

Databehandleravtale (DPA)

Sist oppdatert 1. mai 2026 · Avtale etter art. 28 i GDPR.

Dette er en oversettelse som kun er til informasjon. Ved forskjeller mellom denne oversettelsen og den engelske versjonen gjelder den engelske versjonen.

Slik fungerer det

Denne databehandleravtalen er en del av bruksvilkårene. Den trer automatisk i kraft når et arbeidsområde opprettes og personopplysninger lagres i det. Kundeorganisasjonen som eier arbeidsområdet, er behandlingsansvarlig; Dazr er databehandler. Det trengs ingen signatur; hvis innkjøpsprosessen deres krever et eksemplar signert av begge parter, skriv til legal@dazr.eu.

1. Definisjoner

Begreper i denne avtalen har den betydningen de har i forordning (EU) 2016/679 (GDPR). «Kundens personopplysninger» er personopplysninger som den behandlingsansvarlige (eller medlemmer og revisorer som handler på dennes vegne) legger inn i arbeidsområdet, inkludert personopplysninger i kontrollopgaver, dokumentasjon, kommentarer, filer, risikoer, hendelser, leverandøroppføringer, medlemmer og invitasjoner, innmeldinger via den åpne portalen og aktivitetsloggen.

2. Gjenstand, varighet, art og formål

- Gjenstand: behandling av kundens personopplysninger slik at den behandlingsansvarlige kan styre sitt complianceprogram for informasjonssikkerhet og personvern via plattformen Dazr Compliance.
- Varighet: den behandlingsansvarliges abonnementsperiode og overgangsperioden etter opphør som står i bruksvilkårene.
- Art og formål: drift, lagring, overføring, gjenfinning, sletting og handlingene som er beskrevet i bruksvilkårene og personvernerklæringen.
- Type personopplysninger: identifikasjonsopplysninger om medlemmer av arbeidsområder og inviterte revisorer (e-post, navn, rolle); der det er relevant, identifikasjonsopplysninger om personer som melder inn via den åpne portalen eller rapporterer hendelser; kontaktopplysninger om arbeidsgivere og driftsmetadata som den behandlingsansvarlige laster opp. Den behandlingsansvarlige sørger for ikke å laste opp særlige kategorier av personopplysninger med mindre eget rettslig grunnlag tillater det.
- Kategorier av registrerte: den behandlingsansvarliges ansatte, konsulenter og inviterte eksterne revisorer, og alle personer som nevnes i compliance-innhold den behandlingsansvarlige velger å laste opp.

3. Databehandlerens plikter

1. Vi behandler kundens personopplysninger bare etter dokumenterte instruksjoner fra den behandlingsansvarlige. Instruksene består i bruken av plattformens tiltenkte funksjoner; mener vi at en instruks er i strid med GDPR eller annen personvernlovgivning i EU/EØS eller et medlemsland, gir vi den behandlingsansvarlige beskjed.
2. Vi sørger for at personer med tilgang til å behandle kundens personopplysninger har forpliktet seg til konfidensialitet.
3. Vi gjennomfører alle tiltak som kreves etter artikkel 32 i GDPR (sikkerhet ved behandlingen). Dagens tiltak er beskrevet i avsnitt 7.
4. Vi overholder vilkårene i artikkel 28 nr. 2 og 4 for bruk av underdatabehandlere (se avsnitt 6).
5. Ut fra behandlingens art og informasjonen vi har, bistår vi den behandlingsansvarlige med å svare på henvendelser fra registrerte, melde avvik, gjennomføre vurderinger av personvernkonsekvenser og forhåndsdrøfting med tilsynsmyndigheter (artikkel 28 nr. 3 bokstav e og f).
6. Etter den behandlingsansvarliges valg sletter eller returnerer vi alle kundens personopplysninger når

tjenesten opphører, og sletter eksisterende kopier, med mindre EU/EØS-retten eller nasjonal rett krever lagring.

7. Vi gir den behandlingsansvarlige all informasjon som trengs for å vise at artikkel 28 overholdes, og legger til rette for og bidrar til revisjoner, inkludert inspeksjoner (se avsnitt 9).

4. Den behandlingsansvarliges plikter

- Den behandlingsansvarlige innestår for å ha et behandlingsgrunnlag etter artikkel 6 (og der det er relevant artikkel 9) for personopplysningene som legges inn i arbeidsområdet.
- Den behandlingsansvarlige er ansvarlig for at kundens personopplysninger er korrekte, og for å svare på henvendelser fra registrerte om sitt arbeidsområde (henvendelser vi mottar, sender vi videre, og vi bistår etter artikkel 28 nr. 3 bokstav e).
- Den behandlingsansvarlige styrer tilgangen (medlemmenes roller, invitasjoner av revisorer og den åpne innmeldingsportalen) via plattformens innstillinger.

5. Internasjonale overføringer

Kundens personopplysninger lagres som standard i Den europeiske union. Har en underdatabehandler hovedkontor utenfor EU, skjer overføringer etter EU-kommisjonens standardpersonvernbestemmelser (beslutning 2021/914), modul 3 (databehandler til databehandler), med tilleggstiltakene som er beskrevet i avsnitt 7. Den gjeldende listen over underdatabehandlere og hvor de holder til, står på [/legal/subprocessors](#).

