophør af tjenesterne vedrørende behandling af personoplysninger er databehandleren forpligtet til at slette alle personoplysninger, der er behandlet på vegne af den dataansvarlige, forudsat at databehandleren har modtaget en **skriftlig instruks om sletning** fra den dataansvarlige.

13.2 Databehandleren handler som udgangspunkt efter instruks fra den dataansvarlige og foretager ikke sletning af personoplysninger uden forudgående, udtrykkelig og skriftlig instruks. Sletning kan dog ske uden særskilt instruks, hvis det følger af databehandlerens, de mellem parterne aftalte, og til enhver tid gældende generelle vilkår og betingelser. Det påhviler derfor den dataansvarlige som udgangspunkt at fremsende en skriftlig instruks, såfremt sletning ønskes gennemført i overensstemmelse med punkt 13.1.

13.3 Når sletning er sket efter instruks, skal databehandleren bekræfte dette skriftligt over for den dataansvarlige.

13.4 Såfremt databehandleren ikke modtager en skriftlig instruks om sletning af personoplysninger, vil databehandleren række ud til den dataansvarlige for at anmode om instruks. Hvis der ikke modtages svar fra den dataansvarlige inden for en rimelig tidsramme, vil databehandleren slette personoplysningerne i overensstemmelse med de gældende regler og bestemmelser i GDPR.

13.5 Følgende regler i EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedrørende behandling af personoplysninger, herunder, men ikke begrænset til:

a) **Bogføringsloven**, som kræver opbevaring af regnskabsmateriale i 5 år fra udgangen af det regnskabsår, materialet vedrører.

b) **Skatte- og afgiftslovgivningen**, herunder regler fra Skattestyrelsen, der kan stille krav til opbevaring af oplysninger til brug for dokumentation vedrørende løn, honorarer og skatteforhold.

c) **Arbejdsretlig lovgivning**, hvor opbevaring af visse oplysninger kan være nødvendig for at dokumentere ansættelsesforhold og overholde eventuelle forældelsesfrister i ansættelsesretlige tvister.

13.6 Databehandleren er forpligtet til alene at opbevare sådanne oplysninger i det omfang og så længe det er nødvendigt for at overholde disse forpligtelser og må ikke anvende oplysningerne til andre formål.

14 REVISION, HERUNDER INSPEKTION

Oplysninger der skal stilles til rådighed

14.1 Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og denne Databehandleraftale, 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.

14.2 Databehandleren er forpligtet til at afsætte de ressourcer, der er nødvendig(e) for, at den dataansvarlige eller dennes rådgiver/repræsentant kan gennemføre sin inspektion og/eller revision hos databehandleren eller dennes underdatabehandlere.

14.3 Databehandlerens udgifter i forbindelse med en fysisk inspektion og/eller en på vegne den dataansvarlige udført revision hos databehandleren eller dennes underdatabehandlere, afholdes af den dataansvarlige. Databehandlerens og/eller dennes underdatabehandleres tid godtgøres med de af databehandleren til enhver tid anvendte timsatser, som fremgår på databehandlerens Generelle Vilkår og Betingelser.

14.4 Procedurerne for den Dataansvarliges revisioner, herunder inspektioner, med Databehandleren og underdatabehandlere er nærmere angivet i denne Databehandleraftales bilag C.

Adgang til Databehandlerens faciliteter

14.5 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.

15 PARTERNES AFTALER OM ANDRE FORHOLD

15.1 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 denne Databehandleraftale eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

15.2 Databehandleren er ansvarlig for at behandle personoplysninger i overensstemmelse med denne aftale, instruksen og gældende databeskyttelseslovgivning, herunder Databeskyttelsesforordningen (GDPR). Databehandleren er alene ansvarlig for direkte tab, som den dataansvarlige lider som følge af databehandlerens væsentlige misligholdelse af sine forpligtelser i henhold til denne aftale eller gældende lovgivning. Databehandlerens samlede erstatningsansvar i henhold til denne aftale er begrænset til begrænset til det i abonnementsbetingelserne anførte, medmindre andet følger af ufravigelig lovgivning. Uanset ovenstående gælder ansvarsbegrænsningen ikke i det omfang, den ville medføre en indskrænkning af de registreredes rettigheder eller frihedsrettigheder i henhold til databeskyttelsesforordningen.

