



PERSONUPPGIFTSBITRÄDESAVTAL GDPR HERO REGISTER

GDPR HERO AB, Trollebergsvägen 5A, 222 29 Lund

Ver. 2024:1

Personuppgiftsbiträdesavtal

Detta personuppgiftsbiträdesavtal ("PuB-avtal") upprättas i enlighet med EU-kommissionens genomförandebeslut (EU) 2021/915 av den 4 juni 2021, som fastställer standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden enligt artikel 28.7 i Europaparlamentets och rådets förordning (EU) 2016/679 (GDPR).

PuB-avtalet utgör en integrerad del av de allmänna villkor och eventuella skriftliga tilläggsavtal ("Villkor") som ingåtts mellan parterna. Det reglerar hur GDPR Hero AB (org. nr 559088-5116) ("GDPR Hero"), i egenskap av personuppgiftsbiträde, behandlar personuppgifter för den personuppgiftsansvariges räkning ("Kund", även benämnd "personuppgiftsansvarig") inom ramen för molntjänsten GDPR Hero ("Tjänsten").

Innehållsförteckning

| | |
|---|-----------|
| AVSNITT I..... | 4 |
| <i>Klausul 1 - Syfte och tillämpningsområde</i> | <i>4</i> |
| <i>Klausul 2 - Klausulernas oföränderlighet.....</i> | <i>4</i> |
| <i>Klausul 3 - Tolkning.....</i> | <i>4</i> |
| <i>Klausul 4 - Hierarki</i> | <i>5</i> |
| <i>Klausul 5 (Frivillig) - Dockningsklausul.....</i> | <i>5</i> |
| AVSNITT II - PARTERNAS SKYLDIGHETER | 5 |
| <i>Klausul 6 - Beskrivning av behandlingen</i> | <i>5</i> |
| <i>Klausul 7 - Parternas skyldigheter</i> | <i>5</i> |
| 7.1 Instruktioner | 5 |
| 7.2 Ändamålsbegränsning..... | 5 |
| 7.3 Varaktigheten för behandlingen av personuppgifter | 6 |
| 7.4 Säkerhet i samband med behandlingen | 6 |
| 7.5 Känsliga uppgifter | 6 |
| 7.6 Dokumentation och efterlevnad | 6 |
| 7.7 Användning av underleverantörer..... | 7 |
| 7.8 Internationella överföringar | 7 |
| <i>Klausul 8 - Stöd till den personuppgiftsansvarige</i> | <i>8</i> |
| <i>Klausul 9 - Anmälan av personuppgiftsincidenter.....</i> | <i>8</i> |
| 9.1 Personuppgiftsincidenter som rör uppgifter som behandlas av den personuppgiftsansvarige | 8 |
| 9.2 Personuppgiftsincident som rör uppgifter som behandlas av personuppgiftsbiträdet | 9 |
| AVSNITT III – SLUTBESTÄMMELSER | 10 |
| <i>Klausul 10 - Bristande efterlevnad av klausulerna och uppsägning</i> | <i>10</i> |
| TILLÄGGSKLAUSULER | 10 |
| <i>Rätt till ersättning</i> | <i>10</i> |
| <i>Ansvar</i> | <i>11</i> |
| BILAGA I - Förteckning över parter | 12 |
| BILAGA II - Beskrivning av behandlingen | 13 |
| BILAGA III - Tekniska och organisatoriska åtgärder | 14 |
| BILAGA IV - Förteckning över godkända underbiträden | 15 |

STANDARDAVTALSKLAUSULER

AVSNITT I

Klausul 1 - Syfte och tillämpningsområde

- a) Syftet med dessa standardavtalsklausuler (klausulerna) är att säkerställa överensstämmelse med artikel 28.3 och 28.4 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
- b) De personuppgiftsansvariga och de personuppgiftsbiträden som anges i bilaga I har kommit överens om att tillämpa dessa klausuler för att säkerställa efterlevnaden av artikel 28.3 och 28.4 i förordning (EU) 2016/679.
- c) Dessa klausuler är tillämpliga på behandling av personuppgifter i enlighet med bilaga II.
- d) Bilagorna I–IV utgör en integrerad del av klausulerna.
- e) Dessa klausuler påverkar inte de skyldigheter som den personuppgiftsansvarige har enligt förordning (EU) 2016/679.
- f) Genom dessa klausuler säkerställs inte i sig att skyldigheterna i samband med internationella överföringar i enlighet med kapitel V i förordning (EU) 2016/679 fullgörs.

