# Databehandleraftale (DPA)

Edudata.io (3460068-8) — Cloudpoint Oy (Virksomheds-ID (FI) 2325703-6, Moms FI23257036) • Malminkaari 17–19 B, 00700 Helsinki, Finland • DPO: tietosuoja@cloudpoint.fi

**[OFFICIELT OFFENTLIGGJORT · H-AI-H]** Menneskeligt verificeret officiel sprogversion (H-AI-H Human–AI–Human; ved uoverensstemmelse har EN-hovedversionen forrang).
**Verification Role:** LEGAL_COUNSEL_AND_RELEASE_OWNER | **Verified UTC:** 2026-11-25T08:36:41Z

| | | | |
|---|---|---|---|
| **Dokument-ID** | `edudata.dpa.da.v2.0.0-r01` | **Version** | **v2.0** (`v2.0.0-r01`) |
| **Gældende fra** | 2026-11-10 | **Næste gennemgang** | 2027-11-10 |
| **Sprog** | Dansk (da-DK) | **Sikkerhedscertificering** | ISO/IEC 27001:2022 (#123522, Prescient Security LLC) |
| **Styringsmodel** | **H-AI-H (Human–AI–Human)** | **Sprogrolle / Hovedversion** | Lokaliseret oversættelse (fra EN-hovedversion) |
| **Kanonisk webadresse** | `https://www.edudata.io/da/trust-center#dpa` | | |
| **Indholdets SHA-256 (UTF-8 NFC)** | `8c6cfd287a00d0a926eef5f4f20a88d98112f336311aa213352f964ae4248275` | | |

Den juridisk bindende databehandleraftale (DPA), der regulerer behandlingen af personoplysninger for Edudata.io-platformen mellem dataansvarlig og databehandleren.

## EDUDATA.IO DATABEHANDLERAFTALE

Denne lokaliserede version er en AI-assisteret oversættelse af den
originale engelske version
og er kun til information og reference. I tilfælde af uoverensstemmelser er den engelske version gældende.

Version 2.0 | Gyldig fra: 10.11.2026

Denne databehandleraftale ("DPA", Version 2.0) gælder for EDUDATA-tjenesten ("Tjenesten") leveret af Cloudpoint Oy og er et tillæg til samt en integreret del af hovedaftalen (inklusive servicevilkårene). I tilfælde af uoverensstemmelse har denne DPA forrang med hensyn til databeskyttelse.

### Kontraktpartnere:

**Databehandler:** Cloudpoint Oy (2325703-6) / Edudata.io (3460068-8), som er en del af Cloudpoint Oy (2325703-6, momsnummer FI23257036), Malminkaari 17-19B, 00700 Helsinki, Finland (Databeskyttelsesrådgiver / DPO: Jasse Tenko, tietosuoja@cloudpoint.fi, ISM-leder: Hesham Abboud, kundeservice: info@edudata.io, tlf. +358 9 4257 9280)
**Dataansvarlig:** Kunden (Kommunen / Uddannelsesudbyderen)

### 1. Definitioner

- **Dataansvarlig:** Den fysiske eller juridiske person, offentlige myndighed, institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger (GDPR Art 4(7)).
- **Databehandler:** Den fysiske eller juridiske person, offentlige myndighed, institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne (GDPR Art 4(8)).
- **GDPR:** Europa-Parlamentets og Rådets forordning (EU) 2016/679 (generel forordning om databeskyttelse).

- **Personoplysninger:** Enhver form for information om en identificeret eller identificerbar fysisk person (GDPR Art 4(1)).
- **Behandling:** Enhver aktivitet eller række af aktiviteter, som personoplysninger eller en samling af personoplysninger gøres til genstand for, med eller uden brug af automatisk behandling.

Alle øvrige begreber, der ikke er defineret i denne DPA, har samme betydning som i GDPR.

## 2. Baggrund og formål

Den dataansvarlige har valgt tjenesteudbyderen (Cloudpoint Oy) til at fungere som databehandler i overensstemmelse med artikel 28, stk. 3, i forordning (EU) 2016/679 (generel forordning om databeskyttelse, "GDPR").

Denne DPA udgør en integreret del af Hovedaftalen indgået mellem Parterne, hvorefter Databehandleren leverer Edudata-tjenesten (primært *Edudata Compliance* og *Edudata Compliance Service* samt, hvis særskilt aftalt, tilvalgsmodulerne *Edudata Privacy* og *Edudata Security*) til den dataansvarlige, medmindre andet er aftalt i Hovedaftalen.

Databehandleren behandler oplysninger om en identificeret eller identificerbar fysisk person på den dataansvarliges vegne. De nærmere detaljer om databehandlingen er beskrevet i Bilag 1 (Version 2.0 — 10.11.2026) til denne DPA.

