Personuppgiftsbiträdesavtal — på vanlig svenska

Vägledning till Adminors Personuppgiftsbiträdesavtal version 2026-08-05

Det här dokumentet förklarar vårt formella Personuppgiftsbiträdesavtal (DPA) på vanlig svenska. **Det är inte juridiskt bindande** - vad som faktiskt gäller står i den formella DPA:n. Den här texten är till för att hjälpa dig förstå vad du faktiskt accepterar när du blir kund hos Adminor.

Varje rubrik motsvarar en paragraf i den formella DPA:n.

Vad är ett DPA överhuvudtaget?

Ett Personuppgiftsbiträdesavtal är ett **lagkrav från GDPR**. Närhelst ett företag (du, kunden) lämnar ut personuppgifter till en leverantör (Adminor) för att vi ska kunna leverera en tjänst, måste det finnas ett skriftligt avtal som reglerar vad vi får göra med dem.

Du är "Personuppgiftsansvarig" - du bestämmer vad som lagras och varför. **Adminor är "Personuppgiftsbiträde"** - vi gör jobbet enligt dina instruktioner.

---

§ 1 Definitioner — vad orden betyder

Termer i avtalet följer GDPR:s definitioner. Inget speciellt här.

---

§ 2 Vad gör vi egentligen med personuppgifterna?

§ 2.1 Vi listar exakt vad vi behandlar och varför:

- **Vad vi gör:** driftar, lagrar, backupar, övervakar och ger teknisk support på era applikationer, e-post och data
- **Hur länge:** så länge ni är kund hos oss, plus tiden vi måste behålla data enligt lag
- **Vilken data:** tekniska loggar (IP, sessions), det innehåll ni själva lägger in i tjänsterna, e-post som passerar
- **Vem datan handlar om:** era anställda och er egen verksamhet - era kunder, leverantörer osv som ni väljer att lagra info om

§ 2.2 Avtalet är en bilaga till våra Allmänna villkor. Listan över vilka andra företag vi använder finns i Bilaga 2.

Det finns också en **Bilaga 3**, men den gäller bara om vi sköter era egna system åt er, alltså om vi administrerar er Microsoft 365-miljö, era datorer eller ger fjärrsupport. Har ni bara hosting hos oss berör den er inte. Bilaga 3 börjar dessutom gälla först när båda parter skriftligen enats om den, den kan inte börja gälla bara för att vi publicerar den.

§ 2.3 Det här avtalet gäller företagskunder. När vi behandlar uppgifter om dig som vår kund (din kontaktinformation, fakturering) regleras det av vår Sekretesspolicy, inte av det här avtalet. Bra att hålla isär.

---

§ 3 Hur vi behandlar er data

§ 3.1-3.6 Standardklausuler om att vi följer era instruktioner, gör databaskopior för tester (raderas efter 14 dagar), säger till om vi tycker en instruktion strider mot lag.

§ 3.7 (NY) Ni har också skyldigheter:

- Ni måste ha laglig grund för det ni lagrar (samtycke, avtal, intresseavvägning etc.)
- Ni måste informera era registrerade om behandlingen
- Ni för ert eget register över behandlingar
- **Ni får inte ladda upp särskilt känsliga uppgifter** (hälsodata, etnicitet, biometri, brottmål etc.) utan att först prata med oss. Våra standardtjänster är inte byggda för sådan data.

Det här skyddar oss båda. Om ni laddar upp tyngre data utan att säga till och något händer, ligger ansvaret på er.

---

§ 4 När vi får (och inte får) dela personuppgifter

Vi delar bara personuppgifter med tredje part när:

- Ni har sagt åt oss att integrera med en tredjepartstjänst (Stripe, Klarna etc.)
- Ni gett oss skriftligt OK
- Svensk eller EU-lag kräver det (typ myndighetsbeslut)

Om en myndighet eller registrerad frågar oss direkt - skickar vi till er.

---

§ 5 Underbiträden (andra leverantörer vi använder)

Vi får använda andra leverantörer (t.ex. Stripe för betalningar). En **fullständig lista finns i Bilaga 2**.

