

PERSONUPPGIFTSBITRÄDESAVTAL

1 PARTER

Detta personuppgiftsbiträdesavtal ("Biträdesavtal") reglerar villkoren mellan kund under Avtalet ("PuA") och Barium AB ("PuB"), var för sig benämnd "Part" och tillsammans "Parterna", avseende Personuppgiftsbitrådets Behandling av Personuppgifter för Personuppgiftsansvarigs räkning.

2 KONTAKTPERSONER

Parterna ska utse var sin kontaktperson med ansvar för parternas samarbete gällande dataskydd. Ändring av kontaktperson eller kontaktuppgifter ska skriftligen meddelas den andra parten.

3 DEFINITIONER

<i>Personuppgifter</i>	Varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringuppgift eller onlineidentifikator eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska ekonomiska, kulturella eller sociala identitet.
<i>Behandling av personuppgifter</i>	En åtgärd eller i kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiskt eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, lösning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning radering eller förstöring.
<i>PuA</i>	Personuppgiftsansvarig. En fysisk eller juridisk person, offentlig myndighet, intuition eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.
<i>PuB</i>	Personuppgiftsbiträde. En fysisk eller juridisk person, offentlig myndighet intuition eller annat organ som behandlar personuppgifter för PuAs räkning.
<i>Underbiträde</i>	Även kallad underleverantör. En fysisk eller juridisk person, offentlig myndighet intuition eller annat organ, anlitad av <i>PuB</i> för att utföra behandling av personuppgifter vilka tillhör <i>PuA</i> .
<i>Den registrerade</i>	En fysisk person vars personuppgifter är ämne för behandling i någon form.
<i>Personuppgiftsincident</i>	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller förändring eller obehörigt röjande av eller obehörig åtkomst till de personuppgifter som behandlats.

<i>Tillsynsmyndighet</i>	En oberoende offentlig myndighet. I Sverige är detta Datainspektionen.
<i>Tredje part</i>	En fysisk eller juridisk person, offentlig myndighet intuition eller annat organ som inte är den registrerade, PuA eller PuB eller de personer som under PuAs eller PuBs direkta ansvar är behöriga att behandla personuppgifterna.
<i>Tredje land</i>	En stat som inte ingår i Europeiska unionen eller är ansluten till Europeiska ekonomiska samarbetsområdet.
<i>EU-lagstiftningen</i>	Avser (i) vid ikraftträdandet av detta Avtal, Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, samt alla ändringar och tillägg till detta, och (ii) när det blir tillämpligt, 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, nedan även angivet som "GDPR".
<i>Tillämplig dataskyddslag</i>	Avser sådan integritets- och personuppgiftslagstiftning samt all annan eventuell lagstiftning (inklusive förordningar och föreskrifter) som är tillämplig på den personuppgiftsbehandling som sker under Avtalet (såsom personuppgiftslagen (1998:204)) och EU-lagstiftningen, såsom denna kan komma att förändras över tid. Begrepp i detta Biträdesavtal som inte används med versal, såsom "personuppgiftsansvarig", "personuppgiftsbiträde", "personuppgifter", "behandling", "registrerad", m.fl. ska anses ha den betydelse som anges i EU-lagstiftningen.
<i>Avtalet</i>	Avtalet innefattar tjänster som PuB ska tillhandahålla PuA (Barium Live, konsulttjänster mm). Avtalet med eventuella bilagor tillsammans med detta Biträdesavtal reglerar vad PuB ska ansvara för och utföra åt PuA. Detta Biträdesavtal utgör en integrerad del av Avtalet.

4 SYFTE OCH INNEHÅLL

1. Syftet med detta Biträdesavtal är att uppfylla Tillämplig dataskyddslags krav på avtal mellan PuA och en PuB. Behandlingen måste ske i enlighet med krav i Tillämplig dataskyddslagstiftning samt enligt övriga krav och instruktioner som överenskommits i Avtalet, inklusive detta Biträdesavtal.
2. Mellan PuA och PuB har ett Avtal avseende Bariums tjänster, bl. a. i form av tillgång till Barium Live tecknats.
3. Ändringar eller tillägg till detta Biträdesavtal ska göras skriftligen och undertecknas av båda Parter för giltighet.

