Personuppgiftsbiträdesavtal

Version 3.0 · 26 maj 2026 · OptiTech Sverige AB (Prakto), org.nr 559489–8917

Detta personuppgiftsbiträdesavtal (“**DPA:t**”) ingår mellan Kunden (“**Kunden**”) och **OptiTech Sverige AB**, org.nr 559489–8917, Karlslundsvägen 8, 177 44 Stockholm, som tillhandahåller tjänsten under varumärket **Prakto** (“**Prakto**”) på de villkor som anges på prakto.se/legal/terms (“**Huvudavtalet**”). DPA:t träder i kraft samtidigt som Huvudavtalet.

Begrepp med stor begynnelsebokstav som inte definieras här har den innebörd som anges i Huvudavtalet. Vid konflikt mellan DPA:t och Huvudavtalet gäller DPA:t i frågor som rör behandling av personuppgifter.

1. Definitioner

1.1. **Tillämplig dataskyddslagstiftning** avser GDPR (förordning (EU) 2016/679), svensk dataskyddslag (2018:218) och övriga regler om behandling av personuppgifter som är tillämpliga.

1.2. **Personuppgift**, **behandling**, **registrerad**, **personuppgiftsincident**, **personuppgiftsansvarig** och **personuppgiftsbiträde** har den innebörd som anges i GDPR.

1.3. **Kunddata** avser personuppgifter som Kunden eller dess användare tillhandahåller till Tjänsten och som Prakto behandlar för Kundens räkning. Kunddata beskrivs i Bilaga A.

1.4. **Kontodata** avser personuppgifter om Kundens administrativa användare som Prakto behandlar för att hantera affärsrelationen, fakturering, identitetsverifiering och säkerhet.

1.5. **Användningsdata** avser teknisk data om hur Tjänsten används, inklusive loggar, prestandadata och säkerhetshändelser.

1.6. **Underbiträde** avser tredje part som Prakto anlitar för att behandla Kunddata.

1.7. **SCC** avser standardavtalsklausulerna i kommissionens beslut (EU) 2021/914.

1.8. **Tjänsten** har den innebörd som anges i Huvudavtalet.

2. Parternas roller och behandlingens detaljer

2.1 Kunden är personuppgiftsansvarig och Prakto är personuppgiftsbiträde för Kunddata. Om Kunden själv är biträde för en tredje part agerar Prakto som under-biträde. För Kontodata och Användningsdata agerar Prakto självständigt ansvarig enligt avsnitt 9.

2.2 Behandlingens art, syfte, varaktighet, kategorier av registrerade och personuppgifter framgår av Bilaga A.

2.3 Prakto behandlar Kunddata endast på Kundens dokumenterade instruktioner. Huvudavtalet och detta DPA utgör Kundens fullständiga instruktioner. Kunden tillser att instruktionerna är lagliga och håller Prakto skadeslöst från krav som uppstår till följd av olagliga eller felaktiga instruktioner.

2.4 Aggregerad och anonymiserad data. Prakto får framställa aggregerad eller anonymiserad statistik och träningsdata härledd ur Kunddata och använda sådan data för att förbättra Tjänsten, förutsätt att resultatet inte rimligen kan hänföras till en enskild registrerad eller till Kunden. Sådan data är inte Kunddata.

2.5 Kunden får inte tillhandahålla eller ladda upp särskilda kategorier av personuppgifter (art. 9 GDPR) eller uppgifter om lagförda överträdelser (art. 10 GDPR) till Tjänsten utan separat skriftlig överenskommelse med Prakto.

2.6 Vid Huvudavtalets upphörande raderar Prakto Kunddata senast nittio (90) dagar därefter, om inte fortsatt lagring krävs enligt lag. På Kundens skriftliga begäran inom trettio (30) dagar från upphörandet tillhandahåller Prakto en kopia av Kunddata i ett maskinläsbart format före radering. Säkerhetskopior raderas enligt Praktos ordinarie rutiner.

