Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

DATABEHANDLERAFTALE

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

mellem

Kunden

(herefter "den dataansvarlige")

og

Whistleblower Partners ApS
CVR Number: 43615661
Kultorvet 11, 4th floor
1175 Copenhagen
Denmark

(herefter "databehandleren")

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

HAR AFTALT følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder:

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

1. PRÆAMBEL

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

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

2. 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 samt 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.

3. DATABEHANDLEREN HANDLER EFTER INSTRUKS

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

2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

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

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

4. FORTROLIGHED

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

2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

3. Databehandleren må kun videregive personoplysninger, som behandles på den dataansvarliges vegne, i det omfang det følger af whistleblowerdirektivet, databeskyttelsesforordningen eller anden lovgivning.

5. 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. Afhængigt af deres relevans kan det omfatte:

   a. Pseudonymisering og kryptering af personoplysninger

   b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder, som behandlingen udgør, og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren, som gør vedkommende i stand til at identificere og vurdere sådanne risici.

3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved 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.

   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.

6. ANVENDELSE AF UNDERDATABEHANDLERE

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

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

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

3. Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 40 dage inden anvendelsen af den pågældende underdatabehandler. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

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

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

6. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som fx gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

7. OVERFØRSEL TIL TREDJELANDE ELLER INTERNATIONALE ORGANISATIONER

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.

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.

8. BISTAND TIL DEN DATAANSVARLIGE

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

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

   a. oplysningspligten ved indsamling af personoplysninger hos den registrerede

   b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede

   c. indsigtsretten

   d. retten til berigtigelse

   e. retten til sletning ("retten til at blive glemt")

   f. retten til begrænsning af behandling

   g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling

   h. retten til dataportabilitet

   i. retten til indsigelse

   j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

2. Databehandleren bistår 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 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.

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 8.1. og 8.2.

9. 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.

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

3. I overensstemmelse med Bestemmelse 8.2.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.

10. SLETNING OG RETURNERING AF OPLYSNINGER

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 dataansvarlige, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

11. REVISION, HERUNDER INSPEKTION

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.

2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i bilag C.7.

3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivning har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

12. PARTERNES AFTALE OM ANDRE FORHOLD

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om fx 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.

13. IKRAFTTRÆDEN OG OPHØR

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

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

3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 10.1 og bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

BILAG A – OPLYSNINGER OM BEHANDLINGEN

14. FORMÅLET MED DATABEHANDLERENS BEHANDLING AF PERSONOPLYSNINGER PÅ VEGNE AF DEN DATAANSVARLIGE

Formålet med behandlingen af personoplysninger er at modtage, opbevare og stille indberetninger til rådighed for sagsbehandlere, som er udpeget af den dataansvarlige til behandling af indberetninger som led i den dataansvarliges rådgivning i forbindelse med whistleblowerordninger, jf. whistleblowerdirektivet.

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

At modtage indberetninger fra slutbrugere samt at opbevare og stille indberetninger til rådighed for sagsbehandlere, som er udpeget af den dataansvarlige til at behandle oplysninger.

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

A.1 BEHANDLINGEN OMFATTER FØLGENDE TYPER AF PERSONOPLYSNINGER OM DE REGISTRERERE

Databehandleren modtager og behandler persondata i overensstemmelse med databehandlingsaftalen. Dataejer overfører nedenstående typer persondata til databehandleren:

ARTIKEL 6, ALMINDELIGE PERSONINFORMATIONER	ARTIKEL 9, FØLSOMME PERSONINFORMATIONER	ARTIKEL 10, PERSONINFORMATION VEDRØRENDE STRAFFEDOMME OG LOVOVERTRÆDELSER
✓ Kontaktinformation *(fx navn, mail, telefon)* ✓ Stamdata *(fx fødselsdata)* ✓ Registrationsnumre *(fx brugerID, databaseID, kundeID)* ✓ Information om ansættelsesforhold *(fx kontrakt, titel, personalefil)* ✓ Information om løn *(fx løninformationer, bankdetaljer)* ✓ Kvalifikationer og certificeringer, ✓ Præstation *(fx overtid, KPIer)* ✓ Relationer *(fx kundestatus, kontaktroller)* ✓ Behavioural information *(fx brugspræferencer, brugshistorik)*	**Information om …** ✓ Race eller etnisk oprindelse. ✓ Politisk overbevisning eller tilhørsforhold. ✓ Religiøs eller filosofisk overbevisning. ✓ Medlemskab af fagforening. ✓ Helbred. ✓ Sexliv. ✓ Seksuel orientering. ✓ Genetiske data. ✓ Biometriske data. ✓ Information om børn. ✓ anden følsom information.	**Information om …** ✓ Straffedomme og lovovertrædelser