16 IKRAFTTRÆDEN OG OPHØR

16.1 Denne Databehandleraftale træder i kraft på datoen for begge Parters underskrift heraf.

16.2 Denne Databehandleraftale er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan denne Databehandleraftale ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem Parterne.

16.3 Begge Parter kan kræve denne Databehandleraftale genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i denne Databehandleraftale giver anledning hertil.

16.4 Parterne forpligter sig til i god tro at drøfte eventuelle indsigelser og tilstræbe at finde en gensidigt acceptabel løsning ved genforhandling af Databehandleraftalen.

16.5 Parterne har ret til at opsige aftalen med virkning fra ønsket ikrafttræden, såfremt ændringerne ikke kan accepteres. Ingen af parterne har krav mod hinanden i anledning heraf.

BILAG

BILAG A OPLYSNINGER OM BEHANDLINGEN

A.1. FORMÅLET MED DATABEHANDLERENS BEHANDLING AF PERSONOPLYSNINGER PÅ VEGNE AF DEN DATAANSVARLIGE

1. Databehandleren stiller på abonnementsbasis software som en service (SaaS) tjenester ("Tjenester") til rådighed for den Dataansvarlige og dennes medarbejdere. Tjenesterne kan dels tilgås via databehandlerens hjemmeside, og dels via databehandlerens applikationer.
2. Den Dataansvarliges brug af databehandlerens cloud-baserede Tjenester sker ved den Dataansvarliges selvbetjening via Databehandlerens hjemmeside, og/eller via Databehandlerens app. Den dataansvarliges medarbejdere kan ligeledes tilgå deres egne oplysninger, så som lønsedler, fraværsoversigter, ferieoversigter, og de dokumenter, som medarbejderen eller kunden har indlæst, eksempelvis ansættelseskontrakt. Både den dataansvarliges og dennes medarbejderes brug kræver et bruger ID og en unik adgangskode.

A.2. DATABEHANDLERENS BEHANDLING AF PERSONOPLYSNINGER PÅ VEGNE AF DEN DATAANSVARLIGE DREJER SIG PRIMÆRT OM (KARAKTEREN AF BEHANDLINGEN)

1. Databehandleren behandler personoplysninger på vegne af den Dataansvarlige som led i leveringen af databehandlerens Tjenester.
2. Databehandlerens behandling af personoplysninger vedrører primært håndtering af Tjenester til at behandle den dataansvarliges:
    a. Lønadministration
    b. HR-administration
    c. Dataintegration/-konsolidering/BI
3. Desuden varetager databehandleren drift, test, vedligeholdelse, udvikling samt fejlretning af de leverede Tjenester.
4. En behandling kan omfatte enhver håndtering af personoplysninger, herunder indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse herunder support.
5. Databehandleren indsamler, opbevarer, analyserer og anvender personoplysninger om både den Dataansvarlige og dennes kunder med det formål at udstede fakturaer, modtage betalingsoplysninger fra betalingsformidlere samt videregive relevante oplysninger til den Dataansvarlige.

A.3. BEHANDLINGEN OMFATTER FØLGENDE TYPER AF PERSONOPLYSNINGER OM DE REGISTREREDE

1. De typer af personoplysninger, som behandles via applikationen, afhænger af den enkelte kunde samt slutbrugerens brug.
2. Behandling af særlige kategorier af personoplysninger, jf. databeskyttelsesforordningens artikel 9, foretages alene, hvis kunden eller slutbrugeren selvstændigt vælger at indtaste sådanne oplysninger i applikationen, hvilket sker under kundens fulde ansvar og kontrol. Applikationen er ikke designet eller tiltænkt til behandling af særlige kategorier af oplysninger. Det kan dog ikke udelukkes, at slutbrugere eller kunden indtaster sådanne oplysninger i fritekstfelter.
3. Typer af personoplysninger, der behandles i sammenhæng med levering af ydelsen, behandlingen af personoplysninger via applikationen varierer derfor afhængigt af brug.