3. Sekretess

Prakto säkerställer att personal som behandlar Kunddata omfattas av sekretessåtagande eller lagstadgad tystnadsplikt och endast får åtkomst till det som behövs för arbetsuppgiften.

4. Auktoriserade underbiträden

4.1 Kunden ger Prakto generellt skriftligt förhandsgodkännande att anlita de underbiträden som anges i Bilaga A. En aktuell förteckning publiceras på prakto.se/legal/subprocessors; den webbpublicerade versionen har företräde vid avvikelse.

4.2 Prakto ingår skriftligt avtal med varje underbiträde med dataskyddsskyldigheter som i sak inte är mindre skyddande än detta DPA och förblir ansvarigt gentemot Kunden för underbiträdets fullgörande.

4.3 Prakto meddelar Kunden minst fjorton (14) dagar i förväg om planerade förändringar i förteckningen. Kunden kan på sakliga dataskyddsgrunder invända inom samma period. Om Parterna inte når enighet inom trettio (30) dagar har Kunden rätt att säga upp den berörda delen av Huvudavtalet; uppsaägningen befriar inte Kunden från redan upparbetade avgifter.

5. Säkerhet

Prakto upprätthåller lämpliga tekniska och organisatoriska åtgärder för att skydda Kunddata, med beaktande av behandlingens art, omfattning och risker. Aktuella åtgärder beskrivs i Bilaga C och kan utvecklas över tid så länge den övergripande skyddsnivån inte väsentligt sänks.

6. Tredjelandsöverföringar

6.1 Prakto är etablerat i Sverige och behandlingen sker primärt inom EU/EES. För underbiträden som behandlar Kunddata utanför EU/EES tillämpas SCC, vilka anses ingångna och införlivade i detta DPA genom ingående av Huvudavtalet.

6.2 Följande gäller för SCC:

- Modul 2 (ansvarig till biträde) när Kunden är ansvarig och Prakto biträde.
- Modul 3 (biträde till under-biträde) när Kunden är biträde och Prakto under-biträde.
- Klausul 7 (Docking Clause) tillämpas inte.
- Klausul 9(a) Option 2 tillämpas; varseltiden är fjorton (14) dagar enligt avsnitt 4.3.
- Klausul 11(a) optionen om oberoende tvistlösningsorgan tillämpas inte.
- Klausul 17 (tillämplig lag): svensk lag.
- Klausul 18 (forum): svenska domstolar.

- Bilaga A till detta DPA utgör Bilaga I och III till SCC; Bilaga C utgör Bilaga II.

7. Registrerades rättigheter

Prakto meddelar Kunden utan onödigt dröjsmål om en begäran från en registrerad och hänvisar den registrerade till Kunden. Prakto bistår Kunden med rimliga tekniska och organisatoriska åtgärder för att uppfylla sina skyldigheter enligt GDPR. Bistånd som går utöver Tjänstens funktioner ersätts av Kunden enligt avsnitt 10.2.

8. Revision och incidenter

8.1 Prakto för dokumentation som styrker efterlevnad av detta DPA. På begäran tillhandahåller Prakto, i den mån sådana finns tillgängliga, certifieringar från oberoende revisorer eller annars egen dokumentation som rimligen styrker att säkerhetsåtgärderna uppfyller branschstandard.

8.2 Om sådan dokumentation inte är rimligt tillräcklig enligt tillämplig lag får Kunden, högst en (1) gång per kalenderår, genomföra revision genom en oberoende tredjepartsrevisor. Revisionen ska föregås av minst trettio (30) dagars skriftligt varsel, ske under ordinarie kontorstid, inte väsentligt störa Praktos verksamhet och bekostas av Kunden inklusive ersättning till Prakto för nedlagd tid.

8.3 Vid en personuppgiftsincident som berör Kunddata meddelar Prakto Kunden skriftligen utan onödigt dröjsmål. Meddelandet ska innehålla, så långt det är möjligt, incidentens art, ungefärligt antal berörda registrerade, sannolika konsekvenser och vidtagna åtgärder. Prakto bistår Kunden vid anmälan till tillsynsmyndighet och information till registrerade. Meddelande eller bistånd utgör inte erkännande av ansvar.