- ✓ Præferencer
  (fx indstillinger, brugerundersøgelser, personlige indstillinger)
- ✓ Logins
- ✓ Teknisk Information
  (fx OS-version, browserversion, IP-adresser)
- ✓ Indkøbshistorik
  (fx boganskaffelser, abonnementer)
- ✓ Fortrolig information
  (fx CPR-nummer)
- ✓ Grove eller gentagne overtrædelser af lovgivningen eller interne retningslinjer eller adfærdskodeks.
- ✓ Andre personinformationer

A.2 BEHANDLINGEN OMFATTER FØLGENDE KATEGORIER AF REGISTREREDE

- ✓ Whistleblowere (*fx ansatte hos slutkunden, som tilføjer information om lovovertrædelser til whistleblowerløsningen*),
- ✓ Kunder eller slutbrugere (*fx formidlere af brugeradgange, systemadministratorer, sagsbehandlere og kundens kontaktpersoner*),
- ✓ Leverandører (logininformationer for personer, som leverer en tjeneste til databehandleren fx i form af vedligehold eller teknik),
- ✓ Ansatte hos databehandleren
- × Besøgende
  (*besøgende på databehandlerens fysiske lokationer eller til arrangementer hos eller uden for databehandleren*)

- ✓ Parter i straffesager eller involverede i lovovertrædelser
  (*fx ansatte hos slutkunden, som er involverede i grove eller gentagne lovovertrædelser eller interne retningslinjer eller adfærdskodeks*)

A.3 DATABEHANDLERENS BEHANDLING AF PERSONOPLYSNINGER PÅ VEGNE AF DEN DATAANSVARLIGE KAN PÅBEGYNDES EFTER DISSE BESTEMMELSERS IKRAFTTRÆDEN. BEHANDLINGEN HAR FØLGENDE VARIGHED

- ✓ Behandlingen er ikke tidsbegrænset og varer, indtil aftalen opsiges eller ophæves af en af parterne. Databehandlingsaftalen har varighed ud over hovedaftalen mellem parterne og har effekt, så længe databehandleren behandler, herunder opbevarer, personinformationer modtaget fra, indsamlet på vegne af den dataansvarlige eller på anden måde behandlet som en del af aftaleforholdet mellem den dataansvarlige og databehandler, indtil databehandler har godtgjort tilbagelevering og destruktion af persondata, jf. databehandlingsaftalens afsnit 10.1.

BILAG B – UNDERDATABEHANDLERE

B.1 GODKENDTE UNDERDATABEHANDLERE

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

SERVICE	CVR	ADDRESS	BRIEF DESCRIPTION OF THE ACTIVITY
Microsoft Azure Services	IE8256796U	Microsoft Ireland Operations Ltd. One Microsoft Place, South County Business Park, Leopardstown, Dublin, D18 P521, Ireland	Opbevaring og backup af data Hosting af applikationslag
Hosting og udvikling	35248021	Unica Net ApS Agenavej 35, 2670 Greve, Danmark	Opbevaring og backup af data

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

B.2 VARSEL FOR GODKENDELSE AF UNDERDATABEHANDLERE

Information om databehandlere varsles skriftligt til den kontraktansvarlige hos den dataansvarlige.

Databehandler varsler den dataansvarlige om ønsket brug af ny underdatabehandler senest 40 dage før forventet ibrugtagning, således at den dataansvarlige har mulighed for at tage stilling til og vurdere ændringer i behandlingsrisiko i god tid før ændringer i behandlingsforholdet.

BILAG C – INSTRUKS VEDRØRENDE BEHANDLING AF PERSONOPLYSNINGER

C.1 BEHANDLINGENS GENSTAND/INSTRUKS

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

Databehandler leverer adgang til databehandlers Whistleblowersystem i overensstemmelse med abonnementsbetingelserne. Slutkunden og slutkundens brugere har mulighed for anonymt at indgive varsel om forhold og at sagsbehandle i et beskyttet miljø. Den dataansvarlige bemyndiges at instruere databehandleren om ændringer i slutkundens data, og databehandleren imødekommer disse uden yderligere beregning, såfremt slutkunden eller den dataansvarlige ikke kan eksekvere kontrol over personinformationer.

Databehandler og dennes underdatabehandlere bemyndiges til behandling af personinformation med henblik på drift og understøttelse af slutkundens eller whistleblowers anvendelse af produktet samt til udvikling, abonnementsstyring og sikring af sikkerhed, nødvendig for leverancen af et stabilt og sikkert produkt, som efterlever gældende lovkrav, jf. whistleblowerdirektivet samt EU2016/679 og EU2019/1937.

