

[Personuppgiftsansvarig], org. nr. [•], härafter benämnd som “kunden” eller “**personuppgiftsansvarig**”, och GS1 Sweden AB, 556667-6770, härafter benämnd som “**personuppgiftsbiträde**”, var för sig “part”; tillsammans “parterna”, har denna dag ingått följande

AVTAL RÖRANDE BEHANDLING AV PERSONUPPGIFTER M.M. (“Personuppgiftsbiträdesavtal”)

1. Bakgrund etc.

- 1.1 I detta Personuppgiftsbiträdesavtal anges rättigheter och skyldigheter för den personuppgiftsansvarige och personuppgiftsbiträdet vid behandling av personuppgifter på uppdrag av kunden.
- 1.2 Personuppgiftsbiträdesavtalet har utformats för att säkerställa parternas uppfyllande av artikel 28.3 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, GDPR).
- 1.3 I samband med personuppgiftsbiträdets fullgörande av Allmänna avtalsvillkor för abonnemang på GS1 Företagsprefix och användning av tjänster i anslutning till GS1 Registry Platform (“**Avtalet**”), kommer personuppgiftsbiträdet att behandla personuppgifter åt den personuppgiftsansvarige i enlighet med Personuppgiftsbiträdesavtalet.
- 1.4 Personuppgiftsbiträdesavtalet ska ha företräde framför liknande bestämmelser i Avtalet eller andra avtal mellan parterna.
- 1.5 Personuppgiftsbiträdesavtalet och dess bilagor ska lagras skriftligt (inklusive elektroniskt) av båda parterna.
- 1.6 Personuppgiftsbiträdesavtalet undantar inte personuppgiftsbiträdet från skyldigheter som personuppgiftsbiträdet omfattas av enligt GDPR eller annan lagstiftning.

2. Den personuppgiftsansvariges rättigheter och skyldigheter

- 2.1 Den personuppgiftsansvarige är ansvarig för att säkerställa att behandlingen av personuppgifter utförs i enlighet med GDPR (se artikel 24 i GDPR), tillämpliga dataskyddsbestämmelser i EU eller medlemsstaten och Personuppgiftsbiträdesavtalet.
- 2.2 Den personuppgiftsansvarige har rätt och skyldighet att besluta om ändamål och medel för behandlingen av personuppgifter.

2.3 Den personuppgiftsansvarige är bland annat ansvarig för att den behandling av personuppgifter som personuppgiftsbiträdet ombeds utföra har rättslig grund.

3. Personuppgiftsbiträdet ska följa instruktionerna

3.1 Personuppgiftsbiträdet får enbart behandla personuppgifter enligt dokumenterade instruktioner från den personuppgiftsansvarige, såvida det inte är skyldigt att göra detta enligt unionsrätten eller medlemsstatens lagstiftning som det omfattas av, varvid personuppgiftsbiträdet ska informera den personuppgiftsansvarige om det rättsliga kravet i förväg, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt. Sådana instruktioner anges i Bilaga 1. Efterföljande instruktioner kan också ges av den personuppgiftsansvarige under behandlingen av personuppgifterna, men sådana instruktioner ska alltid dokumenteras och lagras skriftligt samt elektroniskt i anslutning till Personuppgiftsbiträdesavtalet.

3.2 Personuppgiftsbiträdet ska omedelbart informera den personuppgiftsansvarige om dessa instruktioner enligt personuppgiftsbitrådets uppfattning strider mot GDPR eller tillämpliga dataskyddsbestämmelser i EU eller medlemsstaten.

4. Sekretess

4.1 Parternas skyldighet att iaktta sekretess regleras i Avtalet. I tillägg till detta ska Personuppgiftsbiträdet inte, utan kundens skriftliga samtycke i förväg, lämna ut eller annars tillgängliggöra personuppgifter till tredje man utom såvitt avser underbiträden som har anlåtats i enlighet med Personuppgiftsbiträdesavtalet.