5 BEHANDLING AV PERSONUPPGIFTER

1. I syfte att skydda registrerade individers integritet och att behandling av personuppgifter hanteras korrekt och med adekvata säkerhetsåtgärder ska *PuA* ge grundläggande information till *PuB* rörande de personuppgifter *PuA* vill att *PuB* ska behandla. Denna information finns upptagen i Bilaga A.

6 INSTRUKTIONER

1. *PuB* förbinder sig att endast behandla personuppgifterna i enlighet med Avtalet samt Tillämplig dataskyddslag.
2. Saknas instruktioner som *PuB* bedömer nödvändiga för att genomföra sina åtaganden ska *PuB*, utan dröjsmål, informera *PuA* om detta och invänta instruktioner.
3. *PuB* åtar sig att inte behandla personuppgifterna för egna ändamål.
4. *PuB* skall utan fördröjning informera *PuA* om *PuB* anser att instruktionerna strider mot tillämplig dataskyddslag.

7 PERSONUPPGIFTSBITRÄDETS GENERELLA ÅTAGANDEN

1. *PuB* åtar sig att följa Tillämplig dataskyddslag vid personuppgiftsbehandlingen.
2. *PuB* åtar sig att vidta relevanta säkerhetsåtgärder som krävs för att skydda personuppgifter under behandling i enlighet med artikel 32 i GDPR.
3. *PuB* åtar sig underhålla en allmänt vedertagen certifieringsmekanism för att påvisa att kraven i artikel 32.1 GDPR efterlevs.
4. *PuB* får inte överföra personuppgifterna till tredje land annat än efter skriftligt samtycke från *PuA* eller i enlighet med fastslagna standardkontraktsklausuler eller till part vilken omfattas av Privacy Shield.
5. *PuB* skall (beroende på vad *PuA* väljer) radera eller återlämna alla behandlade personuppgifter till *PuA* eller erbjuda *PuA* möjlighet att exportera personuppgifter efter det att tillhandahållandet av behandlingstjänster har avslutats.
6. *PuB* skall ge den *PuA* tillgång till all information som krävs för att visa att krav i Tillämpad dataskyddslag har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner som genomförs av *PuA* eller av en annan revisor som bemyndigats *PuA* inom ramen för Avtalet. Om särskilda skäl inte föreligger ska sådan inspektion ske högst en (1) gång per år.
7. *PuB* åtar sig att begränsa behandling av personuppgifter till endast de individer inom den egna organisationen som har behov av dem i syfte leverera avtalad leveransnivå i enlighet med Avtalet.
8. *PuB* får inte lämna ut personuppgifterna eller annan information om personuppgiftsbehandlingen till Tredje part, annat än efter i förväg lämnat skriftliga samtycke från *PuA*, med undantag för när sådant utlämnande kan krävas enligt lag.
9. För det fall myndighet eller annan *tredje part* begär ut information från *PuB* som rör personuppgiftsbehandlingen ska *PuB* utan dröjsmål vidarebefordra sådan framställan till *PuA*. *PuB* ska vid behov assistera *PuA* med att ta fram information som begärts av Tredje part.
10. *PuB* har inte rätt att företräda *PuA* eller agera för dennes räkning gentemot Tredje part med undantag från vad som framgår av punkten *Underbiträden*.

11. *PuB* ska utan dröjsmål informera *PuA* vid upptäckt av eller misstanke om Personuppgiftsincidenter som negativt påverkar personuppgifternas integritet.
12. *PuB* åtar sig att säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iakttäta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.

