# Databehandleravtale for Grantify

**Sist oppdatert:** 10. august 2026
**Databehandler:** Grantify AS, org.nr. 937 968 779
**Kontakt:** support@grantify.no

Denne databehandleravtalen inngår som en del av kundeforholdet mellom Grantify AS og Kunden. Avtalen regulerer Grantifys behandling av personopplysninger på vegne av Kunden ved Kundens bruk av Grantify.

## 1. Partene

Denne databehandleravtalen er inngått mellom:

**Kunden**, som behandlingsansvarlig, og
**Grantify AS**, org.nr. 937 968 779, som databehandler.

Kunden og Grantify omtales samlet som **Partene**.

Databehandleravtalen gjelder for alle personopplysninger Grantify behandler på vegne av Kunden i forbindelse med levering av Grantify-tjenesten.

## 2. Forholdet til kundeavtalen

Databehandleravtalen er en del av avtaleverket mellom Partene og gjelder sammen med Grantifys kundeavtale.

Ved motstrid mellom databehandleravtalen og kundeavtalen om behandling av personopplysninger, går databehandleravtalen foran.

Databehandleravtalen gjelder så lenge Grantify behandler personopplysninger på vegne av Kunden.

## 3. Formål med behandlingen

Formålet med behandlingen er å levere, drifte, sikre, supportere og videreutvikle Grantify som programvareløsning for prosjektregnskap, dokumentasjon og rapportering av SkatteFUNN-prosjekter.

Grantify skal bare behandle personopplysninger for å:

a. gi Kunden tilgang til og bruk av tjenesten,
b. administrere brukere, roller og tilganger,
c. muliggjøre timeføring, signering, godkjenning og rapportering,
d. registrere og strukturere prosjektopplysninger, kostnader, lønnsdata, offentlig støtte og annen rapporteringsinformasjon,
e. generere rapporter, eksportfiler og arkiveringsdokumentasjon,
f. yte support, herunder AI-basert brukerstøtte,
g. logge spørsmål og svar i AI-supporten for å levere support, analysere typiske spørsmål, forbedre veiledning, gjennomføre stikkprøvebasert kvalitetskontroll og følge opp Kunden dersom Grantify avdekker svar som kan være uriktige, uklare eller ufullstendige,
h. ivareta informasjonssikkerhet, logging, sikkerhetskopiering og teknisk drift, og
i. oppfylle dokumenterte instrukser fra Kunden.

Grantify kan ikke bruke personopplysninger til egne formål, med mindre dette er særskilt avtalt, følger av lov, eller opplysningene er anonymisert slik at de ikke lenger kan knyttes til Kunden eller enkeltpersoner.

## 4. AI-support og kvalitetskontroll

Grantify kan behandle spørsmål, svar og tilhørende metadata fra AI-supporten for å levere supporttjenesten, forbedre hjelpetekster og funksjonalitet, analysere typiske spørsmål, kvalitetssikre svar og følge opp Kunden dersom Grantify avdekker at et svar kan ha vært uriktig, uklart eller ufullstendig.

Tilgang til chatlogger skal begrenses til personer hos Grantify som har tjenstlig behov for slik tilgang, for eksempel

for support, kvalitetskontroll, sikkerhet, feilretting eller produktforbedring.

Grantify skal ikke bruke Kundens chatlogger til trening eller finjustering av generelle AI-modeller uten særskilt avtale eller annet gyldig grunnlag. Dette er ikke til hinder for at Grantify kan bruke anonymiserte og aggregerte innsikter fra chatlogger til statistikk, analyse, forbedring av hjelpetekster, produktutvikling og kvalitetssikring, forutsatt at opplysningene ikke kan knyttes til Kunden, enkeltpersoner eller konkrete prosjekter.

Kunden er ansvarlig for å informere egne brukere om at spørsmål og svar i AI-supporten kan logges og gjennomgås for kvalitets- og supportformål.

## 5. Behandlingens art

Behandlingen kan omfatte innsamling, registrering, strukturering, lagring, endring, sammenstilling, visning, analyse, eksport, tilgangsstyring, supportbehandling, logging, sikkerhetskopiering, sletting og annen behandling som er nødvendig for å levere tjenesten.

Behandlingen skjer hovedsakelig elektronisk i Grantifys skybaserte løsning.

