Personuppgiftsbiträdesavtal (DPA)

Edudata.io (3460068-8) — Cloudpoint Oy (FO-nummer 2325703-6, Momsreg.nr FI23257036) • Malmbågen 17–19 B, 00700 Helsingfors, Finland • DPO: tietosuoja@cloudpoint.fi

[OFFICIELLT PUBLICERAD · H-AI-H] Mänskligt verifierad officiell språkversion (H-AI-H Human–AI–Human; vid tolkningsavvikelse äger EN-huvudversionen företräde).
Verification Role: LEGAL_COUNSEL_AND_RELEASE_OWNER | **Verified UTC:** 2026-11-25T08:36:41Z

Dokument-ID	`edudata.dpa.sv.v2.0.0-r01`	**Version**	**v2.0** (`v2.0.0-r01`)
Gäller från	2026-11-10	**Nästa granskning**	2027-11-10
Språk	Svenska (sv-SE)	**Informationssäkerhet**	ISO/IEC 27001:2022 (#123522, Prescient Security LLC)
Framställningsprocess	**H-AI-H (Human–AI–Human)**	**Språkroll / Huvudversion**	Lokaliserad översättning (från EN-huvudversion)
Kanonisk webbadress	`https://www.edudata.io/sv/trust-center#dpa`		
Innehålls-SHA-256 (UTF-8 NFC)	`efc3829706e268918e09d018b6243b8a25c97d27528daf6f1d0a938d25639d7a`		

Ett rättsligt bindande personuppgiftsbiträdesavtal som reglerar personuppgiftsbehandlingen för Edudata.io-plattformen mellan personuppgiftsansvarig och biträdet.

EDUDATA.IO PERSONUPPGIFTSBITRÄDESAVTAL

Denna lokaliserade version är en AI-assisterad översättning av den
engelska originalversionen
och tillhandahålls endast i informations- och referenssyfte. Vid eventuella avvikelser ska den engelska versionen äga företräde.

Version 2.0 | Giltigt från: 10 november 2026

Detta personuppgiftsbiträdesavtal ("DPA", Version 2.0) gäller för EDUDATA-tjänsten ("Tjänsten") som tillhandahålls av Cloudpoint Oy och utgör en integrerad del av huvudavtalet (inklusive användarvillkoren). Vid eventuella motstridigheter ska detta DPA äga företräde gällande personuppgiftsbehandling.

Avtalsparter:

Personuppgiftsbiträde: Cloudpoint Oy (2325703-6) / Edudata.io (3460068-8), som är en del av Cloudpoint Oy (2325703-6, momsnummer FI23257036), Malminkaari 17-19B, 00700 Helsingfors, Finland (Dataskyddsombud / DPO: Jasse Tenko, tietosuoja@cloudpoint.fi, ISM-ansvarig: Hesham Abboud, kundtjänst: info@edudata.io, tfn +358 9 4257 9280)
Personuppgiftsansvarig: Kunden (Kommunen / Utbildningsanordnaren)

1. Definitioner

- **Personuppgiftsansvarig:** Den fysiska eller juridiska person, offentliga myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter (GDPR Art 4(7)).
- **Personuppgiftsbiträde (Biträdet):** Den fysiska eller juridiska person, offentliga myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning (GDPR Art 4(8)).
- **GDPR:** Europaparlamentets och rådets förordning (EU) 2016/679 (allmän dataskyddsförordning).

- **Personuppgifter:** Varje upplysning som avser en identifierad eller identifierbar fysisk person (GDPR Art 4(1)).
- **Behandling:** En åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oavsett om de utförs automatiserat eller ej.

Alla andra termer som inte definieras i detta DPA ska ha samma betydelse som i GDPR.

2. Bakgrund och syfte

Den personuppgiftsansvarige har valt tjänsteleverantören (Cloudpoint Oy) att agera som personuppgiftsbiträde i enlighet med artikel 28(3) i Europaparlamentets och rådets förordning (EU) 2016/679 (allmän dataskyddsförordning, "GDPR").