8 SÄKERHETSÅTGÄRDER

1. I syfte att skydda *PuAs* personuppgifter förbinder sig *PuB* att vidta och upprätthålla tekniska och organisatoriska skyddsåtgärder som ingår i standarderbjudandet av avtalad tjänst under Avtalet.
2. *PuB* intygar att *PuBs* verksamhet hanteras på ett sätt som säkerställer efterlevnad av gällande Tillämpad dataskyddslag. Personuppgiftsbiträdet åtar sig att följa myndighetsbeslut gällande säkerhetsåtgärder för personuppgiftshanteringen.
3. Personuppgifter som enligt GDPR definieras som Känsliga personuppgifter får inte skickas med e-post ut från Barium Live. Ingen part kan garantera fullgott skydd för känsliga personuppgifter när de lämnar Barium Live via e-post.
4. I syfte att skydda personuppgifter förbinder sig *PuA* att använda lämpliga inbyggda och tillhandahållna säkerhetsfunktioner i Barium Live. Exempel på dessa funktioner är gallringsrutiner, konfidentiella formulärfält och rättighetsstrukturer för användarkonton i Barium Live. Vidare förbinder sig *PuA* att följa råd och rekommendationer från *PuB* som kommuniceras i samband med utveckling av nya säkerhetsfunktioner i Barium Live.
5. För att kunna säkerställa att *PuB* vidtar tillräckliga säkerhetsåtgärder har *PuA* rätt till nödvändig och skäligen insyn i *PuBs* verksamhet, system och personuppgiftshantering.
 - a. *PuB* åtar sig att, på *PuAs* begäran, tillhandahålla *PuA* med den information *PuA* behöver för att utöva sin insyn.
 - b. *PuB* har rätt att debitera *PuA* för kostnader förknippade med detta insynsutövande.

9 UNDERBITRÄDEN

Nya Underbiträden för befintlig behandling

PuA lämnar härmed ett allmänt skriftligt godkännande för *PuB* att anlita ett annat Underbiträde för sådan behandling som utförs av befintliga Underbiträden vid Avtalets ingående. *PuB* skal informera *PuA* om sina avsikter att byta ut ett Underbiträde. *PuB* har vid Avtalets ingående tecknat avtalat med Underbiträden upptagna i Bilaga B för behandling av personuppgifter.

Underbiträden för ny behandling

PuB får inte utan *PuAs* skriftliga medgivande anlita ett *Underbiträde* för annan behandling av personuppgifter för *PuAs* räkning som inte omfattas av första stycket. Sådant medgivande ska inte innehållas såvida det inte föreligger objektiva skäl därtill i förhållande till de krav som finns upptagna i detta Avtal. Lämnar *PuA* ej medgivande för anlitan av *Underbiträde* skall *PuB* äga rätt, men ej skyldighet, att säga upp *Avtalet* med den enda konsekvens att förutbetalda abonnemangsavgifter belöpande på kvarvarande avtalsperiod skall återbetalas.

I de fall *PuB* anlitar ett *Underbiträde* för utförande av specifik behandling å *PuAs* vägnar skall detta *Underbiträde*, genom avtal eller annan rättsakt, åläggas samma skyldigheter i fråga om dataskydd som de som fastställs i biträdesavtalet mellan *PuA* och *PuB*.

10 RÄTTELSE OCH RADERING AV PERSONUPPGIFTER

1. *PuB* åtar sig att (i situationer då *PuA* inte själv har möjlighet att genomföra behandlingen) på begäran och instruktion av *PuA* utan dröjsmål (dock inom trettio (30) dagar) radera eller rätta felaktigheter i registrerade personuppgifter.
2. Begäran och instruktion om radering av personuppgifter måste förmedlas skriftligen till *PuB*.
3. Efter det att *PuA* skriftligen begärt radering av personuppgifter får *PuB* endast behandla personuppgifterna som ett led i raderingsprocessen samt för backuptagning i ytterligare 30 dagar.
4. Vid Avtalets upphörande kommer data som (inkl. personuppgifter) *PuA* ansvarar för raderas. Dock sparas all data i ytterligare 30 dagar i backupper innan den kan anses fullständigt raderad.
5. Innan Avtalet löper ut har *PuA* rätt att begära ut personuppgifterna i ett överenskommet digitalt portabelt format. *PuB* åtar sig att vid händelse av återläsning av backupper ånyo radera data som tidigare raderats i tjänsten.

11 PORTABILITET AV PERSONUPPGIFTER

PuB förbinder sig att (i situationer då *PuA* inte själv har möjlighet att genomföra behandlingen) via skriftlig begäran från *PuA* lämna ut personuppgifter i ett (vid begäran) överenskommet format. *PuB* äger rätt till ersättning för sådana åtgärder och tjänster som ligger utanför vad som framgår av *Avtalet*.

12 ANSVAR FÖR SKADA

I händelse av att registrerad riktar anspråk mot *PuA* på ersättning för uppkommen skada eller om en Tillsynsmyndighet utfärdar vite eller andra administrativa påföljder till följd av *PuB* behandlat personuppgifter i strid med *Avtalet* eller Tillämplig dataskyddslag ska *PuB* ersätta *PuA* för uppkommen skada. Eventuell skyldighet att utge ersättning är begränsad på sätt som är angivet i *Avtalet*.

