

Personuppgiftsbiträdesavtal

Detta personuppgiftsbiträdesavtal utgör en del av huvudavtalet mellan Kunden som personuppgiftsansvarig och R&M Group AB som personuppgiftsbiträde.

Version 1.3

Publicerad: 29 juli 2026

Senast uppdaterad: 26 augusti 2026

01

Parter och avtalets ställning

Personuppgiftsansvarig

Den kund som identifieras i beställningen, företagskontot eller annat huvudavtal med Biträdet.

Personuppgiftsbiträde

R&M Group AB, org.nr 559493-2708, Stationstorget 2E, 269 43 Båstad, Sverige. Kontakt: info@rmdesigns.se.

Avtalet gäller när Biträdet behandlar personuppgifter för Kundens räkning och blir bindande samtidigt som huvudavtalet accepteras. Avtalet ingås elektroniskt när en behörig företrädare för Kunden godkänner den aktuella versionen i samband med kontoskapande eller beställning. Godkännandet dokumenteras med tidpunkt och versionsnummer i företagskontot. Någon separat underskrift krävs inte, om parterna inte uttryckligen kommer överens om annat. Begrepp i GDPR har samma betydelse här.

Vid konflikt om personuppgiftsbehandling har detta avtal företräde framför huvudavtalets övriga villkor.

02

Behandlingens omfattning

Biträdet behandlar personuppgifter genom rekryteringstjänsten Leysi enligt huvudavtalet. Behandlingens föremål, varaktighet, ändamål, kategorier av registrerade och personuppgifter anges i bilaga 1 nedan.

Kunden bestämmer ändamålen med rekryteringen och är ansvarig för laglighet, transparens, uppgiftsminimering, rättslig grund och instruktioner till Biträdet.

03

Dokumenterade instruktioner

Biträdet får endast behandla personuppgifter enligt Kundens dokumenterade instruktioner, detta avtal, huvudavtalet och den användning Kunden gör inom tjänstens avsedda funktioner.

Om Biträdet bedömer att en instruktion strider mot GDPR eller annan dataskyddslag ska Kunden informeras omedelbart. Biträdet får pausa den berörda behandlingen i väntan på en laglig instruktion.

Om lag kräver behandling utöver Kundens instruktioner informerar Biträdet Kunden före behandlingen, om inte lagen förbjuder sådan information.

04

Sekretess och behörighet

Biträdet säkerställer att personer som får behandla Kundens personuppgifter omfattas av sekretess eller lämplig lagstadgad tystnadsplikt och endast får åtkomst i den utsträckning som arbetsuppgifterna kräver.

Åtkomst ska tilldelas individuellt, begränsas efter roll och tas bort när behovet upphör.

05

Tekniska och organisatoriska åtgärder

Biträdet ska upprätthålla en säkerhetsnivå som är lämplig med hänsyn till behandlingens art, omfattning, sammanhang, ändamål och risker. Nuvarande huvudåtgärder anges i bilaga 2.

- tenant-isolering för företag, kandidater och filer
- autentisering och individuell behörighetskontroll
- servervalidering av ansökningar och signerade analysresultat
- begränsning av filformat och storlek

- krypterad transport och leverantörshanterad kryptering i vila
- loggning, felsökning och incidenthantering
- automatisk radering enligt fastställda lagringstider
- regeltester och kontroller före ändringar i åtkomstregler

06

Underbiträden

Kunden ger Biträdet ett generellt skriftligt tillstånd att använda de underbiträden som anges i bilaga 3. Biträdet ska säkerställa att underbiträden omfattas av dataskyddsskyldigheter som i sak motsvarar detta avtal.

Biträdet förblir fullt ansvarigt gentemot Kunden för att underbiträden fullgör sina dataskyddsskyldigheter.

Biträdet ska informera Kunden via kontots registrerade e-postadress om ett planerat nytt eller ersatt underbiträde minst 30 dagar innan ändringen börjar gälla när det är praktiskt möjligt. Kunden får göra en sakligt motiverad invändning av dataskyddsskäl. Om parterna inte kan lösa invändningen får Kunden säga upp den berörda tjänsten.