Detta DPA utgör en integrerad del av Huvudavtalet mellan Parterna, enligt vilket Biträdet tillhandahåller den personuppgiftsansvarige Edudata-tjänsten (primärt *Edudata Compliance* och *Edudata Compliance Service* samt, om särskilt avtalats, tillvalsmodulerna *Edudata Privacy* och *Edudata Security*), såvida inte annat avtalats i Huvudavtalet.

Biträdet kommer att behandla uppgifter som avser en identifierad eller identifierbar fysisk person för den personuppgiftsansvariges räkning. De detaljerade rutinerna för personuppgiftsbehandlingen beskrivs i Bilaga 1 (Version 2.0 — 10.11.2026) till detta DPA.

Syftet med detta avtal är att reglera parternas rättigheter och skyldigheter vid behandling av personuppgifter i enlighet med GDPR och att säkerställa skyddet för de registrerades fri- och rättigheter under behandlingen.

3. Roller och ansvar

Biträdet ska behandla personuppgifter endast i enlighet med detta DPA och dokumenterade instruktioner från den personuppgiftsansvarige. Biträdet förbinder sig att inte använda personuppgifterna för några andra ändamål än vad som avtalats i detta DPA och i den personuppgiftsansvariges instruktioner. Den personuppgiftsansvariges instruktioner måste vara förenliga med tillämplig dataskyddslagstiftning och detta DPA.

Om Biträdet upptäcker att en instruktion från den personuppgiftsansvarige strider mot tillämplig lagstiftning eller är otillräcklig ska Biträdet omedelbart informera den personuppgiftsansvarige om detta.

Den personuppgiftsansvarige ansvarar för att det finns en laglig grund för behandlingen av personuppgifterna, för att informera de registrerade om behandlingen av deras personuppgifter samt för övriga skyldigheter som åvilar den personuppgiftsansvarige enligt GDPR.

Den personuppgiftsansvarige är skyldig att informera Biträdet om kontaktuppgifterna till sitt dataskyddsombud (DPO) och sin utsedda kontaktperson samt se till att dessa kontaktuppgifter hålls uppdaterade för direkta skriftliga meddelanden om underbiträdesändringar, avtalsuppdateringar och eventuella personuppgiftsincidenter.

4. Tekniska och organisatoriska säkerhetsåtgärder

Biträdet ska upprätthålla lämpliga tekniska och organisatoriska säkerhetsåtgärder (GDPR art. 32 och ett ISO/IEC 27001:2022-certifierat ledningssystem för informationssäkerhet) för att skydda personuppgifterna mot obehörig eller olaglig behandling och åtkomst samt mot oavsiktlig förlust, förstöring eller skada. Vid valet av säkerhetsåtgärder ska Biträdet beakta den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter.

En detaljerad beskrivning av de tillämpade säkerhetsåtgärderna finns i Bilaga 2 (Version 2.0 — 10.11.2026) till detta DPA.

5. Skyldighet att bistå och svarsfrist vid registerutdrag (DSAR SLA)

Biträdet behandlar personuppgifter i enlighet med detta DPA, instruktioner från den personuppgiftsansvarige och tillämplig dataskyddslagstiftning. Biträdet åtar sig att säkerställa att personer som arbetar för Biträdet följer villkoren i detta DPA och informeras om relevant lagstiftning. Biträdet bistår

den personuppgiftsansvarige med att säkerställa att skyldigheterna enligt artiklarna 28 och 32–36 i GDPR uppfylls (inklusive konsekvensbedömningar avseende dataskydd [DPIA], förhandssamråd och de registrerades rättigheter).

Ingen extra kostnad för lagstadgad assistans: All sedvanlig assistans enligt GDPR artikel 28 och artiklarna 32–36 ingår i abonnemangsavgiften för Tjänsten utan extra kostnad. Endast kundanpassat utvecklings- eller integrationsarbete som uttryckligen beställs av Kunden utöver GDPR:s lagstadgade krav debiteras efter skriftlig förhandsöverenskommelse.

