Databehandleravtale (DPA)

Edudata.io (3460068-8) — Cloudpoint Oy (Org.nr (FI) 2325703-6, MVA FI23257036) • Malminkaari 17–19 B, 00700 Helsingfors, Finland • DPO: tietosuoja@cloudpoint.fi

[OFFISIELT PUBLISERT · H-AI-H] Menneskelig verifisert offisiell språkversjon (H-AI-H Human–AI–Human; ved avvik går EN-hovedversjonen foran).
Verification Role: LEGAL_COUNSEL_AND_RELEASE_OWNER | **Verified UTC:** 2026-11-25T08:36:41Z

Dokument-ID	`edudata.dpa.no_nb.v2.0.0-r01`	**Versjon**	**v2.0** (`v2.0.0-r01`)
Gjeldende fra	2026-11-10	**Neste gjennomgang**	2027-11-10
Språk	Norsk Bokmål (nb-NO)	**Sikkerhetssertifisering**	ISO/IEC 27001:2022 (#123522, Prescient Security LLC)
Styringsmodell	**H-AI-H (Human–AI–Human)**	**Språkrolle / Hovedversjon**	Lokalisert oversettelse (fra EN-hovedversjon)
Kanonisk nettadresse	`https://www.edudata.io/no/trust-center#dpa`		
Innholdets SHA-256 (UTF-8 NFC)	`c9b1689fe983b330ae3dfe7cdff3545eb5019463a85bc71fefd975dcb948ec13`		

Den rettslig bindende databehandleravtalen (DPA) som regulerer behandlingen av personopplysninger for Edudata.io-plattformen mellom behandlingsansvarlig og databehandleren.

EDUDATA.IO DATABEHANDLERAVTALE

> Denne lokaliserte versjonen er en AI-assistert oversettelse av den opprinnelige engelske versjonen
> og er kun ment som informasjon og referanse. Ved eventuelle uoverensstemmelser skal den engelske versjonen gjelde.

Versjon 2.0 | Gjeldende fra: 10.11.2026

Denne databehandleravtalen ("DPA", Versjon 2.0) gjelder for EDUDATA-tjenesten ("Tjenesten") levert av Cloudpoint Oy og utgjør en integrert del av hovedavtalen (inkludert brukervilkårene). Ved uoverensstemmelse har denne DPA-en forrang når det gjelder personopplysningsbehandling.

Avtaleparter:

Databehandler: Cloudpoint Oy (2325703-6) / Edudata.io (3460068-8), som er en del av Cloudpoint Oy (2325703-6, MVA-nr. FI23257036), Malminkaari 17-19B, 00700 Helsingfors, Finland (Personvernombud / DPO: Jasse Tenko, tietosuoja@cloudpoint.fi, ISM-leder: Hesham Abboud, kundeservice: info@edudata.io, tlf. +358 9 4257 9280)
Behandlingsansvarlig: Kunden (Kommunen / Utdanningsleverandøren)

1. Definisjoner

- **Behandlingsansvarlig:** Den fysiske eller juridiske personen, offentlige myndigheten, institusjonen eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal brukes (GDPR Art 4(7)).
- **Databehandler (Databehandleren):** Den fysiske eller juridiske personen, offentlige myndigheten, institusjonen eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige (GDPR Art 4(8)).

- **GDPR:** Europaparlaments- og rådsforordning (EU) 2016/679 (generell personvernforordning).
- **Personopplysninger:** Enhver opplysning om en identifisert eller identifiserbar fysisk person (GDPR Art 4(1)).
- **Behandling:** Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke.

Alle andre begreper som ikke er definert i denne DPA-en skal ha samme betydning som i GDPR.

2. Bakgrunn og formål

Den behandlingsansvarlige har valgt tjenesteleverandøren (Cloudpoint Oy) til å opptre som databehandler i samsvar med artikkel 28(3) i forordning (EU) 2016/679 (generell personvernforordning, "GDPR").

Denne DPA-en utgjør en integrert del av Hovedavtalen inngått mellom Partene, der Databehandleren leverer Edudata-tjenesten (primært *Edudata Compliance* og *Edudata Compliance Service* samt, hvis særskilt avtalt, tilleggsmodulene *Edudata Privacy* og *Edudata Security*) til den behandlingsansvarlige, med mindre annet er avtalt i Hovedavtalen.

