ÆNDRINGSLOG

VERSION	DATO	FORFATTER (INITIALER)	ÆNDRINGER	GODDKENDT AF
1.1	X	Datatilsynet	Ændringer i Bestemmelserne 7.7., 9.2., 10.4. og Bilag C.8. *(Tastefejl og opdaterede krydshenvisninger).*	Intect
1.2	X	Datatilsynet	Ændringer i Bestemmelse 7.6 *(Bestemmelsen er gjort valgfri og ordlyden er blevet modificeret)*	Ikke implementeret
1.2	01-05-2026	Intect (SK)	Offentliggjort	Intect Management
1.25	01-08-2025	Intect (SK)	Ændringer til: • Parterne og underskrifterne er flyttet til begyndelsen af dokumentet. • Afsnit 9 (Anvendelse af underdatabehandlere). • Afsnit 13 (Sletning og tilbagelevering af data). • Indsættelse af klausul 15.2. Bilag A, B og C er alle opdateret i deres helhed.	Intect Management
1.26	01-10-2026	Intect (SK)	Ændringer til: • Design Følgende er tilføjet: • Afsnit 4.3 • Afsnit 11.2 • Afsnit A3.1 • Afsnit C.4.5 – Lovpligtig opbevaring • Afsnit C.7. 1., 2., 7., 8. ,12., 14., 17 – Revision Følgende formuleringer er ændret: • Afsnit 2.4 • Afsnit B.1 – Link til underdatabehandlere via Trust Center • Afsnit D.1–D.4	Intect Management

Standardkontraktsbestemmelser

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

2. Denne Databehandleraftale indgås mellem Intect ApS, CVR. 37035084 (herefter benævnt "Databehandleren") og den kunde, der har indgået aftale med Intect om anvendelse af Intects ydelser (herefter benævnt "den Dataansvarlige") der hver især er en ”part” og sammen udgør ”parterne”

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

Underskrift

1. Denne databehandleraftale indgås og underskrives elektronisk som led i etableringen af aftaleforholdet mellem Kunden og Intect.

2. Kundens elektroniske accept af denne databehandleraftale udgør Kundens underskrift på aftalen.

Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

På vegne af databehandleren:
Navn: Signe K.
Stilling: Intect, DPO
Telefonnummer: +45 71 99 11 22
E-mail: dpo@intect.io

1. Indhold

ÆNDRINGSLOG....1
Kontaktpersoner hos den dataansvarlige og databehandleren....2
2. Præambel....4
3. Den dataansvarliges rettigheder og forpligtelser....5
4. Databehandleren handler efter instruks....5
5. Fortrolighed....5
6. Behandlingssikkerhed....6
7. Anvendelse af underdatabehandlere....7
8. Overførsel til tredjelande eller internationale organisationer....8
9. Bistand til den dataansvarlige....8
10. Underretning om brud på persondatasikkerheden....10
11. Sletning og returnering af oplysninger....11
12. Revision, herunder inspektion....11
13. Parternes aftale om andre forhold....11
14. Ikrafttræden og ophør....12
Bilag A Oplysninger om behandlingen....13
Bilag B Underdatabehandlere....15
Bilag C Instruks vedrørende behandling af personoplysninger....17
Bilag D Parternes regulering af andre forhold....24

2. Præambel

1. Denne aftale er baseret på Datatilsynets standardkontraktbestemmelser (SCC) for databehandleraftaler og er tilpasset med henblik på at understøtte Parternes overholdelse af gældende databeskyttelseslovgivning.Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.

2. Disse kontraktbestemmelser (Bestemmelserne) fastsætter den dataansvarliges og databehandlerens rettigheder og forpligtelser, når databehandleren behandler personoplysninger på vegne af den dataansvarlige.

3. 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).

Tjeneste

4. Databehandleren leverer de ydelser, der er beskrevet i Hovedaftalen og/eller de generelle vilkår mellem parterne, og vil med henblik på at opfylde Hovedaftalen behandle databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

5. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

Bilag:

6. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

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

Opbevaring af Databehandler Aftalen

7. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

Overholdelse af gældende lovgivning

8. 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 medlemsstaternes[1] 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.

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

Behandling af personoplysninger

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.

3. Håndtering af ulovlige instrukser er beskrevet i C.1.

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.

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

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.

Dokumentation for medarbejderes tavsheds- og fortrolighedspligt

3. 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.

Databehandlerens ansvar i henhold til artikel 32

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.

