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

PERSONUPPGIFTSBITRÄDESAVTAL

i enlighet med artikel 28.3 i förordning 2016/679 (GDPR) avseende Personuppgiftsbiträdets behandling av personuppgifter

mellan

Kunden

(nedan kallad ”den Personuppgiftsansvarige”)

och

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

(nedan kallad ”Personuppgiftsbiträdet”)

var och en av dem är en ”part” och utgör tillsammans ”parterna”

HAR ENATS om följande standardavtalsbestämmelser (Bestämmelserna) för att följa dataskyddsförordningen och för att säkerställa skyddet av fysiska personers integritet och grundläggande rättigheter och friheter:

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

1. INGRESS

1. I dessa Bestämmelser fastställs de rättigheter och skyldigheter som ett personuppgiftsbiträde har när det utför behandling av personuppgifter för den personuppgiftsansvariges räkning.
2. Dessa bestämmelser är utformade för att säkerställa att parterna följer artikel 28.3 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för enskilda personer med avseende på behandling av personuppgifter och om fritt utbyte av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
3. I samband med tillhandahållandet av Whistleblower Partners visselblåsarlösning behandlar Personuppgiftsbiträdet personuppgifter för den Personuppgiftsansvariges räkning i enlighet med dessa bestämmelser. Enligt visselblåsardirektivet får personuppgifter behandlas när det är nödvändigt för att behandla rapporter som har mottagits inom ramen för ett visselblåsarsystem.
4. Dessa bestämmelser ska ha företräde framför eventuella motsvarande bestämmelser i andra avtal mellan parterna.
5. Det finns fyra bilagor till dessa förordningar och bilagorna utgör en integrerad del av bestämmelserna.
6. Bilaga A innehåller uppgifter om behandlingen av personuppgifter, inklusive syftet med och arten av behandlingen, typen av personuppgifter, kategorierna av registrerade och behandlingens varaktighet.
7. Bilaga B innehåller den Personuppgiftsansvariges villkor för Personuppgiftsbiträdets användning av underbiträden och en förteckning över underbiträden vars användning har godkänts av den Personuppgiftsansvarige.
8. Bilaga C innehåller den Personuppgiftsansvariges instruktioner om Personuppgiftsbiträdets behandling av personuppgifter, en beskrivning av de säkerhetsåtgärder som Personuppgiftsbiträdet minst ska genomföra och hur Personuppgiftsbiträdet och eventuella underbiträden ska övervakas.
9. Bestämmelserna och deras bilagor ska lagras skriftligen, även på elektronisk väg, av båda parter.
10. Dessa bestämmelser befriar inte Personuppgiftsbiträdet från de skyldigheter som åligger Personuppgiftsbiträdet enligt dataskyddsförordningen eller annan lagstiftning.

2. DEN PERSONUPPGIFTSANSVARIGES RÄTTIGHETER OCH SKYLDIGHETER

1. Den Personuppgiftsansvarige ansvarar för att behandlingen av personuppgifter sker i enlighet med dataskyddsförordningen (se artikel 24 i förordningen), dataskyddsbestämmelser i annan EU-lagstiftning eller medlemsstaternas nationella lagstiftning och dessa bestämmelser.

2. Den Personuppgiftsansvarige har rätt och skyldighet att besluta för vilka ändamål och på vilket sätt personuppgifter får behandlas.

3. Den Personuppgiftsansvarige ansvarar bland annat för att se till att det finns en behandlingsgrund för den behandling av personuppgifter som Personuppgiftsbiträdet får i uppdrag att utföra.

3. PERSONUPPGIFTSBITRÄDET AGERAR PÅ INSTRUKTIONER

1. Personuppgiftsbiträdet får endast behandla personuppgifter på grundval av en dokumenterad instruktion från den Personuppgiftsansvarige, såvida det inte krävs enligt den EU-lagstiftning eller den nationella lagstiftning i en medlemsstat som Personuppgiftsbiträdet omfattas av. Denna instruktion ska specificeras i bilagorna A och C. Den Personuppgiftsansvarige kan också ge efterföljande instruktioner medan personuppgifterna behandlas, men instruktionen ska alltid dokumenteras och lagras skriftligen, även elektroniskt, tillsammans med dessa bestämmelser.

2. Personuppgiftsbiträdet ska utan dröjsmål informera den Personuppgiftsansvarige om denne anser att en instruktion strider mot dataskyddsförordningen eller mot bestämmelser om uppgiftsskydd i annan EU-lagstiftning eller medlemsstats nationella lagstiftning.

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

4. KONFIDENTIALITET

1. Personuppgiftsbiträdet ska endast ge åtkomst till personuppgifter som behandlas för den Personuppgiftsansvariges räkning till personer som omfattas av Personuppgiftsbiträdet befogenhet att ge instruktioner, som har åtagit sig att hålla dem konfidentiella eller som omfattas av en lämplig rättslig skyldighet att hålla dem konfidentiella, och endast i den utsträckning som det är nödvändigt. Förteckningen över de personer som har beviljats åtkomst ska ses över löpande. På grundval av denna genomgång kan åtkomsten till personuppgifter stängas om åtkomsten inte längre är nödvändig, och personuppgifterna ska då inte längre vara tillgängliga för dessa personer.