Databehandleren vil behandle opplysninger knyttet til en identifisert eller identifiserbar fysisk person på vegne av den behandlingsansvarlige. De detaljerte rutinene for behandlingen av personopplysninger er beskrevet i Vedlegg 1 (Versjon 2.0 — 10.11.2026) til denne DPA-en.

Formålet med denne avtalen er å regulere Partenes rettigheter og plikter ved behandling av personopplysninger i samsvar med GDPR og å ivareta de registrertes friheter og rettigheter under behandlingen.

3. Roller og ansvar

Databehandleren skal behandle personopplysninger kun i samsvar med denne DPA-en og dokumenterte instrukser fra den behandlingsansvarlige. Databehandleren forplikter seg til ikke å bruke personopplysningene til andre formål enn det som er avtalt i denne DPA-en og i den behandlingsansvarliges instrukser. Den behandlingsansvarliges instrukser må være i samsvar med gjeldende personvernlovgivning og denne DPA-en.

Dersom Databehandleren oppdager at en instruks fra den behandlingsansvarlige er i strid med gjeldende lovgivning eller er utilstrekkelig, skal Databehandleren straks informere den behandlingsansvarlige om dette.

Den behandlingsansvarlige er ansvarlig for at det foreligger et behandlingsgrunnlag for personopplysningene, for å informere de registrerte om behandlingen av deres personopplysninger, samt for øvrige plikter som påhviler den behandlingsansvarlige etter GDPR.

Den behandlingsansvarlige er ansvarlig for å informere Databehandleren om kontaktinformasjonen til sitt personvernombud (DPO) og utpekte kontaktperson og for å sikre at kontaktinformasjonen holdes oppdatert.

4. Tekniske og organisatoriske sikkerhetstiltak

Databehandleren skal opprettholde egnede tekniske og organisatoriske sikkerhetstiltak (GDPR art. 32 og et ISO/IEC 27001:2022-sertifisert styringssystem for informasjonssikkerhet) for å beskytte mot uautorisert eller ulovlig behandling eller tilgang samt mot utilsiktet tap, ødeleggelse eller skade.

En detaljert beskrivelse av de iverksatte tiltakene fremgår av Vedlegg 2 (Versjon 2.0 — 10.11.2026) til denne DPA-en.

5. Plikt til å bistå og svarfrist for registrertes forespørsler (DSAR SLA)

Databehandleren behandler personopplysninger i samsvar med denne DPA-en, instrukser fra den behandlingsansvarlige og personvernlovgivningen, og bistår den behandlingsansvarlige med å sikre oppfyllelse av forpliktelsene i artikkel 28 og 32–36 i GDPR (inkludert personvernkonsekvensvurderinger [DPIA], forhåndsdrøftinger og de registrertes rettigheter).

Ingen ekstra kostnad for lovpålagt bistand: All standardbistand i henhold til GDPR artikkel 28 og artikkel 32–36 er inkludert i abonnementsavgiften uten ekstra kostnad.

Svarfrist på høyst fem (5) virkedager (DSAR SLA): Databehandleren forplikter seg til uten ugrunnet opphold og **senest innen fem (5) virkedager** å underrette den behandlingsansvarlige om alle mottatte forespørsler fra registrerte (DSAR) samt levere teknisk bistand og dataeksport innen 5 virkedager.

6. Internasjonale overføringer, HubSpot EU1-styring og adskillelse av programvareutvikling

Vi behandler alle produksjonsdata og databaser utelukkende på Google Cloud-servere plassert i Det europeiske økonomiske samarbeidsområdet (EU/EØS, primært `europe-north1` Finland samt EU-multiregion). Det skjer ingen regelmessige overføringer av produksjonsdata utenfor EU/EØS.

HubSpot Ireland Ltd (EU1 Frankfurt-datalagring og forbud mot 5 datakategorier i supportsaker): HubSpot er låst til EU-datasentre (`dataHostingLocation = eu1` , `app-eu1.hubspot.com` , AWS `eu-central-1` Frankfurt, Tyskland med failover i Dublin, Irland), håndhever GDPR Compliance Toolkit (inkludert *GDPR Permanent Delete* innen 90 dager etter avtalens opphør eller på forespørsel) og AI-sperrer (`customer_data_training_enabled = False` , `crm_sensitive_pii_access_enabled = False`), støttet av EU–U.S. Data Privacy Framework (DPF), EUs standardkontraktsbestemmelser (SCC 2021/914) og en Transfer Impact Assessment (TIA). I tillegg forbyr Cloudpoints *Data Management Policy v1.1.0* strengt at fem (5) datakategorier legges inn i HubSpot-supportsaker: (1) elev- og studentdata, (2) særlige kategorier av personopplysninger, (3) detaljer om sikkerhetshendelser, (4) autentiseringslegitimasjon/tokens og (5) sikkerhetslogger.