Databehandlerens bistand til den dataansvarlige i relation til artikel 32

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).

Forudgående generel godkendelse

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 **FORUDGÅENDE GENERELLE GODKENDELSE** til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst **10 KALENDERDAGE** varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e).

Liste over underdatabehandlere (ROSP)

4. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

Underdatabehandleres forpligtelser

5. 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.

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

Fremsendelse af underdatabehandleraftalen og eventuelle ændringer

8. 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.

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

8. Overførsel til tredjelande eller internationale organisationer

Overførsel af personoplysninger

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 personoplysninger i henhold til EU-retten eller medlemsstaternes nationale ret

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.

3. 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

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 bilag C.6.

5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser 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

Besvarelse af anmodninger om udøvelse af registreredes rettigheder

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

Forpligtelse til at bistå med passende foranstaltninger

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 unødig forsinkelse og om muligt senest **72 TIMER**, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, **DATATILSYNET** medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

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

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

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

Beskrivelse af de nødvendige tekniske og organisatoriske foranstaltninger

3. 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 unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

Tidsfrist for underretning

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.

Bistand ved anmeldelse af brud på persondatasikkerheden

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

Sletning eller returnering

1. Ved ophør af tjenesterne 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 EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

2. Sletning eller tilbagelevering er beskrevet i bilag C.4.

12. Revision, herunder inspektion

Oplysninger, der skal stilles til rådighed

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. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmeret 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

Ikrafttrædelse

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift af HOVEDAFTALEN.

Genforhandling

2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

3. Parterne forpligter sig til i god tro at drøfte eventuelle indsigelser og bestræbe sig på at finde en gensidigt acceptabel løsning gennem genforhandling af Databehandleraftalen.

4. Parterne har ret til at opsige Aftalen med virkning fra den ønskede ikrafttrædelsesdato, hvis ændringerne ikke kan accepteres. Ingen af Parterne kan i den forbindelse gøre krav gældende mod den anden Part.

Varighed

5. 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.

Ophør

6. 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 **skriftlig varsel** af begge parter.

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 data-ansvarliges 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. Alle personoplysninger, som databehandleren får adgang til, skal behandles fortroligt.

2. De typer af personoplysninger, som behandles via applikationen, afhænger af den enkelte kunde samt slutbrugerens brug.

3. 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.

4. Typer af personoplysninger, der behandles i sammenhæng med levering af ydelsen, behandlingen af personoplysninger via applikationen varierer derfor afhængigt af brug.

5. 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 registrerede

1. Se oversigten i A3.

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

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

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

1. Ved underdatabehandling i henhold til denne aftale forstås ydelser, der har direkte tilknytning til leveringen af tjenesten. Dette omfatter ikke hjælpeydelser såsom telekommunikationstjenester, post- og transporttjenester, vedligeholdelses- og brugersupporttjenester eller bortskaffelse af datamedier samt andre foranstaltninger til sikring af fortroligheden, tilgængeligheden, integriteten og robustheden af hardware og software på databehandlingsudstyr.

2. Databehandleren skal vedligeholde en ajourført liste over godkendte underdatabehandlere på sin hjemmeside. Den dataansvarlige anerkender og accepterer, at offentliggørelse af opdateringer til denne liste på hjemmesiden udgør underretning om ændringer i underdatabehandlere i henhold til denne aftale.

3. Opdateringer af listen offentliggøres på hjemmesiden, og den dataansvarlige underrettes herom via e-mail eller en anden aftalt kommunikationskanal.

4. Listen over underdatabehandlere, der allerede er godkendt af den dataansvarlige, findes på Intect Trust Center (underdatabehandlere)

5. Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af anførte underdatabehandlere for den beskrevne behandlingsaktivitet.

B.2. Varsel for godkendelse af underdatabehandlere

1. Databehandleren har den dataansvarliges GENERELLE GODKENDELSE til at gøre brug af underdatabehandlere i overensstemmelse med klausul 7.2.

2. Enhver underretning, der kræves i henhold til denne aftale, skal ske i overensstemmelse med klausul 7.3.

3. For god ordens skyld (fra klausul 7.3):

> Databehandleren har den dataansvarliges **FORUDGÅENDE GENERELLE GODKENDELSE** til brug af underdatabehandlere.
>
> Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst **10 KALENDERDAGE** varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e).

4. Databehandleren skal dermed give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer, inden de pågældende underdatabehandlere tages i brug.

