

PERSONUPPGIFTSBITRÄDESAVTAL (DPA)

1. Bakgrund och syfte

Biträdet tillhandahåller tjänsten Kvorrum, en digital plattform för organisationsstyrning, dokumenthantering och kommunikation, till den Personuppgiftsansvarige enligt separat tjänsteavtal ("Huvudavtalet").

I samband med att tjänsten tillhandahålls behandlar Biträdet personuppgifter för den Personuppgiftsansvariges räkning. Detta avtal reglerar sådan behandling i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 ("GDPR"), artikel 28.

2. Definitioner

Med "Personuppgifter" avses all information som direkt eller indirekt kan hänföras till en fysisk person, och som behandlas av Biträdet inom ramen för tjänsten.

Med "Registrerade" avses de fysiska personer vars personuppgifter behandlas, typiskt den Personuppgiftsansvariges anställda, styrelseledamöter och övriga användare av plattformen.

Med "Underbiträde" avses tredje part som Biträdet anlitar för att utföra viss behandling för den Personuppgiftsansvariges räkning.

3. Behandlingens föremål och syfte

Biträdet behandlar personuppgifter uteslutande för att kunna tillhandahålla Kvorrum-plattformen enligt Huvudavtalet. Behandlingen sker på den Personuppgiftsansvariges instruktion och för dennes räkning. Biträdet behandlar inte personuppgifterna för egna ändamål.

I den mån den Personuppgiftsansvarige använder tilläggstjänsten Avtals-analys behandlar Bitrådets personal även de dokument som den Personuppgiftsansvarige skickar in för manuell granskning. Sådan behandling sker på den Personuppgiftsansvariges instruktion och uteslutande för att utföra det beställda uppdraget.

I den mån den Personuppgiftsansvarige använder funktionen för automatisk avläsning i modulen Avtalsklockan behandlas de avtalsdokument som den Personuppgiftsansvarige laddar upp där för automatiserad avläsning med AI-stöd. Avläsningen utförs genom Bitrådets underbiträde Google (Vertex AI / Gemini) inom EU/EES, i syfte att föreslå strukturerade uppgifter ur dokumentet. Behandlingen sker på den Personuppgiftsansvariges instruktion och uteslutande för att utföra det beställda uppdraget. Avläsningen utgör inte automatiserat beslutsfattande enligt GDPR artikel 22; de föreslagna uppgifterna får verkan först sedan en användare hos den Personuppgiftsansvarige har granskat och bekräftat dem. Utöver den lagring av dokumentet som redan sker i tjänsten lagrar avläsningsfunktionen ingen ytterligare kopia av dokumentets innehåll; endast de föreslagna strukturerade uppgifterna, med tillhörande källcitat, behandlas vidare.

I den mån den Personuppgiftsansvarige beställer import av befintliga avtal laddar Bitrådets behöriga personal upp de dokument som den Personuppgiftsansvarige tillhandahåller och

låter dem avläsas på samma sätt som vid automatisk avläsning i Avtalsklockan. Bitrådets personal granskar de föreslagna uppgifterna innan avtalen läggs in i den Personuppgiftsansvariges del av tjänsten. Behandlingen sker på den Personuppgiftsansvariges instruktion och uteslutande för att utföra det beställda uppdraget.

Tjänsten skickar e-post till användare genom Bitrådets underbiträde för e-postutskick (se avsnitt 5). Utskicken avser inbjudningar till tjänsten och påminnelser om avtalsfrister.

Kategorier av registrerade: Anställda, styrelseledamöter, förtroendevalda och övriga användare hos den Personuppgiftsansvarige.

Kategorier av personuppgifter: Namn, e-postadress, roll och titel, tillhörighet till rum, inloggnings-IP-adress, inloggningstidsstämplar, namn på betrodda enheter (operativsystem och webbläsare), uppgifter om vem som har skapat eller ändrat poster i tjänsten och när, innehåll i supportärenden, teknisk felinformation vid fel i tjänsten (användar-id, organisation, tidpunkt, felmeddelande, sida i tjänsten, appversion och webbläsartyp), samt innehåll i de dokument och protokoll som den Personuppgiftsansvarige lagrar i tjänsten. I förekommande fall kan särskilda kategorier av personuppgifter enligt GDPR artikel 9 förekomma i det innehåll som den Personuppgiftsansvarige lagrar eller skickar in. Den Personuppgiftsansvarige ansvarar för att det finns rättslig grund för behandling av sådana uppgifter.