Formålet med denne aftale er at fastlægge Parternes rettigheder og forpligtelser i forbindelse med behandling af personoplysninger i overensstemmelse med GDPR og at sikre beskyttelsen af de registreredes frihedsrettigheder og rettigheder under behandlingen.

## 3. Roller og ansvar

Databehandleren behandler kun personoplysninger i overensstemmelse med denne DPA og dokumenterede instrukser fra den dataansvarlige. Databehandleren forpligter sig til ikke at anvende personoplysningerne til andre formål end dem, der er aftalt i denne DPA og i den dataansvarliges instrukser. Den dataansvarliges instrukser skal være i overensstemmelse med gældende databeskyttelseslovgivning og denne DPA.

Hvis Databehandleren opdager, at en instruks fra den dataansvarlige er i strid med gældende lovgivning eller er utilstrækkelig, skal Databehandleren straks underrette den dataansvarlige herom.

Den dataansvarlige er ansvarlig for, at der foreligger et lovligt grundlag for behandlingen af personoplysningerne, for at oplyse de registrerede om behandlingen af deres personoplysninger samt for øvrige forpligtelser, der påhviler den dataansvarlige i henhold til GDPR.

Den dataansvarlige er ansvarlig for at oplyse Databehandleren om kontaktoplysningerne på sin databeskyttelsesrådgiver (DPO) og udpegede kontaktperson samt for at sikre, at kontaktoplysningerne holdes ajour til brug for direkte skriftlige underretninger.

## 4. Tekniske og organisatoriske sikkerhedsforanstaltninger

Databehandleren skal opretholde passende tekniske og organisatoriske sikkerhedsforanstaltninger (GDPR art. 32 og et ISO/IEC 27001:2022-certificeret ledelsessystem for informationssikkerhed) for at beskytte mod uautoriseret eller ulovlig behandling eller adgang samt mod hændeligt tab, tilintetgørelse eller beskadigelse. Ved valget af sikkerhedsforanstaltninger skal Databehandleren tage hensyn til det aktuelle tekniske niveau, implementeringsomkostningerne og behandlingens karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

En detaljeret beskrivning af de anvendte foranstaltninger fremgår af Bilag 2 (Version 2.0 — 10.11.2026) til denne DPA.

## 5. Pligt til at bistå og svarfrist for registreredes anmodninger (DSAR SLA)

Databehandleren behandler personoplysninger i overensstemmelse med denne DPA, den dataansvarliges instrukser og databeskyttelseslovgivningen. Databehandleren forpligter sig til at sikre, at personer, der arbejder for Databehandleren, overholder vilkårene i denne DPA og er informeret om relevant lovgivning.

Databehandleren bistår den dataansvarlige med at sikre overholdelse af forpligtelserne i artikel 28 og 32–36 i GDPR (herunder konsekvensanalyser vedrørende databeskyttelse [DPIA], forudgående høring og de registreredes rettigheder).

**Ingen ekstraomkostninger for lovpligtig bistand:** Al standardbistand i henhold til GDPR artikel 28 og artikel 32–36 er inkluderet i abonnementsgebyret uden ekstra omkostninger. Kun skræddersyet udviklings- eller integrationsarbejde bestilt af Kunden ud over lovkravene i GDPR faktureres efter forudgående skriftlig aftale.

**Svarfrist på højst fem (5) arbejdsdage (DSAR SLA):** Databehandleren forpligter sig til uden unødigt ophold og **senest inden for fem (5) arbejdsdage** at underrette den dataansvarlige om alle modtagne anmodninger fra registrerede (DSAR) samt levere teknisk bistand og dataeksport inden for 5 arbejdsdage efter anmodning.

## 6. Internationale overførsler, HubSpot EU1-styring og adskillelse af softwareudvikling

Vi behandler alle produktionsdata og databaser udelukkende på Google Cloud-servere placeret i Det Europæiske Økonomiske Samarbejdsområde (EU/EØS, primært `europe-north1` Finland samt EU-multiregion). Der finder ingen regelmæssige overførsler af produktionsdata sted uden for EU/EØS.