Om vi vill lägga till en ny leverantör säger vi till **30 dagar i förväg**. Ni kan invända. Om vi inte är överens har ni rätt att säga upp avtalet utan kostnad.

---

§ 6 Hur vi skyddar er data

§ 6.4 (NY) Konkret vad vi gör:

Område	Vad
Kryptering	TLS 1.2+ för all överföring, kryptering av backuper
Åtkomstkontroll	Bara behörig personal kommer åt data, MFA krävs, allt loggas
Nätverk	Brandväggar, segmentering mellan kunder, DDoS-skydd
Fysiskt	ISO 27001-certifierade datahallar, kortpassage, kameraövervakning, 24/7
Backup	Regelbundna säkerhetskopior inom EU/EES
Personal	Sekretessåtagande + säkerhetsutbildning
Incidenter	Loggning + dokumenterad incidenthanteringsprocess

---

§ 7 Vad händer om något går fel? (Säkerhetsincidenter)

§ 7.1 Om det blir en incident som påverkar era personuppgifter säger vi till **inom 72 timmar** efter att vi upptäckt det. Vi ger er all info ni behöver för att kunna anmäla till IMY (Integritetsskyddsmyndigheten) inom era egna 72 timmar.

§ 7.2 Vi hjälper er med själva myndighetsanmälan och informationen till registrerade om det behövs.

---

§ 8 Granskning och revision

Ni har rätt att en gång om året granska att vi följer avtalet. Vi släpper in juristen / IT-revisorn på rimligt sätt.

Om ni vill göra fysisk revision på vår infrastruktur: vi släpper inte in i delar där andra kunders data finns (av sekretessskäl), men vi visar er **ISO 27001-certifikat**, ISAE 3402-rapporter, pentest-resultat etc. som bevisar att vi gör vårt jobb.

Om ni vill göra fler än en granskning per år får ni betala för tiden.

---

§ 9 Vad händer när avtalet slutar?

§ 9.1 Vi raderar eller lämnar tillbaka era data inom **30 dagar** efter att avtalet slutat.

§ 9.2 Undantag - vi behåller viss data enligt lag:

- **Bokföringsmaterial: 7 år** (Bokföringslagen kräver)
- **Moms- och skatteunderlag** (Skatteförfarandelagen)
- **Säkerhetsloggar: 12-24 månader** (för incidentundersökning)
- **Pågående juridiska processer** (måste behållas som bevis)
- **Preskriptionsskydd** (om någon kan komma och kräva pengar tillbaka senare)

Detta är inte att vi väljer att behålla - det är **vad lagen tvingar oss till**.

§ 9.3 Det vi behåller skyddas på samma sätt och raderas så fort lagkravet upphör.

---

§ 10 Ansvar — vem betalar om något går fel?

Detta är den paragraf som juridiskt är mest komplex. Den enkla versionen:

§ 10.1-10.2 Om vi bryter mot avtalet kan ni kräva ersättning. Maxbeloppet är **det ni faktiskt betalat oss för tjänsten under senaste 12 månaderna**. Standard för B2B-hosting.

§ 10.3 Vi har ansvarsförsäkring: minst 3 miljoner kronor för konsultansvar och minst 10 miljoner för allmänt ansvar per skada. Vi håller skyddet aktivt under hela avtalstiden och visar försäkringsbeviset om ni ber om det. Byter vi försäkringsbolag behöver avtalet inte skrivas om, så länge skyddet inte blir sämre.

§ 10.4 Maxbeloppet gäller inte i tre fall:

1. Vi gjorde det med flit eller var jättevårdslösa (svensk lag tillåter inte begränsning här)
2. Tvingande lag säger annat (typ GDPR-skadestånd som EU-rätten kräver)
3. Vi bryter mot sekretess

§ 10.5 Era anställda och kunder behåller sin egen rätt enligt GDPR. Om en av era anställda lider skada och stämmer oss direkt enligt GDPR Art. 82, kan vi inte gömma oss bakom det här avtalet. EU-rätten ger dem rätten direkt.