Behandlingarnas art: Lagring, visning, sökning, export, säkerhetskopiering, e-postutskick, loggning av tekniska fel för felsökning och support, manuell granskning (vid Avtals-analys och import), automatiserad avläsning med AI-stöd (vid Avtalsklockan och import) och radering av ovanstående uppgifter via plattformens funktioner.

4. Bitrådets åtaganden

4.1 Instruktionsbundenhet. Bitrådet behandlar personuppgifter endast enligt dokumenterade instruktioner från den Personuppgiftsansvarige, om inte unionsrätten eller svensk lagstiftning kräver annat. I sådant fall underrättar Bitrådet den Personuppgiftsansvarige innan behandlingen påbörjas, om inte lagen förbjuder sådan underrättelse.

4.2 Konfidentialitet. Bitrådet säkerställer att personal som har tillgång till personuppgifterna är bundna av konfidentialitetsåtaganden och har fått nödvändig utbildning i dataskydd.

4.3 Tekniska och organisatoriska säkerhetsåtgärder. Bitrådet vidtar lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna mot obehörig åtkomst, förlust eller förstörelse, i enlighet med GDPR artikel 32. Åtgärderna innefattar bland annat:

- Kryptering av data i transit (TLS) och i vila (AES-256 via Google Cloud)
- Rollbaserad åtkomstkontroll inom plattformen
- Autentisering via Firebase Authentication med tvåstegsverifiering (TOTP)
- Regelbunden säkerhetskopiering till en krypterad lagringsenhet i Bitrådets lokaler i Sverige

- Automatiserad rensning av personuppgifter enligt dokumenterad datalagringspolicy (se Bilaga 2A)

4.4 Bistånd till den Personuppgiftsansvarige. Biträdet bistår den

Personuppgiftsansvarige, i den mån det är möjligt och skäligt, med att uppfylla sina skyldigheter avseende:

- Registrerades rättigheter (tillgång, rättelse, radering, begränsning, portabilitet och invändning)
- Säkerhetsincidenter enligt GDPR artikel 33–34
- Konsekvensbedömningar (DPIA) enligt GDPR artikel 35

4.5 Underrättelse vid personuppgiftsincident. Biträdet underrättar den

Personuppgiftsansvarige utan onödigt dröjsmål, och senast inom 48 timmar, efter att ha fått kännedom om en personuppgiftsincident som rör den Personuppgiftsansvariges data.

4.6 Radering vid avtalets upphörande. När Huvudavtalet upphör behåller den

Personuppgiftsansvarige åtkomst till tjänsten under trettio (30) dagar i enlighet med Huvudavtalet för att kunna hämta ut sina data. Därefter raderar Biträdet all kunddata inom trettio (30) dagar från det att åtkomstperioden har löpt ut, om inte Parterna skriftligen avtalat annat eller lagstiftning kräver fortsatt lagring. Kopior i säkerhetskopior raderas i takt med att säkerhetskopiorna gallras enligt Bilaga 2A.

4.7 Revision. Biträdet tillhandahåller den information som krävs för att den

Personuppgiftsansvarige ska kunna kontrollera att skyldigheterna enligt detta avtal uppfylls. Den Personuppgiftsansvarige, eller av denne utsedd revisor, äger rätt att genomföra revision med skäligt förvarning (minst 30 dagars varsel) och på Parternas gemensamma bekostnad.

5. Underbiträden

Biträdet har den Personuppgiftsansvariges generella tillstånd att anlita underbiträden.

Biträdet anlitar för närvarande följande underbiträden:

Underbiträde	Tjänst	Region
Google LLC / Google Cloud Platform	Firebase Firestore (databas), Firebase Authentication (inloggning), Firebase Storage (filer), Cloud Functions (serverlogik), Firebase App Check (skydd mot automatiserat missbruk), Vertex AI / Gemini (AI-assisterad avläsning av uppladdade avtalsdokument)	EU/EES — Firestore: europe-north2 (Stockholm), Storage: europe-north1 (Finland), Functions/Vertex AI: europe-west1 (Belgien), App Check (reCAPTCHA Enterprise): global tjänst som kan behandla uppgifter utanför EU/EES, bl.a. i USA (SCC)
Plus Five Five, Inc. (Resend)	E-postutskick: inbjudningar till tjänsten och påminnelser om avtalsfrister. Behandlar mottagarens e-postadress	Utskick från EU (Irland, eu-west-1). Resend är ett amerikanskt bolag och kan behandla uppgifter i USA.