9. Praktos roll som självständig ansvarig

Prakto är självständig personuppgiftsansvarig för Kontodata och Användningsdata och behandlar sådan data för att (i) hantera affärsrelationen med Kunden, (ii) driva Praktos kärnverksamhet (bokföring, revision, skatt och regelefterlevnad), (iii) förebygga och utreda bedrägeri, säkerhetsincidenter och missbruk av Tjänsten, (iv) verifiera identitet, (v) uppfylla rättsliga skyldigheter, samt (vi) drifta, optimera och vidareutveckla Tjänsten. Sådan behandling sker enligt Praktos integritetspolicy på prakto.se/legal/privacy.

10. Allmänt

10.1 **Ansvarsbegränsning.** Parternas ansvar enligt detta DPA omfattas av samma ansvarsbegränsningar som anges i Huvudavtalet. Inget i detta DPA utvidgar någondera partens ansvar utöver vad som följer av Huvudavtalet eller tvingande lag.

10.2 **Ersättning för bistånd.** Prakto har rätt till skälig ersättning enligt vid var tid gällande prislista, eller om sådan saknas självkostnad plus rimligt påslag, för bistånd enligt avsnitt 7 och 8 som går utöver vad som rimligen ingår i Tjänsten.

10.3 **Konflikt.** Vid konflikt gäller följande ordning: (i) SCC i Bilaga A när tillämpligt, (ii) detta DPA, (iii) Huvudavtalet, (iv) Praktos integritetspolicy.

10.4 **Ändringar.** Prakto får uppdatera detta DPA för att avspegla ändringar i tillämplig dataskyddslagstiftning, branschstandarder eller underbiträdesförteckningen genom skriftligt meddelande

till Kunden minst trettio (30) dagar före ikraftträdande. Materiella ändringar som väsentligt minskar Kundens skydd kräver Kundens skriftliga godkännande.

10.5 Meddelanden. Meddelanden enligt detta DPA skickas till de kontaktuppgifter som anges i Huvudavtalet och, för Prakto, till dpo@prakto.se.

10.6 Lag och forum. Svensk lag tillämpas på detta DPA. Tvister löses enligt Huvudavtalet, eller om sådan bestämmelse saknas, vid Stockholms tingsrätt som första instans.

10.7 Ingående. Detta DPA blir bindande vid Kundens ingående av Huvudavtalet. Separat undertecknande krävs inte; sker det ändå är det enbart en bekräftelse av redan gällande villkor.

Bilaga A · Behandlingsdetaljer

Kategorier av registrerade	• Studenter och elever • Lärare, studie- och yrkesvägledare och annan skolpersonal • Handledare och kontaktpersoner hos företag • Vårdnadshavare (vid behov för minderåriga) • Kundens administrativa användare
Kategorier av personuppgifter	• Identifikationsuppgifter: namn, personnummer (vid behov), foto • Kontaktuppgifter: e-post, telefon, adress • Anställnings- och utbildningsuppgifter: skola, program, klass, befattning • Praktikrelaterade uppgifter: placering, period, närvaro, omdömen, dokumentation • Tekniska uppgifter: IP-adress, sessionsdata, loggar
Särskilda kategorier (art. 9 & 10 GDPR)	Behandlas ej.
Behandlingens art	Lagring, radering, rättelse, analys, överföring, aggregering, säkerhetskopiering och teknisk drift.
Ändamål	Administration av praktik, LIA, APL, VFU och prao samt tillhörande funktioner.
Överföringens frekvens	Kontinuerlig under Huvudavtalets löptid.
Lagringstid	Under Huvudavtalets löptid. Radering enligt avsnitt 2.6.
Tillsynsmyndighet	Integritetsskyddsmyndigheten (IMY), Sverige.