Teknisk adskillelse av programvareutvikling i Egypt (Aimpulse — GDPR art. 25 & 32): Aimpulse er Cloudpoint Oys dedikerte utviklingsenhet / partnerenhet (Kairo, Egypt), som opererer utelukkende under Cloudpoint Oys operasjonelle kontroll og ISO/IEC 27001:2022-sertifiserte ISMS. Utviklerne i Egypt deltar aktivt i programvareutviklingen i **isolerte ikke-produksjonsmiljøer (`edudata-compliance-staging`) med 100 % syntetiske testdata** (*CP-ISMS-DLP-001 v1.2*) og har **ingen tilgang til operasjonelle kundedata eller personopplysninger i produksjonsmiljøet (`edudata-compliance-prod`)**. Kundesupport og administrasjon av produksjonspersonopplysninger utføres utelukkende i EU/EØS (Finland), og avtaleforholdet er dekket av EUs standardkontraktsbestemmelser (SCC Module 3), TIA og uforanderlige 400-dagers revisjonslogger.

7. Taushetsplikt

Databehandleren og alle fysiske personer som arbeider for Databehandleren skal overholde både konfidensialitet og taushetsplikt under behandlingen. Databehandleren sikrer at alle fysiske personer som arbeider for Databehandleren er bundet av en taushetsavtale.

Databehandleren sikrer at det foreligger en konfidensialitetsavtale (NDA) med underdatabehandlerne samt taushetsavtaler mellom underdatabehandleren og alle fysiske personer som arbeider for underdatabehandleren og deltar i behandlingen. Denne taushetsplikten gjelder også etter at Hovedavtalen og denne databehandleravtalen er opphørt.

8. Rett til revisjon

Den behandlingsansvarlige har rett til i rimelig utstrekning å gjennomføre revisjon av Databehandlerens lokaler og behandlingsaktiviteter for å undersøke beskyttelses- og sikkerhetsnivået som følger av denne DPA-en, og for å vurdere Databehandlerens etterlevelse av bestemmelsene i denne DPA-en. Databehandleren fremlegger på forespørsel sin aktuelle ISO/IEC 27001:2022-revisjonsdokumentasjon (Prescient Security) og revisjonssammendrag.

Hver part bærer sine egne kostnader ved revisjon. Den behandlingsansvarlige skal skriftlig varsle Databehandleren minst 14–30 dager i forveien før revisjonen gjennomføres.

Den behandlingsansvarliges rett til revisjon kan utøves høyst én gang hver tolvte (12) måned, med mindre et spesifikt brudd på personopplysningssikkerheten eller en velbegrunnet bekymring gjør en tidligere revisjon nødvendig.

Der en revisjon kan føre til avsløring av Databehandlerens forretnings- eller bedriftshemmeligheter, eller true Databehandlerens immaterielle rettigheter, skal det benyttes en uavhengig ekspert til å utføre revisjonen, og denne eksperten skal forplikte seg til å være bundet av en taushetsavtale.

9. Underdatabehandlere

Databehandleren har rett til å benytte underdatabehandlere til å behandle personopplysninger i forbindelse med leveringen av Tjenesten. Godkjente underdatabehandlere er oppført i Vedlegg 1.

Databehandleren sikrer at involverte underdatabehandlere opererer under en skriftlig databehandleravtale (GDPR art. 28(4)) med Databehandleren og overholder tilsvarende databeskyttelsesforpliktelser.

Direkte skriftlig forhåndsvarsel (minst 30 kalenderdager): Databehandleren gir den behandlingsansvarliges utpekte kontaktperson direkte skriftlig forhåndsvarsel (via e-post) **minst tretti (30) kalenderdager i forveien** før en underdatabehandler legges til eller byttes ut. Den behandlingsansvarlige har tretti (30) kalenderdager fra varslingen til å protestere skriftlig på saklige personvernrettslige grunner. Dersom det ikke oppnås en løsning innen 30 kalenderdager, har den behandlingsansvarlige rett til å si opp Tjenesten.

