PERSONUPPGIFTSBITRÄDESAVTAL
GDPR HERO REGISTER

Ver. 2022:1

GDPR HERO AB, Bankgatan 1A, 223 52 Lund

INNEHÅLLSFÖRTECKNING

1. BAKGRUND OCH SYFTE

1.1 Detta personuppgiftsbiträdesavtal med bilagor (“**PuB-avtal**”) utgör en del av de allmänna villkor samt eventuella skriftliga ändringar (”**Villkor**”) som slutits mellan Parterna och reglerar personuppgiftsbiträdet GDPR Hero AB:s (559088-5116)(”**GDPR Hero**”) behandling av personuppgifter för den personuppgiftsansvariges (”**Kund**”) räkning, i molntjänsten GDPR Hero (”**Tjänsten**”), var och en benämnd som **Part** och tillsammans **Parterna**.

1.2 Syftet med detta PuB-avtal är att GDPR Hero ska lämna tillräckliga garantier om att lämpliga tekniska och organisatoriska åtgärder har genomförts på ett sådant sätt att behandlingen uppfyller kraven i GDPR och säkerställer att den registrerades rättigheter skyddas. Inget i detta PuB-avtal ska tolkas som en rättighet eller förpliktelse för en Part att behandla personuppgifter på ett sätt som inte är förenligt med gällande dataskyddslagstiftning.

2. DEFINITIONER

2.1 I detta PuB-avtal har termerna, nedan, med inledande versal följande betydelse:

”Dataskyddslag”
avser GDPR, lag (2018:218) om kompletterande bestämmelser till EU:s dataskyddsförordning och andra, vid var tid gällande, författningar avseende skyddet för registrerades fri- och rättigheter vid behandling av personuppgifter enligt detta PuB-avtal.

”GDPR”
avser 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).

”Kund”
avser en juridisk eller fysisk person som ingått Villkor och som, inom ramen för detta PuB-avtal, är den personuppgiftsansvarige.

”Underbiträde”
avser ett personuppgiftsbiträde till GDPR Hero.

2.2 Begrepp som definieras i GDPR har samma betydelse i detta PuB-avtal.

3. KUNDENS FÖRPLIKTELSER

3.1 Kunden instruerar GDPR Hero att behandla personuppgifter enligt följande:

(a) för att tillhandahålla Tjänsten;

(b) för att efterleva Kundens dokumenterade instruktioner enligt Bilaga 1; och

(c) för att efterleva övriga instruktioner i skriftlig form, godkända av GDPR Hero inom ramen för detta PuB-avtal, innefattande ändringar i tekniska eller organisatoriska åtgärder.

4. GDPR HERO:S FÖRPLIKTELSER

4.1 GDPR Hero får endast behandla personuppgifter enligt avsnitt 3 (Kundens förpliktelser), ovan, om inte något av följande är tillämpligt:

(a) en annan behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som GDPR Hero omfattas av (i så fall ska GDPR Hero informera Kunden om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt); eller

(b) instruktionerna strider mot Dataskyddslag.

4.2 GDPR Hero ska på begäran från Kund bistå denne med att säkerställa att skyldigheterna enligt artikel 32–36 GDPR fullgörs och svara på begäran om utövande av rättigheter i enlighet med III kapitel GDPR med beaktande av typen av behandling och den information som GDPR Hero har att tillgå.

4.3 Om GDPR Hero finner att Kundens instruktioner är otydliga, i strid med Dataskyddslag eller saknas och GDPR Hero bedömer att nya eller kompletterande instruktioner är nödvändiga för att genomföra sina förpliktelser enligt detta PuB-avtal ska GDPR Hero utan dröjsmål informera Kunden, i den mån det är möjligt tillfälligt upphöra med behandlingen och invänta nya instruktioner.

5. SÄKERHET

5.1 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 ska GDPR Hero vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt:

(a) pseudonymisering och kryptering av personuppgifter;

(b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos Tjänsten;

(c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident; och

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

Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

5.2 GDPR Hero och personer som utför arbete under GDPR Hero:s överinseende, och som får tillgång till personuppgifter, får endast behandla dessa på instruktion från Kund, såvida han

eller hon inte är skyldig att göra det enligt unionsrätten eller medlemsstaternas nationella rätt.