6. Underdatabehandlere

1. Den behandlingsansvarlige gir oss tillatelse til å bruke underdatabehandlere for å levere tjenesten. Den gjeldende listen står på [/legal/subprocessors](#).
2. Vi varslar den behandlingsansvarlige om planlagte tillegg eller utskiftninger minst 30 dager i forveien via e-postabonnementet på den siden eller via e-post til eieren av arbeidsområdet.
3. Den behandlingsansvarlige kan protestere av rimelige personverngrunner. Kan vi ikke imøtekomme protesten, kan den behandlingsansvarlige si opp den berørte tjenesten og få forholdsmessig refusjon for den ubrukte delen av inneværende faktureringsperiode.
4. Vi pålegger hver underdatabehandler ved skriftlig avtale personvernforpliktelser som beskytter minst like godt som denne avtalen, og vi er ansvarlige overfor den behandlingsansvarlige for at underdatabehandleren oppfyller sine forpliktelser.

7. Sikkerhetstiltak (artikkel 32)

- Kryptering. Kundens personopplysninger krypteres i hvile med AES-256-GCM på applikasjonsnivå, i tillegg til lagringsleverandørens egen kryptering. All overføring skjer via HTTPS med HSTS preload, uten ukryptert alternativ. Nøklene utledes med HKDF fra en hovednøkkel som bare finnes i miljøvariabler i produksjonsinfrastrukturen.
- Tilgangsstyring. Rollebasert tilgangsstyring i plattformen (eier, administrator, medlem, revisor); tidsbegrensede revisorøker som kan trekkes tilbake. Driftstilgang er begrenset til et lite supportteam via supportportalen, som med vilje bare viser metadata.
- Autentisering. Innlogging uten passord med engangskode. HMAC-signerte økttokener med begrenset levetid. Begrensning av antall forespørsler på alle åpne endepunkter, også administratorinnloggingen.
- Robusthet og integritet. Aktivitetslogg som bare kan legges til i, over hver handling som endrer en tilstand. Sikkerhetskopier i EU. Integriteten til lagrede data kontrolleres med AEAD-autentiseringsmerker; manipulert kryptert tekst gir en feil og leveres ikke ut.
- Nettverk og headere. Streng Content-Security-Policy med en liste over tillatte innebygde skript etter hash, streng X-Frame-Options, X-Content-Type-Options nosniff og HSTS preload.

- Sårbarhetshåndtering. Avhengigheter er låst til faste versjoner; vi følger sikkerhetsvarsler og installerer oppdateringer etter en plan som passer alvorlighetsgraden.

8. Brudd på personopplysningssikkerheten

Hvis vi blir kjent med et brudd på personopplysningssikkerheten som berører kundens personopplysninger, varsler vi eieren av arbeidsområdet uten ugrunnet opphold og senest 72 timer etter at vi ble kjent med det (artikkel 33 nr. 2). Varselet beskriver, så langt det er kjent: bruddets art, de sannsynlige konsekvensene, tiltakene som er gjennomført eller foreslått, og et kontaktpunkt for mer informasjon. Vi bistår den behandlingsansvarlige med dennes egne meldeplikter etter artikkel 33 og 34.

9. Revisjoner

Den behandlingsansvarlige (eller en ekstern revisor som denne har utpekt) kan revidere at vi overholder denne avtalen én gang hver tolvte måned, med minst 30 dagers skriftlig varsel og i arbeidstiden, på en måte som ikke forstyrrer driften vår urimelig og som respekterer konfidensialiteten til andre kunders data. Vi kan kreve et rimelig gebyr for revisjoner utover dette. Kan en revisjonsplikt etter artikkel 28 nr. 3 bokstav h oppfylles med en erklæring fra en tredjepart som vi har, gir vi den i stedet for en revisjon på stedet.

10. Ansvar

Hver parts ansvar etter denne avtalen er underlagt begrensningene i bruksvilkårene. Disse begrensningene begrenser ikke ansvaret for skade som registrerte lider etter artikkel 82 i GDPR.

11. Varighet og opphør

Denne avtalen gjelder så lenge vi behandler kundens personopplysninger, og gjelder etter at bruksvilkårene har opphørt i det omfang og så lenge vi fortsatt har slike opplysninger. Avsnitt 8 (brudd), 9 (revisjoner) og 12 (tilbakelevering og sletting) gjelder også etter opphør.

12. Tilbakelevering og sletting

Når tjenesten opphører, kan den behandlingsansvarlige eksportere data fra arbeidsområdet med plattformens eksportverktøy i overgangsperioden på 30 dager som står i bruksvilkårene. Etter overgangsperioden sletter vi kundens personopplysninger; sikkerhetskopier utløper etter vår lagringsplan. Opplysninger vi er pålagt å oppbevare (for eksempel fakturering etter italiensk handelsrett), oppbevares bare så lenge plikten gjelder.

13. Rangfølge

Ved motstrid mellom denne avtalen og bruksvilkårene eller personvernerklæringen har denne avtalen forrang i spørsmål om behandling av personopplysninger. Standardpersonvernbestemmelser som inngår for overføring utenfor EU, har forrang foran denne avtalen og bruksvilkårene i spørsmålene de regulerer.

14. Meldinger

- Til Dazr: privacy@dazr.eu (personvern) eller security@dazr.eu (hendelser).
- Til den behandlingsansvarlige: e-postadressen til eieren av arbeidsområdet som er registrert når meldingen sendes.