

Personuppgiftsbiträdesavtal (PUB/DPA)

Mellan

Clubmate AB, org.nr **559378-3458**, adress **Adlerbethsgatan 15, 112 55 Stockholm**
("Biträdet" eller "Clubmate")

och

Ansluten säljare (skolklass/lag/förening) ("**Personuppgiftsansvarig**" eller "**Säljaren**"), enligt de kontaktuppgifter som framgår av Säljarens konto i Tjänsten.

Tillsammans "Parterna".

Bakgrund: Säljaren använder Clubmates plattform för att sälja varor till konsumenter. I detta upplägg är **Säljaren personuppgiftsansvarig** för kunddata i syfte att genomföra försäljning, leverans, kundservice m.m. Clubmate behandlar dessa personuppgifter som **personuppgiftsbiträde** för Säljarens räkning när Tjänsten används. Detta avtal kompletterar Parternas Plattforms-ToS och reglerar biträdesförhållandet enligt GDPR art. 28.

1. Definitioner

Med "**GDPR**" avses Europaparlamentets och rådets förordning (EU) 2016/679. "**Personuppgifter**", "**Behandling**", "**Registrerad**" m.fl. har samma betydelse som i GDPR. "**Underbiträde**" avser tredje part som Biträdet anlitar för Behandling för den Personuppgiftsansvariges räkning.

2. Behandling enligt instruktioner

2.1 Biträdet får endast behandla Personuppgifter enligt dokumenterade **instruktioner** från den Personuppgiftsansvarige, inklusive avseende överföringar till tredje land, om inte EU-rätten eller svensk rätt kräver annat.

2.2 Parternas gemensamma dokumentation (t.ex. beställningar i portalen) utgör instruktioner. Detaljeras i **Bilaga A**.

3. Syften och kategorier (Bilaga A)

3.1 Syften omfattar bl.a. tillhandahållande av portal/shopsidor, order- och kundhantering, leveransstöd, support, felsökning och säkerhet.

3.2 Kategorier: kunders kontaktuppgifter, order- och leveransdata, betalstatus (manuellt registrerad), kommunikation, samt Säljarens användaruppgifter (admin).

3.3 Särskilda kategorier behandlas **inte** avsiktligt. Säljaren ska inte registrera känsliga uppgifter i Tjänsten.

4. Sekretess

4.1 Biträdet säkerställer att endast behörig personal får tillgång till Personuppgifter och att dessa omfattas av lämplig **sekretess** eller lagstadgad tystnadsplikt.

5. Säkerhet (TOMs)

5.1 Biträdet ska vidta **lämpliga tekniska och organisatoriska åtgärder** enligt art. 32 GDPR, med beaktande av risker, kategori av uppgifter och Behandlingens natur.

5.2 Exempel på åtgärder framgår av **Bilaga C** (bl.a. kryptering i transit, åtkomstkontroller, loggning, separata miljöer, backuper, princip om minsta åtkomst).

6. Underbiträden

6.1 Personuppgiftsansvarig ger härmed Biträdet ett allmänt **förhandstillstånd** att anlita Underbiträden för Behandlingen.

6.2 Biträdet ska föra och publicera en **aktuell lista** över Underbiträden (Bilaga B) och underrätta den Personuppgiftsansvarige inför väsentliga ändringar, varvid denne har rätt att invända på sakliga grunder.

6.3 Biträdet ska ingå skriftliga **biträdesavtal** med Underbiträden som ålägger motsvarande dataskyddsåtaganden. Biträdet ansvarar för Underbiträdens handlingar såsom för egna.

7. Hjälp och assistans

7.1 Biträdet ska, med beaktande av Behandlingens art, bistå den Personuppgiftsansvarige med lämpliga tekniska och organisatoriska åtgärder för att uppfylla skyldigheter avseende **registrerades rättigheter** (kapitel III GDPR).

7.2 Biträdet bistår med **dataskyddsbedömningar** (DPIA) och samråd med tillsynsmyndighet i den mån Behandlingen hos Biträdet berörs. Skäliga kostnader kan tillkomma om arbetet är omfattande och ej beror på Bitrådets fel.

8. Incidenter och rapportering

8.1 Biträdet ska utan onödigt dröjsmål underrätta den Personuppgiftsansvarige vid **personuppgiftsincident**. Meddelandet ska innehålla kända fakta, konsekvenser och föreslagna åtgärder.

8.2 Biträdet ska dokumentera incidenter och stödja den Personuppgiftsansvariges utredning och eventuell anmälan till IMY och Registerade.

9. Överföringar till tredje land

9.1 Överföring får endast ske enligt **instruktion** och i enlighet med kapitel V GDPR (t.ex. EU-kommissionens **standardavtalsklausuler** – SCC).

9.2 Om Biträdet bedömer att instruktionen inte kan följas lagligt ska Biträdet omgående informera den Personuppgiftsansvarige.