4. De personoplysninger, som behandles af databehandleren i forbindelse med den dataansvarliges brug af databehandlerens Tjenester er forskellige alt efter hvilken kategori den registrerede tilhører, jf. følgende oversigt:

Tabel 1: Tabel A3 - Behandling af personoplysninger

KATEGORIER AF DATA SUBJEKTER	PERSONOPLYSNINGER
Kunder (Dataansvarlig)	• Kontaktpersoner hos den dataansvarlige, herunder disses kontaktoplysninger, så som telefon, email, titel, afdeling, adresse • CVR-nummer
Den dataansvarliges nuværende og tidligere medarbejdere	**Almindelige oplysninger:** Identifikationsoplysninger: • Navn, adresse, telefonnummer, fødselsdato, E-mail -privat og firma, medarbejder-ID, kundenummer Andre oplysninger: • Arbejdssted og tjenstlige forhold • Billede • Bil • Sprogpræference • Tids- og fraværsregistreringer **Fortrolige oplysninger:** • CPR-nummer • Oplysninger om strafbare forhold, herunder straffeattest • Pas og kørekort • Oplysninger om sociale problemer • Oplysninger skilsmisse **Økonomiske oplysninger:** • betalingskortoplysninger, skat, ferieafregning, pensionsafregning, bankkonto, løndata
Partnere	• Navn • Adresse • CVR-nummer • Kontaktoplysninger • Kontaktpersoner hos Support, herunder disses kontaktoplysninger, så som telefon, e-mail, titel, afdeling, adresse
Oplysninger relateret til brugeraktivitet	• IP-adresser, revisionsspor og logdata • Købshistorik • Cookie ID

A.4. BEHANDLINGEN OMFATTER FØLGENDE KATEGORIER AF REGISTRERETE

1. Se oversigten i A3.

A.5. DATABEHANDLERENS BEHANDLING AF PERSONOPLYSNINGER PÅ VEGNE AF DEN DATAANSVARLIGE KAN PÅBEGYNDES EFTER DISSE BESTEMMELSERS IKRAFTTRÆDEN.

1. Denne Databehandleraftale er gældende, så længe Databehandleren behandler personoplysninger på vegne af den Dataansvarlige i overensstemmelse med hovedaftalen.

BILAG B UNDERDATABEHANDLERE

B1 GODKENDTE UNDERDATABEHANDLERE

1. Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere i nedenstående tabel.
2. Seneste opdatering af underdatabehandlere er foretaget: **01-08-2025**.

B2 VARSEL FOR GODKENDELSE AF UNDERDATABEHANDLERE

1. Varslingsperioden for godkendelse af underdatabehandlere fremgår af afsnit 9.

Generelt:

Tabel 2: Generelle underdatabehandlere

Underdatabehandler	Lokation	Virksomheds ID	Behandlingsaktivitet
ECIT A/S	NO	Rolfsbuktveien 2 1364 Fornebu Norge	Back-office services
ECIT Services A/S	EU	Hørkær 12A, DK-2730 Herlev DK36495022	Udviklings- og supportassistance
ECIT Solutions A/S	DK	Rudolfgårdsvej 1B DK-8260 Viby J Denmark DK28843151	Hosting af data Udviklings- og supportassistance Fysisk sikkerhed
Hubspot Ireland Limited	EU	1 Sir John Rogerson's Quay Dublin 2, Dublin 2, Ireland IE515723	Marketing og kundehåndtering
JetBrains	EU	Kavčí Hory Office Park, Na Hřebenech II 1718/8, Praha 4 - Nusle, 140 00, Czech Republic	Projektstyring i udvikling, herunder projektstyring ved 2nd line support.
Microsoft Ireland Operations Ltd	EU	One Microsoft Place, South County Business Park Leopardstown, Dublin 18, D18 P521 Ireland IE8256796U	Hosting af data i Azure, arkivering af data i Sharepoint og mailhåndtering
Visma e-conomic A/S	EU	Langebrogade 1, DK1411 København K DK29403473	Salgsfakturering
ZENDESK Inc.	EU	Njalsgade 72C 1205 København Denmark DK30801830	Kundesupport og engagement
Twilio Inc.	EU	Unter den Linden 10 10117 Berlin Germany IE3335493BH	Systemnotifikationer -og systememails.

