

Personuppgiftsbiträdesavtal (PUB/DPA)

Mellan

Leverantören

och

[Säljaren] = skolklass/lag/förening som är säljare (merchant of record) mot konsument ("Personuppgiftsansvarig" eller "Säljaren").

Tillsammans "Parterna".

Syfte: Leverantören behandlar Personuppgifter för Säljarens räkning i syfte att **plocka, packa och leverera varor**, hantera **returer/Reklamationer (RMA)** och tillhandahålla **avräknings-/fakturaunderlag**.

1. Definitioner

Begrepp i detta avtal har betydelsen enligt **GDPR**. "Underbiträde" = tredje part som Leverantören anlitar för Behandling för Säljarens räkning.

2. Roller och instruktioner

2.1 Roller: Säljaren är **personuppgiftsansvarig**. Leverantören är **personuppgiftsbiträde**.

2.2 Instruktioner: Leverantören får endast behandla Personuppgifter enligt Säljarens **dokumenterade instruktioner** (orderfiler, API-specar, e-postbekräftelser samt denna DPA). Om Leverantören anser att en instruktion strider mot lag ska Leverantören omgående meddela Säljaren.

2.3 Begränsning av ändamål: Behandling får endast ske för ändamål i **Bilaga A. Egen marknadsföring, profilering eller återanvändning** av uppgifter är förbjuden.

3. Sekretess

Leverantören säkerställer att endast behörig personal får tillgång till Personuppgifter och att dessa omfattas av **sekretess**.

4. Säkerhet (TOMs)

4.1 Leverantören ska vidta **lämpliga tekniska och organisatoriska åtgärder** enligt art. 32 GDPR, beaktat risker och Behandlingens natur.

4.2 Minimikrav framgår av **Bilaga C** (åtkomstkontroll, loggning, kryptering i transit, rensning av temporär data, backuper, incidentprocess).

5. Underbiträden

5.1 Säljaren ger Leverantören ett **allmänt förhandstillstånd** att anlita Underbiträden (t.ex. **transportörer**, returportaler, print- & paketeringspartner, IT-drift).

5.2 Leverantören ska föra och på begäran tillhandahålla **aktuell lista** över Underbiträden och underrätta Säljaren inför väsentliga ändringar.

5.3 Leverantören ingår skriftliga **biträdesavtal** med Underbiträden på minst motsvarande dataskyddsnivå och **ansvarar** för deras handlingar såsom för egna.

6. Plats för behandling och överföringar

6.1 Behandling sker i första hand inom **EU/EES**.

6.2 Överföring till tredjeland får endast ske med **lagligt stöd** (t.ex. EU-kommissionens **SCC** enligt **Bilaga E**) och lämpliga tilläggsåtgärder.

6.3 Leverantören får inte ge fjärråtkomst från tredjeland utan Säljarens förhandsgodkännande.

7. Registrerades rättigheter och assistans

7.1 Leverantören ska utan onödigt dröjsmål **bistå** Säljaren vid begäranden från Registrerade (t.ex. tillgång, rättelse, radering).

7.2 Leverantören bistår vid **DPIA** och kontakter med tillsynsmyndighet i den mån Behandlingen hos Leverantören berörs. Skäliga kostnader kan tillkomma om arbetet är omfattande och inte beror på Leverantörens fel.

8. Incidenter

8.1 Leverantören ska **omedelbart och utan onödigt dröjsmål** underrätta Säljaren om **personuppgiftsincidenter**, beskriva händelsen, konsekvenser, vidtagna och föreslagna åtgärder, samt hålla löpande uppdatering tills incidenten stängts.

8.2 Dokumentation av incidenter ska hållas tillgänglig för Säljaren.

9. Kontroller och revision

9.1 Säljaren har rätt att **granska** Leverantörens efterlevnad **högst en gång per år** eller vid berättigad misstanke om väsentlig brist.

9.2 Revision sker efter rimligt förhandsbesked och utan onödigt störande av verksamheten. Sekretessavtal kan krävas. Sammanfattande rapport tillhandahålls.

10. Lagring och radering

10.1 Personuppgifter får **inte bevaras längre än nödvändigt** för ändamålen i Bilaga A.

10.2 På Säljarens instruktion, eller när avtalet upphör, ska Leverantören **radera eller återlämna** Personuppgifter samt radera befintliga kopior (med beaktande av lagkrav).

10.3 Loggar/backuper rensas enligt Leverantörens raderingspolicy och tekniska cykler; på begäran intygas radering.

11. Ansvar

11.1 Parternas ansvar följer **artikel 82 GDPR**.

12. Giltighet och upphörande

12.1 Avtalet gäller så länge Leverantören behandlar Personuppgifter för Säljarens räkning.

12.2 Vid upphörande ska §10 tillämpas.

13. Tillämplig lag och forum

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

Bilaga A – Behandlingsinstruktion

Ändamål: Plock/pack/leverans till Kund; retur/RMA; reklamationsstöd; avräknings-/fakturaunderlag och leveransspårning.

Kategorier av Registrerade: Kunder (mottagare), Säljarens kontaktpersoner.

Uppgifter: Namn, leveransadress, kontakt (e-post/telefon), ordernummer, orderrader (artikel/antal), spårningslänk/leveransstatus, kommunikationslogg kopplad till leverans/retur; **inga särskilda kategorier**.

Behandlingar: Mottagning av orderdata, lagring, åtkomst, utskrift av etiketter, överföring till transportör, uppdatering av status, returhantering, generering av avräkningsunderlag, radering.

Lagringstid: Endast så länge som krävs för ändamålen och enligt lag (t.ex. reklamations- och bokföringskrav).

Plats: EU/EES; tredjelandsöverföring enbart enligt §6.

Bilaga B – Kommunikationsram mot Kund

- Leverantören får kontakta Kund **endast** i syfte att fullgöra leverans/retur/reklamation (t.ex. avisering, adressfråga, spårning).
- **Marknadsföring utan giltigt stöd** (t.ex. samtycke) är förbjuden.
- All kommunikation ska ske i **Säljarens namn** där så är lämpligt (dropship i säljarens namn).

Bilaga C – Tekniska och organisatoriska åtgärder (minimikrav)

- **Åtkomstkontroll:** RBAC, minsta privilegium, stark autentisering, loggning av åtkomst.

- **Kryptering:** TLS i transit; krypterad lagring där det är rimligt; säkra nyckelrutiner.
- **Systemdrift:** Patchning, sårbarhetsskanning, separata miljöer, backuper och återställningstester.
- **Dataminimering & sanering:** Endast nödvändiga fält; rensning av temporära filer/etiketter efter utskrift; tidsstyrd radering.
- **Incidentprocess:** Triage, containment, rotorsak, notifiering, åtgärdsplan.
- **Transportörers säkerhet:** Avtalade villkor som kräver skydd av personuppgifter och begränsning av ändamål.

Bilaga D – Underbiträden

- **Transportörer:** PostNord, DHL, Bring m.fl.
- **IT/Drift:** Hosting, WMS/TA-system, etikett-/adressvalidering.
- **Retur/Service:** Returportaler, reparations-/bytespartners.

Bilaga E – Överföringar utanför EU/EES

- Om Underbiträde eller system finns i tredjeland används **SCC (2021/914)** samt vid behov **tilläggsåtgärder** (kryptering, åtkomstbegränsningar, TIA).
 - Leverantören ska dokumentera överföringsmekanismer och göra dem tillgängliga för Säljaren på begäran.
-