**HubSpot Ireland Ltd (EU1 Frankfurt-datalagring og forbud mod 5 datakategorier i supporttickets):** Vores supportticket- og kontaktstyringssystem i HubSpot er låst til EU-datacentre ( `dataHostingLocation = eu1` , `app-eu1.hubspot.com` , AWS `eu-central-1` Frankfurt, Tyskland med failover i Dublin, Irland). HubSpot håndhæver GDPR Compliance Toolkit (herunder *GDPR Permanent Delete* inden for 90 dage efter aftalens ophør eller på anmodning) og AI-spærrer ( `customer_data_training_enabled = False` , `crm_sensitive_pii_access_enabled = False` ), understøttet af EU–U.S. Data Privacy Framework (DPF), EU's standardkontraktbestemmelser (SCC 2021/914) og en Transfer Impact Assessment (TIA). Derudover forbyder Cloudpoints *Data Management Policy v1.1.0* strengt indtastning eller overførsel af fem (5) datakategorier i HubSpot-supporttickets: (1) elev- og studenterdata, (2) følsomme personoplysninger (særlige kategorier), (3) detaljer om sikkerhedshændelser, (4) adgangskoder/autentificeringstokens og (5) sikkerhedslogfiler.

**Teknisk adskillelse af softwareudvikling i Egypten (Aimpulse — GDPR art. 25 & 32): Aimpulse** er Cloudpoint Oy's dedikerede udviklingsenhed / partnerenhed (Kairo, Egypten), der udelukkende opererer under Cloudpoint Oy's operationelle kontrol og ISO/IEC 27001:2022-certificerede ISMS. Udviklerne i Egypten deltager aktivt i softwareudviklingen i **isolerede ikke-produktionsmiljøer ( `edudata-compliance-staging` ) med 100 % syntetiske testdata** (*CP-ISMS-DLP-001 v1.2*) og har **ingen adgang til operationelle kundedata eller personoplysninger i produktionsmiljøet ( `edudata-compliance-prod` )**. Kundesupport og administration af produktionspersonoplysninger udføres udelukkende i EU/EØS (Finland), og aftaleforholdet er dækket af EU's standardkontraktbestemmelser (SCC, afgørelse (EU) 2021/914, Module 3), TIA og uforanderlige 400-dages revisionslogfiler.

## 7. Tavshedspligt

Databehandleren og alle fysiske personer, der arbejder for Databehandleren, skal iagttage fortrolighed og tavshedspligt under behandlingen. Databehandleren sikrer, at alle fysiske personer, der arbejder for Databehandleren, er bundet af en fortrolighedsaftale.

Databehandleren sikrer, at der foreligger en hemmeligholdelsesaftale (NDA) med underdatabehandlerne samt fortrolighedsaftaler mellem underdatabehandleren og alle fysiske personer, der arbejder for underdatabehandleren og deltager i behandlingen. Denne tavshedspligt forbliver i kraft også efter ophøret af Hovedaftalen og denne databehandleraftale.

## 8. Ret til revision

Den dataansvarlige har ret til i rimeligt omfang at foretage revision (audit) af Databehandlerens faciliteter og behandlingsaktiviteter for at undersøge det beskyttelses- og sikkerhedsniveau, der følger af denne DPA, og for at vurdere Databehandlerens overholdelse af bestemmelserne i denne DPA. Databehandleren stiller på anmodning sin aktuelle ISO/IEC 27001:2022-revisionsdokumentation (Prescient Security) og revisionsrapporter til rådighed.

Hver part afholder sine egne omkostninger forbundet med gennemførelsen af en revision (eller som aftalt i Hovedaftalen). Den dataansvarlige skal skriftligt varsle Databehandleren mindst 14–30 dage i forvejen, før revisionen gennemføres.

Den dataansvarliges ret til revision kan udøves højst én gang hver tolvte (12) måned, medmindre et specifikt brud på persondatasikkerheden, et påbud fra en tilsynsmyndighed eller en velbegrundet bekymring nødvendiggør en tidligere revision.

Hvor en revision kan føre til videregivelse af Databehandlerens forretnings- eller erhvervshemmeligheder eller true Databehandlerens intellektuelle ejendomsrettigheder, skal der anvendes en uafhængig ekspert til at gennemføre revisionen, og denne ekspert skal forpligte sig til at være bundet af en fortrolighedsaftale.

## 9. Underdatabehandlere

Databehandleren har ret til at benytte underdatabehandlere til at behandle personoplysninger i forbindelse med leveringen af Tjenesten, i det omfang en sådan udpegning ikke fører til manglende overholdelse af Databehandlerens forpligtelser i henhold til denne DPA. Godkendte underdatabehandlere fremgår af Bilag 1.

Databehandleren sikrer, at de involverede underdatabehandlere handler i henhold til en skriftlig databehandleraftale (GDPR art. 28, stk. 4) med Databehandleren og overholder databeskyttelsesforpligtelser, der er mindst lige så strenge som forpligtelserne i denne aftale.

