

Standard Databehandleravtale (Mal)

Utarbeidet i henhold til GDPR artikkel 28 og 30 | Revisjonsdato: 29. oktober 2026 | curiosa.no/trust

1. Avtalens parter, virkeområde og Dual-Edition

Denne databehandleravtalen regulerer behandling av personopplysninger mellom Skoleeier / Kommune / Fylkeskommune (Behandlingsansvarlig) og Chromo AS, org.nr. 937 967 675 (Databehandler) ved bruk av Full skoleutgave (curiosa.no/full) og tilhørende nettleserutvidelse (Curiosa Skoleassistent).

Merknad om Lokal utgave (standard på curiosa.no): I 100 % Lokal og Anonym Elevmodus lagres 0 personopplysninger om elever hos Databehandler (all elevprogresjon lagres lokalt i elevens egen nettleser/Skole-OneDrive og leveres som lokal PDF i Teams). For skoler som kun benytter Lokal utgave for elever, kreves det derfor ingen databehandleravtale for elevdata.

2. Behandlingens art, formål og kategorier (GDPR art. 28 og 30)

Formålet med behandlingen i Full skoleutgave er å levere en digital plattform for lesing av fagtekster, gjennomføring av oppgaver og prøver, lesestøtte samt vurderingsstøtte til faglærere i henhold til opplæringslova § 13-1 / § 25-1.

Kategorier av registrerte: Elever og lærere/undervisningspersonell.

Kategorier av personopplysninger: Fornavn/brukernavn, elev-ID, klasse, skole, e-post (kun for lærere), oppgavebesvarelser, muntlige vurderinger, egne notater og tekniske prøvehendelser (fraværstid ved fokusavbrudd under låst prøve). Det behandles ingen særlige kategorier av personopplysninger (GDPR art. 9) eller fødselsnummer. Komplette RoPA-tabeller etter GDPR art. 30 ligger på curiosa.no/trust.

3. Sikkerhet og tekniske tiltak (GDPR artikkel 32)

Databehandler har iverksatt følgende tekniske og organisatoriske sikkerhetstiltak:

- Tilgangskontroll og skoleisolering: Streng rolle- og attributtbasert tilgangskontroll (RBAC/ABAC) via Firebase Authentication, Feide og autoritative sikkerhetsregler i Firestore og Cloud Storage med låste identitetsfelter (rolle-immutabilitet) og skille mellom enkelt-oppslag (get) og liste-uthenting (list).
- Kryptering og integritet: All data krypteres med AES-256 ved lagring (at rest) og TLS 1.3 med Strict-Transport-Security (HSTS) under overføring. Lokale Prøve-PDF-er signeres med kryptografisk SHA-256-kontrollkode.
- KI-vern og Prompt Injection Guard: Språkmodeller leveres via Google Cloud Vertex AI i EU multi-region under Enterprise DPA uten modelltrening på kundedata. Elevnavn strippest før innsending, og elevtekst renses automatisk for skjulte instruksjoner (Prompt Injection Guard).
- Automatisert sikkerhetsverifisering: 57 automatiserte sikkerhetstester kjøres i CI/CD for å verifisere tilgangskontroll, flerskole-isolasjon og domenesikring.

4. Godkjente underdatabehandlere (EU/EØS)

Databehandler benytter kun følgende underdatabehandlere innenfor EU/EØS:

1. Google Cloud EMEA Limited (europe-west1 Belgia / EU multi-region): Database (Firestore), fillagring (Cloud Storage), serverløse funksjoner (Cloud Functions) og Vertex AI under Google Cloud Data Processing Addendum (DPA).
2. Sikt - Kunnskapssektorens tjenesteleverandør (Norge): Autentiseringstjenester via Feide.

5. Sletting, innsyn, avviksvarsling og revisjon

Innsyn og portabilitet: Plattformen har innebygd selvbetjent eksport (JSON og PDF) for både elev og lærer.

Sletterutiner: Lærere kan slette elever med umiddelbar kaskaderende virkning i alle tabeller. Sanntidsøkter (CuriLive) slettes etter 24 timer, og inaktive elevprofiler slettes automatisk etter 365 dager. Ved opphør av avtalen sletter Databehandler alle personopplysninger tilhørende Behandlingsansvarlig.

Avviksvarsling: Databehandler varsler Behandlingsansvarlig uten ugrunnet opphold og senest innen 72 timer etter at et brudd på personopplysningssikkerheten er oppdaget. Kontakt: kontakt@curiosa.no.