C.2 BEHANDLINGSSIKKERHED

Under hensyntagen til den store mængde persondata klassificeret under persondataforordningens (GDPR) artikel 6, følsomme personoplysninger omfattet af GDPR artikel 9, informationer om straffedomme eller lovovertrædelser omfattet af GDPR artikel 10, omhandlende sårbare, defineret som stående i et uligt magtforhold til den dataansvarlige eller udsatte, jf. informationernes karakter, datasubjekter, herunder børn, som vil kunne misbruges af den dataansvarlige, databehandleren eller tredjepart, anses, at behandlingen udgør en høj risiko for datasubjektet, hvorfor et tilsvarende højt niveau for behandlings- og datasikkerhed anlægges.

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.

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

- Sikre, at data opbevares krypteret i overensstemmelse med best practice for data, som kan indeholde fortrolige eller følsomme informationer, som minimum krypteret til AES256 eller tilsvarende krypteringsstandard.
- Sikre, at krypterede data og krypteringsnøgler opbevares separat. Hvis muligt overgives kontrol over krypteringsnøgler til slutbrugeren.
- Sikre, at kommunikation mellem tjenesten og slutbruger er sikret via SSL eller foregår via en tilsvarende sikret forbindelse, som lever op til gældende krav.
- Sikre, at data opbevaret i løsningen er segregerede, således at slutbrugers informationer ikke kan tilgås af uvedkommende uden slutbrugers direkte tilladelse.
- Sikre, at data kan genskabes efter tekniske eller fysiske hændelser, og har procedurer på plads i form af Disaster Recovery- og Business Continuity-planer til at sikre fortsat drift.
- Sikre, at persondata i løsningen begrænses til det absolut nødvendige, og at databehandler og underdatabehandlere i videst mulige omfang begrænses til at behandle pseudonymiserede persondata og ikke har, eller uden Kundens tilladelse eller viden kan tilgå, sensitive eller fortrolige persondata indeholdt i anmeldelser.

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

- Sikre, at den dataansvarlige på baggrund af Kundens instruks, kan styre adgang til Kundens løsning, og at ændringer i adgangsforhold logges og gemmes i op til et år, eller så længe kundeforholdet varer.
- Sikre, at alle adgange fra udviklings- og support teams, som kan give adgang til persondata, som minimum følger ISO2700-standarder for sikring af adgange.
- Sikre, at tredjepart, som optager legitim adgang til løsningen, kun får adgang til krypterede data, samt at aktiviteter, som indebærer adgang til sensitive eller fortrolige persondata, logges, og at tredjepart er underlagt tavshedsklausul.
- Sikre, at adgang til systemer er kontrolleret og underlagt validering i form af fx MFA, samt at adgangsidentifikatorer og logintid registreres i op til 30 dage.
- Have procedurer på plads til at opdage og håndtere databrud, således at den dataansvarlige kan informere brugere af løsningen uden unødig forsinkelse.
- Sikre, at fornøden information registreres ved opdagelse af databrud med henblik på sagsanalyse og til evt. opfølgende undersøgelser forlangt af Kunden.
- Sikre, at fornødne sikkerhedstiltag er på plads til at forhindre og begrænse eksekvering af malware eller lignende kode, blandt andet gennem kontinuerlig rettidig opdatering af software, hardware og kommunikationssystemer, kodevalidering, samt ved løbende at afprøve løsningens hårdhed og resistens igennem penetrationstestning.
- Have procedurer for korrekt og sikker behandling af fysisk materiale udtaget af løsningen til legale formål, herunder også opbevaring, distribution samt data udtrukket fra hjemmearbejdspladser, og sørger for, at databehandlers medarbejdere er instrueret i korrekt behandling af persondata, har modtaget sikkerhedstræning, er underlagt tavshedsklausuler og lignende eller tilsvarende organisatoriske tiltag.
- Sikre, at Kunden kan se, hvis indholdet af løsningen er blevet ændret og af hvem.
- Sikre, at slutbrugeren, som har anvendt løsningen, har mulighed for selv at rette eller tilføje information til løsningen, samt at slutbrugeren har mulighed for at trække sin anmeldelse tilbage.
- Sikre, at Kunden kan trække fornødne data ud af løsningen, såfremt Kunden ønsker at ophøre med brugen af løsningen. Data kan trækkes ud i et maskinlæsbart format af Kunden selv, således at den dataansvarliges eller databehandleres adgang til sensitive eller fortrolige persondata minimeres.

C.3 BISTAND TIL DEN DATAANSVARLIGE

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 8.1 og 8.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

Databehandleren udvikler nødvendig teknisk information, som kan overdrages til den dataansvarliges risikoanalyse.