5. 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.

6. 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 HOVEDAFTALEN med øjeblikkelig virkning. Ingen af parterne har krav mod hinanden i anledning heraf.

7. Hvis den dataansvarlige ikke har gjort indsigelse mod ændringen af en underdatabehandler eller inddragelsen af en ny underdatabehandler inden for den fastsatte frist, anses underdatabehandleren for at være godkendt.

8. Hvis ændringen af listen over underdatabehandlere indebærer tilføjelse af en underdatabehandler i et tredjeland, skal den dataansvarlige underrettes som aftalt i bilag C, punkt C.6.

Forpligtelser for underdatabehandlere

9. Der skal indgås en databehandleraftale (DPA) med alle relevante underdatabehandlere, hvori deres forpligtelser og ansvar i henhold til databeskyttelseslovgivningen specificeres.

10. Databehandleren skal implementere en proces, der sikrer, at alle leverandører og underdatabehandlere løbende overholder kravene i aftalen.

11. Der skal udarbejdes en tilsynsplan for at sikre, at relevante underdatabehandlere er underlagt passende tilsyn.

Brug af global leverandør

12. 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.

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

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 databehandle-ren udfører behandlingsaktiviteterne som er beskrevet i bilag A.

Instruks ved brug af Tredjeparts-app(s).

2. 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.

3. 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

4. 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. 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. Uanset ovenstående, er databehandleren ikke forpligtet til aktivt at efterprøve eller undersøge lovligheden af den dataansvarliges instrukser.

7. 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.

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 2: 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 3: 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 følgende tekniske og organisatoriske foranstaltninger.

2. Såfremt den dataansvarlige ønsker databehandlerens bistand til de ydelser, der er beskrevet under Bestemmelse 9.2 (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.

C.4 Opbevaringsperiode/sletterutine

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.

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 11.1.

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

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.

   Lovpligtig opbevaringspligt

5. Som databehandler behandler og opbevarer Intect udelukkende personoplysninger på vegne af og efter instruks fra den dataansvarlige. Eventuelle lovbestemte opbevaringsforpligtelser vedrørende løn-, bogførings- eller skattedokumentation påhviler som udgangspunkt den dataansvarlige.

C.5 Lokalitet for behandling

1. Behandlingen af personoplysninger, der er omfattet af disse klausuler, finder sted på databehandlerens egne lokationer samt hos godkendte underdatabehandlere.

2. Den dataansvarlige instruerer hermed om, at personoplysninger må behandles af de underdatabehandlere, der fremgår af Trust Center ved aftalens ikrafttræden, samt på de lokationer, der er angivet heri.

3. Den dataansvarlige accepterer hermed, at behandling af personoplysninger også kan finde sted i forbindelse med fjernarbejde, forudsat at behandlingen udføres i overensstemmelse med databehandlerens interne politik for fjernarbejde.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

1. Databehandleren skal bestræbe sig på at sikre, at personoplysninger behandles og opbevares inden for EU/EØS. Som hovedregel må overførsel af personoplysninger til lande uden for EU/EØS ikke finde sted.

2. I visse tilfælde kan personoplysninger overføres til Grønland, men udelukkende i forbindelse med behandling af oplysninger vedrørende grønlandske virksomheder og i overensstemmelse med den dataansvarliges instrukser.

3. Underdatabehandlere i Grønland må kun inddrages i behandlingen af oplysninger vedrørende grønlandske virksomheder og skal overholde de relevante databeskyttelseskrav, der gælder for den pågældende behandling.

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

1. Den dataansvarlige må ikke gennemføre mere end én revision inden for en periode på 12 måneder, medmindre:

   a) det kræves i henhold til gældende lovgivning,
   b) der er sket et brud på persondatasikkerheden, eller
   c) den dataansvarlige har rimelig grund til at mistænke væsentlig manglende overholdelse af denne aftale.

2. Omkostninger, som databehandleren afholder i forbindelse med en fysisk inspektion og/eller en revision, der gennemføres på vegne af den dataansvarlige hos databehandleren eller dennes underdatabehandlere, skal afholdes af den dataansvarlige. Databehandlerens og/eller dennes underdatabehandleres tidsforbrug honoreres i overensstemmelse med de til enhver tid gældende timesatser, som databehandleren anvender, og som fremgår af databehandlerens generelle vilkår og betingelser.

   Revisorerklæringer

3. 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.

4. 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.