10. Brudd på personopplysningssikkerheten (To-trinns 24/7-overvåking og NIS2 art. 23 / GDPR art. 33-modell)

Databehandleren følger en dokumentert hendelsesprosedyre (*CP-ISMS-IR-002 v1.0* samt VPM-38 4-trinns SLA: P1 < 1 t, P2 < 4 t, P3 < 24 t, P4 < 72 t) og varsler den behandlingsansvarlige i to trinn:

- **Trinn 1 — Automatisert 24/7/365-overvåking og tidlig forhåndsvarsel (Early Warning ≤ 24 timer):** Produksjonsinfrastrukturen overvåkes 24/7/365 (inkludert helger og helligdager) av automatiske sikkerhets- og anomalialarmer. Ved oppdaget eller begrunnet mistanke om sikkerhetsbrudd sender Databehandleren et foreløpig **tidlig varsel (Early Warning) senest innen 24 timer** (med oppdagelsestidspunkt, berørt tjeneste, aktive tekniske begrensningstiltak og kontaktpunkter).
- **Trinn 2 — Formell DPO-vurdering og detaljert 8-punktsrapport (neste virkedag / ≤ 72 timer):** Formell rotårsaksanalyse og DPO-konsekvensvurdering (DPO Jasse Tenko / ISM-leder Hesham Abboud, `tietosuoja@cloudpoint.fi`) utføres i arbeidstiden og leveres **neste virkedag** (og alltid innenfor 72-timersfristen i GDPR art. 33), med alle 8 obligatoriske datapunkter: (1) oppdagelsestidspunkt, (2) berørte systemer og data, (3) berørte kategorier og estimert antall registrerte, (4) berørte underdatabehandlere/land, (5) sannsynlige konsekvenser, (6) iverksatte og planlagte tiltak, (7) DPO/ISM-kontaktinformasjon (`tietosuoja@cloudpoint.fi`, tlf. +358 9 4257 9280) og (8) tidspunkt for neste statusrapport.

11. Tilbakelevering og sletting av personopplysninger (30 dager primærdata / 90 dager sikkerhetskopier)

Før avtalens opphør har den behandlingsansvarlige rett til å eksportere alle kommunale data (inkludert metadata, beslutningshistorikk og revisjonslogger). Etter opphør slettes personopplysninger etter følgende frister:

- **Primære produksjonsdata (høyst 30 dager):** Slettes fra produksjonsdatabasene **senest innen tretti (30) dager** etter avtalens opphør.
- **Sikkerhetskopier (høyst 90 dager etter primær sletting):** Krypterte sikkerhetskopier (Cloud SQL `edudata-comp-db` 21d + 7d PITR, `edudata-ai-db` 7d + 7d PITR, Firestore 7–90d og Cloud Storage 7d soft-delete `604800s`) overskrives ugjenkallelig **senest innen nitti (90) dager** etter primær sletting (mens uforanderlige `_Required` 400d / `_Default` 365d sikkerhetslogger uten kundeinnhold utløper automatisk).
- **Skriftlig bekreftelse på sletting på forespørsel:** Gjennom hele slettevinduet er data beskyttet med AES-256 og strengt sperret for bruk. På forespørsel gir Databehandleren en skriftlig bekreftelse på sletting (f.eks. per e-post) når slettingen er gjennomført.

Inaktive brukerkontoer slettes automatisk fra brukerdatabasen når det har gått 366 dager siden siste innlogging.

12. AI-assistert behandling (Vertex AI / Gemini & Document AI) og ansvarsbegrensning

AI-behandlingsgarantier (EU/EØS-låsing og forbud mot modelltrening): Valgfrie AI-assisterte funksjoner utføres utelukkende via **Google Cloud Vertex AI (Gemini Enterprise-modeller)** og **Google Cloud Document AI** innenfor EU/EØS (`europe-north1` Finland og `eu`-multiregion, `edudata-ai-db`, 30d sletting / 7d sikkerhetskopier). Kundedata, instrukser (prompts), inndata eller utdata **brukes aldri til å trene, finjustere eller forbedre generelle eller tverrgående AI-modeller** (*Data Management Policy v1.1.0*). Det skjer ingen automatiserte avgjørelser eller profilering etter GDPR artikkel 22 (kun *Human-in-the-Loop* beslutningsstøtte).