2. Personuppgiftsbiträdet måste på begäran av den Personuppgiftsansvarige kunna visa att de berörda personer som omfattas av Personuppgiftsbiträdet befogenheter att ge instruktioner omfattas av den ovannämnda tystnadsplikten.

3. Personuppgiftsbiträdet får endast lämna ut personuppgifter som behandlas för den Personuppgiftsansvariges räkning i den utsträckning som föreskrivs i visselblåsardirektivet, den allmänna dataskyddsförordningen eller annan lagstiftning.

5. SÄKERHET VID BEHANDLING

1. Enligt artikel 32 i dataskyddsförordningen ska den Personuppgiftsansvarige och Personuppgiftsbiträdet med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa en skyddsnivå som är lämplig i förhållande till de risker som föreligger, vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

   Den personuppgiftsansvarige måste bedöma de risker för fysiska personers rättigheter och friheter som behandlingen medför och vidta åtgärder för att hantera dessa risker. Beroende på relevans kan detta innefatta:

   a. pseudonymisering och kryptering av personuppgifter,

b. förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,

c. förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,

d. ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

2. Enligt artikel 32 i förordningen ska Personuppgiftsbiträdet – oberoende av den Personuppgiftsansvarige – också bedöma de risker för fysiska personers rättigheter som behandlingen medför och vidta åtgärder för att hantera dessa risker. För denna bedömning ska den Personuppgiftsansvarige tillhandahålla nödvändig information till Personuppgiftsbiträdet för att göra det möjligt för denne att identifiera och bedöma sådana risker.

3. Dessutom ska Personuppgiftsbiträdet hjälpa den Personuppgiftsansvarige att uppfylla den Personuppgiftsansvariges skyldighet enligt artikel 32 i förordningen, bland annat genom att förse den Personuppgiftsansvarige med nödvändig information om de tekniska och organisatoriska säkerhetsåtgärder som Personuppgiftsbiträdet redan har vidtagit i enlighet med artikel 32 i förordningen och all annan information som krävs för att den Personuppgiftsansvarige ska kunna uppfylla sin skyldighet enligt artikel 32 i förordningen.

   Om det enligt den personuppgiftsansvariges bedömning krävs ytterligare åtgärder för att hantera de identifierade riskerna utöver de åtgärder som redan har vidtagits av personuppgiftsbiträdet, ska den personuppgiftsansvarige ange vilka ytterligare åtgärder som ska vidtas i bilaga C.

6. ANVÄNDNING AV UNDERBITRÄDEN

1. Personuppgiftsbiträdet måste uppfylla villkoren i artikel 28.2 och 28.4 i den allmänna dataskyddsförordningen för att kunna använda sig av ett annat personuppgiftsbiträde (ett underbiträde).

2. Personuppgiftsbiträdet får således inte använda sig av ett underbiträde för att uppfylla dessa bestämmelser utan den Personuppgiftsansvariges särskilda skriftliga samtycke i förväg.

3. Personuppgiftsbiträdet får endast använda underbiträden med den Personuppgiftsansvariges särskilda skriftliga förhandsgodkännande. Personuppgiftsbiträdet ska lämna in en begäran om ett särskilt godkännande minst 40 dagar innan det berörda underbiträdet används. Förteckningen över de underbiträden som den Personuppgiftsansvarige redan har godkänt återfinns i bilaga B.

4. Om Personuppgiftsbiträdet använder sig av ett underbiträde för att utföra specifika behandlingsåtgärder för den Personuppgiftsansvariges räkning, ska Personuppgiftsbiträdet genom ett avtal eller annan rättslig handling enligt EU-rätten eller medlemsstaternas nationella lagstiftning ålägga underbiträdet samma skyldigheter i fråga om uppgiftsskydd som de som fastställs i dessa bestämmelser, och särskilt ge nödvändiga garantier för att underbiträdet ska genomföra de tekniska och organisatoriska åtgärderna på ett sådant sätt att behandlingen uppfyller kraven i dessa bestämmelser och i dataskyddsförordningen.

   Personuppgiftsbiträdet är därför ansvarigt för att kräva att underbiträdet åtminstone uppfyller Personuppgiftsbiträdet skyldigheter enligt dessa Bestämmelser och dataskyddsförordningen.

5. Kopior av underbiträdesavtal och eventuella senare ändringar av dessa ska på begäran av den Personuppgiftsansvarige skickas till den Personuppgiftsansvarige, som därigenom ska ha möjlighet att se till att underbiträdet åläggs likvärdiga dataskyddsskyldigheter enligt dessa bestämmelser. Bestämmelser om kommersiella villkor som inte påverkar dataskyddsinnehållet i avtalet om underbiträden ska inte skickas till den Personuppgiftsansvarige.

6. Personuppgiftsbiträdet ska i sitt avtal med underbiträdet inkludera den Personuppgiftsansvarige som tredje part som är förmånstagare i händelse av att Personuppgiftsbiträdet går i konkurs, så att den Personuppgiftsansvarige kan åberopa Personuppgiftsbiträdets rättigheter och genomdriva dem gentemot underbiträden, som till exempel genom att göra det möjligt för den Personuppgiftsansvarige att beordra underbiträdet att radera eller återlämna personuppgifterna.