4.2 Åtagandet i punkt 4.1 ovan gäller inte information som personuppgiftsbiträdet föreläggs utge i enlighet med lagstadgad skyldighet enligt unionsrätten eller medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av. I så fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet i förväg i enlighet med punkt 3.1.

4.3 Personuppgiftsbiträdet ska endast bevilja tillgång till de personuppgifter som behandlas på uppdrag av den personuppgiftsansvarige för personer som är underställda personuppgiftsbiträdet och har åtagit sig att iaktta konfidentialitet eller som omfattas av en lämplig lagstadgad tystnadsplikt och endast i den uträkning det är nödvändigt. Förteckningen över de personer som har beviljats tillgång ska granskas regelbundet. Med granskningen som grund kan sådan tillgång till personuppgifter återkallas om tillgången inte längre är nödvändig. Personuppgifterna ska därefter inte längre vara tillgängliga för dessa personer.

4.4 Personuppgiftsbiträdet ska på begäran av den personuppgiftsansvarige kunna visa att berörda personer som är underställda personuppgiftsbiträdet iakttar ovannämnda sekretess.

4.5 Personuppgiftsbiträdet är medvetet om att lag om skydd för företagshemligheter (1990:409) kan äga tillämplighet avseende personuppgifter och annan av kunden ägd information och data.

4.6 Punkt 4.1, 4.2 och 4.5 gäller även om Personuppgiftsbiträdesavtalet i övrigt upphör att gälla.

5. Säkerhet vid behandling

5.1 I artikel 32 i GDPR anges att med beaktande av tidigare känd teknik, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt risken, av varierande sannolikhets- och allvarlighetsgrad, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Den personuppgiftsansvarige ska utvärdera riskerna avseende fysiska personers rättigheter och friheter vid behandlingen och vidta åtgärder för att minska dessa risker.

5.2 Enligt artikel 32 i GDPR ska personuppgiftsbiträdet även – fristående från kunden – utvärdera riskerna för fysiska personers rättigheter och friheter vid behandlingen och vidta åtgärder för att minska dessa risker. Dessutom ska personuppgiftsbiträdet bistå kunden i att säkerställa efterlevnad av kundens skyldigheter enligt artikel 32 i GDPR, genom att bland annat förse kunden med information avseende tekniska och organisatoriska åtgärder som redan har genomförts av personuppgiftsbiträdet enligt artikel 32 i GDPR, samt all övrig information som krävs för att kunden ska kunna fullgöra sin skyldighet enligt artikel 32.

5.3 Om därefter – enligt kundens bedömning – det krävs att ytterligare åtgärder vidtas av personuppgiftsbiträdet än de som redan har vidtagits enligt artikel 32 i GDPR för att riskerna ska minska, ska kunden specificera dessa ytterligare åtgärder och de ska implementeras i Bilaga 1.

5.4 Om personuppgiftsbiträdet gör ändringar i de tekniska och organisatoriska åtgärder som vidtas, ska den personuppgiftsansvariges godkännande inhämtas i förväg. Ändringarna ska återspeglas genom att Bilaga 1 uppdateras.

6. Användning av underbiträden

6.1 Personuppgiftsbiträdet ska uppfylla de krav som anges i artikel 28.2 och 28.4 i GDPR om ett annat personuppgiftsbiträde anlitas (ett underbiträde).

6.2 Personuppgiftsbiträdet får enbart anlita underbiträden med ett specifikt förhandstillstånd från kunden. Den förteckning över underbiträden som har godkänts av kunden återfinns i Bilaga 2.

6.3 Om personuppgiftsbiträdet använder ett underbiträde för att utföra specifik behandling på uppdrag av kunden, ska samma skyldigheter rörande dataskydd som anges i Personuppgiftsbiträdesavtalet åläggas underbiträdet via avtal eller annan rättsakt enligt unionsrätten eller medlemsstatens rätt, särskilt avseende tillräckliga garantier att vidta lämpliga tekniska och organisatoriska åtgärder på

ett sådant sätt att behandlingen uppfyller kraven i Personuppgiftsbiträdesavtalet och GDPR.