Ansvarsbegrensning: Databehandleren er ikke ansvarlig for indirekte tap eller følgeskader under denne DPA-en. Databehandlerens samlede maksimale ansvar er begrenset til 100 % av betalingene for Tjenesten i løpet av de foregående 12 månedene, med mindre en slik begrensning ville være ulovlig.

13. Gyldighetstid

Denne DPA-en (Versjon 2.0, gjelder fra 10.11.2026) og Edudata.io sine Brukervilkår (Versjon 3.1) inngås og trer i kraft samtidig enten elektronisk via **Cloudpoint Portal (`portal.cloudpoint.fi`)** (ved bruk av sterk elektronisk identifikasjon `Bink.fi` FTN / `Swedish BankID` med en kryptografisk `SHA-256`-hash arkivert i `GCS WORM` i `europe-north1`) eller via en ekstern elektronisk signatur på Hovedavtalen / Bestillingen registrert i `portal.cloudpoint.fi` for sentralisert styring av kontrakter, moduler og DPO-kontaktinformasjon. Denne DPA-en forblir i kraft inntil Databehandleren har sluttet å behandle personopplysningene og har fullført sletting etter punkt 11.

14. Tvisteløsning og verneting

Denne DPA-en er underlagt bestemmelsene om tvisteløsning og verneting i Hovedavtalen (Helsingfors tingrett og finsk lov, med mindre lokal domstol og lov er avtalt i Hovedavtalen).

15. Endringshåndtering (3-trinns styringsmodell for Trust Center og DPA)

- **Trinn 1 — Ikke-vesentlige, presiserende og sikkerhetsforbedrende oppdateringer (0 dagers varsel, garanti mot forringelse):** Cloudpoint kan oppdatere Trust Center og tekniske beskrivelser uten forhåndsvarsel ved tekniske presiseringer, nye sertifiseringer (som ISO/IEC 27001:2022) eller styrkede sikkerhetstiltak, **forutsatt at oppdateringene aldri endrer de avtalte formålene eller medfører en vesentlig forringelse av Tjenestens sikkerhets- eller personvernforpliktelser (*No Material Degradation Guarantee*)**.
- **Trinn 2 — Endringer av underdatabehandlere og operasjonelle varsler (minst 30 kalenderdagers skriftlig forhåndsvarsel og rett til å protestere):** Tilføyelse eller bytte av underdatabehandlere (GDPR art. 28 nr. 2, jf. pkt. 9) varsles skriftlig (via e-post) direkte til den behandlingsansvarliges kontaktperson **minst tretti (30) kalenderdager før ikrafttredelse**, med 30 kalenderdagers rett til å protestere på saklige personverngrunner.
- **Trinn 3 — Vesentlige endringer i hvordan personopplysninger behandles og kundespesifikke endringer i Hovedavtalen (minst 30 kalenderdagers varsel + uttrykkelig elektronisk godkjenning fra den behandlingsansvarlige):** Databehandleren gjennomfører ingen vesentlige endringer i hvordan personopplysninger behandles (som formål, kategorier av personopplysninger eller registrerte, lagringsregioner, lagringstider eller kjerneforpliktelser etter GDPR art. 28 nr. 3) uten den behandlingsansvarliges godkjenning. Slike endringer sendes minst 30 kalenderdager i forveien til elektronisk godkjenning av den behandlingsansvarliges administrator eller beslutningstaker via **Edudata.io eller Cloudpoint Portal (`portal.cloudpoint.fi`) (med mulighet til å videresende godkjenningsforespørselen direkte til organisasjonens signeringsberettigede)**.

Signaturer

Partene har godkjent og signert denne DPA-en (Versjon 2.0) samt Brukervilkårene (Versjon 3.1) samtidig enten elektronisk via **Cloudpoint Portal (`portal.cloudpoint.fi`)** (med sterk e-ID `Bink.fi` / `Swedish BankID` og en kryptografisk `SHA-256`-sjekksum arkivert i `GCS WORM` `europe-north1`) eller via en ekstern elektronisk signatur på Hovedavtalen / Bestillingen registrert i `portal.cloudpoint.fi` for sentralisert kontrakt-, modul- og DPO-kontaktstyring.