Klausul 2 - Klausulernas oföränderlighet

- a) Parterna förbinder sig att inte ändra klausulerna, förutom för att lägga till information i bilagorna eller uppdatera informationen i dem.
- b) Detta hindrar inte parterna från att inkludera de standardavtalsklausuler som fastställs i dessa klausuler i ett mer omfattande avtal eller att lägga till andra klausuler eller ytterligare skyddsåtgärder, under förutsättning att de inte direkt eller indirekt strider mot klausulerna eller begränsar de registrerades grundläggande rättigheter eller friheter.

Klausul 3 - Tolkning

- a) Om de begrepp som definieras i förordning (EU) 2016/679 används i dessa klausuler ska dessa begrepp ha samma betydelse som i den förordningen.
- b) Dessa klausuler ska läsas och tolkas mot bakgrund av bestämmelserna i förordning (EU) 2016/679.
- c) Dessa klausuler ska inte tolkas så att de strider mot de rättigheter och skyldigheter som föreskrivs i förordning (EU) 2016/679 eller påverkar de registrerades grundläggande rättigheter eller friheter.

Klausul 4 - Hierarki

Om dessa klausuler strider mot bestämmelser i tillhörande avtal mellan parterna som gäller vid den tidpunkt då dessa klausuler avtalas eller ingås därefter, ska dessa klausuler ha företräde.

Klausul 5 (Frivillig) - Dockningsklausul

- a) Varje enhet som inte är part i dessa klausuler får, med godkännande från samtliga parter, när som helst ansluta sig till dessa klausuler som personuppgiftsansvarig eller personuppgiftsbiträde genom att fylla i bilagorna och underteckna bilaga I.
- b) När de bilagor som avses i led a har fyllts i och undertecknats ska den anslutande enheten behandlas som part i dessa klausuler och ha de rättigheter och skyldigheter som gäller personuppgiftsansvariga eller personuppgiftsbiträden i överensstämmelse med dess intagande i bilaga I.
- c) Den anslutande enheten ska inte ha några rättigheter eller skyldigheter som följer av dessa klausuler innan den blir part.

AVSNITT II - PARTERNAS SKYLDIGHETER

Klausul 6 - Beskrivning av behandlingen

Närmare uppgifter om behandlingen, särskilt kategorierna av personuppgifter och de ändamål för vilka personuppgifterna behandlas för den personuppgiftsansvariges räkning, anges i bilaga II.

Klausul 7 - Parternas skyldigheter

7.1 Instruktioner

- a) Personuppgiftsbiträdet får endast behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av. I så fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida detta inte är förbjudet med hänvisning till ett viktigt allmänintresse enligt denna rätt. Den personuppgiftsansvarige får även ge efterföljande instruktioner under hela den tid som personuppgifterna behandlas. Dessa instruktioner ska alltid dokumenteras.
- b) Personuppgiftsbiträdet ska omedelbart informera den personuppgiftsansvarige om personuppgiftsbiträdet anser att en instruktion från den personuppgiftsansvarige strider mot förordning (EU) 2016/679 eller mot unionens eller medlemsstaternas tillämpliga dataskyddsbestämmelser.

7.2 Ändamålsbegränsning

Personuppgiftsbiträdet får behandla personuppgifterna endast för det eller de specifika ändamål med behandlingen som anges i bilaga II, såvida det inte erhåller ytterligare instruktioner från den personuppgiftsansvarige.

7.3 Varaktigheten för behandlingen av personuppgifter

Behandling som utförs av personuppgiftsbiträdet får endast äga rum under den tid som anges i bilaga II.