## 6. Typer personopplysninger

Grantify kan behandle følgende typer personopplysninger på vegne av Kunden:

a. navn,
b. e-postadresse og telefonnummer,
c. rolle og tilgangsnivå i løsningen,
d. selskaps- og prosjektrolle, for eksempel selskapsadministrator, prosjektleder, prosjektdeltaker eller revisor,
e. timeføringsdata, herunder dato, antall timer, arbeidspakke, beskrivelse og status,
f. signerings- og godkjenningshistorikk, herunder tidspunkt og bruker,
g. lønnsdata som Kunden registrerer, for eksempel avtalt årslønn, stillingsprosent og beregnet timesats,
h. kostnads- og prosjektdata som kan knyttes til enkeltpersoner,
i. opplysninger om offentlig støtte, redusert arbeidsgiveravgift eller annen rapporteringsinformasjon som kan knyttes til ansatte eller prosjektdeltakere,
j. bruksmønster, tekniske logger, innloggingshistorikk og hendelseslogger,
k. annen informasjon Kunden selv registrerer i tjenesten,
l. spørsmål og fritekst Kunden eller Kundens brukere legger inn i AI-supporten,
m. svar, anbefalinger og annen respons generert av AI-supporten, og
n. metadata knyttet til AI-support, herunder tidspunkt, bruker, rolle, prosjekt-/selskapskontekst og eventuell vurdering eller merking av svarkvalitet.

Grantify skal ikke be Kunden registrere særlige kategorier av personopplysninger, slik som helseopplysninger, fagforeningsmedlemskap, religion, politisk oppfatning eller lignende. Dersom Kunden likevel registrerer slike opplysninger, er Kunden ansvarlig for at det foreligger gyldig behandlingsgrunnlag og at opplysningene er nødvendige.

## 7. Kategorier av registrerte

Behandlingen kan gjelde følgende kategorier av registrerte:
a. prosjektledere,
b. prosjektdeltakere,
c. selskapsadministratorer,
d. eksterne rådgivere eller konsulenter som Kunden gir tilgang, og
e. andre personer Kunden registrerer eller gir tilgang til i tjenesten.

## 8. Varighet

Grantify behandler personopplysninger på vegne av Kunden så lenge kundeforholdet består og så lenge det er nødvendig for å oppfylle formålet med behandlingen.

Kunden har tilgang til tjenesten for rapporteringsåret og i 6 måneder etter utløpet av rapporteringsåret

(«tilgangsperioden»), med mindre annet er avtalt.

Etter utløpet av tilgangsperioden kan Grantify lagre Kundens data i en begrenset periode for å muliggjøre reaktivering, support, feilhåndtering, sikkerhetskopiering og oppfølging av avtaleforholdet.

Kundens data slettes eller anonymiseres senest 12 måneder etter utløpet av tilgangsperioden, med mindre annet er avtalt, annet følger av Kundens dokumenterte instruks, eller videre lagring er nødvendig for å oppfylle lovpålagte plikter eller håndtere krav eller tvister.

## 9. Kundens ansvar og instrukser

Kunden er behandlingsansvarlig og bestemmer formålet med behandlingen og hvilke personopplysninger som skal behandles i tjenesten.

Kunden er ansvarlig for at:

a. det foreligger gyldig behandlingsgrunnlag for personopplysningene som registreres i Grantify,
b. de registrerte får nødvendig informasjon om behandlingen,
c. personopplysningene som registreres er relevante, korrekte og nødvendige,
d. Kundens brukere bare gis nødvendige tilganger,
e. personopplysninger ikke lagres lenger enn nødvendig, og
f. Kunden har interne rutiner for bruk, kontroll, eksport og sletting.

Grantify skal bare behandle personopplysninger etter dokumenterte instrukser fra Kunden. Denne databehandleravtalen, kundeavtalen, Kundens bruk av tjenesten og Kundens konfigurasjon av løsningen utgjør Kundens instrukser.

Dersom Grantify mener at en instruks er i strid med personvernlovgivningen, skal Grantify informere Kunden om dette, med mindre lov forbyr slik informasjon.