Cloudpoint Oy / Edudata.io

Personvernombud (DPO) og bemyndiget representant, Cloudpoint Oy (Databehandler)

Versjon 2.0 | Dato: 10.11.2026

[Kundens representant]

Bemyndiget representant (Behandlingsansvarlig)

Dato: [Dato for godkjenning]

VEDLEGG 1: Beskrivelse av behandlingen (Versjon 2.0 — 10.11.2026)

1. Formålet med behandlingen av personopplysninger

Databehandleren behandler personopplysninger på vegne av den behandlingsansvarlige for å levere Edudata-tjenesten, håndtere føderert SSO og rollebasert tilgangskontroll (RBAC), administrere personvern- og risikovurderinger (DPIA) samt opprettholde informasjonssikkerhet og revisjonslogger i samsvar med Hovedavtalen, denne DPA-en og dokumenterte instrukser.

2. Kategorier av registrerte og modulmatrise

- **Kommunalt ansatte og administratorer (*Edudata Compliance* & *Edudata Compliance Service* — kjerneplattformen):** Kommunalt ansatte, administratorer, rektorer, lærere, systemansvarlige, saksbehandlere, beslutningstakere og personvernombud (DPO).
- **Elever, studenter og foresatte (KUN hvis tilleggsmodulene *Edudata Privacy* eller *Edudata Security* er aktivert):** Personopplysninger om elever eller foresatte **behandles ikke** i kjerneplattformen *Edudata Compliance*, men kun dersom kommunen har aktivert de valgfrie modulene *Edudata Privacy* eller *Edudata Security*.
- **Beskyttelsesregel for fritekstfelt (Free-Text Safeguard):** Hvis en bruker utilsiktet legger inn personopplysninger om elever eller foresatte i et fritekstfelt, er opplysningene beskyttet av AES-256, TLS 1.2/1.3, tenant-isolasjon og RBAC, og kan slettes umiddelbart av kommunens administratorer eller Cloudpoint.

3. Typer av personopplysninger og autentisering (Null passord — CP-ISMS-AUTH-001 v1.1)

Databehandleren behandler følgende typer av personopplysninger på tvers av brukerrollene (*Lærer, Lærer+, Saksbehandler, Beslutningstaker, Kundeadministrator* samt i tilleggsmoduler *Elev/Student*):

- **Identitets- og organisasjonsdata:** Unik bruker-ID (Edudata UID), for- og etternavn (visningsnavn), jobb-e-postadresse, kommunal/organisatorisk tilhørighet og domene, RBAC-rolle, språk og valgfritt profilbilde.
- **Føderterte SSO-autentiseringsdata (null passord):** Kun føderert SSO (Microsoft Entra ID / M365 eller Google Workspace via Firebase Auth i `edudata-compliance-prod`), inkludert IdP-ID, OAuth 2.0 / OIDC JWT-tokens, innloggingstidsstempler, økt-ID, IP-adresse og nettleser-/enhetsdata. **Ingen passord eller autentiseringshemmeligheter mottas, behandles eller lagres noensinne** (*CP-ISMS-AUTH-001 v1.1*).
- **Valgfri tredjeparts-appmetadata (OAuth App Discovery):** Behandles kun hvis den valgfrie OAuth App Discovery-modulen er aktivert.

4. 7-punkts Google Cloud-ansvarsmatrise, 3-trinns logglagring (CP-ISMS-LOG-001 v1.2) og kommunal arkivering

7-punkts Google Cloud-ansvarsmatrise: (1) **Cloudpoint Oy** eier og administrerer produksjonsprosjektet `edudata-compliance-prod`; (2) Cloudpoint Oy har inngått Google CDPA med **Google Cloud EMEA Limited / Google Ireland Ltd**; (3) All datalagring for basiskontoer, vurderinger og relasjonsdatabaser er låst til `europe-north1` (Finland) og `eu`-multiregion i Cloud SQL (`edudata-comp-db`, `edudata-ai-db`) og en separat Firestore-database (for eksisterende kunder på lagringsmodell v1 med den valgfrie SSO-/apploggmodulen kan disse loggene ligge i kundespesifikke Google Cloud Firestore-prosjekter, mens nye implementeringer bruker vår sentraliserte EU-multitenant-arkitektur v2 med full bakoverkompatibilitet via `TenantStorageRouter`); (4) Cloudpoint styrer IAM med obligatorisk Yubico YubiKey

2SV; (5) Cloudpoint håndhever AES-256 GMEK og Secret Manager; (6) Cloudpoint utfører teknisk sletting (30d primærdata / 90d sikkerhetskopier); (7) Cloudpoint lagrer Cloud Audit Logs i EU BigQuery (`edudata_compliance_logging`).

