

Personuppgiftsbiträdesavtal (DPA)

Senast uppdaterad 1 maj 2026 · Avtal enligt art. 28 i GDPR.

Detta är en översättning som endast är avsedd som information. Vid skillnader mellan översättningen och den engelska versionen gäller den engelska versionen.

Så fungerar det

Detta biträdesavtal är en del av användarvillkoren. Det börjar gälla automatiskt när en arbetsyta skapas och personuppgifter sparas i den. Den kundorganisation som äger arbetsytan är personuppgiftsansvarig; Dazr är personuppgiftsbiträde. Ingen underskrift behövs; om er inköpsprocess kräver ett exemplar som båda parter har undertecknat, skriv till legal@dazr.eu.

1. Definitioner

Begrepp i detta avtal har den betydelse de har i förordning (EU) 2016/679 (GDPR). "Kundens personuppgifter" är de personuppgifter som den personuppgiftsansvarige (eller de medlemmar och revisorer som agerar på dess vägnar) lägger in i arbetsytan, inklusive personuppgifter i kontrolluppgifter, bevis, kommentarer, filer, risker, incidenter, leverantörsposter, medlemmar och inbjudningar, rapporter via den öppna portalen och aktivitetsloggen.

2. Föremål, varaktighet, art och ändamål

- Föremål: behandling av kundens personuppgifter så att den personuppgiftsansvarige kan styra sitt complianceprogram för informationssäkerhet och dataskydd via plattformen Dazr Compliance.
- Varaktighet: den personuppgiftsansvariges abonnemangsperiod och den övergångsperiod efter upphörande som anges i användarvillkoren.
- Art och ändamål: drift, lagring, överföring, hämtning, radering och de åtgärder som beskrivs i användarvillkoren och integritetspolicyn.
- Typ av personuppgifter: identifieringsuppgifter om medlemmar i arbetsytor och inbjudna revisorer (e-post, namn, roll); i förekommande fall identifieringsuppgifter om personer som rapporterar via den öppna portalen eller anmäler incidenter; kontaktuppgifter om arbetsgivare och driftsmetadata som den personuppgiftsansvarige laddar upp. Den personuppgiftsansvarige ansvarar för att inte ladda upp känsliga personuppgifter om inte dess egen rättsliga grund tillåter det.
- Kategorier av registrerade: den personuppgiftsansvariges anställda, konsulter och inbjudna externa revisorer samt alla personer som nämns i det complianceinnehåll som den personuppgiftsansvarige väljer att ladda upp.

3. Personuppgiftsbitrådets skyldigheter

1. Vi behandlar kundens personuppgifter endast enligt dokumenterade instruktioner från den personuppgiftsansvarige. Instruktionerna består i användningen av plattformens avsedda funktioner; om vi anser att en instruktion strider mot GDPR eller annan dataskyddslagstiftning i EU eller en medlemsstat informerar vi den personuppgiftsansvarige.
2. Vi säkerställer att de personer som har behörighet att behandla kundens personuppgifter har åtagit sig att iaktta konfidentialitet.
3. Vi vidtar alla åtgärder som krävs enligt artikel 32 i GDPR (säkerhet i samband med behandlingen). De nuvarande åtgärderna beskrivs i avsnitt 7.
4. Vi följer villkoren i artikel 28.2 och 28.4 för att anlita underbiträden (se avsnitt 6).
5. Med hänsyn till behandlingens art och den information vi har bistår vi den personuppgiftsansvarige med att besvara begäranden från registrerade, anmäla incidenter, göra konsekvensbedömningar och genomföra

förhandssamråd med tillsynsmyndigheter (artikel 28.3 e och f).

6. Efter den personuppgiftsansvariges val raderar eller återlämnar vi alla kundens personuppgifter när tjänsten upphör och raderar befintliga kopior, om inte unionsrätten eller nationell rätt kräver lagring.
7. Vi ger den personuppgiftsansvarige tillgång till all information som behövs för att visa att artikel 28 följs, och möjliggör och bidrar till granskningar, inklusive inspektioner (se avsnitt 9).

4. Den personuppgiftsansvariges skyldigheter

- Den personuppgiftsansvarige garanterar att den har en rättslig grund enligt artikel 6 (och i förekommande fall artikel 9) för de personuppgifter som läggs in i arbetsytan.
- Den personuppgiftsansvarige ansvarar för att kundens personuppgifter är korrekta och för att besvara begäranden från registrerade om sin arbetsyta (begäranden som vi tar emot vidarebefordrar vi till den personuppgiftsansvarige, och vi bistår enligt artikel 28.3 e).
- Den personuppgiftsansvarige styr åtkomsten (medlemmarnas roller, inbjudningar av revisorer och den öppna rapportportalen) via plattformens inställningar.

5. Internationella överföringar

Kundens personuppgifter lagras som standard i Europeiska unionen. Om ett underbiträde har sitt huvudkontor utanför EU sker överföringar enligt Europeiska kommissionens standardavtalsklausuler (beslut 2021/914), modul 3 (biträde till biträde), med de kompletterande åtgärder som beskrivs i avsnitt 7. Den aktuella listan över underbiträden och var de finns står på </legal/subprocessors>.