## 10. Grantifys forpliktelser

Grantify skal:

a. behandle personopplysninger kun i samsvar med denne avtalen og Kundens dokumenterte instrukser,
b. sørge for at personer med tilgang til personopplysninger er underlagt taushetsplikt eller annen egnet konfidensialitetsforpliktelse,
c. gjennomføre egnede tekniske og organisatoriske sikkerhetstiltak,
d. bistå Kunden med å oppfylle plikter etter personvernlovgivningen, innenfor det som er rimelig og relevant for tjenesten,
e. bistå Kunden ved forespørsler fra registrerte,
f. varsle Kunden ved brudd på personopplysningssikkerheten,
g. føre nødvendig dokumentasjon for å kunne vise etterlevelse av denne avtalen, og
h. slette eller tilbakelevere personopplysninger ved opphør i samsvar med punkt 17.

## 11. Konfidensialitet

Grantify skal sikre at personer som får tilgang til Kundens personopplysninger, bare behandler opplysningene når det er nødvendig for å levere tjenesten, yte support, utføre drift, håndtere sikkerhet eller oppfylle avtalte forpliktelser.

Personer med tilgang til personopplysninger skal være underlagt konfidensialitetsforpliktelser.

Konfidensialitetsplikten gjelder også etter at avtaleforholdet er avsluttet.

## 12. Informasjonssikkerhet

Grantify skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet ut fra risikoen ved behandlingen.

Tiltakene kan blant annet omfatte:

a. tilgangsstyring og rollebaserte tilganger,
b. autentisering og kontroll med brukeradgang,
c. logging av relevante hendelser,
d. sikkerhetskopiering,
e. tiltak for konfidensialitet, integritet, tilgjengelighet og robusthet,
f. rutiner for håndtering av sikkerhetshendelser,
g. begrensning av tilgang til personopplysninger til personer med tjenstlig behov,
h. testing, vurdering og evaluering av sikkerhetstiltak, og
i. bruk av underleverandører med egnede sikkerhetstiltak.

Følgende underleverandører benyttes i leveransen:

- **Auth0 by Okta** (Okta, Inc.) – Benyttes som leverandør av identitets- og tilgangsstyring (Identity and Access Management – IAM), herunder autentisering og Single Sign-On (SSO). For brukere som ikke benytter SSO, behandler Auth0 nødvendige personopplysninger for autentisering, herunder brukeridentitet, innloggingsopplysninger og kryptografisk sikring av passord. Auth0 håndterer autentiseringsprosessen og verifisering av brukerens identitet på vegne av behandlingsansvarlig, og sender systemgenererte e-poster knyttet til kontoadministrasjon (e-postverifisering og tilbakestilling av passord). Tjenesten kjøres i Auth0s EU-region.
- **Microsoft Azure** (Microsoft Ireland Operations Limited) – Benyttes som skyplattform for drift, hosting, lagring, databaser, nettverk og øvrige infrastrukturtjenester som er nødvendige for levering av tjenesten, herunder sikker lagring av krypteringsnøkler og applikasjonshemmeligheter. All lagring i disse infrastrukturtjenestene skjer i Azure-regionen Sweden Central (Sverige, EØS).
- **Grafana Cloud** (Grafana Labs) – Benyttes til overvåking, logging, visualisering og analyse av applikasjonens ytelse, tilgjengelighet og driftsdata, herunder feilsøking og hendelseshåndtering. Applikasjonslogger, spor og metrikker overføres til og lagres i Grafana Cloud i EU-region (Sverige). Innholdsdata (som timeføringer, lønnsopplysninger og chat-innhold) logges ikke, men loggene kan inneholde opplysninger som identifiserer brukeren, herunder e-postadresse, bruker-ID og IP-adresse.
- **Azure Communication Services** (Microsoft) – Benyttes til utsendelse av e-post fra tjenesten (varsler og onboarding-e-poster) samt tilhørende leveringsstatus og logger der dette er nødvendig for tjenestens funksjonalitet. Tjenesten er konfigurert med datalokasjon «Europe».
- **Microsoft Azure OpenAI Service via Azure AI Foundry** (Microsoft) – Benyttes til AI-basert brukerstøtte (chat-assistent) og til assistert tolkning av opplastede timelister ved import (gjenkjenning av kolonner og aktiviteter). Meldinger og filutdrag behandles av språkmodeller driftet av Microsoft i Microsofts egne datasentre innenfor EU-datasonen; ingen data overføres til OpenAI LLC eller andre tredjeparter. Chat-meldinger screenes i tillegg av Azure AI Content Safety. Dersom personopplysninger inngår i forespørsler til AI-tjenestene, behandles disse utelukkende for å levere den aktuelle funksjonaliteten og benyttes ikke til trening av modeller, i samsvar med Microsofts produktvilkår for Azure OpenAI Service.