- 6.4 Personuppgiftsbiträdet ska därför kräva att underbiträdet som ett minimum fullgör de skyldigheter som gäller för personuppgiftsbiträdet enligt Personuppgiftsbiträdesavtalet och GDPR.
- 6.5 En kopia av ett sådant underbiträdesavtal och efterföljande ändringar ska – på begäran av kunden – skickas till kunden, och därmed ge kunden möjlighet att säkerställa att samma skyldigheter avseende dataskydd som anges i Personuppgiftsbiträdesavtalet gäller för underbiträdet. Kontraktsvillkor avseende affärsrelaterade frågor som inte påverkar det legala innehållet i underbiträdesavtalet såvitt gäller dataskydd, behöver inte lämnas till kunden.
- 6.6 Om underbiträdet inte fullgör sina skyldigheter avseende dataskydd är personuppgiftsbiträdet fullt ansvarigt gentemot kunden för fullgörandet av underbitrådets skyldigheter. Detta påverkar inte de registrerades rättigheter enligt GDPR – särskilt de som föreskrivs i artiklarna 79 och 82 i GDPR – gentemot kunden och personuppgiftsbiträdet, inklusive underbiträdet.

7. Överföring av uppgifter till tredjeland eller internationella organisationer

- 7.1 All överföring av personuppgifter till tredjeland eller internationella organisationer av personuppgiftsbiträdet får endast utföras enligt dokumenterade instruktioner från kunden och ska alltid utföras i enlighet med kapitel V i GDPR.
- 7.2 Om överföringar till tredjeland eller internationella organisationer, vilka personuppgiftsbiträdet inte har instruerats att utföra av kunden, krävs enligt unionsrätten eller medlemsstatens lagstiftning som omfattar personuppgiftsbiträdet, ska personuppgiftsbiträdet informera kunden om det rättsliga kravet innan behandlingen utförs, såvida inte sådan information är förbjuden enligt denna lagstiftning av hänsyn till allmänintresset.
- 7.3 För det fall att överföringsmekanismerna enligt kapitel V i GDPR (oavsett vilken som används för överföringen) inte längre är tillräckliga för att uppfylla kraven i tillämplig dataskyddslagstiftning för överföring av personuppgifter till tredje land, ska personuppgiftsbiträdet använda alla rimliga ansträngningar för att implementera en alternativ överföringsmekanism som uppfyller kraven i tillämplig dataskyddslagstiftning för att möjliggöra överföringen till tredje land eller upphöra med sådan överföring. Om personuppgiftsbiträdet misslyckas med att introducera en sådan alternativ överföringsmekanism eller förändring i tjänsten, får kunden säga upp Avtalet med omedelbar effekt, eller med skälig tidsfrist som fastställs av kunden.

8. Assistans till den personuppgiftsansvarige

- 8.1 Med beaktande av behandlingens art ska personuppgiftsbiträdet bistå kunden med lämpliga tekniska och organisatoriska åtgärder när det är möjligt, i syfte att

fullgöra kundens skyldigheter att besvara förfrågningar om utövande av den registrerades rättigheter enligt kapitel III i GDPR.

8.2 Förutom personuppgiftsbiträdets skyldighet att bistå kunden enligt punkt 5.2, ska personuppgiftsbiträdet dessutom, med beaktande av behandlingens art och den information som finns tillgänglig för personuppgiftsbiträdet, bistå kunden för att säkerställa efterlevnad av:

- a) kundens skyldighet att utan dröjsmål och om möjligt, inte senare än 72 timmar efter upptäckten, anmäla en personuppgiftsincident till behörig tillsynsmyndighet, såvida det inte är osannolikt att personuppgiftsincidenten innebär någon risk för fysiska personers rättigheter och friheter;
- b) kundens skyldighet att utan dröjsmål underrätta den registrerade om en personuppgiftsincident, när personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter;
- c) kundens skyldighet att utföra en bedömning av den påverkan som de planerade behandlingsåtgärderna får på skyddet av personuppgifter (en konsekvensbedömning avseende dataskydd);
- d) kundens skyldighet att samråda med den behöriga tillsynsmyndigheten, före behandlingen där en konsekvensbedömning avseende dataskydd visar att behandlingen skulle innebära en hög risk om inga åtgärder vidtas av kunden för att minska risken.