7. Om underbiträdet inte uppfyller sina skyldigheter i fråga om uppgiftsskydd ska underbiträdet förbli fullt ansvarigt gentemot den Personuppgiftsansvarige för fullgörandet av underbiträdets skyldigheter. Detta påverkar inte de registrerades rättigheter enligt dataskyddsförordningen, särskilt artiklarna 79 och 82, gentemot den Personuppgiftsansvarige och Personuppgiftsbiträdet, inklusive underbiträdet.

7. ÖVERFÖRING TILL TREDJE LAND ELLER INTERNATIONELLA ORGANISATIONER

1. Varje överföring av personuppgifter till tredje land eller internationella organisationer får endast göras av Personuppgiftsbiträdet på grundval av en dokumenterad instruktion om detta från den Personuppgiftsansvarige, och måste alltid göras i enlighet med kapitel V i dataskyddsförordningen.

2. Om överföring av personuppgifter till tredje land eller internationella organisationer, som den Personuppgiftsansvarige inte har instruerat Personuppgiftsbiträdet om att utföra, krävs enligt EU-rätten eller medlemsstaternas nationella lagstiftning, som Personuppgiftsbiträdet omfattas av, ska Personuppgiftsbiträdet underrätta den Personuppgiftsansvarige om detta rättsliga krav före behandlingen, såvida inte sådan lagstiftning förbjuder en sådan underrättelse på grund av viktiga allmänna intressen.

3. Utan en dokumenterad instruktion från den Personuppgiftsansvarige kan Personuppgiftsbiträdet således inte inom ramverket för dessa bestämmelser:

   a. Överföra personuppgifter till en personuppgiftsansvarig eller ett personuppgiftsbiträde i ett tredje land eller en internationell organisation
   b. Överlåta behandlingen av personuppgifter till ett underbiträde i ett tredje land

   c. Behandla personuppgifterna i ett tredje land

4. Den Personuppgiftsansvariges instruktioner om överföring av personuppgifter till ett tredje land, inklusive den eventuella överföringsgrunden i kapitel V i dataskyddsförordningen som överföringen grundar sig på, ska anges i bilaga C.6.

5. Dessa bestämmelser får inte förväxlas med standardavtalsbestämmelser i den mening som avses i artikel 46.2 c och d i dataskyddsförordningen och dessa bestämmelser får inte utgöra en grund för överföring av personuppgifter i den mening som avses i kapitel V i dataskyddsförordningen.

8. STÖD TILL DEN PERSONUPPGIFTSANSVARIGE

1. Personuppgiftsbiträdet ska, så långt det är möjligt och med hänsyn till behandlingens art, genom lämpliga tekniska och organisatoriska åtgärder bistå den Personuppgiftsansvarige med att uppfylla den Personuppgiftsansvarige skyldighet att svara på begäran om att utöva de registrerades rättigheter enligt kapitel III i dataskyddsförordningen.

   Detta innebär att Personuppgiftsbiträdet i möjligaste mån ska hjälpa den Personuppgiftsansvarige att säkerställa efterlevnaden av:

   a. Skyldigheten att tillhandahålla information när personuppgifter samlas in hos den registrerade

   b. Skyldigheten att tillhandahålla information om personuppgifter inte har samlats in hos den registrerade

   c. Rätten till information

   d. Rätten till rättelser

   e. Rätten till radering ("rätten att bli bortglömd")

   f. Rätten till begränsning av behandling

g. Anmälningsskyldigheten avseende rättelse eller radering av personuppgifter och begränsning av behandling

h. Rätten till dataportabilitet

i. Rätten att göra invändningar

j. Rätten att inte bli föremål för ett beslut som enbart grundar sig på automatiserad behandling, inbegripet profilering

2. Personuppgiftsbiträdet bistår även den Personuppgiftsansvarige, med beaktande av behandlingens art och den information som är tillgänglig för Personuppgiftsbiträdet, med:

a. Den Personuppgiftsansvariges skyldighet att underrätta den behöriga tillsynsmyndigheten, Integritetsskyddsmyndigheten, om en personuppgiftsincident utan onödigt dröjsmål och, om möjligt, inom 72 timmar efter att ha fått kännedom om den, såvida det inte är osannolikt att personuppgiftsincidenten utgör en risk för fysiska personers rättigheter eller friheter

b. Skyldigheten för den Personuppgiftsansvarige att utan onödigt dröjsmål underrätta den registrerade om en personuppgiftsincident, när det är sannolikt att incidenten leder till en hög risk för fysiska personers rättigheter och friheter

c. Skyldigheten för den Personuppgiftsansvarige att före behandlingen göra en analys av hur den planerade behandlingen påverkar skyddet av personuppgifter (en konsekvensbedömning)

d. Skyldigheten för den Personuppgiftsansvarige att samråda med den behöriga tillsynsmyndigheten, Integritetsskyddsmyndigheten, före behandlingen, om en konsekvensbedömning av dataskyddet visar att behandlingen skulle leda till en hög risk om den Personuppgiftsansvarige inte vidtar några åtgärder för att minska risken.