**Direkte skriftligt forudgående varsel (mindst 30 kalenderdage):** Databehandleren giver den dataansvarliges udpegede kontaktperson direkte skriftligt varsel (via e-mail) **mindst tredive (30) kalenderdage i forvejen** før tilføjelse eller udskiftning af en underdatabehandler. Den dataansvarlige har tredive (30) kalenderdage fra underretningen til skriftligt at gøre indsigelse på saglige databeskyttelsesretlige grunde. Hvis der ikke opnås en løsning inden for 30 kalenderdage, har den dataansvarlige ret til at opsige Tjenesten uden sanktioner.

## 10. Brud på persondatasikkerheden (To-trins 24/7-overvågning og NIS2 art. 23 / GDPR art. 33-model)

Databehandleren følger en dokumenteret beredskabsprocedure (*Security Incident Management Procedure CP-ISMS-IR-002 v1.0* samt VPM-38 4-trins hændelsesberedskabs-SLA: P1 < 1 t., P2 < 4 t., P3 < 24 t., P4 < 72 t.) og underretter den dataansvarlige i to trin:

- **Trin 1 — Automatiseret 24/7/365-overvågning og tidlig varsling (Early Warning ≤ 24 timer):** Produktionsinfrastrukturen (`edudata-compliance-prod`) overvåges 24/7/365 (inklusive weekender og helligdage) af automatiske sikkerheds- og anomalialarmer. Ved konstateret eller begrundet mistanke om brud på persondatasikkerheden sender Databehandleren en indledende skriftlig eller automatiseret **tidlig varsling (Early Warning) senest inden for 24 timer** efter opdagelse (med opdagelsestidspunkt, berørt tjeneste, aktive tekniske inddæmningsforanstaltninger og kontaktpunkter).
- **Trin 2 — Formel DPO-vurdering og detaljeret 8-punktsrapport (næste arbejdsdag / ≤ 72 timer):** Formel undersøgelse, årsagsanalyse (RCA) og DPO-konsekvensvurdering (DPO Jasse Tenko / ISM-leder Hesham Abboud, `tietosuoja@cloudpoint.fi`) gennemføres inden for normal arbejdstid og leveres **næste arbejdsdag** (og altid inden for 72-timersfristen i GDPR art. 33) med alle otte (8) påkrævede datapunkter: (1) tidspunkt for hændelse og opdagelse, (2) berørte systemer og data, (3) berørte kategorier og estimeret antal registrerede, (4) berørte underdatabehandlere/lande, (5) sandsynlige konsekvenser, (6) trufne og planlagte inddæmnings- og afbødningsforanstaltninger, (7) DPO/ISM-kontaktoplysninger (`tietosuoja@cloudpoint.fi`, tlf. +358 9 4257 9280) og (8) tidspunkt for næste statusrapport.

## 11. Tilbagelevering og sletning af personoplysninger (30 dage primærdata / 90 dage sikkerhedskopier)

Inden aftalens ophør har den dataansvarlige ret til at eksportere alle kommunale vurderinger, beslutninger, metadata og revisionsspor i et struktureret, maskinlæsbart format (JSON/CSV/PDF). Efter ophøret af denne DPA sletter Databehandleren personoplysninger i henhold til følgende frister:

- **Primære produktionsdata (højst 30 dage):** Alle aktive kunde- og personoplysninger slettes fra produktionsdatabaserne (Cloud SQL `edudata-comp-db`, `edudata-ai-db` og Firestore) **senest inden for**

**tredive (30) dage** efter aftalens ophør.

- **Sikkerhedskopier (højst 90 dage efter primær sletning):** Krypterede sikkerhedskopier (Cloud SQL `edudata-comp-db` 21 dages daglige sikkerhedskopier + 7 dages PITR, `edudata-ai-db` 7 dages sikkerhedskopier + 7 dages PITR, Firestore 7–90 dage samt Cloud Storage 7 dages soft-delete `604800s`) overskrives og slettes uigenkaldeligt **senest inden for halvfems (90) dage** efter primær sletning (mens uforanderlige `_Required` 400 dages / `_Default` 365 dages sikkerhedslogfiler uden kundeindhold udløber automatisk).
- **Skriftlig bekræftelse på sletning på anmodning:** Under hele sletningsvinduet er data beskyttet med AES-256-kryptering og strengt spærret for brug. Efter anmodning leverer Databehandleren en skriftlig bekræftelse på sletning (f.eks. pr. e-mail), når sletningen er gennemført.

Inaktive brugerkonti slettes automatisk fra brugerdatabasen, når der er gået 366 dage siden seneste login.