8.3 Parterna ska i Bilaga 1 ange de lämpliga tekniska och organisatoriska åtgärder som personuppgiftsbiträdet ska bistå kunden med samt omfattningen av det stöd som krävs.

9. Underrättelse om personuppgiftsincident

9.1 Vid en personuppgiftsincident ska personuppgiftsbiträdet omedelbart anmäla personuppgiftsincidenten till kunden efter att personuppgiftsbiträdet fått kännedom om personuppgiftsincidenten för att göra det möjligt för kunden att fullgöra skyldigheten att underrätta behörig tillsynsmyndighet om personuppgiftsincidenten.

9.2 I enlighet med punkt 8.2 a) ska personuppgiftsbiträdet bistå kunden med att underrätta behörig tillsynsmyndighet om personuppgiftsincidenten och bistå vid insamlingen av den information som anges nedan, vilket enligt artikel 33.3 i GDPR ska anges i kundens underrättelse till behörig tillsynsmyndighet:

- a) Personuppgifternas art, inbegripet om så är möjligt de kategorier och ungefärliga antal registrerade som berörs, samt de kategorier och ungefärliga antal personuppgiftsposter som berörs;
- b) De troliga konsekvenserna av personuppgiftsincidenten;

- c) De åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att hantera personuppgiftsincidenten, inbegripet när så är lämpligt åtgärder för att mildra dess potentiellt skadliga effekter.

10. Radera och återlämna uppgifter

- 10.1 Vid upphörandet av tjänsterna som innefattar personuppgiftsbehandling ska personuppgiftsbiträdet vara skyldigt att, utifrån vad kunden väljer, radera eller återlämna alla personuppgifter till kunden utan oskäligt dröjsmål och vilket fall inte senare än inom nittio (90) dagar och radera befintliga kopior, såvida inte det enligt unionsrätten eller medlemsstats lagstiftning krävs att personuppgifterna lagras. På kundens begäran ska personuppgiftsbiträdet tillhandahålla en skriftlig redogörelse för de åtgärder som vidtagits avseende personuppgifter efter upphörande av tjänsterna som innefattar personuppgiftsbehandling.

11. Granskning och inspektion

- 11.1 Personuppgiftsbiträdet ska för kunden tillgängliggöra all information som krävs för att visa att de skyldigheter som anges i artikel 28 i GDPR och i Personuppgiftsbiträdesavtalet efterlevs, samt underlätta och bidra till granskningar, inbegripet inspektioner, som utförs av kunden eller annan granskare på uppdrag av kunden.
- 11.2 Personuppgiftsbiträdet ska ha en skyldighet att ge de tillsynsmyndigheter som enligt tillämplig lagstiftning har tillgång till kundens och personuppgiftsbitrådets lokaler, eller ombud som agerar på uppdrag av sådana tillsynsmyndigheter, tillgång till personuppgiftsbitrådets fysiska lokaler vid uppvisande av lämplig identifikation.
- 11.3 Rätten till granskning och inspektion som anges i detta Personuppgiftsbiträdesavtal ska inte i något avseende begränsa kundens eller någon tillsynsmyndighets rätt till granskning och inspektion enligt övriga bestämmelser i Avtalet.

