

# Databehandleraftale (DPA)

Senest opdateret 1. maj 2026 · Aftale efter art. 28 i GDPR.

Dette er en oversættelse, der kun er til orientering. Ved forskelle mellem denne oversættelse og den engelske version har den engelske version forrang.

## Sådan fungerer det

Denne databehandleraftale er en del af vilkårene for brug. Den træder automatisk i kraft, når et arbejdsområde oprettes, og der gemmes personoplysninger i det. Den kundeorganisation, der ejer arbejdsområdet, er dataansvarlig; Dazr er databehandler. Der kræves ingen underskrift; hvis jeres indkøbsproces kræver et eksemplar underskrevet af begge parter, så skriv til [legal@dazr.eu](mailto:legal@dazr.eu).

## 1. Definitioner

Begreber i denne aftale har den betydning, de har i forordning (EU) 2016/679 (GDPR). "Kundens personoplysninger" er de personoplysninger, som den dataansvarlige (eller de medlemmer og revisorer, der handler under dennes ansvar) lægger ind i arbejdsområdet, herunder personoplysninger i kontrolopgaver, dokumentation, kommentarer, filer, risici, hændelser, leverandørposter, medlemmer og invitationer, indberetninger via den offentlige portal og aktivitetsloggen.

## 2. Genstand, varighed, karakter og formål

- Genstand: behandling af kundens personoplysninger, så den dataansvarlige kan styre sit complianceprogram for informationssikkerhed og databeskyttelse via platformen Dazr Compliance.
- Varighed: den dataansvarliges abonnementsperiode plus den overgangsperiode efter ophør, som vilkårene for brug fastsætter.
- Karakter og formål: hosting, opbevaring, overførsel, fremsøgning, sletning og de handlinger, der er beskrevet i vilkårene for brug og privatlivspolitikken.
- Typer af personoplysninger: identifikationsoplysninger om medlemmer af arbejdsområder og inviterede revisorer (e-mail, navn, rolle); hvor det er relevant, identifikationsoplysninger om personer, der indberetter via den offentlige portal eller melder hændelser; kontaktoplysninger om arbejdsgivere og driftsmetadata, som den dataansvarlige uploader. Den dataansvarlige sørger for ikke at uploade følsomme personoplysninger, medmindre dennes eget retsgrundlag tillader det.
- Kategorier af registrerede: den dataansvarliges medarbejdere, konsulenter og inviterede eksterne revisorer samt alle personer, der nævnes i det compliance-indhold, den dataansvarlige vælger at uploade.

## 3. Databehandlerens forpligtelser

1. Vi behandler kun kundens personoplysninger efter dokumenteret instruks fra den dataansvarlige. Instruksen består i brugen af platformens tilsigtede funktioner; hvis vi mener, at en instruks er i strid med GDPR eller anden databeskyttelseslovgivning i EU eller en medlemsstat, giver vi den dataansvarlige besked.
2. Vi sikrer, at de personer, der har adgang til at behandle kundens personoplysninger, har forpligtet sig til fortrolighed.
3. Vi træffer alle foranstaltninger, der kræves efter artikel 32 i GDPR (behandlingssikkerhed). De nuværende foranstaltninger er beskrevet i afsnit 7.
4. Vi overholder betingelserne i artikel 28, stk. 2 og 4, for brug af underdatabehandlere (se afsnit 6).
5. Under hensyntagen til behandlingens karakter og de oplysninger, vi har, bistår vi den dataansvarlige med at besvare anmodninger fra registrerede, anmelde brud, udarbejde konsekvensanalyser og gennemføre forudgående høring af tilsynsmyndigheder (artikel 28, stk. 3, litra e og f).
6. Efter den dataansvarliges valg sletter eller returnerer vi alle kundens personoplysninger, når tjenesten

ophører, og sletter eksisterende kopier, medmindre EU-retten eller national ret kræver opbevaring.

7. Vi stiller alle oplysninger til rådighed for den dataansvarlige, som er nødvendige for at påvise overholdelse af artikel 28, og giver mulighed for og bidrager til revisioner, herunder inspektioner (se afsnit 9).

## 4. Den dataansvarliges forpligtelser

---

- Den dataansvarlige indestår for at have et retsgrundlag efter artikel 6 (og hvor relevant artikel 9) for de personoplysninger, der lægges ind i arbejdsområdet.
- Den dataansvarlige er ansvarlig for, at kundens personoplysninger er korrekte, og for at besvare anmodninger fra registrerede om sit arbejdsområde (anmodninger, vi modtager, sender vi videre til den dataansvarlige, og vi bistår efter artikel 28, stk. 3, litra e).
- Den dataansvarlige styrer adgangen (medlemmernes roller, invitationer af revisorer og den offentlige indberetningsportal) via platformens indstillinger.

## 5. Internationale overførsler

---

Kundens personoplysninger opbevares som standard i Den Europæiske Union. Har en underdatabehandler hovedsæde uden for EU, sker overførsler efter Europa-Kommissionens standardkontraktbestemmelser (afgørelse 2021/914), modul 3 (databehandler til databehandler), med de supplerende foranstaltninger, der er beskrevet i afsnit 7. Den aktuelle liste over underdatabehandlere og deres placering findes på [/legal/subprocessors](#).