7.4 Säkerhet i samband med behandlingen

- a) Personuppgiftsbiträdet ska åtminstone genomföra de tekniska och organisatoriska åtgärder som anges i bilaga III för att säkerställa säkerheten för personuppgifterna. Detta omfattar att skydda uppgifterna mot säkerhetsincidenter som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till uppgifterna (personuppgiftsincident). Vid bedömningen av lämplig säkerhetsnivå ska parterna ta vederbörlig hänsyn till den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för de registrerade.
- b) Personuppgiftsbiträdet ska bevilja sin personal tillgång till de personuppgifter som behandlas endast i den mån det är absolut nödvändigt för att genomföra, förvalta och övervaka avtalet. Personuppgiftsbiträdet ska säkerställa att personer med behörighet att behandla de erhållna personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.

7.5 Känsliga uppgifter

Om behandlingen omfattar personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, genetiska uppgifter eller biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller en persons sexualliv eller sexuella läggning eller uppgifter om fällande domar i brottmål och överträdelser (känsliga uppgifter), ska personuppgiftsbiträdet tillämpa särskilda begränsningar och/eller ytterligare skyddsåtgärder.

7.6 Dokumentation och efterlevnad

- a) Parterna ska kunna visa att dessa klausuler följs.
- b) Personuppgiftsbiträdet ska skyndsamt och på lämpligt sätt hantera förfrågningar från den personuppgiftsansvarige om behandlingen av uppgifter i enlighet med dessa klausuler.
- c) Personuppgiftsbiträdet ska ge den personuppgiftsansvarige tillgång till all information som behövs för att påvisa efterlevnad av de skyldigheter som fastställs i dessa klausuler och härrör direkt från förordning (EU) 2016/679. På den personuppgiftsansvariges begäran ska personuppgiftsbiträdet även tillåta och bidra till granskningar av den behandling som omfattas av dessa klausuler, med rimliga intervall eller om det finns tecken på bristande efterlevnad. Vid beslut om översyn eller granskning får den personuppgiftsansvarige ta hänsyn till relevanta certifieringar som personuppgiftsbiträdet innehar.
- d) Den personuppgiftsansvarige kan välja att själv utföra granskningen eller bemyndiga en oberoende revisor. Granskningar får även omfatta inspektioner i personuppgiftsbitrådets lokaler eller fysiska anläggningar och ska vid behov utföras med rimligt varsel.
- e) Parterna ska på begäran göra den information som avses i denna klausul, inklusive resultaten av eventuella granskningar, tillgänglig för den (de) behöriga tillsynsmyndigheten(-erna).

7.7 Användning av underleverantörer

- a) Allmänt skriftligt tillstånd: Personuppgiftsbiträdet har erhållit ett allmänt tillstånd från den personuppgiftsansvarige att anlita underleverantörer från en överenskommen förteckning. Personuppgiftsbiträdet ska skriftligen informera den personuppgiftsansvarige om eventuella planerade ändringar av förteckningen genom att underleverantörer läggs till eller ersätts minst 30 dagar i förväg, så att den personuppgiftsansvarige får tillräckligt med tid för att kunna invända mot sådana ändringar innan den eller de berörda underleverantörerna anlitas. Personuppgiftsbiträdet ska tillhandahålla den personuppgiftsansvarige den information som krävs för att denne ska kunna utöva sin rätt att göra invändningar.
- b) Om personuppgiftsbiträdet anlitar en underleverantör för att utföra en specifik behandling (för den personuppgiftsansvariges räkning) ska personuppgiftsbiträdet göra detta genom ett avtal som i sak ålägger underleverantören samma skyldigheter i fråga om uppgiftsskydd som de som personuppgiftsbiträdet åläggs i enlighet med dessa klausuler. Personuppgiftsbiträdet ska se till att underleverantören uppfyller de skyldigheter som personuppgiftsbiträdet omfattas av enligt dessa klausuler och förordning (EU) 2016/679.
- c) På den personuppgiftsansvariges begäran ska personuppgiftsbiträdet tillhandahålla den personuppgiftsansvarige en kopia av ett sådant underleverantörsavtal och eventuella senare ändringar. I den mån det är nödvändigt för att skydda affärshemligheter eller annan konfidentiell information, inbegripet personuppgifter, får personuppgiftsbiträdet redigera avtalstexten innan kopian delas.
- d) Personuppgiftsbiträdet ska fortsatt vara fullt ut ansvarig gentemot den personuppgiftsansvarige för att underleverantören fullgör sina skyldigheter i enlighet med sitt avtal med personuppgiftsbiträdet. Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige om underleverantören underlåter att uppfylla sina skyldigheter enligt avtalet.
- e) Personuppgiftsbiträdet och underleverantören ska avtala om en klausul om tredjepartsberättigande, enligt vilken den personuppgiftsansvarige – om personuppgiftsbiträdet har upphört att existera i faktisk eller rättslig mening eller har hamnat på obestånd – ska ha rätt att säga upp underleverantörsavtalet och instruera underleverantören att radera eller återlämna personuppgifterna.