3-trinns ISO/IEC 27001-logglagringsmatrise (*CP-ISMS-LOG-001 v1.2*): (1) **400 dager** `_Required` Admin Activity- og System Event-revisjonslogger + EU BigQuery (`edudata_compliance_logging`); (2) **365 dager** `_Default` Cloud Run-, Cloud SQL (`cloudsql_mysql_audit`)- og VPC-sikkerhetslogger + EU BigQuery (samt **15–30 dager** Datadog APM feil-/latensspor med maskert PII); (3) **366 dager** sletting av inaktive brukere, **30 dager** ubesvarte rolleforespørsler og **18 måneder** valgfri OAuth-apptelemetri.

Vurderinger, beslutninger og forespørsler (lagring i hele avtaleperioden + 30 dagers slettefrist etter avtalens opphør): Vurderinger, DPIA-er, beslutninger og forespørsler **slettes ikke før kundens avtale med Edudata.io-tjenesten opphører** (med mindre den Behandlingsansvarlige selv sletter dem), og kunden har full eksporttilgang i hele avtaleperioden. Etter at avtalen er opphørt, følger vi en **slettefrist på 30 kalenderdager** for sletting av data fra primære datalagre (og 90 kalenderdager for krypterte sikkerhetskopier).

5. Godkjente underdatabehandlere

Databehandleren benytter følgende godkjente underdatabehandlere:

Underdatabehandlerens navn	Behandlingens omfang, lokasjon og garantier
Google Ireland Ltd (Google Cloud EMEA Limited)	Produksjons-skyinfrastruktur (`edudata-compliance-prod`), Cloud SQL, Firestore, Firebase Auth SSO samt valgfri Vertex AI (Gemini) & Document AI i **`europe-north1` (Finland) & `eu` -multiregion**. Gjelder alle brukere (Google CDPA, EU SCC & DPF).
HubSpot Ireland Ltd	Supportsaksystem og kontaktpersoner (ingen elevdata; forbud mot 5 datakategorier). Lokasjon: **EU/EØS (`dataHostingLocation = eu1` , AWS `eu-central-1` Frankfurt, Tyskland)** (EU SCC, DPF & TIA).
Datadog, Inc.	15–30 dagers APM-latens- og feilalarmering med maskert PII (ingen vurderingsdata) (EU SCC & DPF).
Aimpulse (Cloudpoint Oys dedikerte utviklingsenhet / partnerenhet, Kairo, Egypt)	Programvareutvikling utelukkende under Cloudpoint Oys operasjonelle kontroll og ISO/IEC 27001:2022-sertifiserte ISMS i **isolert ikke-produksjonsmiljø (`edudata-compliance-staging`) med 100 % syntetiske testdata** (`CP-ISMS-DLP-001 v1.2`); **ingen tilgang til operasjonelle kundedata eller personopplysninger i produksjonsmiljøet (`edudata-compliance-prod`)** (EU SCC Module 3, TIA & 400d revisjonslogg).
Online Partner AB	**Betinget partner:** Gjelder **kun** der Kunden har inngått avtale med Online Partner AB som lokal forhandler/1.-linjesupportpartner; behandler ikke data for direkte Cloudpoint-kommunekunder (EU/EØS).
Visma AB	**Kun Cloudpoints B2B-fakturering:** Brukes utelukkende til Cloudpoint Oys lovpålagte B2B-økonomifakturering som behandlingsansvarlig; behandler ikke plattformens vurderingsdata (EU/EØS).

6. Internasjonale overføringer

Alle produksjonsdatabaser er plassert i EU/EØS (`europe-north1` Finland og `eu` -multiregion). Eventuelle overføringer utenfor EØS via underdatabehandlere skjer i samsvar med kapittel V i GDPR (DPF, EU SCC 2021/914 og TIA).

VEDLEGG 2: Tekniske og organisatoriske sikkerhetstiltak (Versjon 2.0 — 10.11.2026)

Databehandleren implementerer og opprettholder tekniske og organisatoriske sikkerhetstiltak i samsvar med GDPR art. 32 og sitt ISO/IEC 27001:2022-sertifiserte ISMS.

