

# Personuppgiftsbiträdesavtal (DPA)

Mall för kunder av Rosenbok · Media Rosenqvist · Version 1.0 · 2026-07-19

## 1. Parter

Personuppgiftsbiträde: Media Rosenqvist, med varumärket Rosenbok ("Biträdet"), Sverige.  
Kontakt: kontakt@mediarosenqvist.com.

Personuppgiftsansvarig: Kunden som tecknat abonnemang på Rosenbok ("Ansvarige"),  
företräd av behörig firmatecknare.

## 2. Bakgrund och syfte

Detta avtal reglerar Bitrådets behandling av personuppgifter för Ansvariges räkning i samband med tillhandahållande av Rosenbok — en molnbaserad bokförings- och fakturerings tjänst. Avtalet uppfyller kraven i artikel 28 i EU:s dataskyddsförordning (GDPR 2016/679).

## 3. Behandlingens omfattning

| Kategori                   | Innehåll                                                                                                        |
|----------------------------|-----------------------------------------------------------------------------------------------------------------|
| Föremål                    | Behandling som krävs för att leverera Rosenbok enligt huvudavtal.                                               |
| Varaktighet                | Så länge Ansvarige har aktivt abonnemang, plus 30 dagars uppsägningsperiod.                                     |
| Art                        | Insamling, lagring, strukturering, analys, sammanställning, radering.                                           |
| Ändamål                    | Bokföring, fakturering, momsredovisning, betalningsuppföljning, rapportgenerering.                              |
| Personuppgifter            | Namn, e-post, telefon, adress, personnummer/organisationsnummer, bankkontouppgifter, IP-adress, användarloggar. |
| Kategorier av registrerade | Ansvariges anställda, kunder, leverantörer och andra affärskontakter.                                           |

## 4. Instruktioner

Biträdet får endast behandla personuppgifter enligt Ansvariges dokumenterade instruktioner. Huvudavtalet, denna DPA samt Ansvariges aktiva användning av tjänsten (t.ex. inbjudan av användare, uppladdning av kvitton, skapande av fakturor) utgör sådana instruktioner. Instruktioner som strider mot tillämplig rätt måste Biträdet omgående meddela Ansvarige.

## 5. Tystnadsplikt

Biträdet säkerställer att personer med åtkomst till personuppgifter är bundna av tystnadsplikt eller lagstadgad sekretess. Åtkomst begränsas enligt principen om minsta möjliga behörighet.

## 6. Säkerhetsåtgärder (art. 32 GDPR)

Biträdet vidtar följande tekniska och organisatoriska åtgärder:

- Kryptering i transport (TLS 1.3) och i vila (AES-256).
- Row-Level Security per bolag i Postgres — logisk isolering mellan tenants.
- Tvåfaktorsautentisering (TOTP) tillgänglig, obligatorisk för ägare/administratörer.
- Kontroll av lösenord mot Have I Been Pwned vid registrering och byte.
- SHA-256-integritetshash på varje verifikat; låsta perioder kan inte ändras.
- Automatiska säkerhetskopior dygnsvis, Point-in-Time Recovery 7 dagar.
- Aktivitets- och säkerhetsloggar med minst 24 respektive 3 månaders retention.
- Beroendescanner mot kända CVE:er; migrationer via CI med typkontroll.
- Dokumenterad incidenthanteringsprocess (bekräftelse 24h, notifiering 72h).

## 7. Underbiträden

Ansvarige godkänner följande underbiträden:

| Underbiträde                           | Syfte                                             | Region               |
|----------------------------------------|---------------------------------------------------|----------------------|
| Supabase (via Lovable Cloud)           | Databas, autentisering, fillagring                | EU (Frankfurt)       |
| Cloudflare                             | CDN, DDoS-skydd, TLS-terminering                  | EU / global failover |
| Google Gemini (via Lovable AI Gateway) | AI-assisterade bokföringsförslag                  | EU                   |
| Paddle.com Market Ltd                  | Betalning, fakturering, moms (Merchant of Record) | EU / UK              |
| Transaktionsmail-leverantör            | E-post för fakturor och notiser                   | EU                   |

Nya eller utbytta underbiträden meddelas minst 30 dagar i förväg. Ansvarige har rätt att göra sakligt grundad invändning; om parterna inte når enighet får Ansvarige säga upp avtalet med iakttagande av 30 dagars uppsägningstid.

## 8. Registrerades rättigheter

Biträdet bistår Ansvarige med lämpliga tekniska och organisatoriska åtgärder för att fullgöra begäran från registrerade om åtkomst, rättelse, radering, begränsning, portabilitet och invändning. Export finns som JSON i Inställningar → Integritet; radering hanteras via samma vy.

## 9. Personuppgiftsincident

Biträdet meddelar Ansvarige utan onödigt dröjsmål och senast inom 48 timmar efter det att en personuppgiftsincident konstaterats. Meddelandet innehåller (så långt känt) art, kategorier och antal registrerade, sannolika konsekvenser samt vidtagna eller föreslagna åtgärder. Biträdet bistår Ansvarige i eventuell anmälan till Integritetsskyddsmyndigheten (IMY) enligt art. 33.

## 10. Överföring till tredje land

All primär lagring sker inom EU/EES. Vid överföring till tredje land tillämpas EU-kommissionens standardavtalsklausuler (2021/914) samt kompletterande

skyddsåtgärder efter Schrems II-bedömning.

## 11. Granskning och revision

Biträdet tillhandahåller på begäran information som styrker efterlevnaden av art. 28 GDPR. Ansvarige har rätt att en gång per år, med minst 30 dagars varsel och på egen bekostnad, låta en oberoende och tystnadsförbunden revisor granska Bitrådets tekniska och organisatoriska åtgärder. Revisioner ska ske under ordinarie arbetstid och på ett sätt som inte stör Bitrådets drift.

## 12. Åtgärder vid avtalets upphörande

Vid avtalets upphörande erbjuder Biträdet Ansvarige 30 dagars nedladdning av data (SIE-4, JSON). Därefter raderas eller anonymiseras personuppgifter, med undantag för uppgifter som Biträdet enligt lag är skyldigt att bevara (t.ex. bokföringslagen 1999:1078, 7 år). Bevarade uppgifter skyddas med samma säkerhetsåtgärder som under avtalstiden.

## 13. Ansvar

Ansvarsbegränsningar följer huvudavtalet mellan parterna. Ingenting i denna DPA inskränker de rättigheter registrerade har enligt GDPR.

## 14. Tillämplig lag och tvister

Detta avtal styrs av svensk rätt. Tvister avgörs i svensk allmän domstol med Stockholms tingsrätt som första instans.

## 15. Signatur

### Personuppgiftsansvarig (Kund)

---

Namnteckning

---

Namnförtydligande / titel

---

Ort och datum

### Personuppgiftsbiträde (Media Rosenqvist)

---

Namnteckning

---

Namnförtydligande / titel

---

Ort och datum