Underbiträde	Tjänst	Berörda uppgifter
Google Firebase / Google Cloud	Databas, autentisering och fillagring	Konto-, jobb- och kandidatdata
Vercel	Webbdrift och serverfunktioner	Trafikdata och uppgifter som behandlas i tjänstens serverflöden
OpenAI	AI-baserad analys av ansökningsunderlag	Ansökningshandlingar, frågesvar och kravprofil
Stripe	Betalningar och abonnemang	Företags-, kontakt- och betalningsuppgifter; inte kandidat-CV:n
Resend	E-postleverans	Kontaktuppgifter och innehåll i e-post som skickas från tjänsten
Microsoft 365 / Microsoft Graph	Frivillig kalender- och Teams-integration	Kontouppgifter, kalenderhändelser, deltagare, intervjutider och möteslänkar för anslutna användare
Cloudflare	DNS, trafikskydd och leverans av webbtrafik	IP-adress, tekniska loggar och förfrågningsmetadata

Leysis produktionsdatabas i Cloud Firestore är konfigurerad i multiregionen eur3 inom Europa och Firebase Storage är konfigurerad i regionen europe-west1 inom Europa.

07

Internationella överföringar

Biträdet får endast överföra personuppgifter utanför EU/EES enligt Kundens instruktioner och när kraven i GDPR kapitel V är uppfyllda.

När adekvansbeslut inte kan användas ska överföringen normalt stödjas på EU-kommissionens standardavtalsklausuler och vid behov kompletterande tekniska och organisatoriska skyddsåtgärder. Biträdet ska på begäran lämna rimligt tillgänglig information om aktuell mekanism.

08

Hjälp med registrerades rättigheter

Biträdet ska, med hänsyn till behandlingens art och i den mån det är möjligt, hjälpa Kunden att besvara begäranden om information, tillgång, rättelse, radering, begränsning, dataportabilitet, invändning och automatiserat beslutsfattande.

Om en registrerad vänder sig direkt till Biträdet om Kundens data ska Biträdet vidarebefordra begäran till Kunden och inte besvara den i sak utan instruktion, om inte lag kräver annat.

09

Personuppgiftsincidenter

Biträdet ska informera Kunden utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident som berör Kundens personuppgifter.

Informationen ska, i den mån den är tillgänglig, beskriva incidentens art, berörda kategorier och ungefärligt antal registrerade och poster, sannolika konsekvenser, genomförda eller föreslagna åtgärder samt kontaktväg för uppföljning. Kompletterande information kan lämnas stegvis.

Kunden ansvarar för bedömning och eventuell anmälan till IMY och information till registrerade, om inte parterna skriftligen kommit överens om annat.

10

Konsekvensbedömning och efterlevnad

Biträdet ska lämna rimlig hjälp med Kundens säkerhetsbedömning, konsekvensbedömning och förhandssamråd när hjälpen avser behandlingen i tjänsten och informationen är tillgänglig för Biträdet.

Biträdet ska tillhandahålla den information som skäligen behövs för att visa efterlevnad av artikel 28 GDPR.

11

Granskning och revision

Kunden får högst en gång per år, eller när det skäligen behövs efter en väsentlig incident eller misstänkt brist, begära en rimlig granskning av Bitrådets efterlevnad. Begränsningen gäller inte när en behörig tillsynsmyndighet kräver ytterligare granskning. Granskningen ska i första hand ske genom dokumentation, rapporter och skriftliga svar.

En platsrevision kräver skäligt förhandsbesked, ska genomföras under normal arbetstid, får inte äventyra andra kunders data eller säkerhet och bekostas av Kunden, om inte granskningen visar ett väsentligt avtalsbrott från Biträdet.

12

Återlämnande och radering

Under avtalstiden kan Kunden radera kandidatposter genom tjänstens funktioner. Kandidatdata raderas annars enligt standardtiden sex månader efter ansökan.