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

3. Parterna ska i bilaga C ange de nödvändiga tekniska och organisatoriska åtgärder genom vilka Personuppgiftsbiträdet ska bistå den Personuppgiftsansvarige, samt omfattningen och utsträckningen av detta bistånd. Detta gäller de skyldigheter som följer av bestämmelserna 8.1 och 8.2.

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

9. ANMÄLAN OM BROTT MOT PERSONUPPGIFTSSÄKERHETEN

1. Personuppgiftsbiträdet ska underrätta den Personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått kännedom om att en personuppgiftsincident har inträffat.

2. Personuppgiftsbiträdets anmälan till den Personuppgiftsansvarige ska om möjligt göras inom 24 timmar efter det att den Personuppgiftsansvarige fått kännedom om brottet, så att den Personuppgiftsansvarige kan uppfylla sin skyldighet att anmäla personuppgiftsbrottet till den behöriga tillsynsmyndigheten i enlighet med artikel 33 i den allmänna dataskyddsförordningen.

3. I enlighet med bestämmelse 8.2.a ska Personuppgiftsbiträdet hjälpa den Personuppgiftsansvarige att underrätta den behöriga tillsynsmyndigheten om brottet. Detta innebär att Personuppgiftsbiträdet måste hjälpa till med att tillhandahålla följande information, som enligt artikel 33.3 ska ingå i den Personuppgiftsansvariges anmälan av brottet till den behöriga tillsynsmyndigheten:

    a. Arten av personuppgiftsincident, inklusive, om möjligt, kategorierna och det ungefärliga antalet berörda registrerade personer samt kategorierna och det ungefärliga antalet registrerade personuppgifter som berörs

    b. De troliga konsekvenserna av personuppgiftsincidenten

    c. De åtgärder som den Personuppgiftsansvarige har vidtagit eller avser att vidta för att hantera personuppgiftsincidenten, inklusive i förekommande fall, åtgärder för att begränsa dess eventuella skadliga effekter.

4. Parterna ska i bilaga C specificera den information som ska tillhandahållas av Personuppgiftsbiträdet för att bistå den Personuppgiftsansvarige i dennes skyldighet att anmäla överträdelser av personuppgifter till den behöriga tillsynsmyndigheten.

10. RADERING OCH ÅTERLÄMNANDE AV UPPGIFTER

1. När tjänsterna för behandling av personuppgifter upphör är Personuppgiftsbiträdet skyldig att radera alla personuppgifter som har behandlats för den Personuppgiftsansvariges räkning, och att bekräfta för den Personuppgiftsansvarige att uppgifterna har raderats, såvida inte EU:s eller medlemsstatens nationella lagstiftning föreskriver att personuppgifterna ska lagras.

11. REVISION, INKLUSIVE INSPEKTION

1. Personuppgiftsbiträdet ska tillhandahålla den Personuppgiftsansvarige all information som behövs för att visa att artikel 28 i dataskyddsförordningen och dessa Bestämmelser efterlevs och ska tillåta och bidra till revisioner, inklusive inspektioner, som utförs av den Personuppgiftsansvarige eller en annan revisor som godkänts av den Personuppgiftsansvarige.

2. Förfarandena för den Personuppgiftsansvariges revisioner, inklusive inspektioner av Personuppgiftsbiträdet och underbiträden beskrivs i detalj i bilagan C.7.

3. Personuppgiftsbiträdet är skyldig att ge tillsynsmyndigheter som i enlighet med gällande lagstiftning har tillträde till den Personuppgiftsansvariges eller Personuppgiftsbiträdets anläggningar, eller till företrädare som agerar på tillsynsmyndighetens vägnar, tillträde till Personuppgiftsbiträdets fysiska anläggningar mot uppvisande av behörig legitimation.

12. PARTERNAS ÖVERENSKOMMELSE OM ANDRA FRÅGOR

1. Parterna får komma överens om andra bestämmelser som rör tjänsten om behandling av personuppgifter, om t.ex. ersättningsansvar, så länge dessa andra bestämmelser inte direkt eller indirekt strider mot bestämmelserna eller försämrar den registrerades grundläggande rättigheter och friheter, som följer av dataskyddsförordningen.

13. IKRAFTTRÄDANDE OCH UPPHÖRANDE

1. Bestämmelserna ska träda i kraft den dag då de undertecknas av båda parter.

2. Båda parter kan begära omförhandling av bestämmelserna om ändringar i lagstiftningen eller felaktiga bestämmelserna föranleder ett sådant krav.

3. Bestämmelserna gäller under hela den tid som tjänsten med behandling av personuppgifter pågår. Under denna period får Bestämmelserna inte sägas upp, såvida inte parterna kommer överens om andra bestämmelser om tillhandahållandet av tjänsten i samband med behandlingen av personuppgifter.

4. Om tillhandahållandet av tjänsterna för behandling av personuppgifter avslutas, och personuppgifterna har raderats eller återlämnats till den Personuppgiftsansvarige i enlighet med punkt 10.1 och bilaga C.4, kan bestämmelserna sägas upp av endera parten genom ett skriftligt meddelande.