Intect Payroll

Tabel 3: Intect HR - underdatabehandlere

Underdatabehandler	Lokation	Virksomheds ID	Behandlingsaktivitet
e-Boks A/S	DK	Hans Bekkevolds Allé 7, DK-2900 Hellerup, DK25674154	Elektronisk post primært til levering af lønsedler til dataansvarliges ansatte
Skatteforvaltningen	DK	Brændgårdvej 10, DK-7400 Herning, DK19552101	Rapportering af person- og løndata
Danmarks Statistik	DK	Sejrøgde 11, DK-2100 København Ø, DK17150413	Rapportering af lønstatistik
POSTNORD STRÅLFORS A/S	EU	Hedegaardsvej 88 DK-2300 København S Denmark DK10068657	Distribution af elektronisk post til e-boks og Kivra i Sverige
Visma LogBuy ApS	DK	Gærtorvet 3 DK-1799 København V Danmark DK29912971	Indkøbstjenester, der specialiserer sig i at sikre rabatter gennem gruppeindkøb.
Mastercard payment services DK A/S	DK	Lautrupbjerg 10, 2750 Ballerup Denmark DK40695869	Anmodning om pengeoverførsler via kundens bankkonto og overførsel af oplysninger til modtageren af pengeoverførslen
MDC DATA GREENLAND ApS	GL	Imaneq 1, DK-3900 Nuuk DK21717584	Behandling begrænset til grønlandske virksomheder
Repenso ApS	GL	Imaneq 30, DK-3900 Nuuk DK12926626	Support af grønlandske virksomheder

Intect Flow

Tabel 4: Underdatabehandlere - Intect Flow

Underdatabehandler	Lokation	Virksomheds ID	Behandlingsaktivitet
TS NoCode ApS	DK	Blokken 15 1 DK-3460 Birkerød Denmark DK37114898	Processoftware til datastyring.
ECIT Automate ApS	DK	Rudolfgårdsvej 1b DK-8260 Viby J Denmark DK39302284	Support og udvikling af Intect Flow.

Intect Expense

Tabel 5: Underdatabehandlere - Intect Expense

Underdatabehandler	Lokation	Virksomheds ID	Behandlingsaktivitet
ADATO AS	EU	Rolfsbuktveien 2 NO-1364 Fornebu Norway NO:995 221 608	Integrationstjenester og behandling af udgifter og kilometergodtgørelse.

Intect HR

Tabel 6: Underdatabehandlere Intect HR

Underdatabehandler	Lokation	Virksomheds ID	Behandlingsaktivitet
Verismo Systems AB	EU	Regeringsgatan 79 111 39 Stockholm, Sweden Org.nr556767-2067	Human Resource Management

BILAG C INSTRUKS VEDRØRENDE BEHANDLING AF PERSONOPLYSNINGER

C.1. BEHANDLINGENS GENSTAND/INSTRUKS

1. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører behandlingsaktiviteterne som er beskrevet i bilag A.

C.2. BEHANDLINGSSIKKERHED

1. Databehandleren er forpligtet til at implementere alle nødvendige tekniske og organisatoriske foranstaltninger i overensstemmelse med databeskyttelsesforordningens artikel 32 for at sikre et højt sikkerhedsniveau.
2. Foranstaltningerne skal tage højde for det aktuelle teknologiske niveau, implementeringsomkostninger, behandlingens karakter, omfang, sammenhæng og formål samt de risici, som behandlingen udgør for registreredes rettigheder og frihedsrettigheder.
3. Databehandleren skal dog løbende evaluere disse foranstaltninger og sikre overholdelse af ISAE3000 eller et tilsvarende rammeværk.
4. Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etablere det nødvendige (og aftalte) sikkerhedsniveau.
5. Hvis den dataansvarlige anmoder om oplysninger vedrørende sikkerhedsforanstaltninger, dokumentation eller andre typer oplysninger om, hvordan databehandleren behandler personoplysninger, og disse oplysninger går ud over de standardoplysninger, som den dataansvarlige normalt stiller til rådighed for at opfylde gældende lovgivning om behandling af personoplysninger som databehandler, og dette medfører ekstra arbejde for databehandleren, er databehandleren berettiget til at kræve betaling fra den dataansvarlige for dette ekstra arbejde.
6. Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