7.8 Internationella överföringar

- a) Personuppgiftsbiträdet får endast överföra uppgifter till ett tredjeland eller en internationell organisation på grundval av dokumenterade instruktioner från den personuppgiftsansvarige eller för att uppfylla ett särskilt krav enligt unionsrätten eller en medlemsstats lagstiftning som personuppgiftsbiträdet omfattas av, och överföringen ska genomföras i enlighet med kapitel V i förordning (EU) 2016/679.
- b) Den personuppgiftsansvarige samtycker till att, om personuppgiftsbiträdet anlitar en underleverantör i enlighet med klausul 7.7 för att utföra specifik behandling (för den personuppgiftsansvariges räkning) och denna behandling omfattar en överföring av personuppgifter i den mening som avses i kapitel V i förordning (EU) 2016/679, personuppgiftsbiträdet och underleverantören kan säkerställa att kapitel V i förordning (EU) 2016/679 efterlevs genom att använda standardavtalsklausuler som antagits av kommissionen i enlighet med artikel 46.2 i förordning (EU) 2016/679, förutsatt att villkoren för att använda dessa standardavtalsklausuler är uppfyllda.

Klausul 8 - Stöd till den personuppgiftsansvarige

- a) Personuppgiftsbiträdet ska utan dröjsmål underrätta den personuppgiftsansvarige om varje begäran som erhållits från den registrerade. Personuppgiftsbiträdet ska inte själv besvara begäran, såvida inte den personuppgiftsansvarige har godkänt detta.
- b) Personuppgiftsbiträdet ska hjälpa den personuppgiftsansvarige att fullgöra sin skyldighet att besvara framställningar från registrerade för att utöva sina rättigheter, med hänsyn till behandlingens art. Personuppgiftsbiträdet ska följa den personuppgiftsansvariges instruktioner när det fullgör sina skyldigheter i enlighet med leden a och b.
- c) Utöver personuppgiftsbitrådets skyldighet att bistå den personuppgiftsansvarige enligt klausul 8 b ska personuppgiftsbiträdet dessutom bistå den personuppgiftsansvarige med att säkerställa att följande skyldigheter fullgörs, med beaktande av uppgiftsbehandlingens art och den information som personuppgiftsbiträdet har att tillgå:
 - 1) Skyldigheten att utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter (en konsekvensbedömning avseende dataskydd) om en typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.
 - 2) Skyldigheten att samråda med den (de) behöriga tillsynsmyndigheten(-erna) före behandling om en konsekvensbedömning avseende dataskydd visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken.
 - 3) Skyldigheten att säkerställa att personuppgifterna är korrekta och uppdaterade genom att utan dröjsmål informera den personuppgiftsansvarige om personuppgiftsbiträdet får kännedom om att de personuppgifter som behandlas är felaktiga eller har blivit föråldrade.
 - 4) Skyldigheterna i artikel 32 i förordning (EU) 2016/679.
- d) Parterna ska i bilaga III ange de lämpliga tekniska och organisatoriska åtgärder genom vilka personuppgiftsbiträdet ska bistå den personuppgiftsansvarige vid tillämpningen av denna klausul samt räckvidden och omfattningen av det bistånd som krävs.

Klausul 9 - Anmälan av personuppgiftsincidenter

Vid en personuppgiftsincident ska personuppgiftsbiträdet samarbeta med och bistå den personuppgiftsansvarige för att denne ska kunna fullgöra sina skyldigheter enligt artiklarna 33 och 34 i förordning (EU) 2016/679, i tillämpliga fall, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå.