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

BILAGA A – INFORMATION OM BEHANDLINGEN

A.1 SYFTET MED PERSONUPPGIFTSBITRÄDETS BEHANDLING AV PERSONUPPGIFTER FÖR DEN PERSONUPPGIFTSANSVARIGES

Syftet med behandlingen av personuppgifter är att ta emot, lagra och göra rapporter tillgängliga för handläggare som utsetts av den Personuppgiftsansvarige för att behandla rapporter som en del av den Personuppgiftsansvariges rådgivning i samband med visselblåsarsystem, se visselblåsardirektivet.

A.2 PERSONUPPGIFTSBITRÄDETS BEHANDLING AV PERSONUPPGIFTER FÖR DEN PERSONUPPGIFTSANSVARIGES RÄKNING HANDLAR PRIMÄRT OM (KARAKTÄREN PÅ BEHANDLINGEN)

Att ta emot rapporter från slutanvändare och för att lagra och göra rapporter tillgängliga för handläggare som är utsedda av den Personuppgiftsansvarige för att behandla information.

A.3 BEHANDLINGEN OMFATTAR FÖLJANDE TYPER AV PERSONUPPGIFTER OM DE REGISTRERADE

Personuppgiftsbiträdet tar emot och behandlar personuppgifter i enlighet med avtalet om databehandling. Uppgiftsägaren överför följande typer av personuppgifter till Personuppgiftsbiträdet:

ARTIKEL 6, ALLMÄNNA PERSONUPPGIFTER	ARTIKEL 9, KÄNSLIGA PERSONUPPGIFTER	ARTIKEL 10, PERSONUPPGIFTER OM FÄLLANDE DOMAR OCH BROTT
✓ Kontaktinformation *(t.ex. namn, e-post, telefon)* ✓ Stamdata *(t.ex. födelseuppgifter)* ✓ Registreringsnummer *(t.ex. användar-ID, databas-ID, kund-ID)* ✓ Information om anställningsförhållanden *(t.ex. kontrakt, titel, personalakter)* ✓ Information om lön *(t.ex. löneinformation, bankuppgifter)* ✓ Kvalifikationer och certifieringar, ✓ Prestationer *(t.ex. övertid, nyckeltal)* ✓ Relationer *(t.ex. kundstatus, kontaktroller)* ✓ Beteendeinformation *(t.ex. användningspreferenser, användningshistorik)* ✓ Preferenser *(t.ex. inställningar,*	**Information om …** ✓ Etniskt ursprung. ✓ Politisk övertygelse eller politisk tillhörighet. ✓ Religiös eller filosofisk övertygelse. ✓ Medlemskap i fackförening. ✓ Hälsa. ✓ Sexliv. ✓ Sexuell läggning. ✓ Genetiska data. ✓ Biometriska data. ✓ Information om barn. ✓ Annan känslig information.	**Information om …** ✓ Fällande domar och lagöverträdelser

användarundersökningar, personliga inställningar)

- ✓ Inloggningar
- ✓ Teknisk Information *(t.ex. OS-version, webbläsarversion, IP-adresser)*
- ✓ Inköpshistorik *(t.ex. inköp av böcker, abonnemang)*
- ✓ Konfidentiell information *(t.ex. personnummer)*
- ✓ Allvarliga eller upprepade överträdelser av lagen eller interna riktlinjer eller uppförandekoder.
- ✓ Andra personuppgifter

A.4 BEHANDLINGEN OMFATTAR FÖLJANDE KATEGORIER AV REGISTRERADE

- ✓ Visselblåsare (t.ex. anställda hos slutkunden som lägger till information om lagöverträdelser i visselblåsarlösningen),
- ✓ Kunder eller slutanvändare (*t.ex. leverantörer av användaråtkomst, systemadministratörer, handläggare och kundens kontaktpersoner*)
- ✓ Leverantörer (inloggningsinformation för personer som tillhandahåller en tjänst till Personuppgiftsbiträdet t.ex. i form av underhåll eller teknik),
- ✓ Anställda hos Personuppgiftsbiträdet
- × Besökare
- ✓ *(besökare till Personuppgiftsbiträdets fysiska platser eller till evenemang på eller utanför Personuppgiftsbiträdets lokaler*)
- ✓ Parter i straffrättsliga förfaranden eller inblandade i brott *(t.ex. anställda hos slutkunden som är inblandade i allvarliga eller upprepade överträdelser av interna riktlinjer eller uppförandekoder*)

A.5 PERSONUPPGIFTSBITRÄDETS BEHANDLING AV PERSONUPPGIFTER FÖR DEN PERSONUPPGIFTSANSVARIGES RÄKNING KAN PÅBÖRJAS EFTER IKRAFTTRÄDANDET AV DESSA BESTÄMMELSER. BEHANDLINGEN HAR FÖLJANDE GILTIGHETSTID

- ✓ Behandlingen är inte tidsbegränsad och pågår tills avtalet sägs upp eller hävs av en av parterna. Avtalet om databehandling ska ha en längre giltighetstid än huvudavtalet mellan parterna, och ska gälla så länge som Personuppgiftsbiträdet behandlar, inklusive lagrar, personuppgifter som mottagits från, samlats in på uppdrag av eller på annat sätt behandlats som en del av avtalsförhållandet mellan den Personuppgiftsansvarige och Personuppgiftsbiträdet, tills dess att Personuppgiftsbiträdet har lämnat dokumentation på att personuppgifterna har återlämnats och förstörts, se avsnitt 10.1 i avtalet om databehandling.