Tabel 7: Tekniske foranstaltninger

Tekniske foranstaltninger:	Beskrivelse:
Adgangsstyring	Adgangen til personoplysninger og systemer begrænses efter need-to-know-princippet, således at kun medarbejdere med et arbejdsbetinget behov får adgang til de relevante data. Adgangsrettigheder tildeles individuelt og gennemgås løbende for at sikre, at de er opdaterede og passende i forhold til den enkelte medarbejders arbejdsopgaver. Alle brugere har unik adgang i form af individuelle brugernavne og adgangskoder, som oprettes og håndteres efter alment anerkendte sikkerhedsprincipper. To-faktor-autentificering (2FA/MFA) benyttes, hvor det er muligt, for at styrke sikkerheden. Adgangen til personoplysninger er endvidere begrænset til autoriserede medarbejdere, som er instrueret i at handle i overensstemmelse med kundens instrukser og gældende databeskyttelseslovgivning.
Kryptografi	Databehandleren skal sikre, at følsomme personoplysninger altid beskyttes mod uautoriseret adgang under overførsel og opbevaring. Al kommunikation, der involverer følsomme personoplysninger, skal ske over sikre, krypterede forbindelser.

	Overføres sådanne oplysninger uden for databehandlerens kontrollerede netværk, skal de som minimum være beskyttet ved stærk kryptering. Hvor det er relevant og muligt, anvender databehandleren også pseudonymisering eller anonymisering for at begrænse risikoen ved behandling og opbevaring af personoplysninger.
Driftssikkerhed	Databehandleren skal sikre, at der implementeres passende driftsikkerhed for at beskytte systemer og data mod trusler som virus, malware og uautoriseret adgang. Dette omfatter følgende foranstaltninger: • Antivirus • Fysisk firewall • Central bruger- og gruppestyring • Overvågning • VPN • Patching • Anvendelse af sikrede forbindelser • Separate administratorkonti Anskaffelse, udvikling og vedligeholdelse af systemer: • Proces for sikker udvikling Lagring af data og krypteret backup • Onsite backup (point-in-time) • Offsite backup • Backup er krypteret.
Kommunikationssikkerhed	Beskyttelse og opdeling af netværk Etablerede sikre kommunikationsformer
Styring af informationssikkerhedsbrud og brud på persondatasikkerheden	Databehandleren skal implementere en incident response-plan til effektiv håndtering af persondatasikkerhedsbrud. Denne proces skal sikre, at alle hændelser identificeres, vurderes og håndteres hurtigt og korrekt. Der skal desuden være en proces for underretning af den dataansvarlige, som sikrer, at den dataansvarlige informeres uden unødig forsinkelse, og at alle nødvendige oplysninger om hændelsen videregives, herunder omfanget, risici og de trufne foranstaltninger.
Audit logs	Der skal føres auditlogs over systemadgange og aktiviteter, herunder logdata.. Alle ændringer, der vedrører behandlingen af persondata, skal også logges. Det er nødvendigt at have aktive systemlogs på alle endpoint-enheder samt servere for at sikre, at alle relevante aktiviteter overvåges og kan efterprøves ved behov.