I tillegg benyttes **Google Workspace** (Google Ireland Limited) til håndtering av supporthenvendelser sendt til Grantifys supportadresse. Fakturering av kundeforholdet skjer gjennom Folio (Folio AS, Norge); dette er behandling Grantify utfører som behandlingsansvarlig for eget formål, og den er derfor nærmere beskrevet i Grantifys personvernerklæring og ikke i denne avtalen.

Ved pålogging med ekstern identitetsleverandør (Google eller Microsoft) opptrer identitetsleverandøren som selvstendig behandlingsansvarlig for sin egen behandling, og er derfor ikke underdatabehandler etter denne avtalen. Tjenestens oppslag mot offentlige registre (Brønnøysundregistrene og Kartverket) innebærer ikke behandling av personopplysninger på vegne av Kunden.

En fullstendig oversikt over underdatabehandlere med behandlingssted og overføringsgrunnlag fremgår av **Vedlegg 2**. Konkrete tekniske og organisatoriske sikkerhetstiltak er beskrevet i **Vedlegg 3**.

Kunden er ansvarlig for sikkerhetstiltak på egen side, herunder sikker bruk av tjenesten, tilgangsstyring, interne rutiner, opplæring av brukere og sikring av egne enheter og innloggingsopplysninger.

## 13. Bruk av underdatabehandlere

Kunden gir Grantify generell tillatelse til å bruke underdatabehandlere for å levere, drifte, sikre, supportere og videreutvikle tjenesten.

Grantify skal sørge for at underdatabehandlere pålegges tilsvarende personvernforpliktelser som følger av denne databehandleravtalen, i den grad underdatabehandleren behandler personopplysninger på vegne av Kunden.

Grantify er ansvarlig overfor Kunden for at underdatabehandlere oppfyller sine forpliktelser knyttet til behandlingen.

Grantify skal føre en oversikt over underdatabehandlere som benyttes.

Oversikten over underdatabehandlere ved avtaleinngåelse fremgår av **Vedlegg 2**, med angivelse av navn, formål, type behandling, behandlingssted og eventuell overføring utenfor EØS for hver underdatabehandler.

## 14. Endringer i underdatabehandlere

Grantify kan gjøre endringer i bruk av underdatabehandlere.

Grantify skal varsle Kunden om vesentlige endringer i underdatabehandlere, for eksempel ved tillegg eller utskifting av underdatabehandlere som behandler Kundens personopplysninger.

Varsel om vesentlige endringer gis via e-post til Kundens selskapsadministrator(-er) i løsningen.

Kunden kan protestere mot endringen dersom Kunden har saklig grunn knyttet til personvernrisiko. Protest må fremsettes skriftlig innen 14 dager etter at varsel er gitt. Dersom Partene ikke finner en rimelig løsning, kan Kunden si opp avtalen med virkning for fremtidig bruk av tjenesten.

Generelle endringer som ikke vesentlig påvirker behandlingen eller risikoen for Kundens personopplysninger kan varsles gjennom oppdatert oversikt i løsningen, hjelpesenter eller på nettside.

## 15. Overføring utenfor EØS

Grantify skal ikke overføre personopplysninger til land utenfor EØS uten at det foreligger gyldig overføringsgrunnlag etter personvernlovgivningen.

Dersom personopplysninger overføres til land utenfor EØS, skal Grantify sikre at overføringen skjer på gyldig grunnlag, for eksempel ved bruk av EUs standard personvernbestemmelser, beslutning om tilstrekkelig beskyttelsesnivå eller annet lovlig overføringsgrunnlag.

Grantify skal informere Kunden om relevante overføringer utenfor EØS gjennom oversikt over underdatabehandlere eller på annen egnet måte.

All lagring og ordinær behandling av personopplysninger i tjenesten skjer innenfor EØS: applikasjon og database driftes i Microsoft Azure-regionen Sweden Central (Sverige), e-postutsendelse er konfigurert med datalokasjon «Europe», autentiseringstjenesten kjøres i Auth0s EU-region, AI-behandlingen skjer innenfor EU-datasonen i Azure, og telemetri lagres i Grafana Cloud i EU-region (Sverige).

Enkelte underdatabehandlere er amerikanske selskaper eller inngår i konsern med morselskap i USA (Okta, Inc., Raintank, Inc. (Grafana Labs), Google og Microsoft), og fjerntilgang fra tredjeland kan unntaksvis forekomme, for eksempel i forbindelse med support. For supporthenvendelser som sendes på e-post og håndteres i Google Workspace, kan lagring utenfor EØS også forekomme. Slik tilgang og lagring er regulert gjennom EUs standard personvernbestemmelser (SCC) og, der leverandøren er sertifisert, EU-US Data Privacy Framework. For Microsoft-tjenestene gjelder i tillegg Microsofts EU Data Boundary. Se Vedlegg 2 for oversikt per underdatabehandler.

## 16. Bistand til Kunden

Grantify skal, så langt det er mulig og rimelig ut fra behandlingens art, bistå Kunden med å oppfylle Kundens plikter etter personvernlovgivningen.

Dette kan blant annet gjelde bistand knyttet til:

a. innsyn, retting, sletting og begrensning av behandling,
b. dataportabilitet der dette er relevant,
c. protester fra registrerte,

d. informasjonssikkerhet,
e. vurdering av personvernkonsekvenser dersom relevant,
f. forhåndsdrøftelser med tilsynsmyndighet dersom relevant, og
g. dokumentasjon av behandlingen.

Grantify kan kreve rimelig vederlag for bistand som går utover ordinær support eller som skyldes forhold på Kundens side, med mindre bistanden er nødvendig som følge av Grantifys mislighold.

## 17. Innsyn, eksport, tilbakelevering og sletting

Kunden kan i avtaleperioden eksportere dokumentasjon og data fra tjenesten gjennom tilgjengelig eksportfunksjonalitet.

Ved opphør av kundeforholdet skal Kunden som hovedregel selv eksportere nødvendig dokumentasjon før tilgangsperioden utløper.

Ved opphør skal Grantify, etter Kundens valg, slette eller tilbakelevere alle personopplysninger som behandles på vegne av Kunden, og slette eksisterende kopier, med mindre videre lagring er pålagt ved lov. Uten særskilt instruks fra Kunden slettes eller anonymiseres Kundens data etter utløpet av tilgangsperioden i samsvar med punkt 8, med mindre Kunden har kjøpt nytt årsabonnement, bedt om reaktivering, eller det foreligger annet lovlig grunnlag for videre lagring.

På Kundens skriftlige anmodning kan Grantify bistå med eksport, tilbakelevering eller sletting i den grad dette er teknisk mulig og rimelig. Slik bistand kan faktureres etter særskilt avtale dersom den går utover standard funksjonalitet.

Sletting fra sikkerhetskopier kan skje i tråd med Grantifys ordinære rutiner for sikkerhetskopiering og rotasjon, forutsatt at sikkerhetskopier er sikret mot uautorisert tilgang og ikke brukes til andre formål enn gjenoppretting, sikkerhet og driftskontinuitet.

## 18. Brudd på personopplysningssikkerheten

Grantify skal varsle Kunden uten ugrunnet opphold dersom Grantify blir kjent med et brudd på personopplysningssikkerheten som gjelder Kundens personopplysninger.

Varslet skal, så langt informasjonen er tilgjengelig, beskrive:

a. hva som har skjedd,
b. hvilke kategorier personopplysninger og registrerte som kan være berørt,
c. sannsynlige konsekvenser,
d. tiltak Grantify har iverksatt eller foreslår å iverksette, og
e. kontaktpunkt for videre oppfølging.

Kunden er ansvarlig for å vurdere om bruddet skal meldes til Datatilsynet eller de registrerte, med mindre annet følger av lov. Grantify skal bistå Kunden med nødvendig informasjon som er tilgjengelig for Grantify.

## 19. Revisjon og dokumentasjon

Grantify skal gjøre tilgjengelig nødvendig informasjon for å vise etterlevelse av denne databehandleravtalen og personvernlovgivningen.

Kunden kan be om dokumentasjon på Grantifys relevante sikkerhetstiltak, rutiner og bruk av underdatabehandlere.

Revisjon eller kontroll skal gjennomføres med rimelig varsel, på en måte som ikke unødig forstyrrer Grantifys drift, sikkerhet eller andre kunders konfidensialitet.

Grantify kan i første omgang oppfylle revisjonsforpliktelsen ved å fremlegge relevant dokumentasjon, sikkerhetsbeskrivelser, tredjepartsrapporter, egenerklæringer eller annen egnet dokumentasjon. Dersom slik dokumentasjon ikke er tilstrekkelig til å vise etterlevelse, kan Kunden eller en uavhengig revisor på Kundens vegne gjennomføre nærmere kontroll, herunder inspeksjon, i samsvar med vilkårene i dette punktet.

Kunden dekker egne kostnader ved revisjon. Grantify kan kreve rimelig vederlag for bistand ved revisjon som går

utover ordinær dokumentasjonsfremleggelse, med mindre revisjonen avdekker vesentlig mislighold fra Grantifys side.

## 20. Varsler og kontaktpunkter

Varsler etter denne databehandleravtalen kan sendes til Kundens registrerte selskapsadministrator(-er) i løsningen.

Kunden er ansvarlig for at kontaktopplysninger til enhver tid er korrekte og oppdaterte.

Grantifys kontaktpunkt for personvernrelaterte henvendelser er:

**support@grantify.no**

## 21. Bruk av anonymiserte og aggregerte data

Grantify kan bruke anonymiserte og aggregerte data til statistikk, analyse, produktforbedring, sikkerhet, benchmarking og videreutvikling av tjenesten.

Slike data skal ikke kunne identifisere Kunden, enkeltpersoner, konkrete prosjekter eller Kundens forretningshemmeligheter.

Anonymiserte data regnes ikke som personopplysninger dersom anonymiseringen er reell og opplysningene ikke lenger kan knyttes til en identifisert eller identifiserbar fysisk person.

## 22. Lovpålagt behandling

Dersom Grantify etter lov eller pålegg fra offentlig myndighet er forpliktet til å behandle eller utlevere personopplysninger, skal Grantify informere Kunden om dette før behandlingen eller utleveringen skjer, med mindre slik informasjon er forbudt ved lov.

## 23. Ansvar

Partenes ansvar for brudd på denne databehandleravtalen reguleres av kundeavtalen, med mindre ufravikelig personvernlovgivning bestemmer noe annet.

Grantify er ikke ansvarlig for behandling som skjer som følge av Kundens instrukser, Kundens registrering av opplysninger, Kundens tilgangsstyring, Kundens brukere eller Kundens manglende eksport, sletting eller internkontroll, med mindre Grantify har opptrådt i strid med denne databehandleravtalen eller personvernlovgivningen.

## 24. Varighet og opphør

Databehandleravtalen gjelder så lenge Grantify behandler personopplysninger på vegne av Kunden.

Ved opphør av kundeavtalen skal personopplysninger slettes, anonymiseres eller tilbakeleveres i samsvar med denne avtalen, kundeavtalen og Kundens dokumenterte instrukser.

Bestemmelser om konfidensialitet, sikkerhet, sletting, ansvar og revisjon gjelder også etter opphør så langt de etter sin art fortsatt er relevante.

## 25. Lovvalg og tvister

Databehandleravtalen er underlagt norsk rett.

Tvister skal søkes løst gjennom dialog og forhandlinger. Dersom Partene ikke kommer til enighet, kan saken bringes inn for de ordinære domstolene.

Avtalt verneting er **Oslo tingrett**.

---

# Vedlegg 1 – Behandlingsoversikt

## 1. Formål

Levering av Grantify som SaaS-løsning for prosjektregnskap, dokumentasjon og rapportering av SkatteFUNN-prosjekter.

## 2. Behandlingsaktiviteter

Behandlingen kan omfatte:

a. brukeradministrasjon,
b. tilgangsstyring,
c. registrering av prosjektdeltakere og roller,
d. timeføring, signering og godkjenning,
e. registrering av lønnsdata, kostnader, offentlig støtte og salgsinntekter,
f. rapportering og eksport,
g. support og AI-basert veiledning,
h. logging og sikkerhetsovervåking,
i. sikkerhetskopiering, og
j. sletting og anonymisering.

## 3. Typer personopplysninger

Se punkt 6 i databehandleravtalen.

## 4. Kategorier av registrerte

Se punkt 7 i databehandleravtalen.

## 5. Behandlingssted

Personopplysninger i tjenesten lagres og behandles innenfor EØS. Applikasjon og database driftes i Microsoft Azure, region Sweden Central (Sverige). Autentisering skjer i Auth0s EU-region, AI-behandling innenfor EU-datasonen i Azure, og telemetri lagres i Grafana Cloud i EU-region (Sverige). Eventuell tilgang fra land utenfor EØS er beskrevet i punkt 15 i databehandleravtalen og i Vedlegg 2.

## 6. Lagringstid

Personopplysninger behandles i avtaleperioden og slettes eller anonymiseres senest 12 måneder etter utløpet av tilgangsperioden, med mindre annet følger av avtalen, lovpålagt plikt, tvist, reaktivering eller Kundens dokumenterte instruks.

Chatlogger fra AI-supporten lagres så lenge det er nødvendig for formålene beskrevet i denne avtalen. Med mindre annet er nødvendig for å håndtere en konkret supportsak, sikkerhetshendelse, kvalitetsavvik, tvist eller lovpålagt plikt, slettes eller anonymiseres chatlogger senest 12 måneder etter at samtalen fant sted.

---

# Vedlegg 2 – Underdatabehandlere

Følgende underdatabehandlere benyttes ved avtaleinngåelse. Grantify vedlikeholder oversikten og varsler endringer i samsvar med punkt 14 i databehandleravtalen.

| Leverandør | Formål | Type behandling | Behandlingssted | Overføring utenfor EØS | Overføringsgrunnlag |
|---|---|---|---|---|---|
| Microsoft Ireland Operations Limited | Drift, hosting, database og lagring | Lagring og behandling av alle opplysninger | Sverige (Sweden Central) | Unntaksvis (fjerntilgang ved support/drift) | Microsofts EU Data Boundary; SCC / EU-US |

| Leverandør | Formål | Type behandling | Behandlingssted | Overføring utenfor EØS | Overføringsgrunnlag |
|---|---|---|---|---|---|
| (Microsoft Azure) | | registrert i tjenesten, sikkerhetskopiering, nøkkel- og hemmelighetshåndtering | | | Data Privacy Framework |
| Okta, Inc. (Auth0) | Autentisering og tilgangsstyring | Brukeridentitet, e-postadresse, passordhash, innloggingsmetadata (tidspunkt, IP-adresse, enhet), utsendelse av kontoadministrasjons-e-post | EU (Auth0 EU-region) | Unntaksvis (fjerntilgang ved support/drift) | SCC / EU-US Data Privacy Framework |
| Microsoft (Azure Communication Services) | Utsendelse av varsler og systemmeldinger på e-post | Navn, e-postadresse, e-postinnhold, leveringsstatus | EU (datalokasjon «Europe») | Unntaksvis (fjerntilgang ved support/drift) | Microsofts EU Data Boundary; SCC / EU-US Data Privacy Framework |
| Google Ireland Limited (Google Workspace) | Håndtering av supporthenvendelser på e-post | Avsenders navn og e-postadresse samt innholdet i henvendelser til Grantifys supportadresse | EU/EØS primært | Kan forekomme i Googles globale infrastruktur | SCC / EU-US Data Privacy Framework |
| Microsoft (Azure OpenAI Service / Azure AI Foundry, inkl. Azure AI Content Safety) | AI-basert brukerstøtte og veiledning samt tolkning av opplastede timelister ved import | Spørsmål, kontekst og eventuelle personopplysninger brukeren oppgir i chat, samt kolonneoverskrifter, eksempelrader og aktivitetstekster fra opplastede timelister (kan inneholde navn/e-postadresser); brukes ikke til modelltrening | EU (EU-datasone) | Unntaksvis (fjerntilgang ved support/drift) | Microsofts EU Data Boundary; SCC / EU-US Data Privacy Framework |
| Raintank, Inc. dba Grafana Labs (Grafana Cloud) | Overvåking, logging, sikkerhet og feilhåndtering | Tekniske logger, spor og metrikker, herunder e-postadresse, bruker-ID, IP-adresse og tidspunkter | EU (Sverige) | Unntaksvis (fjerntilgang ved support/drift) | SCC / EU-US Data Privacy Framework |

Fakturering av kundeforholdet (Folio AS, Norge) er behandling Grantify utfører som behandlingsansvarlig for eget formål, og er derfor ikke oppført som underdatabehandling. Se Grantifys personvernerklæring.

---

# Vedlegg 3 – Tekniske og organisatoriske sikkerhetstiltak

## 1. Tilgangsstyring

Grantify benytter rollebaserte tilganger for å begrense tilgang til personopplysninger etter brukerens rolle og behov.

## 2. Autentisering

Autentisering håndteres av Auth0 (Okta) med OpenID Connect. Brukere kan logge inn med e-post og passord eller via Single Sign-On med Google eller Microsoft Entra ID (arbeidskonto).