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

BILAGA B – UNDERBITRÄDEN

B.1 GODKÄNDA UNDERBITRÄDEN

När Bestämmelserna träder i kraft har den Personuppgiftsansvarige godkänt användningen av följande underbiträden:

SERVICE	ORGANISATIONSNUMMER	ADRESS	KORTFATTAD BESKRIVNING AV VERKSAMHETEN
Microsoft Azure-tjänster	IE8256796U	Microsoft Ireland Operations Ltd. One Microsoft Place, South County Business Park, Leopardstown, Dublin, D18 P521, Irland	Datalagring och säkerhetskopiering Hosting av applikationstyp
Hosting och utveckling	35248021	Unica Net ApS Agenavej 35, 2670 Greve, Danmark	Datalagring och säkerhetskopiering

När Bestämmelserna träder i kraft har den Personuppgiftsansvarige godkänt användningen av ovan nämnda underbiträden för den beskrivna behandlingsverksamheten. Personuppgiftsbiträdet får inte – utan den Personuppgiftsansvariges skriftliga samtycke – använda sig av ett underbiträde för annan behandlingsverksamhet än den som beskrivits och avtalats, eller använda sig av ett annat underbiträde för denna behandlingsverksamhet.

B.2 MEDDELANDE OM GODKÄNNANDE AV UNDERBITRÄDEN

Uppgifter om personuppgiftsbiträden meddelas skriftligen till kontraktschefen hos den Personuppgiftsansvarige

Personuppgiftsbiträdet ska meddela den Personuppgiftsansvarige om den planerade användningen av ett nytt underbiträde minst 40 dagar innan verksamheten förväntas inledas, så att den Personuppgiftsansvarige har möjlighet att ta ställning till och bedöma förändringar i behandlingsrisken i god tid före förändringar i behandlingsförhållandet.

BILAGA C – INSTRUKTIONER OM BEHANDLING AV PERSONUPPGIFTER

C.1 BEHANDLINGENS ÄMNE/INSTRUKTIONER

Personuppgiftsbiträdets behandling av personuppgifter för den Personuppgiftsansvariges räkning utförs enligt följande:

Personuppgiftsbiträdet ger tillgång till Personuppgiftsbiträdets visselblåsarsystem i enlighet med prenumerationsvillkoren. Slutkunden och slutkundens användare har möjlighet att anonymt lämna meddelanden om förhållanden och handlägga ärenden i en skyddad miljö. Den Personuppgiftsansvarige har behörighet att instruera Personuppgiftsbiträdet om ändringar i slutkundens uppgifter och Personuppgiftsbiträdet tillgodoser dessa utan extra kostnad, om slutkunden eller den Personuppgiftsansvarige inte kan utöva kontroll över personuppgifterna.

Personuppgiftsbiträdet och detta underbiträde har rätt att behandla personuppgifter i syfte att driva och stödja slutkundens eller visselblåsares användning av produkten, samt för utveckling, abonnemangshantering och säkerställande av den säkerhet som krävs för att leverera en stabil och säker produkt som uppfyller tillämpliga rättsliga krav, se visselblåsardirektivet, samt EU2016/679 och EU2019/1937.

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

C.2 SÄKERHET VID BEHANDLING

Med hänsyn till den stora mängden personuppgifter som klassificeras enligt artikel 6 i den allmänna dataskyddsförordningen (GDPR), omfattas känsliga personuppgifter av artikel 9 i GDPR, information om brottsdomar eller brott som omfattas av artikel 10 i GDPR, rörande utsatta personer, definierad som att ha en ojämlik makt över den Personuppgiftsansvarige eller utsatta, se arten av information om registrerade, inklusive barn, som kan missbrukas av den Personuppgiftsansvarige, Personuppgiftsbiträdet eller tredje part anses det att behandlingen utgör en hög risk för den registrerade, varför en motsvarande hög nivå av behandling och datasäkerhet upprättas.

Personuppgiftsbiträdet är då berättigad och skyldig att fatta beslut om vilka tekniska och organisatoriska säkerhetsåtgärder som måste vidtas för att fastställa nödvändig (och överenskommen) säkerhetsnivå.

Personuppgiftsbiträdet ska dock – under alla omständigheter och som ett minimum – genomföra följande åtgärder som har avtalats med den Personuppgiftsansvarige:

- Säkerställa att data lagras i krypterad form i enlighet med bästa praxis för data som kan innehålla konfidentiell eller känslig information, som ett minimum krypterad till AES256 eller motsvarande krypteringsstandard.
- Säkerställa att krypterade data och krypteringsnycklar lagras separat. Om möjligt lämnas kontrollen över krypteringsnycklar till slutanvändaren.
- Säkerställa att kommunikationen mellan tjänsten och slutanvändaren är säkrad via SSL eller sker via en liknande säkrad anslutning som uppfyller gällande krav.
- Säkerställ att data som lagras i lösningen är åtskilda, så att slutanvändarens information inte är tillgänglig för obehöriga utan slutanvändarens direkta tillstånd.
- Säkerställa att data kan återställas efter tekniska eller fysiska händelser, och har rutiner på plats i form av Disaster Recovery- och Business Continuity-planer för att säkerställa fortsatt drift.
- Säkerställa att personuppgifter i lösningen begränsas till vad som är absolut nödvändigt, samt att personuppgiftsbiträde och underbiträde begränsas så långt det är möjligt att behandla pseudonymiserade personuppgifter och inte har, eller utan Kundens tillstånd eller kunskap kan komma åt känsliga eller konfidentiella personuppgifter som finns i anmälningarna.