9.1 Personuppgiftsincidenter som rör uppgifter som behandlas av den personuppgiftsansvarige

I händelse av en personuppgiftsincident som rör uppgifter som behandlas av den personuppgiftsansvarige ska personuppgiftsbiträdet bistå den personuppgiftsansvarige med att

- a) anmäla personuppgiftsincidenten till den (de) behöriga tillsynsmyndigheten(-erna), utan onödigt dröjsmål efter det att den personuppgiftsansvarige har fått kännedom om den, i förekommande fall/(med undantag för om det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för fysiska personers rättigheter och friheter),
- b) erhålla följande information som, i enlighet med artikel 33.3 i förordning (EU) 2016/679, ska anges i den personuppgiftsansvariges anmälan, och åtminstone ska omfatta
 - 1) personuppgifternas art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,
 - 2) de sannolika konsekvenserna av personuppgiftsincidenten,
 - 3) de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

Om och i den mån det inte är möjligt att tillhandahålla all denna information samtidigt ska den ursprungliga anmälan innehålla den information som finns tillgänglig, och ytterligare information ska därefter, i den mån den blir tillgänglig, tillhandahållas utan onödigt dröjsmål.

- c) uppfylla, i enlighet med artikel 34 i förordning (EU) 2016/679, skyldigheten att utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten, om den sannolikt kommer att medföra en hög risk för fysiska personers rättigheter och friheter.

9.2 Personuppgiftsincident som rör uppgifter som behandlas av personuppgiftsbiträdet

I händelse av en personuppgiftsincident som rör uppgifter som behandlas av personuppgiftsbiträdet ska personuppgiftsbiträdet underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter det att personuppgiftsbiträdet har fått kännedom om incidenten. En sådan anmäla ska åtminstone innehålla

- a) en beskrivning av incidentens art (inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade och uppgiftsposter som berörs),
- b) uppgifter från en kontaktpunkt där mer information om personuppgiftsincidenten kan erhållas,
- c) de sannolika konsekvenserna och de åtgärder som vidtagits eller föreslagits för att åtgärda incidenten, inbegripet åtgärder för att mildra dess potentiella negativa effekter.

Om och i den mån det inte är möjligt att tillhandahålla all denna information samtidigt ska den ursprungliga anmälan innehålla den information som finns tillgänglig, och ytterligare information ska därefter, i den mån den blir tillgänglig, tillhandahållas utan onödigt dröjsmål.

Parterna ska i bilaga III ange alla andra uppgifter som personuppgiftsbiträdet ska tillhandahålla när denne bistår den personuppgiftsansvarige vid fullgörandet av den

personuppgiftsansvariges skyldigheter enligt artiklarna 33 och 34 i förordning (EU) 2016/679.

AVSNITT III – SLUTBESTÄMMELSER

Klausul 10 - Bristande efterlevnad av klausulerna och uppsägning

- a) Utan att det påverkar tillämpningen av bestämmelserna i förordning (EU) 2016/679 får den personuppgiftsansvarige, om personuppgiftsbiträdet inte fullgör sina skyldigheter enligt dessa klausuler, instruera personuppgiftsbiträdet att avbryta behandlingen av personuppgifter till dess att denne uppfyller dessa klausuler eller avtalet sägs upp. Personuppgiftsbiträdet ska omedelbart underrätta den personuppgiftsansvarige om denne av något skäl inte kan följa dessa klausuler.
- b) Den personuppgiftsansvarige ska ha rätt att säga upp avtalet i den mån det avser behandling av personuppgifter i enlighet med dessa klausuler om
 - 1) personuppgiftsbitrådets behandling av personuppgifter har avbrutits av den personuppgiftsansvarige i enlighet med led a och om efterlevnaden av dessa klausuler inte återställs inom rimlig tid och i alla händelser inom en månad efter det att behandlingen avbrutits,
 - 2) personuppgiftsbiträdet allvarligt eller ihållande åsidosätter dessa klausuler eller sina skyldigheter enligt förordning (EU) 2016/679,
 - 3) personuppgiftsbiträdet underlåter att följa ett bindande beslut från en behörig domstol eller den (de) behöriga tillsynsmyndigheten(-erna) som rör dennes skyldigheter i enlighet med dessa klausuler eller förordning (EU) 2016/679.
- c) Personuppgiftsbiträdet ska ha rätt att säga upp avtalet i den mån det avser behandling av personuppgifter enligt dessa klausuler, om den personuppgiftsansvarige, efter att ha informerats av personuppgiftsbiträdet om att dennes instruktioner strider mot tillämpliga rättsliga krav i enlighet med klausul 7.1 b, insisterar på att instruktionerna följs.
- d) Efter uppsägningen av avtalet ska personuppgiftsbiträdet, beroende på vad den personuppgiftsansvarige väljer, radera alla personuppgifter som behandlats för den personuppgiftsansvariges räkning och intyga för den personuppgiftsansvarige att detta är utfört, eller återlämna alla personuppgifter till den personuppgiftsansvarige och radera befintliga kopior, såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt. Till dess att uppgifterna raderas eller återlämnas ska personuppgiftsbiträdet säkerställa efterlevnaden av dessa klausuler.