	och meddelandets innehåll.	Överföringen sker med stöd av EU–US Data Privacy Framework och EU-kommissionens standardavtalsklausuler (SCC)
--	----------------------------	---

Biträdet underrättar den Personuppgiftsansvarige skriftligen minst 30 dagar i förväg vid tillägg eller byte av Bitrådets underbiträden. Tillägg eller byte av underbiträdens egna underbiträden meddelas den Personuppgiftsansvarige utan onödigt dröjsmål efter att Biträdet fått kännedom om dem. Den Personuppgiftsansvarige har rätt att invända mot sådant byte. Biträdet ansvarar för underbitrådets fullgörande av dataskyddsskyldigheter i samma utsträckning som för sina egna.

6. Överföring till tredjeland

Biträdet strävar efter att personuppgifter behandlas inom EU/EES. Lagring av den Personuppgiftsansvariges data och all AI-assisterad avläsning sker inom EU/EES. E-postutskick sker via underbiträdet Resend från dess EU-region (Irland). Eftersom Resend är ett amerikanskt bolag kan mottagarens e-postadress och meddelandets innehåll även behandlas i USA. Sådan överföring sker med stöd av EU-kommissionens beslut om adekvat skyddsnivå för EU–US Data Privacy Framework samt EU-kommissionens standardavtalsklausuler (SCC), som ingår i Bitrådets personuppgiftsbiträdesavtal med Resend. Firebase App Check (Google reCAPTCHA Enterprise), som skyddar tjänsten mot automatiserat missbruk, är en global tjänst utan åtagande om lagringsplats. Tekniska uppgifter om användarens webbläsare och enhet kan därför behandlas av Google utanför EU/EES, bland annat i USA. Sådan överföring sker med stöd av EU-kommissionens standardavtalsklausuler (SCC) enligt Google Clouds Data Processing Addendum. I den mån andra underbiträden hanterar data i länder utanför EU/EES sker detta med stöd av standardavtalsklausuler eller annat giltigt överföringsverktyg enligt GDPR kapitel V.

7. Ansvar och begränsning

Varje Part ansvarar för skador som uppstår till följd av att denne bryter mot GDPR eller detta avtal. Bitrådets sammanlagda ansvar gentemot den Personuppgiftsansvarige under detta avtal är begränsat till ett belopp motsvarande tolv (12) månaders avgifter under Huvudavtalet, om inte grov vårdslöshet eller uppsåt föreligger.

8. Avtalstid

Detta avtal gäller under samma tid som Huvudavtalet och upphör automatiskt när Huvudavtalet upphör, om inte annat följer av tvingande lag.

9. Tillämplig lag och tvist

Detta avtal regleras av svensk rätt. Tvister som uppstår med anledning av avtalet ska i första hand lösas genom förhandling. Om förhandling inte leder till lösning inom 60 dagar ska tvisten avgöras av allmän domstol med Helsingborgs tingsrätt som första instans.

LAGRINGSTIDER

Personuppgifter som behandlas inom tjänsten raderas enligt följande:

Kategori	Lagringstid	Åtgärd
Aktiva medlemmar	Under avtalstiden samt 30 dagars åtkomstperiod därefter	Raderas inom 30 dagar efter att åtkomstperioden löpt ut
Arkiverade medlemmar	1 år från arkiveringsdatum	Uppgifterna raderas automatiskt
Inloggnings-IP och betrodda enheter på arkiverade medlemmar	Omedelbart vid arkivering	Fälten nollställs automatiskt
Inloggnings-IP på aktiva medlemmar	90 dagar efter senaste inloggning	Fältet nollställs automatiskt
Utgångna och använda inbjudningar	90 dagar efter att inbjudan skapades, när den har använts, arkiverats eller löpt ut	Uppgifterna raderas automatiskt
Poster i papperskorgen (dokument, avtal, licenser, möten, omröstningar)	30 dagar efter att posten flyttats till papperskorgen	Posten och tillhörande filer raderas automatiskt
Stängda supportärenden	2 år efter senaste ändring	Ärendet raderas automatiskt
Systemlogg (audit log)	2 år	Loggposten raderas automatiskt
Felloggar (tekniska fel i tjänsten)	90 dagar från att felet inträffade	Loggposten raderas automatiskt
Säkerhetskopior	Samtliga kopior från de senaste 30 dagarna; därefter en kopia per månad i 12 månader	Äldre kopior raderas automatiskt

Rensning sker via automatiserade schemalagda funktioner som körs dagligen. Varje körning loggas för spårbarhet.