På Kundens val ska Biträdet, när huvudavtalet och den tillämpliga uppsägningstiden eller betalda årsperioden har löpt ut, återlämna personuppgifterna i ett skäligen tillgängligt exportformat eller radera dem och befintliga kopior. Kunden ska begära återlämnande innan avtalet upphör; om ingen sådan begäran har kommit in raderas uppgifterna enligt Bitrådets ordinarie avslutsprocess. Uppgifter får behållas längre när unionsrätt eller svensk rätt kräver det.

Uppgifter i säkerhetskopior och leverantörsloggar raderas eller skrivs över enligt ordinarie rotationscykel och får inte återföras till aktiv användning annat än vid nödvändig återställning.

13

Ansvar, avtalstid och lag

Parternas ansvar regleras av huvudavtalet och tillämplig dataskyddslag. Ingen avtalsbegränsning inskränker ansvar som inte får begränsas enligt GDPR eller annan tvingande lag.

Avtalet gäller så länge Biträdet behandlar personuppgifter för Kundens räkning. Svensk lag gäller och tvist hanteras enligt huvudavtalets tvistbestämmelse.

14

Bilaga 1 - Behandlingsbeskrivning

Del	Beskrivning
Föremål och ändamål	Ta emot, lagra, strukturera, analysera, sortera, visa, kommunicera och radera ansökningar samt administrera intervjuer och samarbete i Kundens rekrytering.
Varaktighet	Under huvudavtalets löptid och därefter under avtalad raderingsperiod.
Registrerade	Kandidater, Kundens användare, externa intervjudeltagare och personer som nämns i inskickade rekryteringshandlingar eller kalenderbokningar.
Personuppgifter	Kontaktuppgifter, CV, personligt brev, utbildning, erfarenhet, kompetenser, frågesvar, bedömningsunderlag, status, intervjuanteckningar, interna teamkommentarer, kalenderhändelser, mötestider, deltagaruppgifter, platser, möteslänkar och tekniska uppgifter.
Särskilda kategorier	Ingår inte i tjänstens avsedda behandling. Kan förekomma om Kandidaten eller Kunden ändå lämnar sådana uppgifter; Kunden ansvarar då för instruktion och rättsligt stöd.
Behandlingsmoment	Insamling, registrering, organisering, lagring, läsning, AI-analys, sortering, kalender- och mötessynkronisering, överföring till avtalade underbiträden, ändring, export och radering.

15

Bilaga 2 - Säkerhetsåtgärder

- Separering av Kunders data genom ägarfält och server- och databasregler.
- Autentiserad åtkomst till arbetsgivarvyer och privat lagring av kandidatfiler.
- Ingen direkt klientskrivning av publika ansökningar till databasen eller fillagringen.
- Validering och begränsning av filtyp, filstorlek och indata i serverroute.
- Signering och verifiering av AI-analys innan en kandidatpost skapas.
- Automatiserad gallring av kandidat-, jobb- och kontodata.
- Versionsloggning av visad policy och villkor.
- Beroende-, typ-, lint-, build- och regeltester före produktionsändringar.
- Krypterad överföring och leverantörshanterade skydd för lagrad data.
- Rutiner för åtkomstbegränsning, incidenthantering och radering.

16

Bilaga 3 - Underbiträdesförteckning

Underbiträde	Funktion	Berörda uppgifter
Google Firebase / Google Cloud	Databas, autentisering och fillagring	Konto-, jobb- och kandidatdata
Vercel	Webbdrift och serverfunktioner	Trafikdata och uppgifter som behandlas i tjänstens serverflöden
OpenAI	AI-baserad analys av ansökningsunderlag	Ansökningshandlingar, frågesvar och kravprofil
Stripe	Betalningar och abonnemang	Företags-, kontakt- och betalningsuppgifter; inte kandidat-CV:n
Resend	E-postleverans	Kontaktuppgifter och innehåll i e-post som skickas från tjänsten
Microsoft 365 / Microsoft Graph	Frivillig kalender- och Teams-integration	Kontouppgifter, kalenderhändelser, deltagare, intervjutider och möteslänkar för anslutna användare
Cloudflare	DNS, trafikskydd och leverans av webbtrafik	IP-adress, tekniska loggar och förfrågningsmetadata