TILLÄGGSKLAUSULER

Rätt till ersättning

GDPR Hero har rätt till ersättning för det arbete som utförs i enlighet med detta avtal, inkluderande men inte begränsat till följande:

- a) Utförande av nya instruktioner enligt Bilaga II.
- b) Bistånd som begärs av den personuppgiftsansvarige, i enlighet med Klausul 8.
- c) Granskningar och inspektioner, i enlighet med Klausul 7.6.c.
- d) Tillhandahållande av kopior av avtal med underbiträden, i enlighet med Klausul 7.7.c.

Ersättning ska utgå i enlighet med gällande prislista eller enligt överenskommelse mellan Parterna.

Ansvar

Vid ersättning för skada som uppstår i samband med behandling av personuppgifter och som, genom fastställd dom eller förlikning, ska utgå till en registrerad på grund av överträdelse av detta PuB-avtal och/eller tillämplig dataskyddslagstiftning, ska artikel 82 GDPR tillämpas.

Eventuella administrativa sanktionsavgifter enligt artikel 83 GDPR eller 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ska bäras av den Part som påförts sådan avgift, i enlighet med tillämplig lagstiftning.

Om någon av Parterna blir medveten om en omständighet som kan orsaka skada för den andra Parten, ska den omedelbart informera motparten om förhållandet. Parterna ska därefter samarbeta aktivt för att förhindra och minimera potentiella skador.

BILAGA I - Förteckning över parter

Personuppgiftsansvarig

Namn (organisationsnummer): Kund, specificeras i det övriga avtalsdokument som styr Parternas samarbete (t.ex. allmänna villkor för tjänsten, offert eller annan överenskommelse).

Adress: Specificeras i ovan nämnda avtalsdokument.

Kontaktpersonens namn, befattning och kontaktuppgifter: Specificeras i ovan nämnda avtalsdokument.

Underskrift och anslutningsdatum: Specificeras i ovan nämnda avtalsdokument eller enligt digital signering.

Personuppgiftsbiträde

Namn (organisationsnummer): GDPR Hero AB (559088-5116)

Adress: Trollebergsvägen 5A, 222 29 Lund

Kontaktpersonens namn, befattning och kontaktuppgifter: Julianne Ahlesten, jurist, julianne@gdprhero.se.

Underskrift och anslutningsdatum: Enligt digitalt avtalsslut.