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

- Säkerställa att den Personuppgiftsansvarige på grundval av Kundens instruktioner kan styra åtkomsten till Kundens lösning, och att ändringar i åtkomstvillkoren loggas och lagras i upp till ett år, eller så länge som kundrelationen består.
- Säkerställa att all åtkomst från utvecklings- och supportteam, som kan ge tillgång till personuppgifter, åtminstone följer ISO2700-standarderna för att säkra åtkomsten.
- Säkerställa att tredje part som registrerar legitim åtkomst till lösningen endast har tillgång till krypterade data, och att aktiviteter som innebär åtkomst till känsliga eller konfidentiella personuppgifter loggas och att tredje part omfattas av en sekretessklausul.
- Säkerställa att åtkomsten till systemen är kontrollerad och valideras i form av t.ex. MFA, samt att åtkomstidentifierare och inloggningstid registreras i upp till 30 dagar.
- Ha rutiner på plats för att upptäcka och hantera dataintrång så att den Personuppgiftsansvarige kan informera användarna av lösningen utan onödigt dröjsmål.
- Säkerställa att nödvändig information registreras när dataintrång upptäcks i syfte att analysera ärendet och för ev. uppföljande undersökningar som krävs av Kunden.
- Säkerställa att nödvändiga säkerhetsåtgärder har införts för att förhindra och begränsa exekvering av skadlig kod eller liknande kod, bland annat genom kontinuerlig aktuell uppdatering av mjukvara, hårdvara och kommunikationssystem, kodvalidering och genom att kontinuerligt testa lösningens hårdhet och motstånd genom intrångstestning.
- Ha rutiner för korrekt och säker behandling av fysiskt material som tagits från lösningen för lagliga ändamål, inklusive lagring, distribution och data utvunna från hemarbetsplatser, och se till att Personuppgiftsbiträdets anställda instrueras i korrekt behandling av personuppgifter, har fått säkerhetsutbildning, omfattas av sekretessklausuler och liknande, eller motsvarande organisatoriska åtgärder.
- Säkerställa att Kunden kan se om innehållet i lösningen har ändrats, och av vem.
- Säkerställa att den slutanvändare som har använt lösningen har möjlighet att själv korrigera eller lägga till information i lösningen, och att slutanvändaren har möjlighet att återkalla sin anmälan.
- Säkerställa att Kunden kan extrahera nödvändiga data från lösningen om Kunden vill sluta använda lösningen. Data kan extraheras i ett maskinläsbart format av Kunden

själv, så att den Personuppgiftsansvarige eller Personuppgiftsbiträdets tillgång till känsliga eller konfidentiella personuppgifter minimeras.

C.3 STÖD TILL DEN PERSONUPPGIFTSANSVARIGE

Personuppgiftsbiträdet ska i den mån det är möjligt – inom ramen för den utsträckning och omfattning som anges nedan – bistå den Personuppgiftsansvarige i enlighet med punkterna 8.1 och 8.2 genom att genomföra följande tekniska och organisatoriska åtgärder:

Personuppgiftsbiträdet tar fram nödvändig teknisk information som kan överföras för den Personuppgiftsansvariges riskanalys.

Personuppgiftsbiträdet övriga skyldigheter framgår av samarbetsavtalet mellan Personuppgiftsbiträdet och den Personuppgiftsansvarige under följande leveransparametrar:

- Personuppgiftsbiträdet ska påbörja stödet senast 3 arbetsdagar efter den Personuppgiftsansvariges begäran.
- Om begäran görs på grund av en nödsituation kan den Personuppgiftsansvarige begära att Personuppgiftsbiträdet påbörjar stödet senast samma arbetsdag som begäran lämnas in.
- Om akut hjälp medför kostnader för Personuppgiftsbiträdet och den akuta hjälpen inte är ett resultat av fel eller försummelser eller av inadekvata eller oklara arbetsflöden eller processer för produkten, vilket gör att Personuppgiftsbiträdet inte kan leva upp till sitt ansvar gentemot den Personuppgiftsansvarige, måste den Personuppgiftsansvarige motivera dokumenterbara kostnader och förluster. Om Personuppgiftsbiträdet vill verkställa denna klausul måste Personuppgiftsbiträdet göra detta gällande gentemot den Personuppgiftsansvarige innan stödet påbörjas.

C.4 LAGRINGSPERIOD/RADERINGSRUTIN

Personuppgifter lagras så länge relationen mellan parterna existerar, varefter den raderas av Personuppgiftsbiträdet.

När avtalet om behandling av personuppgifter upphör ska Personuppgiftsbiträdet återlämna och radera personuppgifterna i enlighet med punkt 10.1, såvida inte den Personuppgiftsansvarige – efter undertecknandet av dessa punkter – har ändrat den Personuppgiftsansvariges ursprungliga val. Sådana ändringar ska dokumenteras och lagras skriftligen, även elektroniskt, i anslutning till bestämmelserna.