§ 10.6 Om ni har betalat ut skadestånd till en registrerad och en domstol säger att felet var vårt, ska vi ge er pengarna tillbaka — upp till samma tak som i § 10.2 (det ni faktiskt betalat oss för tjänsten under 12 mån). Om vi gjort något med flit eller varit grovt vårdslösa gäller inget tak.

---

§ 11 Ersättning för extra arbete

Om vi måste göra extra jobb (svara på datainnehavarfrågor, granskningar, myndighetshjälp) som inte är del av vanlig drift fakturerar vi enligt prislista.

---

§ 12 Årlig avstämning

En gång om året kan ni be oss bekräfta skriftligt att allt fortfarande stämmer: kontaktuppgifter, listan över underleverantörer, säkerhetsåtgärderna och beskrivningen av vad vi gör med era uppgifter. Vi svarar inom 30 dagar och berättar om något väsentligt förändrats.

Ni behöver alltså inte skriva under avtalet på nytt varje år. Poängen är att ni ska kunna kontrollera att dokumentet fortfarande stämmer med verkligheten.

---

§ 13 När avtalet börjar och slutar

Träder i kraft när Tjänsteavtalet börjar gälla. Slutar när Tjänsteavtalet slutar. Vissa bestämmelser (t.ex. sekretess) lever vidare även efter uppsägning.

Bilaga 2 (kort förklaring)

Bilaga 2 listar **alla företag vi använder för att leverera tjänsterna åt er**.

Vi delar dem i tre grupper:

Grupp 1 - alltid (affärsstöd)

Hjälper oss driva bolaget:

- **Microsoft 365** (vår e-post)
- **Cloudflare** (säkerhet och prestanda för publika sajter)
- **Stripe** (kortbetalningar)
- **PayPal** (PayPal-betalningar)
- **Fortnox** (bokföring)

Grupp 2 - bara om ni valt tilläggstjänsten

- **Backblaze** - om ni valt backup till Backblaze B2
- **Ubiquiti UniFi** - om vi driftar era UniFi-nätverk via Ubiquitis molntjänst
- **Crayon** - om ni köper Microsoft 365-licenser via oss
- **Splashtop** - om vi ger er fjärrsupport
- **Anthropic (Claude)** - om vi har ett konsultuppdrag hos er. Vi använder verktyget som stöd när vi skriver dokumentation och gör analyser. Era kunduppgifter matas inte in. Namn och kontaktuppgifter till er personal kan förekomma i underlaget.
- **OpenAI** - om ni har säkerhetsövervakning via pentesting.se. Används för att analysera det vi hittar vid genomsökningar.

Använder ni inte tjänsten, behandlas inget hos den leverantören.

Grupp 3 - inga underbiträden, men värt att nämna

- **HostBill** (kundpanel, fakturor) - driftas på vår egen infrastruktur i Sverige
- **Datahallarna** - ISO 27001-certifierade men har inte tillgång till er data (de driver byggnaden, vi driver datorerna)

Vad gör ni om ni är obekväma med något?

1. **Invändning mot underbiträde** - skriftligen, vi kan eventuellt säga upp avtalet utan kostnad
2. **Be om bevis** - ISO 27001-certifikat, försäkringsbevis etc. får ni på begäran
3. **Be om revision** - en gång om året kan ni granska oss
4. **Säga upp** - normala uppsägningsregler enligt Tjänsteavtalet

---

Kontakt

Adminor AB Hunnebergsvägen 13, 167 43 Bromma Org.nr 556227-6351 +46 8-564 314 30 · info@adminor.net · adminor.net

För GDPR-frågor: **gdpr@adminor.net** (om vi har den adressen, annars info@adminor.net)

Det här är en vägledning. Det formella Personuppgiftsbiträdesavtalet version 2026-08-05 är vad som juridiskt gäller. Vid skillnad mellan denna text och den formella DPA:n är det den formella DPA:n som har företräde.