Personuppgiftsbiträdesavtal

Version 2026-11. Avtalet är en del av varje tjänsteavtal med POISE AB och reglerar hur POISE behandlar personuppgifter för kundens räkning enligt artikel 28 i dataskyddsförordningen.

1. Parter och tillämpning

Detta avtal gäller mellan kunden ("den personuppgiftsansvarige") och POISE AB, org.nr 556773-0923, Brunnsgatan 9, 172 68 Sundbyberg ("biträdet"), och är en del av kundens tjänsteavtal. Det reglerar biträdets behandling av personuppgifter för kundens räkning enligt artikel 28 i dataskyddsförordningen (EU) 2016/679.

2. Behandlingens art och ändamål

Behandlingens föremål, varaktighet, art, ändamål, typ av personuppgifter och kategorier av registrerade framgår av bilaga 1 för den eller de tjänster kunden köper.

3. Den personuppgiftsansvariges ansvar

Kunden ansvarar för att behandlingen har rättslig grund, för att instruktionerna till biträdet är lagliga och för att informera de registrerade. Kunden ansvarar för sina egna avtal med plattformsleverantörer (till exempel Microsoft) när biträdet administrerar kundens egna licenser.

4. Biträdets skyldigheter

Biträdet ska

a. behandla personuppgifter endast enligt kundens dokumenterade instruktioner, där tjänsteavtalet och detta avtal utgör instruktioner;
b. säkerställa att personer med tillgång till uppgifterna har åtagit sig tystnadsplikt;
c. vidta de tekniska och organisatoriska åtgärder som anges i avsnitt 6;
d. bistå kunden med att svara på de registrerades begäran, inom fem arbetsdagar från det att biträdet fått del av begäran;
e. bistå kunden med konsekvensbedömningar och förhandssamråd;
f. underrätta kunden utan onödigt dröjsmål, och senast inom 48 timmar från det att biträdet fått kännedom om en personuppgiftsincident som rör kundens uppgifter, med den information biträdet då har;
g. radera eller återlämna alla personuppgifter när tjänsten upphör, enligt avsnitt 9;
h. ge kunden den information som behövs för att visa att skyldigheterna uppfylls och möjliggöra granskning enligt avsnitt 8;
i. omedelbart informera kunden om biträdet anser att en instruktion strider mot dataskyddslagstiftningen;
j. om biträdet enligt unionsrätt eller svensk rätt är skyldigt att behandla eller lämna ut personuppgifter, informera kunden innan behandlingen sker, såvida inte lagen förbjuder det; biträdet lämnar inte ut

uppgifter frivilligt;

k. inte behandla särskilda kategorier av personuppgifter (artikel 9) för kundens räkning annat än om det uttryckligen avtalats; biträdets personal arbetar från Sverige och fjärråtkomst till kundens miljöer sker enbart från EU/EES;
l. när biträdet administrerar kundens Microsoft-tenant göra det genom delegerad administration (Microsoft CSP/GDAP) med de behörigheter kunden tilldelat, vilka kunden när som helst kan återkalla.

Bistånd enligt punkterna d och e ingår i rimlig omfattning. Bistånd därutöver debiteras enligt gällande timpris efter överenskommelse i förväg.

5. Underbiträden

Kunden ger ett allmänt godkännande till att biträdet anlitar underbiträden. Gällande lista finns i bilaga 2 och på poise.se/trust. Biträdet meddelar kunder med avtal minst 30 dagar innan ett nytt underbiträde tas i bruk. Kunden kan invända inom den tiden, och om parterna inte når en lösning får kunden säga upp den berörda tjänsten utan kostnad. Biträdet ingår avtal med varje underbiträde som ger motsvarande skydd som detta avtal och ansvarar gentemot kunden för underbiträdets behandling.

6. Säkerhetsåtgärder

Biträdet upprätthåller minst följande åtgärder för sin egen infrastruktur:

- kryptering under överföring (TLS 1.2 eller senare) och av lagrade hemligheter och säkerhetskopior;
- behörigheter efter roll, personliga konton och flerfaktorsinloggning för all administration;
- löpande uppdatering och härdning av system, nätverkssegmentering och brandväggar;
- loggning av administrativa händelser;
- dagliga krypterade säkerhetskopior, både lokalt i datacentret och som kopia utanför datacentret hos Wasabi i EU-region, med regelbundet testad återläsning;
- regelbunden granskning av den egna säkerheten med samma kontroller som erbjuds kunder.

Åtgärder som gäller plattformar kunden själv licensierar (Microsoft 365, Azure, Bitwarden) framgår av respektive leverantörs dokumentation.

7. Överföring till tredjeland

Biträdets egen behandling sker inom EU/EES. Om ett underbiträde har moderbolag utanför EU/EES används EU-region för lagring och som överföringsmekanism EU–USA Data Privacy Framework eller EU-kommissionens standardavtalsklausuler, enligt bilaga 2. Biträdet överför inte personuppgifter till tredjeland utöver detta utan kundens dokumenterade instruktion.