## 12. AI-assisteret behandling (Vertex AI / Gemini & Document AI) og ansvarsbegrænsning

**AI-behandlingsgarantier (EU/EØS-låsning og forbud mod modeltræning):** Hvor den dataansvarlige anvender valgfrie AI-assisterede funktioner i Tjenesten, udføres behandlingen udelukkende via **Google Cloud Vertex AI (Gemini Enterprise-modeller)** og **Google Cloud Document AI** inden for EU/EØS (`europe-north1` Finland og `eu`-multiregion, `edudata-ai-db`, 30 dages primær sletning / 7 dages sikkerhedskopier). Kundedata, prompts, dokumenter eller output **bruges aldrig til at træne, finjustere eller forbedre generelle eller tværgående AI-modeller** (*Data Management Policy v1.1.0*). Der foretages ingen automatiserede afgørelser eller profilering efter GDPR artikel 22 (udelukkende *Human-in-the-Loop* beslutningsstøtte).

**Ansvarsbegrænsning:** Databehandleren er ikke ansvarlig for indirekte tab eller følgeskader i henhold til denne DPA. Databehandlerens samlede maksimale ansvar over for den dataansvarlige i henhold til denne DPA er begrænset til et beløb svarende til 100 % af de betalinger, som den dataansvarlige har foretaget til Databehandleren for Tjenesten i løbet af de foregående 12 måneder (medmindre andet fremgår af Hovedaftalen). Databehandleren begrænser ikke sit ansvar, hvor en sådan begrænsning ville være ulovlig.

## 13. Varighed

Denne DPA (Version 2.0, gælder fra 10.11.2026) og Edudata.io's Servicevilkår (Version 3.1) indgås og træder i kraft samtidigt enten elektronisk via **Cloudpoint Portal (`portal.cloudpoint.fi`)** (ved brug af stærk elektronisk identifikation `Bink.fi` FTN / `Swedish BankID` med en kryptografisk `SHA-256`-hash arkiveret i `GCS WORM` i `europe-north1`) eller via en ekstern elektronisk underskrift på Hovedaftalen / Ordren registreret i `portal.cloudpoint.fi` til centraliseret styring af kontrakter, moduler og DPO-kontaktoplysninger. Denne DPA forbliver i kraft, indtil Databehandleren er ophørt med at behandle den dataansvarliges personoplysninger og har gennemført sletning efter punkt 11.

## 14. Tvistbilæggelse og værneting

Denne DPA er underlagt bestemmelserne om tvistbilæggelse og værneting i Hovedaftalen (Helsingfors byret og finsk lov, medmindre lokal domstol og lovgivning er aftalt i Hovedaftalen).

## 15. Ændringsstyring (3-trins styringsmodel for Trust Center og DPA)

- **Trin 1 — Ikke-væsentlige, præciserende og sikkerhedsforbedrende opdateringer (0 dages varsel, garanti mod forringelse):** Databehandleren kan opdatere Trust Center og tekniske beskrivelser uden forudgående varsel ved tekniske præciseringer, redaktionelle opdateringer, nye sikkerhedscertificeringer (såsom ISO/IEC 27001:2022) eller skærpede sikkerhedsforanstaltninger, **forudsat at sådanne opdateringer aldrig ændrer de aftalte formål med behandlingen eller medfører en væsentlig forringelse af Tjenestens sikkerheds- eller databeskyttelsesforpligtelser (*No Material Degradation Guarantee*)**.
- **Trin 2 — Ændringer af underdatabehandlere og operationelle meddelelser (mindst 30 kalenderdages skriftligt forudgående varsel og ret til indsigelse):** Tilføjelse eller udskiftning af underdatabehandlere (GDPR art. 28, stk. 2, jf. pkt. 9) varsles skriftligt (via e-mail) direkte til den dataansvarliges kontaktperson **mindst tredive (30) kalenderdage før ikrafttræden**, med 30 kalenderdages ret til indsigelse på saglige databeskyttelsesgrunde.

- **Trin 3 — Væsentlige ændringer i hvordan personoplysninger behandles og kundespecifikke ændringer i Hovedaftalen (mindst 30 kalenderdages varsel + udtrykkelig elektronisk godkendelse fra den dataansvarlige):** Databehandleren foretager ingen væsentlige ændringer i, hvordan personoplysninger behandles (såsom formål, kategorier af personoplysninger eller registrerede, lagringsregioner, opbevaringsperioder eller kerneforpligtelser efter GDPR art. 28, stk. 3), uden den dataansvarliges godkendelse. Sådanne ændringer sendes mindst 30 kalenderdage i forvejen til elektronisk godkendelse af den dataansvarliges administrator eller beslutningstager via **Edudata.io eller Cloudpoint Portal (`portal.cloudpoint.fi`) (med mulighed for at videresende godkendelsesanmodningen direkte til organisationens tegningsberettigede)**.