10. Radering och återlämning

10.1 Vid avtalets upphörande eller på dokumenterad instruktion ska Biträdet **radera eller återlämna** Personuppgifter och radera befintliga kopior inom rimlig tid, om inte lag kräver lagring.

10.2 Loggar och backuper rensas enligt Bitrådets raderingspolicy och tekniska cykler.

11. Ansvar

11.1 Parternas ansvar följer artikel 82 GDPR.

11.2 I förhållandet mellan Parterna begränsas Bitrådets ansvar gentemot den Personuppgiftsansvarige till direkt skada orsakad av Bitrådets överträdelse av detta avtal, dock maximalt till **10 prisbasbelopp** per kalenderår, med undantag för uppsåt/grov vårdslöshet. Begränsning gäller inte lagstadgat ansvar mot Registrerade eller tillsynsmyndighet.

12. Giltighetstid

12.1 Detta avtal gäller så länge Biträdet behandlar Personuppgifter för den Personuppgiftsansvariges räkning inom ramen för Tjänsten.

13. Tillämplig lag och forum

13.1 Svensk lag tillämpas.

13.2 Tvist avgörs av allmän domstol med **Stockholms tingsrätt** som första instans.

Bilaga A – Behandlingsinstruktion

Ändamål: Tillhandahålla plattform (portal/shopsidor), order- och kundhantering, leveransstöd, returer/reklamationer, kommunikation, felsökning och säkerhet, rapportering till Leverantör för leverans/avräkning.

Kategorier av Registrerade: Kunder (konsumenter), Säljarens administratörer/representanter.

Kategorier av uppgifter: Namn, kontaktuppgifter (e-post, telefon), leveransadress, orderrader, betalstatus (manuellt angiven), kommunikationshistorik, tekniska loggar (IP, enhets-/sessionsdata).

Särskilda kategorier: Ej tillåtna att registrera.

Behandlingar: Insamling, strukturering, lagring, läsning, överföring till underbiträden/Leverantör enligt avtal, radering.

Lagringstid: Så länge Säljaren behöver uppgifterna för ovan angivna ändamål och enligt lagkrav. Clubmate tillhandahåller raderings-/exportfunktioner.

Plats för behandling: Primärt inom EU/EES. Tredjelandsoverföringar endast enligt kapitel V GDPR.

Bilaga B – Underbiträden (översikt)

- **Google Cloud Platform & Firebase (Google Cloud)** – hosting/infrastruktur, databaser, lagring, autentisering; dataplacering primärt inom EU/EES när så är konfigurerat.
- **Google Workspace (Google)** – e-post, dokumenthantering och supportärenden.
- **Twilio SendGrid** – e-postutskick/leverans av transaktionsmeddelanden.

Clubmate håller en uppdaterad underbiträdeslista och meddelar väsentliga ändringar i förväg. Överföringar utanför EU/EES hanteras enligt Bilaga E (SCC m.m.).

Bilaga C – Tekniska och organisatoriska åtgärder (TOMs) – Tekniska och organisatoriska åtgärder (TOMs)

- **Styrning:** Dataskyddspolicy, ansvarsfördelning, utbildning av personal, bakgrundskontroller för känsliga roller.
- **Åtkomstkontroll:** SSO/MFA, rollbaserad behörighet, principen om minsta privilegium, tidsbegränsade admin-rättigheter, loggning/granskning.
- **Kryptering:** TLS för data i transit; kryptering av känsliga lagringsytor.
- **Segmentering:** Separata produktions-/testmiljöer, nätverkssegmentering, kunddataseparation.
- **Utveckling/CI:** Kodgranskning, sårbarhets- och beroendeskaning, säkerhets-patchning.
- **Backuper/BCP:** Regelbundna backuper, återställningstester, incident- och kontinuitetsplan.
- **Leverantörsstyrning:** DPA med underbiträden, due diligence, SCC vid tredjeland.
- **Radering:** Raderingsrutiner, anonymisering där möjligt, sanering av backuper enligt cykler.
- **Incidentprocess:** Triage, notifiering, rotorsaksanalys, åtgärdsplan, lärdomar.

Bilaga D – Incidentrapportering (minimikrav)

- Tidpunkt för upptäckt och typ av incident.
- Berörda kategorier och uppskattat antal Registrerade/poster.

- Sannolika konsekvenser.
- Vidtagna/planerade åtgärder.
- Kontaktpunkt för vidare information.
- Rekommenderade åtgärder för den Personuppgiftsansvarige (t.ex. information till Registrerade/IMY).

Bilaga E – Överföringar och SCC

- Om tredjelandsöverföring sker används EU-kommissionens **SCC (2021/914)**, modul **Controller-to-Processor** (C2P) och/eller **Processor-to-Processor** (P2P) beroende på flöde.
 - **Tilläggsåtgärder:** kryptering, åtkomstkontroller, transparens- och rättsliga bedömningar (TIA).
 - Parterna samarbetar för att säkerställa laglig överföring och uppdaterar Bilaga A vid förändringar.
-