8. Granskning

Kunden har rätt att, högst en gång per år eller efter en incident, granska biträdets efterlevnad av detta avtal. Granskning sker efter skälig framförhållning, under kontorstid och på ett sätt som inte stör driften, i första hand genom att biträdet lämnar dokumentation och svarar på frågor. Kostnader för granskning utöver detta bärs av kunden.

9. Återlämnande och radering

När tjänsten upphör återlämnar biträdet, efter kundens val, de personuppgifter som finns i biträdets egen infrastruktur (hosting, servrar, säkerhetskopior, ärendesystem) i ett gängse format eller raderar dem, inom 30 dagar, och bekräftar raderingen skriftligt. Säkerhetskopior raderas i den ordinarie rotationen, senast inom 90 dagar. För plattformar som kunden själv licensierar (till exempel Microsoft 365 och Bitwarden) lämnar biträdet över administratörsrollen och tar bort sina egna behörigheter; uppgifterna finns kvar hos kunden. Uppgifter som biträdet måste spara enligt lag undantas.

10. Ansvar

Vardera partens ansvar enligt detta avtal följer ansvarsbegränsningen i tjänsteavtalet. Saknar tjänsteavtalet en ansvarsbegränsning är vardera partens sammanlagda ansvar enligt detta avtal begränsat till de avgifter kunden betalat för den berörda tjänsten under de tolv månaderna närmast före den händelse som grundar ansvar. Sanktionsavgifter som en tillsynsmyndighet ålägger bärs av den part som ålagts dem. Begränsningen gäller inte vid uppsåt eller grov vårdslöshet.

11. Varaktighet och ändringar

Avtalet gäller så länge biträdet behandlar personuppgifter för kundens räkning. Biträdet kan publicera en ny version; för befintliga kunder gäller den nya versionen 30 dagar efter att kunden meddelats. Invänder kunden inom den tiden fortsätter den tidigare versionen att gälla för den kunden tills parterna enats, dock längst till tjänsteavtalets nästa förlängning.

12. Tillämplig lag

Svensk lag och dataskyddsförordningen. Tvist prövas enligt tjänsteavtalet.

Bilaga 1 – Behandlingens detaljer per tjänst

TJÄNST	FÖREMÅL OCH ART	TYP AV UPPGIFTER	REGISTRERADE
Secure Workplace	Uppsättning och förvaltning av Microsoft 365, skydd av datorer, lösenordshantering, support, månadsrapport	Konto- och inloggningsuppgifter, enhetsdata, säkerhetshändelser, ärendehistorik; vid support tillfällig åtkomst till e-post och filer	Kundens anställda och uppdragstagare
Managed Security	Som ovan samt skyddat nätverk och wifi, nätverks- och säkerhetskontroll, säkerhetsgenomgångar	Nätverksloggar (IP-adresser, enhetsnamn), som ovan	Som ovan samt besökare i kundens nätverk
Total IT	Som ovan samt drift av servrar, hosting, virtuella maskiner, säkerhetskopior och licenser	Allt innehåll på servrar och i säkerhetskopior, inklusive e-post, filer och databaser	Som ovan samt kundens kunder och kontakter i de system som hostas
Tillval: Hotidentifiering i Microsoft 365	Automatiska kontroller av inloggningar, regler, behörigheter och administratörskonton	Tekniska loggar från Microsoft 365 (inloggningshändelser, regeländringar, appregistreringar)	Kundens anställda

Tillval: Utökad nätverksanalys	Analys av nätverkstrafik för avvikelser	Trafikmetadata, IP-adresser, enhetsidentiteter	Som Managed Security
Specialistuppdrag	Enligt uppdragsbeskrivning	Enligt uppdragsbeskrivning	Enligt uppdragsbeskrivning

Varaktighet: tjänsteavtalets löptid.

Bilaga 2 – Underbiträden

Endast leverantörer som behandlar personuppgifter för biträdets räkning. Plattformar som kunden själv licensierar (Microsoft 365, Azure, Bitwarden) är inte underbiträden; där är kunden avtalspart och biträdet administratör.

UNDERBITRÄDE	TJÄNST	REGION	ÖVERFÖRINGSMEKANISM
WatchGuard Technologies (moderbolag USA)	Brandvägg, wifi, AuthPoint MFA, FireCloud zero trust-fjärråtkomst (nod i Stockholm)	EU	EU–USA Data Privacy Framework / standardavtalsklausuler
Bitdefender (EU)	Skydd av datorer och servrar (GravityZone)	EU	Ingen överföring
Lettermint (EU)	Utgående e-post från webbplatsen och tjänsterna	EU	Ingen överföring
Wasabi Technologies (moderbolag USA)	Krypterade säkerhetskopior utanför datacentret	EU	EU–USA Data Privacy Framework / standardavtalsklausuler; kopiorna är krypterade innan de lämnar biträdet
Bahnhof AB (Sverige)	Datacenter och colocation för biträdets egna servrar; ingen logisk åtkomst till data	Sverige	Ingen överföring

Den publicerade listan på poise.se/trust visar samma leverantörer och dessutom kundens egna plattformar, markerade med roll.