12. Ansvar

- 12.1 Vid ersättning för skada i samband med personuppgiftsbehandling som, genom fastställd dom eller förlikning, ska utgå till registrerade på grund av överträdelse av bestämmelse i Personuppgiftsbiträdesavtalet, den personuppgiftsansvariges instruktioner, GDPR och/eller lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ska artikel 82 i GDPR tillämpas.
- 12.2 Sanktionsavgifter enligt artikel 83 i GDPR, eller 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ska bäras av den av parterna som påförts en sådan avgift.
- 12.3 Om endera part får kännedom om omständighet som kan leda till skada för motparten ska parten omedelbart informera motparten om förhållandet och

aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.

13. Ersättning

13.1 Personuppgiftsbiträdet är berättigat till skälig ersättning för assistans till den personuppgiftsansvarige i enlighet med detta Personuppgiftsbiträdesavtal.

14. Tvist

14.1 Alla tvister kopplade till detta Personuppgiftsbiträdesavtal ska slutligt avgöras i enlighet med tvistlösningsbestämmelserna i Avtalet. Personuppgiftsbiträdesavtalet ska tolkas enligt svensk lag, utan hänsyn till dess regler om lagval.

15. Inledande och avslutande

15.1 Personuppgiftsbiträdesavtalet börjar gälla det datum då båda parter har undertecknat det.

15.2 Båda parterna ska ha rätt att kräva att Personuppgiftsbiträdesavtalet omförhandlas om ändringar i tillämplig dataskyddslagstiftning ger anledning till en sådan omförhandling. Personuppgiftsbiträdet ska inte oskäligen vägra att gå med på ändringar som kunden begär.

15.3 Personuppgiftsbiträdesavtalet ska gälla under den tid då personuppgiftsbiträdet behandlar personuppgifter på uppdrag av kunden. Under den tid då personuppgiftsbehandlingen utförs kan inte Personuppgiftsbiträdesavtalet sägas upp, såvida inte parterna har enats om andra bestämmelser som gäller för personuppgiftsbehandlingen.

15.4 Om personuppgiftsbehandlingen avslutas och personuppgifterna raderas eller återlämnas till kunden enligt punkt 10, har vardera parten rätt att skriftligen säga upp Personuppgiftsbiträdesavtalet.

Bilaga 1 – Instruktion om hantering av personuppgifter

Följande instruktioner gäller för hantering av de personuppgifter som kunden är personuppgiftsansvarig för. Utöver vad som redan framgår av detta Personuppgiftsbiträdesavtal ska personuppgiftsbiträdet följa nedanstående instruktioner:

Personuppgiftsbehandling

Ändamål Specificera samtliga ändamål för vilka personuppgifter som kommer behandlas av personuppgiftsbiträdet.	<i>Ändamålet med behandlingen är att utföra tjänster i enlighet med Avtalet (se punkt 4 i Avtalet).</i>
Typer av Personuppgifter Specificera typer av personuppgifter som kommer behandlas av personuppgiftsbiträdet.	<i>Kontaktuppgifter, såsom namn, e-postadress och telefonnummer.</i>
Kategorier av Registrerade Specificera samtliga kategorier av registrerade vars uppgifter kommer behandlas av personuppgiftsbiträdet.	<i>Befattningshavare hos kunden, kontaktpersoner hos kundens affärspartners.</i>
Gallringstid Specificera gallringstid avseende när personuppgifterna som behandlas av personuppgiftsbiträdet ska gallras.	<i>Inaktiva personuppgifter raderas årligen.</i>
Praktisk hantering Specificera hur behandling ska gå till.	<i>Se Tjänstebeskrivningen.</i>

Bilaga 2

Godkända underbiträden

Det här en fullständig lista på alla underbiträden som har anlåtats av personuppgiftsbiträdet som underbiträden. Listan ska uppdateras vid behov för att återspegla alla ändringar avseende godkända underbiträden.

BOLAGSNAMN, ORGANISATIONSNUMMER, ADRESS OCH ETABLERINGSLAND	Beskrivning av behandlingsaktivitet	Startdatum	Plats för personuppgifts- behandling	Mekanismer för laglig överföring till tredje land (standardavtals- klausuler, bindande företags- bestämmelser) – om tillämpligt