Databehandlerens øvrige forpligtelser fastsættes i samarbejdsaftalen mellem databehandleren og den dataansvarlige under følgende leveranceparametre:

- Databehandleren skal iværksætte bistanden senest 3 arbejdsdage efter den dataansvarliges anmodning.
- Såfremt anmodningen fremsættes på baggrund af en akut situation, kan den dataansvarlige anmode databehandleren om at påbegynde bistanden senest på samme arbejdsdag, hvor anmodningen indgives.
- Såfremt akut bistand medfører omkostninger for databehandleren, og den akutte bistand ikke er resultat af fejl eller mangler eller af uhensigtsmæssige eller uigennemskuelige arbejdsgange eller processer i produktet, som betyder, at databehandleren ikke kan leve op til sit ansvar over for den dataansvarlige, skal den dataansvarlige godtgøre dokumenterbare omkostninger og tab. Såfremt databehandleren vil gøre denne klausul gældende, skal databehandleren gøre dette gældende over for den dataansvarlige, inden bistanden påbegyndes.

C.4 OPBEVARINGSPERIODE/SLETTERUTINE

Personoplysninger opbevares, så længe forholdet mellem parterne eksisterer, hvorefter de slettes hos databehandleren.

Ved ophør af aftalen vedrørende behandling af personoplysninger, skal databehandleren tilbagelevere og slette personoplysningerne i overensstemmelse med bestemmelse 10.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarliges oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

C.5 LOKALITET FOR BEHANDLING

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

- **Whistleblower Partners ApS,** Kultorvet 11, 4th floor, 1175 Copenhagen, Danmark.
- **Unica Net ApS**, Agenavej 35, 2670 Greve, Danmark.
- **Microsoft Ireland Operations Ltc**, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521, Irland.

C.6 INSTRUKS VEDRØRENDE OVERFØRSEL AF PERSONOPLYSNINGER TIL TREDJELANDE

Databehandleren har ikke tilladelse til at overføre eller overdrage persondata om EU-borgere, kunder, ansatte, ansøgere, gæster eller andre kategorier af datasubjekter til lokationer i tredjelande uden den dataansvarliges udtrykkelige skriftlige tilladelse.

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

Support af Microsoft Azure Cloud leveres direkte til Microsoft Ireland Operations fra:

- **Microsoft**,
  One Microsoft Way,
  Redmond, Seattle,
  Washington State,
  USA.

Detaljer om serviceleverancen og support leveret af databehandlere i tredjelande kan findes under: https://auzre.microsoft.com/da-dk/support/legal.

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

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

Den dataansvarliges tilsynsaktiviteter udføres som en integreret del af de løbende statusmøder mellem parterne, jf. den model for samarbejde, som er fastsat i hovedaftalen mellem parterne. På statusmøder drøftes blandt andet sikkerhedsspørgsmål og spørgsmål om databehandling på baggrund af parternes gensidige vurdering af trusselsbillede, opdaterede vurderinger af kritiske sårbarheder, identificerede sikkerhedsbrud og lignende, som påvirker den overordnede sikkerhed for de behandlingsaktiviteter, der reguleres af aftalen.

VED ET HØJT RISIKONIVEAU INDHENTES FØLGENDE PÅ ÅRLIG BASIS:	ER DER IKKE TALE OM ET HØJT RISIKONIVEAU, INDHENTES FØLGENDE PÅ ÅRLIG BASIS:
✓ ISAE-3000-periodeerklæring, × ISAE-3402-periodeerklæring, × SOC 3-rapport, × Lignende revisionsmateriale, defineret herunder:	× ISAE-3000-periodeerklæring, × ISAE-3000-punkterklæring, × ISAE-3402-periodeerklæring, × SOC-rapport, × Lignende revisionsmateriale, defineret herunder:
✓ Databehandler udfylder sikkerheds-questionnaire fra den dataansvarlige og rapporterer resultat og metode til den dataansvarlige. ✓ Fysisk inspektion af databehandler med tilhørende inspektionsrapport.	× Databehandler udfylder sikkerheds-questionnaire fra den dataansvarlige. Der dataansvarlig rapporterer resultat og metode til den dataansvarlige. × Fysisk inspektion af databehandler med tilhørende inspektionsrapport.

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

Parterne har i fællesskab vurderet, at der er tale om et højt risikoniveau for datasubjekterne, og det er fastsat, at databehandleren mindst en gang årligt, uden yderligere omkostninger for den dataansvarlige, producerer og forelægger en ISAE 3000-perioderapport for den dataansvarlige som dokumentation for databehandlerens efterlevelse af databehandlingsaftalen. Dette indebærer, at den dataansvarlige gives mulighed for at foretage inspektioner på lokationer for databehandlingen, ligesom databehandleren kan pålægges på årlig basis at udfylde et sikkerhedsspørgeskema, som beskriver databehandlerens sikkerhedsforanstaltninger og adfærd.

Dokumentation fremsendes uden unødig forsinkelse den dataansvarlige til orientering i forståelse af, at den dataansvarlige kan dele indholdet med Kunden. Den dataansvarlige kan anfægte rammerne for og/eller revisionsmetoden og kan i så tilfælde anmode om en ny dokumentation under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultatet er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, af lokaliteterne, hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt.