DATABEHANDLERAVTALE

Bilag til REVIA AS' Standardvilkår

Versjon 1.1 – 01.09.2026.

mellom

Behandlingsansvarlig	Kunden, slik denne er identifisert ved registrering eller bestilling av Tjenesten («Behandlingsansvarlig» eller «Kunden»)
Databehandler	REVIA AS, org.nr. 834 199 262 Tordenskjolds gate 9, 4612 Kristiansand («Databehandler» eller «REVIA»)

Behandlingsansvarlig og Databehandler omtales hver for seg som «Part» og sammen som «Partene».

1. Bakgrunn og formål

1.1 Denne databehandleravtalen («Avtalen») regulerer Databehandlers behandling av personopplysninger på vegne av Behandlingsansvarlig i forbindelse med Behandlingsansvarliges bruk av tjenesten REVIA («Tjenesten») etter REVIA AS' til enhver tid gjeldende standardvilkår («Vilkårene»).

1.2 Avtalen er inngått for å oppfylle kravene i personvernforordningen (EU) 2016/679 («GDPR») artikkel 28 nr. 3, jf. personopplysningsloven.

1.3 Avtalen er et bilag til Vilkårene og utgjør en del av avtaleforholdet mellom Partene. Ved motstrid mellom Avtalen og Vilkårene går Avtalen foran for så vidt gjelder behandling av personopplysninger.

1.4 Avtalen aksepteres ved registrering eller bestilling av Tjenesten, alternativt ved Partenes signering. Behandlingsansvarlig kan når som helst be om et signert eksemplar.

2. Definisjoner

2.1 Begrepene «personopplysninger», «behandling», «behandlingsansvarlig», «databehandler», «registrert», «brudd på personopplysningssikkerheten» og «tilsynsmyndighet» har samme betydning som i GDPR artikkel 4.

2.2 **«Kundedata»** betyr, som i Vilkårene, digitale data, tekst, bilder, dokumenter og annet innhold som Behandlingsansvarlig eller dennes brukere laster opp til, henter inn i eller genererer i Tjenesten, inkludert personopplysninger som inngår i slikt innhold.

2.3 **«Underdatabehandler»** betyr enhver tredjepart som Databehandler engasjerer til å behandle personopplysninger i Kundedata på vegne av Behandlingsansvarlig.

3. Roller og virkeområde

3.1 Behandlingsansvarlig er behandlingsansvarlig for personopplysninger som inngår i Kundedata. Databehandler behandler slike personopplysninger utelukkende på vegne av og etter instruks fra Behandlingsansvarlig.

3.2 Avtalen omfatter ikke personopplysninger som Databehandler behandler som selvstendig behandlingsansvarlig. Dette gjelder opplysninger om Behandlingsansvarliges brukere som er nødvendige for å opprette og administrere brukerkontoer, lisenser, fakturering, kundeoppfølging, support og sikkerhet i Tjenesten. Slik behandling er regulert i Databehandlers personvernerklæring.

3.3 Behandlingens art og formål, varighet, kategorier av registrerte og typer personopplysninger er beskrevet i Vedlegg 1.

4. Instrukser

4.1 Databehandler skal behandle personopplysninger bare etter dokumenterte instrukser fra Behandlingsansvarlig, med mindre annet følger av lov som Databehandler er underlagt. I så fall skal Databehandler informere Behandlingsansvarlig om det rettslige kravet før behandlingen, med mindre loven forbyr slik informasjon.

4.2 Vilkårene, denne Avtalen og Behandlingsansvarliges bruk av Tjenestens funksjoner (opplasting, import fra egne kildesystemer, analyse, søk, deling med prosjektdeltakere, eksport og sletting) utgjør Behandlingsansvarliges fullstendige instrukser ved Avtalens inngåelse.

4.3 Ytterligere instrukser skal gis skriftlig. Databehandler kan kreve dekning av dokumenterte merkostnader for instrukser som går ut over Tjenestens funksjonalitet.

4.4 Databehandler skal umiddelbart informere Behandlingsansvarlig dersom en instruks etter Databehandlers syn er i strid med GDPR eller annen personvernlovgivning.

4.5 Databehandler skal ikke bruke personopplysninger i Kundedata til egne formål. Databehandler kan likevel utarbeide anonymisert og aggregert statistikk om bruk, kvalitet og ytelse av Tjenesten, forutsatt at statistikken ikke kan knyttes til enkeltpersoner eller til Behandlingsansvarlig, og ikke gjengir innhold fra Kundedata.

4.6 Personopplysninger i Kundedata brukes ikke til å trene eller forbedre AI-modeller, verken hos Databehandler eller hos Underdatabehandlere.

5. Taushetsplikt

5.1 Databehandler skal sikre at personer som er autorisert til å behandle personopplysningene, har forpliktet seg til å behandle dem fortrolig eller er underlagt lovbestemt taushetsplikt. Taushetsplikten gjelder også etter at Avtalen er opphørt.

5.2 Tilgang til Kundedata hos Databehandler er begrenset til personell som trenger tilgang for å levere, drifte, sikre, feilrette eller yte support på Tjenesten.

6. Informasjonssikkerhet

6.1 Databehandler skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen, jf. GDPR artikkel 32. Tiltakene ved Avtalens inngåelse er beskrevet i Vedlegg 2.

6.2 Databehandler kan oppdatere og forbedre tiltakene, forutsatt at det samlede sikkerhetsnivået ikke reduseres. Oppdatert beskrivelse gjøres tilgjengelig på forespørsel.

7. Underdatabehandlere

7.1 Behandlingsansvarlig gir Databehandler en generell forhåndsgodkjenning til å benytte Underdatabehandlere. Underdatabehandlere som er godkjent ved Avtalens inngåelse, fremgår av Vedlegg 3.

7.2 Databehandler skal varsle Behandlingsansvarlig skriftlig, til registrert kontaktperson eller lisensansvarlig, minst 30 dager før en ny Underdatabehandler tas i bruk eller en eksisterende byttes ut. Behandlingsansvarlig kan innen fristen fremsette begrunnet innsigelse. Finner Partene ikke en løsning, kan Behandlingsansvarlig si opp den berørte delen av Tjenesten med virkning fra endringen. Forhåndsbetalt vederlag for gjenværende periode refunderes forholdsmessig.

7.3 Databehandler skal gjennom skriftlig avtale pålegge Underdatabehandlere personvernforpliktelser som gir minst samme beskyttelse som denne Avtalen, og er fullt ansvarlig overfor Behandlingsansvarlig for Underdatabehandlernes oppfyllelse.

8. Overføring til land utenfor EU/EØS

8.1 Lagring og ordinær behandling av personopplysninger i Kundedata skjer innenfor EU/EØS. Dette omfatter lagring, tekstgjenkjenning, indeksering, AI-analyse og sikkerhetskopiering. Unntak er begrenset til det som følger av punkt 8.2.

8.2 Overføring til eller tilgang fra land utenfor EU/EØS skal bare skje etter Behandlingsansvarliges dokumenterte instruks, eller der en Underdatabehandler etter Vedlegg 3 unntaksvis kan få tilgang fra tredjeland i forbindelse med support eller drift. Slik overføring forutsetter et gyldig overføringsgrunnlag etter GDPR kapittel V, herunder adekvansbeslutning (som EU-US Data Privacy Framework) eller EU-kommisjonens standardkontraktsklausuler, samt nødvendige tilleggstiltak.

9. Bistand til Behandlingsansvarlig

9.1 Databehandler skal, tatt i betraktning behandlingens art, bistå Behandlingsansvarlig med egnede tekniske og organisatoriske tiltak slik at Behandlingsansvarlig kan oppfylle sin plikt til å svare på anmodninger fra registrerte etter GDPR kapittel III.

9.2 Anmodninger fra registrerte som Databehandler mottar direkte, videresendes til Behandlingsansvarlig uten ugrunnet opphold. Databehandler svarer ikke selv med mindre Behandlingsansvarlig instruerer det.

9.3 Tjenesten gir Behandlingsansvarlig mulighet til selv å søke i, eksportere, rette og slette Kundedata. Bistand ut over dette kan faktureres etter Databehandlers gjeldende timepriser.

9.4 Databehandler skal bistå Behandlingsansvarlig med å oppfylle forpliktelsene i GDPR artikkel 32 til 36 (sikkerhet, melding av brudd, vurdering av personvernkonsekvenser og forhåndsdrøftinger med tilsynsmyndighet), tatt i betraktning behandlingens art og den informasjonen Databehandler har tilgang til.

10. Brudd på personopplysningssikkerheten

10.1 Databehandler skal varsle Behandlingsansvarlig uten ugrunnet opphold, og normalt innen 24 timer, etter å ha fått kjennskap til et brudd på personopplysningssikkerheten som gjelder Kundedata.

10.2 Varselet skal, så langt det er kjent, beskrive bruddets art, kategorier og omtrentlig antall registrerte og personopplysninger som er berørt, sannsynlige konsekvenser, iverksatte og foreslåtte tiltak, samt kontaktpunkt hos Databehandler. Informasjon kan gis trinnvis etter hvert som den blir tilgjengelig.

10.3 Databehandler skal dokumentere alle brudd og samarbeide med Behandlingsansvarlig om oppfølging. Databehandler skal ikke informere tilsynsmyndighet eller registrerte på Behandlingsansvarliges vegne uten instruks, med mindre loven krever det.

11. Dokumentasjon og revisjon

11.1 Databehandler skal på forespørsel gjøre tilgjengelig all informasjon som er nødvendig for å påvise at forpliktelsene i GDPR artikkel 28 er oppfylt, herunder beskrivelse av sikkerhetstiltak, oversikt over Underdatabehandlere og relevante sertifiseringer eller attestasjoner fra Underdatabehandlere.

11.2 Behandlingsansvarlig, eller en uavhengig revisor utpekt av denne, kan gjennomføre revisjon av Databehandlers behandling med minst 30 dagers skriftlig varsel, i ordinær arbeidstid og maksimalt én gang per tolv måneder, med mindre en tilsynsmyndighet krever det eller et brudd på personopplysningssikkerheten gir saklig grunn. Revisjonen skal gjennomføres slik at den i minst mulig grad forstyrrer Databehandlers drift, og revisor skal være underlagt taushetsplikt. Hver Part dekker egne kostnader.

11.3 Kontroll av Underdatabehandlere skjer gjennom deres tilgjengelige revisjonsrapporter og sertifiseringer (for eksempel ISO 27001 og SOC 2), med mindre annet følger av lov.

12. Sletting og tilbakelevering

12.1 Behandlingsansvarlig kan når som helst slette Kundedata i Tjenesten. Sletting omfatter originalfiler, avledede data (tekstuttrekk, søkeindekser, analyseresultater) og sikkerhetskopier innen sikkerhetskopienes normale rotasjonstid på inntil 7 dager.

12.2 Ved opphør av Vilkårene skal Databehandler, etter Behandlingsansvarliges valg, tilbakelevere Kundedata i et alminnelig anvendt, maskinlesbart format og/eller slette alle personopplysninger i Kundedata. Tilbakelevering skjer gjennom Tjenestens eksport- og nedlastingsfunksjoner eller, på forespørsel, som samlet uttrekk fra Databehandler. Har Behandlingsansvarlig ikke bedt om tilbakelevering innen 60 dager etter opphør, slettes Kundedata.

12.3 Sletting etter punkt 12.2 gjennomføres senest 90 dager etter opphør, med mindre fortsatt lagring er pålagt ved lov. Databehandler bekrefter gjennomført sletting skriftlig på forespørsel.

13. Ansvar

13.1 Partenes ansvar for brudd på denne Avtalen følger Vilkårenes bestemmelser om ansvar og ansvarsbegrensning, med mindre annet følger av ufravikelig lov.

13.2 Overtredelsesgebyr ilagt av tilsynsmyndighet bæres av den Part som er ansvarlig for overtredelsen.

14. Varighet

14.1 Avtalen gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig, og opphører når slettingen etter punkt 12 er gjennomført.

15. Endringer

15.1 Databehandler kan endre Avtalen ved endringer i lov, tilsynspraksis eller Tjenesten. Endringer som ikke er til Behandlingsansvarliges fordel, varsles per e-post med samme frist som gjelder for endring av Vilkårene.

16. Lovvalg og tvister

16.1 Avtalen er underlagt norsk rett. Tvister avgjøres ved Oslo tingrett som avtalt verneting, jf. Vilkårene.

Signatur

Signatur er ikke nødvendig når Avtalen er akseptert i Tjenesten. Feltene under benyttes når en Part ønsker et signert eksemplar.

For Behandlingsansvarlig	**For Databehandler (REVIA AS)**
Sted/dato: _____	Sted/dato: _____
Signatur: _____	Signatur: _____
Navn: _____	Navn: _____
Stilling: _____	Stilling: _____

Vedlegg 1 – Beskrivelse av behandlingen

A. Formål med behandlingen

Å levere Tjenesten REVIA til Behandlingsansvarlig: lagring og organisering av prosjektdokumentasjon, AI-assistert analyse og vurdering av dokumentasjon mot kravene i BREEAM-NOR, chat-basert faglig veiledning, generering av samsvarsnotater, fagrapporter og revisjonsrapporter, søk i egne dokumenter, samarbeid mellom prosjektdeltakere, samt drift, sikkerhet, feilretting og support av Tjenesten.

B. Behandlingens art

Innsamling (opplasting eller import fra Behandlingsansvarliges egne kildesystemer), lagring, tekstgjenkjenning (OCR), strukturering og indeksering for søk (vektorisering), automatisert analyse med språkmodeller, søk og gjenfinning, sammenstilling i rapporter, visning for autoriserte brukere, eksport og sletting.

C. Kategorier av registrerte

- Behandlingsansvarliges ansatte og øvrige brukere av Tjenesten.
- Ansatte og kontaktpersoner hos Behandlingsansvarliges oppdragsgivere, samarbeidspartnere, rådgivere, entreprenører, leverandører og offentlige myndigheter.
- Andre personer som er omtalt i prosjektdokumentasjon, for eksempel i møtereferater, sjekklister, befaringsrapporter, sertifikater og signerte dokumenter.

D. Kategorier av personopplysninger

- Identifikasjons- og kontaktopplysninger: navn, e-postadresse, telefonnummer, stilling, arbeidsgiver.
- Opplysninger i prosjektdokumentasjon: roller, ansvarsfordeling, signaturer, deltakerlister, kommentarer og vurderinger.
- Brukergenerert innhold i Tjenesten: chat-meldinger, notater, vurderinger og rapporter.
- Tekniske logger knyttet til bruk av Tjenesten.

E. Særlige kategorier av personopplysninger

Tjenesten er ikke ment for særlige kategorier av personopplysninger (GDPR artikkel 9) eller opplysninger om straffedommer og lovovertredelser (artikkel 10). Behandlingsansvarlig skal ikke laste opp slike opplysninger, herunder HR-, sykefraværs- eller helseopplysninger, med mindre dette er særskilt avtalt skriftlig med Databehandler. Databehandler foretar ingen særskilt uthenting eller profilering av slike opplysninger.

F. Varighet

Så lenge Vilkårene gjelder, med tillegg av slettefristen i Avtalens punkt 12.

G. Automatiserte avgjørelser

Tjenesten treffer ikke avgjørelser med rettsvirkning eller tilsvarende betydelig virkning for enkeltpersoner. AI-genererte resultater er beslutningsstøtte som skal vurderes av Behandlingsansvarlig.

Vedlegg 2 – Tekniske og organisatoriske sikkerhetstiltak

Tiltakene beskriver hva som er sikret, ikke hvordan det er implementert. Gjeldende tekniske løsninger er beskrevet i Databehandlers sikkerhetsbeskrivelse, se siste rad. Vedlegget oppdateres etter punkt 6.2.

Område	Tiltak
Datalokasjon	All lagring og ordinær behandling av Kundedata skjer innenfor EU/EØS, se Vedlegg 3.
Kryptering	Kundedata er kryptert under overføring og ved lagring etter anerkjente standarder. Nøkler og hemmeligheter forvaltes adskilt fra dataene.
Identifikasjon og autorisasjon	Individuell brukerpålogging. Tilgang til Kundedata er begrenset til autoriserte brukere i det enkelte prosjekt og kontrolleres teknisk ved hver forespørsel. Administrativ tilgang er begrenset til navngitt personell hos Databehandler med individuelle konti. Pålogging via kundens egen identitetsleverandør kan tilbys etter avtale.
Konfidensialitet og isolasjon	Kundedata holdes logisk atskilt per kunde og prosjekt i alle lagrings- og søkekomponenter. Søk og AI-analyse avgrenses til det prosjektet brukeren arbeider i.
AI-behandling	AI- og tekstgjenkjenningstjenester benyttes under leverandørvilkår som utelukker bruk av innholdet til modelltrening og begrenser lagring til det som er nødvendig for å levere tjenesten. Innhold behandles kun for den enkelte forespørselen.
Tilgjengelighet og gjenoppretting	Databasen sikkerhetskopieres daglig innenfor samme region, med 7 dagers oppbevaring. Filer lagres redundant hos lagringsleverandøren. Gjenoppretting utføres med leverandørens verktøy.
Logging	Sikkerhetshendelser, feil og AI-forespørsler logges for sporbarhet og feilsøking, innenfor EU/EØS. Logger som kan inneholde utdrag av Kundedata er underlagt samme tilgangskontroll og slettefrister som Kundedata.
Sletting og dataminimering	Sletting i Tjenesten fjerner originaldata og avledede data (tekstuttrekk, indekser, analyseresultater). Sikkerhetskopier roteres ut innen 7 dager. Ved opphør slettes Kundedata etter Avtalens punkt 12.
Endringshåndtering	Versjonskontroll, kodegjennomgang og automatiserte tester. Utvikling og test skjer i egne miljøer adskilt fra produksjon.
Leverandørstyring og sertifisering	Databehandleravtaler med alle Underdatabehandlere. Infrastruktur- og plattformleverandørene er sertifisert etter ISO 27001 og/eller SOC 2 Type II; dokumentasjon fremlegges på forespørsel.
Organisatoriske tiltak	Taushetserklæringer for alt personell. Prinsipp om minste privilegium. Rutine for avvikshåndtering med varsling etter Avtalens punkt 10. Årlig gjennomgang av tiltakene.
Sårbarhetshåndtering	Programvareavhengigheter oppdateres løpende, og sikkerhetsvarsler fra plattformleverandører følges opp uten ugrunnet opphold.

Område	Tiltak
Dokumentasjon	En utfyllende sikkerhetsbeskrivelse av gjeldende tekniske løsninger fremlegges på forespørsel, jf. punkt 11.1. Den kan oppdateres uten endring av denne Avtalen, forutsatt at sikkerhetsnivået ikke reduseres.

Vedlegg 3 – Godkjente underdatabehandlere

Gjeldende fra 01.09.2026.

Underdatabehandler	Formål	Lokasjon for behandling	Overføringsgrunnlag
Amazon Web Services EMEA SARL (Luxembourg)	AI-inferens via Amazon Bedrock: Anthropic Claude (analyse, chat, rapportgenerering) og Cohere Rerank (rangering av søketreff)	Frankfurt, Tyskland (eu-central-1), EU-regional inferens	Ingen overføring (EU/EØS)
Supabase, Inc. (USA)	Database, filager og autentisering	Irland (AWS eu-west-1)	EU-lagring. Eventuell supportaksess: EU-US Data Privacy Framework / SCC
Vercel, Inc. (USA)	Drift av applikasjonen (hosting og serverkjøring)	Stockholm, Sverige (arn1)	EU-drift. Eventuell supportaksess: EU-US Data Privacy Framework / SCC
Google Cloud EMEA Limited (Irland)	Vektorisering (embeddings) av dokumenttekst for søk via Vertex AI	EU (multi-region)	Ingen overføring (EU/EØS)
Mistral AI SAS (Frankrike)	Tekstgjenkjenning (OCR) av opplastede dokumenter	EU	Ingen overføring (EU/EØS)
Functional Software, Inc. (Sentry, USA)	Feillogging og stabilitetsovervåking	Frankfurt, Tyskland (EU-datasenter)	EU-lagring. Eventuell supportaksess: EU-US Data Privacy Framework / SCC

Integrasjoner Behandlingsansvarlig selv aktiverer. Kildesystemer som Behandlingsansvarlig kobler til Tjenesten (for eksempel Microsoft SharePoint via Microsoft Graph, eller Omega 365) er Behandlingsansvarliges egne leverandører. Databehandler henter data derfra på Behandlingsansvarliges instruks, og slike leverandører er ikke Underdatabehandlere under denne Avtalen.

Databehandlers egne systemer. Systemer for kundeoppfølging, fakturering og regnskap behandler kontakt- og avtaleopplysninger som Databehandler er behandlingsansvarlig for. Disse er beskrevet i personvernerklæringen og omfattes ikke av denne listen.