5. Der er enighed mellem parterne om, at følgende typer af certifikat kan anvendes i overensstemmelse med disse Bestemmelser:

   ISAE3000

6. Såfremt der ønskes udarbejdet en ISO27001/ISO27701 eller ISAE3402 revisorerklæring sker dette for den dataansvarliges regning.

7. Certifikatet skal uden unødig forsinkelse stilles til rådighed for den dataansvarlige til orientering via databehandlerens Trust Center.

8. Den dataansvarlige kan gøre indsigelse mod revisionsrammen og/eller revisionsmetoden og kan i sådanne tilfælde anmode om en ny revision **for egen regning** efter andre revisionsrammer og/eller ved anvendelse af en anden metode.

9. 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

10. Den dataansvarlige eller dennes repræsentant(er), herunder repræsentanter, der handler på vegne af tilsynsmyndigheden, skal efter behørig legitimation have ret til at foretage inspektioner af de fysiske faciliteter og systemer, hvorfra databehandleren behandler personoplysninger.

11. Fysiske inspektioner må dog kun finde sted på databehandlerens forretningsadresser.

12. Inden den dataansvarlige anmoder om en inspektion på stedet, skal den dataansvarlige først gennemgå databehandlerens seneste revisionsrapporter, certificeringer og dokumentation for overholdelse af gældende krav. Inspektioner på stedet kan kun anmodes om, hvis denne dokumentation ikke i rimeligt omfang imødekommer den dataansvarliges betænkeligheder.

13. 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.

14. Databehandleren er forpligtet til at stille de nødvendige ressourcer til rådighed for at gøre det muligt for den dataansvarlige eller dennes rådgiver/repræsentant at gennemføre inspektionen og/eller revisionen hos databehandleren.

15. Den Dataansvarlige accepterer at afholde alle omkostninger forbundet med sådanne inspektioner og accepter:

16. 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.

17. Databehandleren kan kræve, at den eller de personer, der gennemfører revisionen, er underlagt en fortrolighedsaftale.

18. Det vederlag, som skal betales til databehandleren i henhold til ovenstående, beregnes på grundlag af den tid, databehandleren bruger på at fremskaffe oplysningerne, efter princippet om betaling for medgået tid og materialer (Time and Materials, T&M) og i overensstemmelse med de timesatser, der er angivet i databehandlerens generelle vilkår og betingelser.

19. Databehandleren er desuden berettiget til at kræve, at den dataansvarlige dækker eventuelle eksterne omkostninger, som databehandleren afholder for at fremskaffe oplysningerne, herunder omkostninger til nødvendig 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 underdata-behandleres 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 Databehandle-ren 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 skrift-lig aftale, fornødne og tilgængelige dokumentation hos underdatabehandlere.

Bilag D Parternes regulering af andre forhold

Versionsstyring og aftalernes indbyrdes forrang

1. Databehandleren forbeholder sig retten til løbende at foretage ændringer i aftalen, herunder præciseringer. Disse ændringer vil typisk være en følge af nye anbefalinger fra eksempelvis Datatilsynet eller Europa-Kommissionen samt ændringer i praksis og lovgivning på området.

2. Efter modtagelse af meddelelse om en ændring har den dataansvarlige **14 ARBEJDSDAGE** til at gøre indsigelse, hvis ændringen ikke med rimelighed kan accepteres.

3. Denne bestemmelse finder ikke anvendelse på ændringer i anvendelsen af underdatabehandlere, som er reguleret i aftalens afsnit 7.

Ansvarsbegrænsning

4. Parterne kan aftale andre klausuler vedrørende leveringen af tjenesten til behandling af personoplysninger, herunder eksempelvis bestemmelser om ansvar, forudsat at disse ikke direkte eller indirekte er i modstrid med klausulerne eller tilsidesætter den registreredes grundlæggende rettigheder eller frihedsrettigheder eller den beskyttelse, der følger af GDPR.

5. Databehandleren er ansvarlig for at behandle personoplysninger i overensstemmelse med denne aftale 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.

6. Databehandlerens samlede ansvar i henhold til denne aftale er begrænset til det beløb, der er angivet i databehandlerens generelle vilkår og betingelser, medmindre ufravigelig lovgivning foreskriver andet.

7. Uanset ovenstående finder ansvarsbegrænsningen ikke anvendelse i det omfang, den ville medføre en begrænsning af de registreredes rettigheder eller frihedsrettigheder i henhold til databeskyttelsesforordningen (GDPR).