### Underskrifter

Parterne har godkendt og underskrevet denne DPA (Version 2.0) samt Servicevilkårene (Version 3.1) samtidigt enten elektronisk via **Cloudpoint Portal (`portal.cloudpoint.fi`)** (med stærk e-ID `Bink.fi` / `Swedish BankID` og en kryptografisk `SHA-256`-kontrolsum arkiveret i `GCS WORM` `europe-north1`) eller via en ekstern elektronisk underskrift på Hovedaftalen / Ordren registreret i `portal.cloudpoint.fi` til centraliseret kontrakt-, modul- og DPO-kontaktstyring.

Cloudpoint Oy / Edudata.io

**Databeskyttelsesrådgiver (DPO) og bemyndiget repræsentant**, Cloudpoint Oy (Databehandler)

Version 2.0 | Dato: 10.11.2026

[Kundens repræsentant]

**Bemyndiget repræsentant** (Dataansvarlig)

Dato: [Dato for godkendelse]

## BILAG 1: Beskrivelse af behandlingen (Version 2.0 — 10.11.2026)

### 1. Formålet med behandlingen af personoplysninger

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere Edudata-tjenesten, håndtere fødereret enkeltsignering (SSO) og rollebaseret adgangskontrol (RBAC), administrere databeskyttelses- og risikovurderinger (DPIA) samt opretholde informationssikkerhed og revisionslogning i overensstemmelse med Hovedaftalen, denne DPA og instrukserne fra den dataansvarlige.

### 2. Kategorier af registrerede og modulmatrix

- **Kommunale medarbejdere og administratorer (*Edudata Compliance* & *Edudata Compliance Service* — kerneplatformen):** Kommunale medarbejdere, administratorer, skoleledere, lærere, systemansvarlige, sagsbehandlere, beslutningstagere og databeskyttelsesrådgivere (DPO).
- **Elever, studerende og værger (KUN hvis tilvalgsmodulerne *Edudata Privacy* eller *Edudata Security* er aktiveret):** Personoplysninger om elever eller værger **behandles ikke** i kerneplatformen *Edudata Compliance*, men udelukkende hvis Kunden har aktiveret de valgfrie moduler *Edudata Privacy* eller *Edudata Security*.
- **Sikkerhedsforanstaltning for fritekstfelter (Free-Text Safeguard):** Hvis en bruger utilsigtet indtaster personoplysninger om elever eller værger i et fritekstfelt, er disse oplysninger fuldt beskyttet af AES-256, TLS 1.2/1.3, tenant-isolering og RBAC, og kan slettes øjeblikkeligt af kommunens administratorer eller Cloudpoint.

### 3. Typer af personoplysninger og autentificering (Ingen adgangskoder — CP-ISMS-AUTH-001 v1.1)

Databehandleren behandler følgende typer af personoplysninger på tværs af brugerrollerne (*Lærer, Lærer+, Sagsbehandler, Beslutningstager, Kundeadministrator* samt i tilvalgsmoduler *Elev/Studerende*):

- **Identitets- og organisationsdata:** Unikt bruger-ID (Edudata UID), for- og efternavn (visningsnavn), arbejds-e-mailadresse, kommunal/organisatorisk tilknytning og domæne, RBAC-rolle, sprog og valgfrit profilbillede.

- **Fødererede SSO-autentificeringsdata (ingen adgangskoder):** Kun fødereret SSO (Microsoft Entra ID / M365 eller Google Workspace via Firebase Auth i `edudata-compliance-prod`), herunder IdP-ID, OAuth 2.0 / OIDC JWT-tokens, oprettelses- og logintidsstempler, sessions-ID, IP-adresse og browser-/enhedsdata. **Ingen adgangskoder eller autentificeringshemmeligheder modtages, behandles eller lagres nogensinde** (*CP-ISMS-AUTH-001 v1.1*).
- **Valgfri tredjeparts-appmetadata (OAuth App Discovery):** Behandles kun, hvis det valgfrie OAuth App Discovery-modul er aktiveret af Kunden.

## 4. 7-punkts Google Cloud-ansvarsmatrix, 3-trins logopbevaring (CP-ISMS-LOG-001 v1.2) og kommunal arkivering

**7-punkts Google Cloud-ansvarsmatrix:** (1) **Cloudpoint Oy** ejer og administrerer produktionsprojektet `edudata-compliance-prod`; (2) Cloudpoint Oy har indgået Google CDPA med **Google Cloud EMEA Limited / Google Ireland Ltd**; (3) AI datalagring for basiskonti, vurderinger og relationsdatabaser 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 lagringsmodel v1 med det valgfrie SSO-/applogmodul kan disse logfiler ligge i kundespecifikke Google Cloud Firestore-projekter, mens nye implementeringer anvender vores centraliserede EU-multitenant-arkitektur v2 med fuld bagudkompatibilitet via `TenantStorageRouter`); (4) Cloudpoint styrer IAM med obligatorisk Yubico YubiKey 2SV; (5) Cloudpoint håndhæver AES-256 GMEK og Secret Manager; (6) Cloudpoint udfører teknisk sletning (30 dages primærdata / 90 dages sikkerhedskopier); (7) Cloudpoint opbevarer centraliserede Cloud Audit Logs i EU BigQuery (`edudata_compliance_logging`).