Underbiträden

Underbiträde	Tjänst	Primär region	Överföringsmekanism
Appwrite B.V. (driftas på Hetzner)	Databas, autentisering och filhantering	EU (Tyskland)	Inom EU/EES
Vercel Inc.	Hosting, CDN och edge-funktioner	EU + globalt edge	SCC + tekniska skyddsåtgärder
Sentry (Functional Software)	Felövervakning och prestandaanalys	EU	Inom EU/EES
Resend, Inc.	Transaktions- och nyhetsbrevs-e-post	USA	SCC + tekniska skyddsåtgärder
Inngest, Inc.	Bakgrundsjobb och notifikationer	USA	SCC
Cloudflare, Inc.	DDoS-skydd, DNS och edge-cache	Globalt edge-nätverk	SCC
Google LLC (Google Workspace)	Internkommunikation och dokument	EU/EES + USA	SCC

Regionsangivelse avser primär lagringsregion. Tillfällig behandling i andra regioner för drift, redundans eller edge-leverans skyddas av angiven överföringsmekanism.

Bilaga B · Parter

Dataexportör (Kunden)

Namn, adress och kontaktuppgifter enligt Huvudavtalet.
Roll: personuppgiftsansvarig eller, när tillämpligt, personuppgiftsbiträde.

Dataimportör (Prakto)

OptiTech Sverige AB, org.nr 559489–8917
Karlslundsvägen 8, 177 44 Stockholm
Kontakt: dpo@prakto.se
Roll: personuppgiftsbiträde.

Parterna är överens om att ingående av Huvudavtalet och detta DPA har samma verkan som undertecknande av SCC, inklusive deras bilagor.

Bilaga C · Tekniska och organisatoriska åtgärder

Prakto upprätthåller administrativa, tekniska och fysiska skyddsåtgärder som rimligen är utformade för att skydda Kunddata. Specifika tekniska val (algoritmer, leverantörer, intervall) kan utvecklas över tid utan föregående meddelande så länge den övergripande skyddsnivån inte väsentligt sänks.

Styrning

Prakto upprätthåller ett informationssäkerhetsprogram med dokumenterade policyer, utsedd säkerhetsansvarig och regelbunden översyn. Säkerhetskrav beaktas vid utveckling av nya funktioner.

Åtkomstkontroll

Åtkomst till Kunddata begränsas enligt principen om minsta nödvändiga privilegium. Stark autentisering med tvåfaktorsautentisering krävs för intern åtkomst. Lösenord lagras hashade med salt. Off-boarding och privilegier kan dras in skyndsamt. Revisionsloggar bevaras för användaraktiviteter och interaktioner med Kunddata.

Segmentering

Kunddata och Praktos interna tjänster driftas i separata miljöer med brandväggar som begränsar trafik mellan dem.

Kryptering

Data i vila krypteras med branschsedvanlig stark kryptering (typiskt AES-256). All nätverkskommunikation skyddas av TLS 1.2 eller högre med moderna ciphersuites. Krypteringsnycklar hanteras via underbiträdenas nyckelhanteringstjänster.

Tillgänglighet och säkerhetskopiering

Regelbundna säkerhetskopior av Kunddata enligt Praktos vid var tid gällande backuprutin. Säkerhetskopior krypteras och lagras separerat från produktionsmiljön. Tillgänglighetsmål för Tjänsten regleras i Huvudavtalets SLA, om sådant finns.

Incidenthantering

Intern övervakning som larmar vid driftavbrott och säkerhetshändelser. Dokumenterad incidentplan som testas och uppdateras regelbundet. Notifiering till Kunden enligt avsnitt 8.3.

Personalskydd

Personal omfattas av sekretessåtagande, genomgår säkerhetsutbildning och bakgrundskontrolleras i den utsträckning som låter sig göras enligt lag.

Testning

Praktos infrastruktur övervakas för att upptäcka avvikelser från säkerhetspolicy. Automatiserad statisk kodanalys och, när Prakto bedömer det lämpligt, oberoende tredjepartstester av säkerhetsläget utförs. Identifierade brister åtgärdas efter risk.