Tabel 8: Organisatoriske foranstaltninger

Organisatoriske foranstaltninger:	
Informationssikkerhedspolitikker	Overordnede retningslinjer og krav til informationssikkerhed.
Organisering af informationssikkerhed	Databehandleren har udpeget en DPO. Medarbejdere, kunder og andre interessenter kan kontakte Intects Data Protection Officer på dpo@intect.io Der er desuden etableret et Compliance team, som har til opgave at overvåge og styre databeskyttelsen i Intect.
Medarbejdersikkerhed	Databehandleren har etableret procedurer for at sikre, at medarbejdere, der behandler personoplysninger, er egnede og betroede. Dette omfatter • Baggrundstjek, herunder gennemgang af straffeattest hvor relevant, før ansættelse i relevante stillinger. • Alle medarbejdere underskriver fortrolighedserklæringer • Medarbejdere gennemfører regelmæssig GDPR awareness-træning i informationssikkerhed og databeskyttelse for at sikre forståelse og efterlevelse af gældende regler og interne politikker. • Faste procedurer for medarbejderens livscyklus.
Fysisk sikring og miljøsikring	Databehandleren forpligter sig til at opretholde passende fysisk sikring og miljøsikring på de lokationer, hvor der behandles eller opbevares personoplysninger, herunder datacentre og eventuelle kontoradresser. Adgang til fysiske lokaliteter, hvor behandlingen af personoplysninger finder sted, er begrænset til autoriserede personer og beskyttet gennem adgangskontrolsystemer såsom nøglekort, alarmer, overvågning eller tilsvarende mekanismer. Databehandleren skal sikre, at fysiske adgangsveje, herunder hovedindgange, serverrum og andre relevante områder, er beskyttet mod uautoriseret adgang, indtrængen og miljømæssige påvirkninger såsom brand, vand- og strømforstyrrelser. I det omfang fysisk sikkerhed og miljøsikring helt eller delvist er outsourcet til tredjepart, forpligter databehandleren sig til at sikre, at sådanne underleverandører efterlever tilsvarende sikkerhedsniveau og krav, som følger af denne aftale og gældende databeskyttelseslovgivning.
Enhedsstyring	Databehandleren har implementeret politikker for sikker håndtering, opbevaring og vedligeholdelse af alt fysisk udstyr for at minimere risikoen for datatab og uautoriseret adgang. Databehandleren fører en fortegnelse over IT-udstyr, der anvendes til behandling af personoplysninger. Ved ophør af ansættelse skal udstyr returneres og kontrolleres.

	Al data på returneret udstyr slettes i overensstemmelse med interne politikker, og udstyr, der tages permanent ud af drift, destrueres og data slettes sikkert. Udstyr skal opbevares forsvarligt uden for arbejdstid og under transport. Al adgang til netværk og systemer fra enheder styres centralt. Mistet eller stjålet udstyr skal straks indrapporteres, hvorefter passende sikkerhedsforanstaltninger iværksættes, herunder fjernsletning.

C.3 BISTAND TIL DEN DATAANSVARLIGE

1. 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 sådanne tekniske og organisatoriske foranstaltninger, som kan bidrage til den dataansvarliges mulighed for at besvare anmodninger om udøvelsen af de registreredes rettigheder

OPBEVARINGSPERIODE/SLETTERUTINE

1. Ved ophør af Aftalen vedrørende behandling af personoplysninger, skal Databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med afsnit 11.

LOKALITET FOR BEHANDLING

1. Behandling af personoplysninger omfattet af nærværende bestemmelser foretages på databehandlerens egne adresser samt hos godkendte underdatabehandlere.
2. Den Dataansvarlige giver instruks til, at personoplysninger behandles af de underdatabehandlere, der er nævnt i bilag B, samt på de pågældende lokationer heri.
3. Behandling af personoplysninger kan desuden finde sted via fjernarbejde, såfremt dette sker i overensstemmelse med databehandlerens interne politik for fjernarbejde.

C.6 INSTRUKS VEDRØRENDE OVERFØRSEL AF PERSONOPLYSNINGER TIL TREDJELANDE

1. Databehandleren tilstræber, at personoplysninger behandles og opbevares inden for EU/EØS. Overførsel af personoplysninger uden for EU/EØS finder som udgangspunkt ikke sted.
2. I enkelte tilfælde kan personoplysninger overføres til Grønland, men alene i relation til behandling af oplysninger om grønlandske virksomheder og i overensstemmelse med den Dataansvarliges instruks.
3. Underdatabehandlere i Grønland er alene involveret i behandling af data for grønlandske virksomheder og efterlever relevante databeskyttelses-krav for den pågældende behandling.