## 6. Underdatabehandlere

---

1. Den dataansvarlige giver os tilladelse til at bruge underdatabehandlere til at levere tjenesten. Den aktuelle liste findes på [/legal/subprocessors](#).
2. Vi giver den dataansvarlige besked om planlagte tilføjelser eller udskiftninger mindst 30 dage i forvejen via e-mailabonnementet på den side eller via e-mail til ejeren af arbejdsområdet.
3. Den dataansvarlige kan gøre indsigelse af rimelige databeskyttelsesmæssige grunde. Kan vi ikke imødekomme indsigelsen, kan den dataansvarlige opsige den berørte tjeneste og få forholdsmæssig refusion for den ubrugte del af den igangværende faktureringsperiode.
4. Vi pålægger ved skriftlig aftale hver underdatabehandler databeskyttelsesforpligtelser, der beskytter mindst lige så godt som denne aftale, og vi hæfter over for den dataansvarlige for underdatabehandlerens opfyldelse af sine forpligtelser.

## 7. Sikkerhedsforanstaltninger (artikel 32)

---

- Kryptering. Kundens personoplysninger krypteres i hvile med AES-256-GCM på applikationsniveau ud over lagerleverandørens egen kryptering. Al transport sker via HTTPS med HSTS preload, uden ukrypteret alternativ. Nøglerne afledes med HKDF fra en hovednøgle, der kun findes i miljøvariabler på produktionsinfrastrukturen.
- Adgangsstyring. Rollebaseret adgangsstyring i platformen (ejer, administrator, medlem, revisor); tidsbegrænsede revisorsessioner, der kan tilbagekaldes. Driftsadgang er begrænset til et lille supportteam via supportportalen, der bevidst kun viser metadata.
- Godkendelse. Login uden adgangskode med engangskode. HMAC-signerede sessionstokens med begrænset levetid. Begrænsning af antallet af forespørgsler på alle offentlige endpoints, også administratorlogin.
- Robusthed og integritet. Aktivitetslog, der kun kan tilføjes til, over hver handling, der ændrer en tilstand. Backup i EU. Integriteten af lagrede data kontrolleres med AEAD-godkendelsesmærker; manipuleret krypteret tekst giver en fejl og udleveres ikke.
- Netværk og headers. Streng Content-Security-Policy med en tilladelsesliste over hashede inline-scripts, streng X-Frame-Options, X-Content-Type-Options nosniff og HSTS preload.
- Sårbarhedsstyring. Afhængigheder er låst til faste versioner; vi følger sikkerhedsadvarsler og installerer

rettelser efter en plan, der passer til alvorligheden.

## 8. Brud på persondatasikkerheden

---

Bliver vi opmærksomme på et brud på persondatasikkerheden, der berører kundens personoplysninger, underretter vi ejeren af arbejdsområdet uden unødigt forsinkelse og senest 72 timer efter, at vi er blevet opmærksomme på det (artikel 33, stk. 2). Underretningen beskriver, så vidt det vides: bruddets karakter, de sandsynlige konsekvenser, de trufne eller foreslåede foranstaltninger og et kontaktpunkt for yderligere oplysninger. Vi bistår den dataansvarlige med dennes egne anmeldelsespligter efter artikel 33 og 34.

## 9. Revisioner

---

Den dataansvarlige (eller en ekstern revisor, som denne har udpeget) kan revidere vores overholdelse af denne aftale én gang hver tolvte måned med mindst 30 dages skriftligt varsel og inden for normal arbejdstid, på en måde, der ikke unødigt forstyrrer vores drift og respekterer fortroligheden af andre kunders data. Vi kan opkræve et rimeligt gebyr for revisioner ud over dette. Kan en revisionsforpligtelse efter artikel 28, stk. 3, litra h, opfyldes med en erklæring fra en tredjepart, som vi har, stiller vi den til rådighed i stedet for en revision på stedet.

## 10. Ansvar

---

Hver parts ansvar efter denne aftale er underlagt begrænsningerne i vilkårene for brug. Disse begrænsninger begrænser ikke ansvaret for skader, som registrerede lider efter artikel 82 i GDPR.

## 11. Varighed og ophør

---

Denne aftale gælder, så længe vi behandler kundens personoplysninger, og består efter ophør af vilkårene for brug i det omfang og så længe, vi stadig har sådanne oplysninger. Afsnit 8 (brud), 9 (revisioner) og 12 (returnering og sletning) gælder også efter ophør.

## 12. Returnering og sletning

---

Når tjenesten ophører, kan den dataansvarlige eksportere data fra arbejdsområdet med platformens eksportværktøjer i den overgangsperiode på 30 dage, som vilkårene for brug fastsætter. Efter overgangsperioden sletter vi kundens personoplysninger; backup udløber efter vores opbevaringsplan. Data, vi er forpligtet til at opbevare (f.eks. fakturering efter italiensk handelsret), opbevares kun i den periode, forpligtelsen gælder.

## 13. Rangorden

---

Er der modstrid mellem denne aftale og vilkårene for brug eller privatlivspolitikken, har denne aftale forrang i spørgsmål om databehandling. Standardkontraktbestemmelser, der indgår ved overførsel uden for EU, har forrang for denne aftale og vilkårene for brug i de spørgsmål, de regulerer.

## 14. Meddelelser

---

- Til Dazr: [privacy@dazr.eu](mailto:privacy@dazr.eu) (databeskyttelse) eller [security@dazr.eu](mailto:security@dazr.eu) (hændelser).
- Til den dataansvarlige: den e-mailadresse for ejeren af arbejdsområdet, der er registreret på tidspunktet for meddelelsen.