5.3 GDPR Hero ska säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.

5.4 Eventuella tillkommande eller ändrade krav på tekniska eller organisatoriska säkerhetsåtgärder från Kunden, efter Parternas tecknande av detta PuB-avtal, ska klassificeras som ändrade instruktioner enligt punkt 3.1.c, ovan.

6. REVISION

6.1 GDPR Hero ska ge Kunden tillgång till all information som krävs för att visa att de skyldigheter som fastställs i detta PuB-avtal har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av Kunden eller av en annan revisor som bemyndigats av Kunden.

6.2 Parterna är eniga om att revision ska utföras av en tredje part som inte är en konkurrent till GDPR Hero. En sådan tredje part ska vara auktoriserad revisor, certifierad informationssäkerhetsrevisor, advokat eller ha motsvarande sakkunskap och erfarenhet.

6.3 I syfte att undvika missförstånd ska Kunden ensamt svara för samtliga kostnader för tredje part inom ramen för revision.

6.4 Kunden ska säkerhetskälla att fysiska personer som genomför revisionen åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.

7. PERSONUPPGIFTSINCIDENT

7.1 GDPR Hero ska underrätta Kunden utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident som rör behandlingar under detta PuB-avtal.

7.2 GDPR Hero:s underrättelse om en personuppgiftsincident ska:

(a) beskriva personuppgiftsincidentens 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;

(b) förmedla namnet på kontaktpunkter där mer information kan erhållas;

(c) beskriva de sannolika konsekvenserna av personuppgiftsincidenten; och

(d) beskriva de åtgärder som GDPR Hero 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 utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

7.3 GDPR Hero ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits.

Dokumentationen ska göra det möjligt för Kunden att kontrollera efterlevnaden av detta avsnitt 7.

8. UNDERBITRÄDEN

8.1 Kunden godkänner härmed att de av GDPR Hero anlitade Underbiträden, som framgår av Bilaga 2, får behandla personuppgifter för Kundens räkning. På begäran av Kunden ska GDPR Hero tillhandahålla en kopia av det underbiträdesavtal som tecknats med ett Underbiträde.

8.2 GDPR Hero ges härmed ett allmänt skriftligt förhandstillstånd att anlita ytterligare Underbiträde inom EU/EES för behandling av personuppgifter. De kriterier som gäller för detta allmänna skriftliga förhandstillstånd är att Underbiträdet ska utföra en del av Tjänstens grundfunktioner, rörande drift, utveckling eller serverhosting och minst motsvara kraven i detta PuB-avtal.

8.3 GDPR Hero ska, i god tid före, informera Kund om att GDPR Hero avser att ersätta eller anlita ett nytt Underbiträde. Informationen ska innehålla uppgift om Underbiträdets namn och platsen för behandlingen samt vilken typ av behandling Underbiträdet ska utföra för Kundens räkning. Om Kund vill invända mot sådana förändringar ska det ske skriftligen och inom trettio (30) dagar från det att Kunden mottagit informationen.

8.4 Personuppgifter får inte behandlas i tredje land, om inte den Personuppgiftsansvarige har godkänt det skriftligen i förväg. Vilket innebär att GDPR Hero inte får, utan ett särskilt skriftligt förhandstillstånd, anlita underbiträde i tredje land.

8.5 GDPR Hero får upphöra att anlita ett Underbiträde utan föregående godkännande från Kund.

8.6 När GDPR Hero anlitar ett Underbiträde för utförande av specifik behandling på Kundens vägnar ska Underbiträdet, genom ett underbiträdesavtal, åläggas samma skyldigheter i fråga om dataskydd som de som fastställs i detta PuB-avtal, och framför allt att ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i detta PuB-avtal. Om Underbiträdet inte fullgör sina skyldigheter i fråga om dataskydd ska GDPR Hero vara fullt ansvarig gentemot Kunden för utförandet av Underbiträdets skyldigheter.

9. ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND

9.1 GDPR Hero får endast överföra personuppgifter till ett tredje land efter Kunds godkännande.

10. ERSÄTTNING

10.1 För arbete enligt nedanstående har GDPR Hero rätt till ersättning.

(a) Nya instruktioner, punkt 3.1.c;

(b) Begäran av bistånd, punkt 4.2;

(c) Nödvändigt arbete för GDPR Hero inför och under Kundens revision, avsnitt 6;

(d) Begäran av kopia av underbiträdesavtal med Underbiträde, punkt 8.1.

11. ANSVAR

11.1 Vid ersättning för skada i samband med behandling av personuppgifter som, genom fastställd dom eller förlikning, ska utgå till den registrerade på grund av överträdelse av bestämmelse i detta PuB-avtal, och/eller bestämmelse i Dataskyddslag ska artikel 82 tillämpas. Sanktionsavgifter enligt artikel 83 GDPR, eller 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ska bäras av den part till detta PuB-avtal som påförts en sådan avgift.

11.2 Om endera Part får kännedom om omständighet som kan leda till skada för motparten ska denna Part omedelbart informera motparten om förhållandet och aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.

11.3 Oaktat vad som stadgas i Villkoren gäller avsnitt 11 i detta PuB-avtal före andra bestämmelser om fördelning mellan Parterna av krav såvitt avser behandling av personuppgifter enligt detta PuB-avtal.

12. LAGVAL OCH TVISTELÖSNING

12.1 Villkors bestämmelser om lagval och tvistelösning är tillämpliga på detta PuB-avtal.

13. UPPSÄGNING

13.1 Vid uppsägning av detta PuB-avtal lagrar GDPR Hero Kundens data, inkluderat personuppgifter, i sextio (60) dagar efter PuB-avtalets sista giltighetsdag, vartefter GDPR Hero äger rätt att radera personuppgifterna om inte annat avtalats. På begäran från Kund ska GDPR Hero radera samtliga lagrade personuppgifter utan dröjsmål. GDPR Hero kan, efter begäran från Kund, överlämna lagrade personuppgifter till Kund.

13.2 Bestämmelser om tystnadsplikt enligt detta PuB-avtal gäller även efter att PuB-avtalet upphört gälla.

***

BILAGA 1: INSTRUKTION FÖR BEHANDLING AV PERSONUPPGIFTER

Ändamål, föremål och art för behandlingen	Ändamålet är främst att Kund inom Tjänsten ska kunna redovisa organisatorisk säkerhet, administrera och dokumentera registerutdrag samt incidentrapporter. Samt visst utrymme för vidare personuppgiftshantering i Att-göra-listor och fritextrutor. Dokumentera kontaktpersoner hos personuppgiftsbiträden, personuppgiftsansvariga, samt dataskyddsombud.
Typer av personuppgifter	Kategorier av personuppgifter inkluderar, men är inte uteslutande, namn, telefonnummer, e-postadress och befattning samt arbetsplats. Kunden intygar att särskilda kategorier av personuppgifter och personuppgifter som rör fällande domar i brottmål samt överträdelser inte registreras i Tjänsten.
Kategorier av registrerade	Kundens anställda, kontaktpersoner hos personuppgiftsbiträden, personuppgiftsansvariga och dataskyddsombud, kundens registrerade vid registerutdrag eller förfrågningar, och andra kategorier av registrerade som Kunden väljer att dokumentera i Tjänsten i syfte att följa och dokumentera enligt GDPR.
Tidsintervall	Personuppgifterna ska raderas av GDPR Hero efter PuB-avtalets upphörande, enligt punkt 13.1.

BILAGA 2: FÖRTECKNING AV UNDERBITRÄDEN

Företag	Organisations-nummer	Syfte	Överförs personuppgifterna utanför EU/EES?
OMMH Scandinavia AB	556720-9092	För att utveckla och upprätthålla funktionaliteten i GDPR Hero.	Nej
Qnova Systems AB	556630-9182	För att kunna upprätthålla Tjänsten använder vi Qnova som en leverantör för server, lagring och back-up inom Sverige.	Nej