13 ÖVERLÅTELSE

Detta avtal får inte överlåtas utan den andra *Partens* föregående godkännande.

14 AVTALSTID

Detta Biträdesavtal är giltigt från dagen för ingåendet av *Avtalet* och tills *PuBs* behandling av personuppgifterna upphör.

15 TVISTER OCH TILLÄMPLIG LAG

Svensk rätt ska vara tillämplig på avtalet. Tvister i anledning av Biträdesavtalet ska slutligt avgöras av på sätt som anges i *Avtalet*.

Bilaga A

ÄNDAMÅL MED BEHANDLINGEN

PuA har genom *Avtalet* givits rätt att nyttja Barium Live med tillhörande tjänster.

PuB ges tillgång till den information som *PuA* har registrerat i systemet.

TYP AV BEHANDLING

PuB kommer behandla uppgifter i samband med att *PuA* nyttjar Barium Live och andra tillhandahållna tjänster inklusive behandling för support och underhåll av tillhandahållna tjänster.

KATEGORIER OCH TYPER AV PERSONUPPGIFTER

De olika typer av personuppgifter som *PuA* kan välja att samla in och behandla i Barium Live är primärt:

KATEGORIER	TYPER
<ul style="list-style-type: none"> • Personuppgifter om anställda. • Personuppgifter om leverantörer, underleverantörer, medarbetare, konsulter osv. • Personuppgifter om medborgare. • Kontaktuppgifter (CRM) till kunder, partner. • Kontaktuppgifter i marknadsföringssyften. 	<ul style="list-style-type: none"> • Namn • Adress • Profilbild • Närmast anhöriga • Lön • Kontonummer • Telefonnummer • Försäkringsnummer • Registreringsnummer • CV/personliga brev • Uppgifter rörande rehabilitering • Storlek arbetskläder • E-postadress • Inköphistorik • Geografisk data • Fakturauppgifter

Därutöver har *PuA* möjlighet att ladda upp andra personuppgifter (inklusive personuppgifter som enligt GDPR definieras som Känsliga personuppgifter) i samband med nyttjande av Barium Live. *PuA* ger härmed *PuB* rätt att behandla dessa personuppgifter.

Bilaga B

Företag och org. nr	Geografisk lokalisering	Uppgift	Mekanism för översyn vid överföring av data till länder utanför EU/ESS.
DGC IB 556625-7340	DGC IB Sveavägen 145 , plan 5 113 64 Stockholm	Hosting av driftmiljö för avtalad tjänst i vilken PuA kan välja att behandla personuppgifter.	Översynsmekanism ej nödvändig då all data lagras i Sverige.
MailGun	Mailgun Technologies, Inc. 535 Mission St. San Francisco, CA 94105 USA	Köhantering (temporär lagring) av utgående e-postmeddelanden från tjänsten. Notera att det är PuA som själv väljer vilken data som skall skicka ut från tjänsten.	EU-U.S. Privacy Shield Framework
MailChimp	The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 USA	PuB använder MailChimp i syfte att informera vissa typer av användare om förändringar i tjänsten. Typen av behandling rör temporär lagring och vidarebefordring av e-postadresser till PuAs administratörer och testanvändare i avtalad tjänst.	EU-U.S. Privacy Shield Framework
Freshwork	Freshworks, Inc. 1250 Bayhill Drive , Suite 315 San Bruno, California 94066 USA	Freshwork levererar molntjänst (Freshdesk) som PuB använder i syfte att lagra och hantera inskickade supportärenden. Notera att det är PuA som själv väljer vilken data som bifogas postade supportärenden.	EU-U.S. Privacy Shield Framework
Atlassian	Atlassian PTY Ltd Atlassian Inc. (San Francisco, Harrison Street Location) 1098 Harrison Street San Francisco, California 94103 USA	Atlassian levererar molntjänst (Jira Software) som PuB använder i syfte att lagra och hantera tekniska supportärenden. Notera att det är PuA som själv väljer vilken data som bifogas postade supportärenden.	EU-U.S. Privacy Shield Framework