**3-trins ISO/IEC 27001-logopbevaringsmatrix (*CP-ISMS-LOG-001 v1.2*):**

- **Trin 1 (400 dage):** Uforanderlige `_Required` Admin Activity- og System Event-revisionslogfiler samt EU BigQuery (`edudata_compliance_logging`) opbevares i **400 dage**.
- **Trin 2 (365 dage / APM 15–30 dage):** `_Default` Cloud Run-, Cloud SQL (`cloudsql_mysql_audit`)- og VPC-sikkerhedslogfiler opbevares i **365 dage** (og Datadog APM-fejl-/latensspor med maskeret PII i **15–30 dage**).
- **Trin 3 (Applikationslivscyklus):** Inaktive brugere slettes efter **366 dage**; ubesvarede rolleanmodninger efter **30 dage**; valgfri OAuth-apptelemetri efter **18 måneder**.

**Vurderinger, beslutninger og anmodninger (opbevaring i hele kontraktperioden + 30 dages sletningsfrist efter aftalens ophør):** Vurderinger, DPIA'er, beslutninger og anmodninger **slettes ikke, før kundens aftale med Edudata.io-tjenesten ophører** (medmindre den Dataansvarlige selv sletter dem), og kunden har fuld eksportadgang (inkl. metadata, versionshistorik og revisionsspor) i hele aftaleperioden. Efter aftalens ophør følger vi en **sletningsfrist på 30 kalenderdage** for sletning af data fra primære datalagre (og 90 kalenderdage for krypterede sikkerhedskopier).

## 5. Godkendte underdatabehandlere

Databehandleren anvender følgende godkendte underdatabehandlere:

| Underdatabehandlerens navn | Behandlingens omfang, lokation og garantier |
|---|---|
| **Google Ireland Ltd** (Google Cloud EMEA Limited) | Produktions-cloudinfrastruktur (`edudata-compliance-prod`), Cloud SQL, Firestore, Firebase Auth SSO samt valgfri Vertex AI (Gemini) & Document AI i **`europe-north1` (Finland) & `eu`-multiregion**. Gælder alle brugere (Google CDPA, EU SCC & DPF). |
| **HubSpot Ireland Ltd** | Supportticketsystem og kontaktpersoner (ingen elevdata; forbud mod 5 datakategorier). Lokation: **EU/EØS (`dataHostingLocation = eu1`, AWS `eu-central-1` Frankfurt, Tyskland)** (EU SCC, DPF & TIA). |
| **Datadog, Inc.** | 15–30 dages APM-latens- og fejlalarmering med maskeret PII (ingen vurderingsdata) (EU SCC & DPF). |

| Underdatabehandlerens navn | Behandlingens omfang, lokation og garantier |
|---|---|
| **Aimpulse** (Cloudpoint Oy's dedikerede udviklingsenhed / partnerenhed, Kairo, Egypten) | Softwareudvikling udelukkende under Cloudpoint Oy's operationelle kontrol og ISO/IEC 27001:2022-certificerede ISMS i **isoleret ikke-produktionsmiljø ( `edudata-compliance-staging` ) med 100 % syntetiske testdata** ( `CP-ISMS-DLP-001 v1.2` ); **ingen adgang til operationelle kundedata eller personoplysninger i produktionsmiljøet ( `edudata-compliance-prod` )** (EU SCC Module 3, TIA & 400 dages revisionslog). |
| **Online Partner AB** | **Betinget partner:** Gælder **kun**, hvor Kunden har indgået aftale med Online Partner AB som lokal forhandler/1.-linjesupportpartner; behandler ikke data for direkte Cloudpoint-kommunekunder (EU/EØS). |
| **Visma AB** | **Kun Cloudpoints B2B-fakturering:** Anvendes udelukkende til Cloudpoint Oy's lovpligtige B2B-økonomifakturering som selvstændig dataansvarlig; behandler ikke platformens vurderingsdata (EU/EØS). |

### 6. Internationale overførsler

Alle produktionsdatabaser er placeret i EU/EØS ( `europe-north1` Finland og `eu` -multiregion). Eventuelle tredjelandsoverførsler via underdatabehandlere sker i henhold til GDPR kapitel V baseret på EU-Kommissionens tilstrækkelighedsafgørelser (DPF) og/eller EU's standardkontraktbestemmelser (SCC 2021/914) samt TIA.