C.7 PROCEDURER FOR DEN DATAANSVARLIGES REVISIONER, HERUNDER INSPEKTIONER, MED BEHANDLINGEN AF PERSONOPLYSNINGER, SOM ER OVERLADT TIL DATABEHANDLEREN

1. Databehandleren skal årligt og uden særskilt vederlag foranledige udarbejdelse af en revisionserklæring omhandlende Databehandlerens informationssikkerhedsniveau, og hvilke foranstaltninger Databehandleren har truffet. Revisionserklæringen skal indeholde en gennemgang af etablerede ledelsessystemer og en afrapportering af effekten heraf samt den udpegede tredjemands anmærkninger.
2. Erklæringen er udarbejdet af en uafhængig tredjepart vedrørende Databehandlerens og underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse bestemmelser.
3. Der er enighed mellem parterne om, at følgende typer af certifikat kan anvendes i overensstemmelse med disse Bestemmelser:
    a. ISAE3000
4. Såfremt der ønskes udarbejdet en ISO27001/ISO27701 eller ISAE3402 revisorerklæring sker dette for den dataansvarliges regning.
5. Certifikatet fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i auditeringen og kan i sådanne tilfælde anmode om en ny auditering for egen regning under andre rammer og/eller under anvendelse af anden metode.
6. Baseret på resultaterne af auditeringen, 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.

Fysisk inspektion

7. Den dataansvarlige eller dennes repræsentant har ret til at gennemføre inspektioner af de fysiske lokaliteter og systemer, hvorfra databehandleren behandler personoplysninger. Fysiske inspektioner kan dog alene finde sted på databehandlerens erhvervsmæssige adresser.
8. For at anmode om at foretage en kontrol skal den Dataansvarlige fremsende en detaljeret kontroloversigt mindst tredive (30) kalenderdage forud for den foreslåede kontroldato til Databehandleren med beskrivelse af det foreslåede omfang, varighed og starttidspunkt for kontrollen.
9. Den Dataansvarlige accepterer at afholde alle omkostninger forbundet med sådanne inspektioner og accepter:
    a. I alle tilfælde skal kontroller foretages inden for normal arbejdstid på det pågældende sted, i medfør af Databehandlerens politikker, og må ikke på urimelig måde gribe forstyrrende ind i Databehandlerens forretningsdrift.
    b. Vederlaget til Databehandleren i henhold til det ovenstående beregnes på grundlag af det tidsforbrug, Databehandleren anvender på fremskaffelsen af informationen, og efter medgået tid (T&M) til timepriserne angivet i databehandlerens Generelle Vilkår og Betingelser.
    c. Databehandleren har derudover krav på, at den Dataansvarlige dækker eventuelle eksterne omkostninger afholdt af Databehandleren til fremskaffelse af informationen, herunder omkostninger afholdt til eventuelt fornøden bistand fra underdatabehandlere.

C.8 PROCEDURER FOR REVISIONER, HERUNDER INSPEKTIONER, MED BEHANDLING AF PERSONOPLYSNINGER, SOM ER OVERLADT TIL UNDERDATABEHANDLERE

1. Databehandleren indhenter på baggrund af en risikovurdering årligt dokumentation for relevante underdatabehandleres overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse bestemmelser. Der er enighed mellem parterne om, at processen for gennemførelse, og tilstrækkeligheden heraf, dokumenteres via den Dataansvarliges revision af Databehandleren jf. C.7.
2. Hvis yderligere information vedrørende underdatabehandleres overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse bestemmelser skal leveres til den Dataansvarlige, vil Databehandleren, for den Dataansvarliges regning, indhente den, efter skriftlig aftale, fornødne og tilgængelige dokumentation hos underdatabehandlere.

BILAG D PARTERNES REGULERING AF ANDRE FORHOLD

1. Øvrige forhold reguleres i hovedaftalen mellem parterne.

ÆNDRINGER

VERSION	DATO	INITIALER	ÆNDRINGER
1.0	Dato: 01-05-2025	SK	Oprettet
1.025	Dato: 01-08-2028	SK	Ændringer i: - Parterne og underskrifter er flyttet frem i dokumentet - Afsnit 9 (Anvendelse af underdatabehandlere) - Afsnit 13 (Sletning og returnering af oplysninger) - Indsat 15.2 - Bilag ABC opdateret i helhed