BILAGA II - Beskrivning av behandlingen

| | |
|---|--|
| Kategorier av registrerade vars personuppgifter behandlas | <p>Kunds anställda, kontaktpersoner hos personuppgiftsbiträden, personuppgiftsansvariga och dataskyddsombud, kunds registrerade vid administrering av registerutdrag eller förfrågningar, och andra kategorier av registrerade som Kund väljer att dokumentera i Tjänsten i syfte att dokumentera och följa GDPR.</p> |
| Kategorier av personuppgifter | <p>De kategorier av personuppgifter som behandlas inkluderar, men är inte begränsade till: namn, telefonnummer, e-postadress och befattning samt arbetsplats. Användarnamn och IP-adress.</p> |
| Känsliga uppgifter som behandlas | <p>Kund intygar att särskilda kategorier av personuppgifter och personuppgifter som rör fällande domar i brottmål samt överträdelser inte registreras i Tjänsten.</p> |
| Behandlingens art | <p>Omfattar en rad aktiviteter som möjliggör för Kund att uppfylla sina skyldigheter enligt GDPR. Dessa aktiviteter inkluderar, men är inte begränsade till, att föra register över behandlingar, registrera och hantera information relaterad till organisatorisk säkerhet, skapa och hantera registerutdrag, samt dokumentera och följa upp personuppgiftsincidenter. Inloggning till Tjänsten loggas. Tjänsten stödjer även vidare behandling av personuppgifter genom funktioner som Att-göra-listor och fritextrutor där Kund själv kan strukturera sin dataskyddshantering. Vidare inkluderar behandlingen lagring, strukturering och dokumentation av kontaktuppgifter till personuppgiftsbiträden, personuppgiftsansvariga och dataskyddsombud, vilket underlättar administration och kommunikation mellan relevanta parter. Det finns även möjlighet att få automatiska påminnelser via e-post.</p> |
| Ändamål för vilka personuppgifterna behandlas för den personuppgiftsansvariges räkning | <p>Stödja Kund i att uppfylla sina skyldigheter enligt GDPR, inklusive dokumentation av behandlingar, hantering av registerutdrag och incidentrapporter samt löpande uppföljning av dataskyddsrelaterade uppgifter. Behandlingen syftar även till att tydliggöra ansvarsroller och säkerställa spårbarhet genom dokumentation av kontaktuppgifter till relevanta aktörer. Tjänsten ger Kund de verktyg som behövs för att systematiskt säkerställa GDPR-efterlevnad.</p> |
| Behandlingens varaktighet | <p>Personuppgifterna ska raderas av GDPR Hero inom 180 dagar efter PuB-avtalets upphörande. Kund styr själv hur länge uppgifter är registrerade i Tjänsten med stöd av funktion för radering/borttagning.</p> |

BILAGA III - Tekniska och organisatoriska åtgärder

En beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som den eller de berörda personuppgiftsbiträdena vidtagit (inbegripet eventuella relevanta certifieringar) för att säkerställa en lämplig säkerhetsnivå, med beaktande av behandlingens art, omfattning, sammanhang och syfte samt riskerna för fysiska personers rättigheter och friheter.

- Data i Tjänsten är endast tillgänglig via säker inloggning.
- Personuppgiftsbiträdet ska säkerställa att administrativ åtkomst till Tjänsten och de system som används för att tillhandahålla Tjänsten endast är möjlig från betrodda enheter och kräver användning av multifaktorsautentisering (MFA).
- Back-up/säkerhetskopia tas dagligen och sparas i 7 dagar.
- Återställningsloggar av back-uper.
- Samtlig personal och underbiträden har tystnadsplikt som regleras bindande sekretessavtal.
- Ändringar i dokumentationen i Tjänsten loggas.
- Information skyddas vid lagring av krypteringsåtgärder.
- Intrusion Detection System (IDS): Implementering av system för intrångsdetektering som övervakar och larmar vid potentiella säkerhetsincidenter.
- 24/7-övervakning: Kontinuerlig övervakning av säkerhetstjänster dygnet runt för att upptäcka och hantera hot i realtid.
- Kontrollerad fysisk åtkomst: Protokollförd åtkomst till system via kortläsare.
- 24/7 CCTV-övervakning: Permanent kameraövervakning för att säkerställa fysiskt skydd av anläggningarna.
- Skyddade serverutrymmen: Servrar förvaras i separata, skyddade utrymmen med elektroniska ID-skannrar för att begränsa åtkomst till behörig personal.

BILAGA IV - Förteckning över godkända underbiträden

Den personuppgiftsansvarige har godkänt att personuppgiftsbiträdet använder följande underleverantörer (underbiträden) för att utföra specifika behandlingar av personuppgifter enligt detta avtal.

| FIRMANAMN | ORGANISATIONS-NUMMER | BESKRIVNING AV BEHANDLING SOM UTFÖRS AV UNDERBITRÄDET | PLATS FÖR BEHANDLING AV PERSONUPPGIFTER |
|------------------------|----------------------|---|---|
| OMMH Scandinavia AB | 556720-9092 | För att utveckla och upprätthålla funktionaliteten i GDPR Hero. | Sverige |
| Qnova Systems AB | 556630-9182 | För att kunna upprätthålla Tjänsten använder vi Qnova som en leverantör för server, lagring och back-up inom Sverige. | Sverige |