Svarsfrist på högst fem (5) arbetsdagar (DSAR SLA): Biträdet åtar sig att utan onödigt dröjsmål och **senast inom fem (5) arbetsdagar** underrätta den personuppgiftsansvarige om alla förfrågningar från registrerade (DSAR) samt tillhandahålla tekniskt bistånd och dataexport inom 5 arbetsdagar från den personuppgiftsansvariges begäran.

6. Internationella överföringar, HubSpot EU1-styrning och separering av mjukvaruutveckling

Vi behandlar samtliga produktionsdata och databaser för Tjänsten uteslutande på Google Cloud-servrar belägna inom Europeiska unionen och Europeiska ekonomiska samarbetsområdet (EU/EES, primärt `europe-north1` Fredrikshamn, Finland samt EU-multiregion). Inga regelbundna överföringar av produktionsdata sker utanför EU/EES.

HubSpot Ireland Ltd (EU1 Frankfurt-datalagring och förbud mot 5 datakategorier i supportärenden): Vårt supportärende- och kontaktverwaltungssystem i HubSpot är låst till EU-datacenter (`dataHostingLocation = eu1` , `app-eu1.hubspot.com` , AWS `eu-central-1` Frankfurt, Tyskland med reservdrift i Dublin, Irland). HubSpot-miljön tillämpar GDPR Compliance Toolkit (inklusive permanent GDPR-radering [*GDPR Permanent Delete*] inom 90 dagar efter avtalets upphörande eller på begäran) samt AI-spärrar (`customer_data_training_enabled = False` , `crm_sensitive_pii_access_enabled = False`). I den mån det amerikanska moderbolaget (HubSpot, Inc.) har en underbiträdesroll skyddas detta av EU–U.S. Data Privacy Framework (DPF), EU:s standardavtalsklausuler (SCC 2021/914) och en konsekvensbedömning för tredjelandsöverföring (TIA). Dessutom förbjuder Cloudpoints datahanteringspolicy (*Data Management Policy v1.1.0*) strikt att fem (5) kategorier av uppgifter någonsin matas in i eller överförs till HubSpot-supportärenden: (1) elev- och studentuppgifter, (2) känsliga personuppgifter (särskilda kategorier), (3) detaljer om säkerhetsincidenter, (4) inloggningsuppgifter/autentiseringstoken samt (5) säkerhetsloggar.

Teknisk separering av programvaruutveckling i Egypten (Aimpulse — GDPR art. 25 och 32): **Aimpulse** är Cloudpoint Oy:s dedikerade utvecklingsenhet / partnerbolag (Kairo, Egypten), som verkar uteslutande under Cloudpoint Oy:s operativa styrning och ISO/IEC 27001:2022-certifierade ISMS. Utvecklarna i Egypten deltar aktivt i mjukvaruutvecklingen i **isolerade icke-produktionsmiljöer (`edudata-compliance-staging`) med 100 % syntetiska testdata** (*Test Data & Production Data Separation Policy CP-ISMS-DLP-001 v1.2*) och har **ingen åtkomst till operativ kunddata eller personuppgifter i produktionsmiljön (`edudata-compliance-prod`)**. Kundsupport och administration av produktionspersonuppgifter utförs uteslutande inom EU/EES (Finland). Avtalsförhållandet regleras av EU:s standardavtalsklausuler (SCC, beslut (EU) 2021/914, Module 3: biträde till biträde), dokumenterad konsekvensbedömning för dataöverföring (TIA) och oföränderliga 400-dagars revisionsloggar.

7. Tystnadsplikt

Biträdet och alla fysiska personer som arbetar för Biträdet ska iaktta såväl konfidentialitet som tystnadsplikt under behandlingen. Biträdet säkerställer att alla fysiska personer som arbetar för Biträdet är bundna av ett sekretessavtal.

Biträdet säkerställer att det finns ett sekretessavtal (NDA) med underbiträdena samt sekretessavtal mellan underbiträdet och alla fysiska personer som arbetar för underbiträdet och deltar i behandlingen. Denna tystnadsplikt består även efter det att Huvudavtalet och detta personuppgiftsbiträdesavtal har upphört att gälla.