For kontoer med e-post og passord gjelder:

a. passordpolicy med krav til minimum 8 tegn og kompleksitet,
b. passord lagres aldri hos Grantify, kun som kryptografisk hash hos Auth0,
c. innebygget beskyttelse mot brute force-angrep, med automatisk sperring ved gjentatte mislykkede innloggingsforsøk, og
d. e-postadressen verifiseres før kontoen gis tilgang til kundedata.

Sesjoner håndteres med sikre, krypterte informasjonskapsler. Tilgang i løsningen styres deretter gjennom rollebaserte tilganger per selskap, jf. punkt 1 i dette vedlegget.

## 3. Logging

Grantify logger relevante tekniske hendelser for sikkerhet, feilsøking og misbruksforebygging.

Det lagres strukturerte applikasjonslogger, feilmeldinger, ytelsesdata (metrikker) og sporingsdata for forespørsler. Innholdsdata (timeføringer, lønnsopplysninger, chat-innhold og lignende) logges ikke. Loggene kan inneholde opplysninger som identifiserer brukeren, herunder e-postadresse, bruker-ID, tidspunkt og IP-adresse, slik at hendelser kan feilsøkes og etterforskes. Innloggingshendelser logges i tillegg hos Auth0.

Telemetri lagres i Grafana Cloud i EU-region (Sverige) og slettes automatisk etter en fast tidsperiode. På gjeldende abonnement slettes logger, sporingsdata og metrikker etter 14 dager; lagringstiden vil ikke overstige 30 dager for logger og sporingsdata og 13 måneder for metrikker. Tilgang til logger er begrenset til Grantify-personell med tjenstlig behov, via personlige, autentiserte kontoer.

## 4. Sikkerhetskopiering

Grantify benytter sikkerhetskopiering for å kunne gjenopprette tjenesten ved feil, driftsavvik eller sikkerhetshendelser.

Databasen sikkerhetskopieres automatisk og kontinuerlig (Azure Database for PostgreSQL), med mulighet for gjenoppretting til et vilkårlig tidspunkt innenfor oppbevaringsperioden («point-in-time restore»). Sikkerhetskopier oppbevares i 30 dager, lagres kryptert i samme region som databasen (Sverige, EØS) og repliseres ikke ut av EØS. Sikkerhetskopiene benyttes kun til gjenoppretting, sikkerhet og driftskontinuitet.

## 5. Kryptering

a. All trafikk mellom brukere og tjenesten krypteres med TLS (HTTPS).
b. Data lagres kryptert i hvile i Microsoft Azure, både i databasen, i tilhørende lagringstjenester og i sikkerhetskopier.
c. Databasen er kun tilgjengelig via et privat virtuelt nettverk og er ikke eksponert mot internett.
d. Applikasjonens krypteringsnøkler beskyttes med egen nøkkel i Azure Key Vault, hvor også øvrige hemmeligheter (tilgangsnøkler, sertifikater og systempassord) oppbevares.
e. Brukerpassord lagres aldri av Grantify; de lagres kun som kryptografisk hash hos Auth0.

## 6. Driftsmiljø og separasjon

Grantify er en flerkundeløsning der kundenes data er logisk adskilt i to uavhengige lag:

a. Applikasjonslaget avgrenser alle oppslag og endringer til den aktuelle kundens data, basert på innlogget brukers tilganger.
b. Radnivåsikkerhet (Row-Level Security) håndheves i tillegg i selve databasen: databasebrukeren som betjener kundetrafikk, kan teknisk sett ikke lese eller endre andre kunders rader, selv ved feil i applikasjonen, og har ikke rettigheter til å omgå denne sperren. En separat, avgrenset administrasjonstilgang uten denne begrensningen benyttes kun til Grantifys egne drifts- og administrasjonsoppgaver, ikke til ordinær kundetrafikk.

Automatiserte tester verifiserer at alle tabeller med kundedata har radnivåsikkerhet aktivert, og endringer stoppes før produksjonssetting dersom en ny tabell mangler slik sikring.

Produksjonsmiljøet driftes adskilt fra test- og utviklingsmiljøer.

## 7. Hendelseshåndtering

Grantify skal ha rutiner for å identifisere, vurdere, håndtere og varsle relevante sikkerhetshendelser.

## 8. Leverandøroppfølging

Grantify skal benytte underdatabehandlere som gir tilstrekkelige garantier for informasjonssikkerhet og personvern.