C.5 PLATS FÖR BEHANDLING

Behandling av personuppgifter som omfattas av bestämmelserna får inte ske utan den Personuppgiftsansvariges skriftliga förhandsgodkännande på andra platser än följande:

- **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 INSTRUKTIONER OM ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND

Personuppgiftsbiträdet får inte överföra eller överlåta personuppgifter om EU-medborgare, kunder, anställda, sökande, gäster eller andra kategorier av registrerade till platser i tredje land utan uttryckligt skriftligt samtycke från den Personuppgiftsansvarige.

Om inte den Personuppgiftsansvarige i dessa bestämmelser eller senare ger en dokumenterad instruktion om överföring av personuppgifter till ett tredje land har Personuppgiftsbiträdet inte rätt att göra sådana överföringar inom ramen för dessa bestämmelser.

Microsoft Azure Cloud-support tillhandahålls direkt till Microsoft Ireland Operations från:

- **Microsoft**,
  One Microsoft Way,

Redmond, Seattle,
Washington State,
USA.

Närmare uppgifter om de tjänster och det stöd som tillhandahålls av personuppgiftsbiträden i tredje land finns på följande adress: https://auzre.microsoft.com/da-dk/support/legal.

C.7 RUTINER FÖR DEN PERSONUPPGIFTSANSVARIGES REVISIONER, INKLUSIVE INSPEKTIONER, MED BEHANDLING AV PERSONUPPGIFTER SOM ANFÖRTROTTS PERSONUPPGIFTSBITRÄDET

Den Personuppgiftsansvariges tillsynsverksamhet ska utföras som en integrerad del av de regelbundna statusmötena mellan parterna, i enlighet med den samarbetsmodell som fastställts i huvudavtalet mellan parterna. Vid statusmötena ska bland annat säkerhets- och databehandlingsfrågor diskuteras mot bakgrund av parternas ömsesidiga hotbilder, uppdaterade bedömningar av kritiska sårbarheter, identifierade säkerhetshot och liknande som påverkar den övergripande säkerheten för den behandlingsverksamhet som regleras av avtalet.

VID EN HÖG RISKNIVÅ INHÄMTAS FÖLJANDE ÅRLIGEN:	OM RISKNIVÅN INTE ÄR HÖG, INHÄMTAS FÖLJANDE ÅRLIGEN:
✓ ISAE-3000-periodredovisning, × ISAE-3402-periodredovisning, × SOC 3-rapport, × Liknande revisionsmaterial, definierat nedan:	× ISAE-3000-periodredovisning, × ISAE-3000-punktredovisning, × ISAE-3402-periodredovisning, × SOC-rapport, × Liknande revisionsmaterial, definierat nedan:

✓ Personuppgiftsbiträdet fyller i säkerhetsformuläret från den Personuppgiftsansvarige och rapporterar resultat och metod till den Personuppgiftsansvarige.	× Personuppgiftsbiträdet fyller i säkerhetsfrågeformulär från den Personuppgiftsansvarige. Den Personuppgiftsansvarige rapporterar resultat och metod till den Personuppgiftsansvarige.
✓ Fysisk inspektion av personuppgiftsbiträde med tillhörande inspektionsrapport.	× Fysisk inspektion av personuppgiftsbiträde med tillhörande inspektionsrapport.

Parterna har gemensamt bedömt att risknivån för de registrerade är hög, och man har kommit överens om att Personuppgiftsbiträdet ska ta fram och lämna in en periodisk ISAE 3000-rapport till den Personuppgiftsansvarige minst en gång om året och utan extra kostnad för den Personuppgiftsansvarige som dokumentation på att underbiträdet följer avtalet om behandling av personuppgifter. Det innebär att den Personuppgiftsansvarige ges möjlighet att genomföra inspektioner på platser för databehandlingen, precis som Personuppgiftsbiträdet kan åläggas att årligen fylla i en säkerhetsenkät som beskriver Personuppgiftsbiträdets säkerhetsåtgärder och beteende.

Dokumentationen ska utan onödigt dröjsmål överlämnas till den Personuppgiftsansvarige för kännedom, under förutsättning att den Personuppgiftsansvarige får dela innehållet med Kunden. Den Personuppgiftsansvarige kan bestrida ramverket och/eller granskningsmetoden, och kan i så fall begära ny dokumentation inom ett annat ramverk och/eller med hjälp av en annan metod.

På grundval av resultatet har den Personuppgiftsansvarige rätt att begära att ytterligare åtgärder vidtas för att säkerställa efterlevnad av dataskyddsförordningen, dataskyddsbestämmelser i annan EU-lagstiftning eller medlemsstaternas nationella lagstiftning och dessa bestämmelser.

Därutöver har den Personuppgiftsansvarige eller en företrädare för den Personuppgiftsansvarige tillgång till att utföra inspektioner, inklusive fysiska inspektioner, av de platser från vilka Personuppgiftsbiträdet behandlar personuppgifter, inklusive fysiska platser och system som används för, eller i samband med behandlingen. Sådana kontroller kan göras när den Personuppgiftsansvarige anser det vara nödvändigt.