8. Rätt till revision

Den personuppgiftsansvarige har rätt att genomföra rimliga revisioner av Biträdets lokaler och behandlingsaktiviteter för att granska den skydds- och säkerhetsnivå som föreskrivs i detta DPA samt för att bedöma Biträdets efterlevnad av bestämmelserna i detta DPA. Biträdet tillhandahåller på begäran sin

aktuella ISO/IEC 27001:2022-revisionsdokumentation (Prescient Security) och revisionssammanfattningar.

Vardera parten står för sina egna kostnader i samband med en revision (eller enligt vad som avtalats i Huvudavtalet). Den personuppgiftsansvarige ska skriftligen informera Biträdet minst 14–30 dagar i förväg innan revisionen genomförs.

Den personuppgiftsansvariges rätt till revision får utövas högst en gång per tolvmånadersperiod (12 månader), såvida inte en specifik personuppgiftsincident, ett föreläggande från tillsynsmyndighet eller en välgrundad misstanke kräver en tidigare revision.

Om en revision kan leda till att Biträdets affärs- eller företagshemligheter röjs, eller hota Biträdets immateriella rättigheter, ska en oberoende sakkunnig (som inte är konkurrent till Biträdet) anlitas för att utföra revisionen, och denna sakkunniga ska förbinda sig att vara bunden av ett sekretessavtal.

9. Underbiträden

Biträdet har rätt att anlita underbiträden för att behandla personuppgifter i samband med tillhandahållandet av Tjänsten, i den utsträckning ett sådant anlitande inte leder till bristande efterlevnad av Biträdets skyldigheter enligt detta DPA. Godkända underbiträden specificeras i Bilaga 1.

Biträdet säkerställer att anlitade underbiträden verkar under ett skriftligt personuppgiftsbiträdesavtal (GDPR art. 28.4) med Biträdet och följer dataskydds- och säkerhetsskyldigheter som är minst lika strikta som de som anges i detta avtal. Biträdet ansvarar fullt ut för sina underbiträdens arbete.

Direkt skriftlig förhandsunderrättelse (minst 30 kalenderdagar): Biträdet ska lämna ett direkt skriftligt förhandsmeddelande (via e-post till den personuppgiftsansvariges utsedda kontaktperson) **minst trettio (30) kalenderdagar i förväg** innan ett nytt underbiträde anlitas eller ett befintligt ersätts. Den personuppgiftsansvarige har trettio (30) kalenderdagar från meddelandet på sig att skriftligen invända på sakliga dataskyddsgrunder. Om parterna inte når en lösning inom 30 kalenderdagar har den personuppgiftsansvarige rätt att säga upp Tjänsten utan avgift eller sanktion.

10. Personuppgiftsincidenter (Tvåstegsmodell med 24/7-övervakning enligt NIS2 art. 23 & GDPR art. 33)

Biträdet tillämpar en dokumenterad rutin för incidenthantering (*Security Incident Management Procedure CP-ISMS-IR-002 v1.0* samt VPM-38 4-nivåers incidentrespons-SLA: P1 < 1 tim, P2 < 4 tim, P3 < 24 tim, P4 < 72 tim) och underrättar den personuppgiftsansvarige om personuppgiftsincidenter enligt en tvåstegsmodell:

- **Steg 1 — Automatiserad 24/7/365-övervakning och tidig förhandsvarning (Early Warning ≤ 24 timmar):** Produktionsinfrastrukturen (`edudata-compliance-prod`) övervakas dygnet runt 24/7/365 (inklusive helger och röda dagar) genom automatiska säkerhets- och anomalilarm. Efter att ha fått kännedom om en konstaterad eller skäligen misstänkt personuppgiftsincident skickar Biträdet en skriftlig eller automatiserad **tidig förhandsvarning (Early Warning) till den personuppgiftsansvariges kontaktperson senast inom 24 timmar** från upptäckt (med tidsstämpel för upptäckt, berörd tjänst, pågående tekniska begränsningsåtgärder och kontaktuppgifter).
- **Steg 2 — Formell DPO-bedömning och detaljerad 8-punktsrapport (nästa arbetsdag / ≤ 72 timmar):** Fördjupad teknisk utredning, rotorsaksanalys (RCA) och konsekvensbedömning av dataskyddsombudet (DPO Jasse Tenko / ISM-ansvarig Hesham Abboud, `tietosuoja@cloudpoint.fi`) genomförs under ordinarie kontorstid och levereras **nästa arbetsdag** (och alltid inom den lagstadgade 72-timmarsgränsen enligt GDPR art. 33). Rapporten innehåller samtliga åtta (8) obligatoriska informationspunkter:
  1. Tidpunkt då incidenten inträffade och upptäcktes (tidsstämplar);
  2. Beskrivning av incidentens art samt berörda system och data;
  3. Berörda kategorier av och ungefärligt antal registrerade samt berörda kategorier av och ungefärligt antal personuppgiftsposter;
  4. Eventuella berörda underbiträden eller tredjeländer;
  5. Beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten;
  6. Beskrivning av vidtagna och planerade tekniska begränsnings- och korrigeringsåtgärder för att mildra potentiella negativa effekter;
  7. Direkta kontaktuppgifter till dataskyddsombud (DPO) och informationssäkerhetsansvarig (ISM)

(`tietosuoja@cloudpoint.fi` , tfn +358 9 4257 9280);
8. Tidpunkt för nästa lägesrapport och slutlig rotorsaksanalys (RCA).

11. Återlämnande och radering av personuppgifter (30 dagar primärdata / 90 dagar säkerhetskopior)

Före avtalets upphörande har den personuppgiftsansvarige rätt att exportera samtliga kommunala bedömningar, beslut, metadata och revisionsloggar i ett strukturerat, allmänt använt och maskinläsbart format (JSON/CSV/PDF).

Efter det att detta DPA och Huvudavtalet har upphört raderar Biträdet personuppgifter enligt följande bindande tidsfrister, såvida inte tvingande EU-rätt eller nationell lag kräver lagring:

- **Primära produktionsdata (högst 30 dagar):** Alla aktiva kund- och personuppgifter raderas från produktionsdatabaserna (Cloud SQL `edudata-comp-db` , `edudata-ai-db` och Firestore) **senast inom trettio (30) dagar** efter avtalets upphörande.
- **Säkerhetskopior (högst 90 dagar efter primär radering):** Alla krypterade säkerhetskopior (Cloud SQL `edudata-comp-db` 21 dagars dagliga säkerhetskopior + 7 dagars PITR-logg, `edudata-ai-db` 7 dagars säkerhetskopior + 7 dagars PITR-logg, Firestore 7–90 dagars återställningspunkter samt Cloud Storage 7 dagars mjuk radering `604800s`) raderas och skrivs över oåterkalleligt **senast inom nittio (90) dagar** efter den primära raderingen (totalt högst 120 dagar från avtalets upphörande). Oföränderliga säkerhets- och revisionsloggar (`_Required` 400 dagar / `_Default` 365 dagar) som inte innehåller kundinnehåll löper ut automatiskt efter sin fasta säkerhetsperiod.
- **Skriftlig raderingsbekräftelse på begäran och skydd under raderingsfönstret:** Under hela raderingsperioden är uppgifterna krypterade med AES-256 och strikt spärrade från all aktiv användning. Personuppgiftsbiträdet lämnar på begäran en skriftlig raderingsbekräftelse (t.ex. per e-post) när raderingen har slutförts.

Inaktiva användarkonton raderas dessutom automatiskt från användardatabasen när 366 dagar har förflutit sedan senaste inloggning.

12. AI-assisterad behandling (Vertex AI / Gemini & Document AI) och ansvarsbegränsning

Begränsningar för AI-behandling (EU/EES-låsning och förbud mot modellträning): I den mån den personuppgiftsansvarige använder Tjänstens valfria AI-assisterade funktioner (såsom preliminär analys av dataskyddsdokument, avtal eller DPIA-bedömningar) utförs behandlingen uteslutande via **Google Cloud Vertex AI (Gemini Enterprise-modeller)** och **Google Cloud Document AI** inom EU/EES (`europe-north1` Finland och `eu` -multiregion, databas `edudata-ai-db` , radering 30 dagar / säkerhetskopior 7 dagar). Kundens data, instruktioner (prompts), dokument eller utdata **används aldrig för att träna, finjustera eller förbättra generella eller kundöverskridande AI-modeller** (*Data Management Policy v1.1.0*). Tjänsten utför inget automatiserat beslutsfattande eller profilering enligt artikel 22 i GDPR, utan fungerar uteslutande som beslutsstöd för handläggaren (*Human-in-the-Loop*).