Alle personer autorisert til å behandle personopplysninger er underlagt taushetsplikt og deltar regelmessig i opplæring innen personvern og informasjonssikkerhet.

- **Cloudpoint Oy sitt ISO/IEC 27001:2022-sertifiserte ISMS (Prescient Security LLC, #123522) & kontinuerlig GRC-overvåking (Vanta):** Cloudpoint Oy (2325703-6) driver et **ISO/IEC 27001:2022-sertifisert** ISMS (*Statement of Applicability v1.2* 20.10.2026; sertifikat `#123522` Issue 1, utstedt 18.11.2026, gyldig til 17.11.2029 av IAS-akkrediterte **Prescient Security LLC**, MSCB-267, IAF MLA; hovedkontor Malminkaari 17-19 B, Helsinki; omfattende skyøkosystemer for offentlig sektor, utdanning og næringsliv, GCP- og Google Workspace-infrastruktur samt de 6 avdelingene), og som overvåkes kontinuerlig via Vanta, inkludert kontrollene VPM-38, VPM-3 og AST-4 – AST-9.
- **Multi-Tenancy & kryptografisk beskyttelse (AES-256, TLS 1.3 & mTLS):** Streng logisk flerbrukerisolasjon per kommune; kryptering ved hvile med AES-256 (GMEK) og under overføring med TLS 1.3 (minimum TLS 1.2) samt mTLS på Cloud SQL (`TRUSTED_CLIENT_CERTIFICATE_REQUIRED`).
- **Tilgangskontroll (Access Control Policy v1.1.0) & maskinvarebasert YubiKey (U2F/FIDO2) MFA:** Rollebasert IAM med kvartalsvise tilgangsgjennomganger, 24-timers tilbakekallings-SLA, obligatorisk maskinvarebasert Yubico YubiKey (U2F/FIDO2) MFA og full diskkryptering (FDE).
- **Uavhengig penetrasjonstest (juni 2026) & sårbarhetshåndtering (7 dager / 14 dager SLA):** Uavhengig ekstern penetrasjonstest gjennomført i juni 2026 (*CP-ISMS-VSR-002 v1.0*, alle funn utbedret og verifisert **16. august 2026**). I henhold til *Vulnerability Management Procedure v2.1* utbedres kritiske CVE-er innen **7 dager** og høye CVE-er innen **14 dager** (automatisert Bitbucket Pipelines + Artifact Registry-skanning + 4-øyne peer review).
- **RTO/RPO & verifiserte gjenopprettingsøvelser (CP-ISMS-BIA-001 v1.1 & CP-ISMS-BCDR-002 v1.1):** RTO < 15 min for Cloud Run API-er/Auth (RPO = 0), RTO < 1 time for Cloud SQL (RPO = 24t daglig / near-zero 7d PITR), RTO < 4 timer for hele plattformen; verifisert gjenopprettingsøvelse **3. juni 2026 (26 minutter)** og PITR-gjenopprettingsøvelse **18. oktober 2026 (9 minutter 52 sekunder)**.
- **3-trinns dataklassifisering & fysisk sikkerhet (Malminkaari 17-19B, 00700 Helsinki):** Kundedata klassifiseres som Confidential / Restricted i Google Cloud (`europe-north1` Finland). Bevoktede kontorlokaler med adgangskontroll og 24/7 videoovervåking i Malminkaari 17-19B, 00700 Helsinki, Finland samt ISO 27001- og SOC 2-sertifiserte Google Cloud EU-datasentre.

Sikkerhetskontroller ved programvareutvikling (SDLC):

- Isolerte utviklings-, test- (`edudata-compliance-staging`) og produksjonsmiljøer (`edudata-compliance-prod`) med 100 % syntetiske testdata (`CP-ISMS-DLP-001 v1.2`).
- Obligatorisk 4-øyne peer review og godkjenning av en seniorutvikler før produksjonssetting.
- Automatisert sårbarhetsskanning i CI/CD og kun krypterte (FDE), MDM-administrerte bærbare datamaskiner.

Skyinfrastruktur og Kundens ansvar:

Cloudpoint Oy eier og forvalter produksjonsmiljøet i Google Cloud (`edudata-compliance-prod`). Kunden, som behandlingsansvarlig, er ansvarlig for administrasjon av sine føderte brukere (Entra ID / Google Workspace) og behandlingsgrunnlaget. Mer informasjon finnes i Google Cloud Security Whitepapers.