## BILAG 2: Tekniske og organisatoriske sikkerhedsforanstaltninger (Version 2.0 — 10.11.2026)

Databehandleren implementerer og opretholder tekniske og organisatoriske sikkerhedsforanstaltninger i henhold til GDPR art. 32 og sit ISO/IEC 27001:2022-certificerede ISMS.

Alle personer autoriseret til at behandle personoplysninger er underlagt fortrolighedsforpligtelser og deltager regelmæssigt i databeskyttelses- og sikkerhedsuddannelse.

- **Cloudpoint Oy's ISO/IEC 27001:2022-certificerede ISMS (Prescient Security LLC, #123522) & kontinuerlig GRC-overvågning (Vanta):** Cloudpoint Oy (2325703-6) driver et **ISO/IEC 27001:2022-certificeret** ISMS (*Statement of Applicability v1.2* 20.10.2026; certifikat `#123522` Issue 1, udstedt 18.11.2026, gyldigt til 17.11.2029 af IAS-akkrediterede **Prescient Security LLC**, MSCB-267, IAF MLA; hovedkontor Malminkaari 17-19 B, Helsinki; omfattende cloud-økosystemer for offentlig sektor, uddannelse og erhverv, GCP- og Google Workspace-infrastruktur samt de 6 afdelinger), og som overvåges kontinuerligt via Vanta, herunder kontrollerne VPM-38, VPM-3 og AST-4 – AST-9.
- **Multi-Tenancy & kryptografisk beskyttelse (AES-256, TLS 1.3 & mTLS):** Streng logisk multi-tenant-isolering pr. kommune; kryptering ved hvile med AES-256 (GMEK) og under overførsel med TLS 1.3 (minimum TLS 1.2) samt mTLS på Cloud SQL ( `TRUSTED_CLIENT_CERTIFICATE_REQUIRED` ).
- **Adgangskontrol (Access Control Policy v1.1.0) & hardwarebaseret YubiKey (U2F/FIDO2) MFA:** Rollebaseret IAM med kvartalsvise adgangsgennemgange, 24-timers tilbagekaldelses-SLA ved fratrædelse, obligatorisk hardwarebaseret Yubico YubiKey (U2F/FIDO2) MFA og fuld diskkryptering (FDE).
- **Uafhængig penetrationstest (juni 2026) & sårbarhedsstyring (7 dage / 14 dage SLA):** Uafhængig ekstern penetrationstest gennemført i juni 2026 (*CP-ISMS-VSR-002 v1.0*, alle fund udbedret og verificeret **16. august 2026**). I henhold til *Vulnerability Management Procedure v2.1* udbedres kritiske CVE'er inden for **7 dage** og høje CVE'er inden for **14 dage** (automatiseret Bitbucket Pipelines + Artifact Registry-scanning + 4-øjne peer review).
- **RTO/RPO & verificerede gendannelsesøvelser (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 dagligt / near-zero 7d PITR), RTO < 4 timer for hele platformen; verificeret gendannelsesøvelse den **3. juni 2026 (26 minutter)** og PITR-gendannelsesøvelse den **18. oktober 2026 (9 minutter 52 sekunder)**.

- **3-trins dataklassifikation & fysisk sikkerhed (Malminkaari 17-19B, 00700 Helsinki):** Kundedata klassificeres som Confidential / Restricted i Google Cloud (`europe-north1` Finland). Bevogtede kontorlokaler med adgangskontrol og 24/7 videoovervågning på Malminkaari 17-19B, 00700 Helsinki, Finland samt ISO 27001- og SOC 2-certificerede Google Cloud EU-datacentre.

**Sikkerhedskontrol ved softwareudvikling (SDLC):**

- Isolerede udviklings-, test- (`edudata-compliance-staging`) og produktionsmiljøer (`edudata-compliance-prod`) med 100 % syntetiske testdata (`CP-ISMS-DLP-001 v1.2`).
- Obligatorisk 4-øjne peer review og godkendelse af en seniorudvikler før produktionsudrulning.
- Automatiseret sårbarhedsscanning i CI/CD og udelukkende krypterede (FDE), MDM-administrerede udviklerbærbare.

**Cloud-infrastruktur og Kundens ansvar:**

Cloudpoint Oy ejer og administrerer produktionsmiljøet i Google Cloud (`edudata-compliance-prod`). Kunden er som dataansvarlig ansvarlig for administration af sine fødererede brugere (Entra ID / Google Workspace) og det lovlige behandlingsgrundlag. Yderligere oplysninger findes i Google Cloud Security Whitepapers.