6. Underbiträden

1. Den personuppgiftsansvarige ger oss tillstånd att anlita underbiträden för att leverera tjänsten. Den aktuella listan finns på </legal/subprocessors>.
2. Vi informerar den personuppgiftsansvarige om planerade tillägg eller byten minst 30 dagar i förväg via e-postprenumerationen på den sidan eller via e-post till arbetsytans ägare.
3. Den personuppgiftsansvarige kan invända av rimliga dataskyddsskäl. Kan vi inte tillmötesgå invändningen kan den personuppgiftsansvarige säga upp den berörda tjänsten och få proportionell återbetalning för den oanvända delen av den pågående faktureringsperioden.
4. Vi ålägger genom skriftligt avtal varje underbiträde dataskyddsskyldigheter som skyddar minst lika bra som detta avtal, och vi ansvarar gentemot den personuppgiftsansvarige för att underbiträdet fullgör sina skyldigheter.

7. Säkerhetsåtgärder (artikel 32)

- Kryptering. Kundens personuppgifter krypteras i vila med AES-256-GCM på applikationsnivå, utöver lagringsleverantörens egen kryptering. All överföring sker via HTTPS med HSTS preload, utan okrypterat alternativ. Nycklarna härleds med HKDF från en huvudnyckel som bara finns i miljövariabler i produktionsinfrastrukturen.
- Åtkomstkontroll. Rollbaserad åtkomstkontroll i plattformen (ägare, administratör, medlem, revisor); tidsbegränsade revisorssessioner som kan återkallas. Driftåtkomst är begränsad till ett litet supportteam via supportportalen, som avsiktligt bara visar metadata.
- Autentisering. Inloggning utan lösenord med engångskod. HMAC-signerade sessionstoken med begränsad giltighetstid. Begränsning av antalet anrop på varje öppen slutpunkt, även administratörsinloggningen.
- Motståndskraft och integritet. Aktivitetslogg som bara kan läggas till i, över varje åtgärd som ändrar ett tillstånd. Säkerhetskopior inom EU. Integriteten i lagrade data kontrolleras med AEAD-autentiseringstagg; manipulerad krypterad text ger ett fel och lämnas inte ut.
- Nätverk och headers. Strikt Content-Security-Policy med en lista över tillåtna inbäddade skript efter hash,

strikt X-Frame-Options, X-Content-Type-Options nosniff och HSTS preload.

- Sårbarhetshantering. Beroenden är låsta till fasta versioner; vi följer säkerhetsmeddelanden och installerar uppdateringar enligt en plan som passar allvarlighetsgraden.

8. Personuppgiftsincidenter

Om vi får kännedom om en personuppgiftsincident som berör kundens personuppgifter underrättar vi arbetsytans ägare utan onödigt dröjsmål och senast 72 timmar efter att vi fått kännedom om den (artikel 33.2).

Underrättelsen beskriver, i den mån det är känt: incidentens art, de sannolika konsekvenserna, de åtgärder som vidtagits eller föreslås och en kontaktpunkt för mer information. Vi bistår den personuppgiftsansvarige med dess egna anmälningsskyldigheter enligt artikel 33 och 34.

9. Granskningar

Den personuppgiftsansvarige (eller en extern revisor som den har utsett) kan granska att vi följer detta avtal en gång var tolfte månad, med minst 30 dagars skriftligt varsel och under kontorstid, på ett sätt som inte stör vår verksamhet orimligt och som respekterar konfidentialiteten för andra kunders data. Vi får ta ut en rimlig avgift för granskningar utöver detta. Om en granskningsskyldighet enligt artikel 28.3 h kan uppfyllas med ett intyg från tredje part som vi har, lämnar vi det i stället för en granskning på plats.

10. Ansvar

Varje parts ansvar enligt detta avtal omfattas av begränsningarna i användarvillkoren. Dessa begränsningar begränsar inte ansvaret för skada som registrerade lider enligt artikel 82 i GDPR.

11. Giltighetstid och upphörande

Detta avtal gäller så länge vi behandlar kundens personuppgifter och fortsätter att gälla efter att användarvillkoren upphört i den omfattning och så länge vi fortfarande har sådana uppgifter. Avsnitt 8 (incidenter), 9 (granskningar) och 12 (återlämnande och radering) gäller även efter upphörandet.

12. Återlämnande och radering

När tjänsten upphör kan den personuppgiftsansvarige exportera arbetsytans data med plattformens exportverktyg under den övergångsperiod på 30 dagar som anges i användarvillkoren. Efter övergångsperioden raderar vi kundens personuppgifter; säkerhetskopior förfaller enligt vår lagringsplan. Uppgifter som vi är skyldiga att spara (t.ex. fakturering enligt italiensk handelsrätt) sparas bara under den tid skyldigheten gäller.

13. Företräde

Om detta avtal strider mot användarvillkoren eller integritetspolicyn har detta avtal företräde i frågor om behandling av personuppgifter. Standardavtalsklausuler som ingår vid en överföring utanför EU har företräde framför detta avtal och användarvillkoren i de frågor de reglerar.

14. Meddelanden

- Till Dazr: privacy@dazr.eu (dataskydd) eller security@dazr.eu (incidenter).
- Till den personuppgiftsansvarige: den e-postadress för arbetsytans ägare som är registrerad när meddelandet skickas.