Ansvarsbegränsning: Biträdet ansvarar inte för några indirekta skador eller följdskador under detta DPA. Biträdets sammanlagda maximala skadeståndsansvar gentemot den personuppgiftsansvarige under detta DPA regleras av Huvudavtalet (eller, om inget annat avtalats i Huvudavtalet, begränsat till ett belopp som motsvarar 100 % av de avgifter som den personuppgiftsansvarige har betalat till Biträdet för Tjänsten under de föregående 12 månaderna). Biträdet begränsar inte sitt ansvar i fall där en sådan begränsning skulle strida mot tvingande lag eller artikel 82 i GDPR.

13. Giltighetstid

Detta DPA (Version 2.0, gäller från 10 november 2026) och Edudata.io:s Användarvillkor (Version 3.1) undertecknas och träder i kraft samtidigt antingen elektroniskt via **Cloudpoint Portal (`portal.cloudpoint.fi`)** (med stark elektronisk identifiering `Bink.fi` FTN / `Swedish BankID` och en kryptografisk `SHA-256` -hash arkiverad i `GCS WORM` i `europe-north1`) eller genom en extern elektronisk underskrift på Huvudavtalet / Beställningen som registreras i `portal.cloudpoint.fi` för centraliserad styrning av avtal, moduler och DPO-kontaktuppgifter. Detta DPA förblir i kraft tills Biträdet har upphört att behandla den personuppgiftsansvariges personuppgifter och slutfört raderingen enligt avsnitt 11, eller tills det ersätts av ett annat avtal mellan Parterna avseende personuppgiftsbehandlingen.

14. Tvistlösning och jurisdiktion

Detta DPA ska vara underkastat bestämmelserna om tvistlösning och jurisdiktion i Huvudavtalet (Helsingfors tingsrätt och finsk lag, såvida inte svensk domstol och svensk lag uttryckligen har avtalats i det kommunala Huvudavtalet).

15. Ändringshantering (3-nivåers styrningsmodell för Trust Center och DPA)

Uppdateringar av detta DPA och Trust Center-dokumentationen omfattas av en 3-nivåers styrningsmodell:

- **Nivå 1 — Icke-väsentliga, förtydligande och säkerhetshöjande uppdateringar (0 dagars varsel, garanti mot försämring):** Biträdet får uppdatera Trust Center och tekniska beskrivningar utan förhandsmeddelande vid redaktionella eller tekniska förtydliganden, nya säkerhetscertifieringar (såsom ISO/IEC 27001:2022) eller förstärkta skyddsåtgärder, **under förutsättning att sådana uppdateringar aldrig ändrar de avtalade ändamålen med behandlingen eller medför någon försämring av Tjänstens säkerhets- eller dataskyddsåtaganden (*No Material Degradation Guarantee*)**.
- **Nivå 2 — Underbiträdesändringar och operativa förhandsmeddelanden (minst 30 kalenderdagars skriftligt förhandsmeddelande och rätt att invända):** Tillägg eller byte av underbiträden (GDPR art. 28.2, se avsnitt 9) och motsvarande operativa uppdateringar meddelas skriftligen (via e-post) direkt till den personuppgiftsansvariges utsedda kontaktperson **minst trettio (30) kalenderdagar innan ändringen träder i kraft**, med 30 kalenderdagars rätt att invända på sakliga dataskyddsgrunder.
- **Nivå 3 — Väsentliga ändringar i hur personuppgifter behandlas och ändringar i Huvudavtalet (minst 30 kalenderdagars förhandsmeddelande + uttryckligt elektroniskt godkännande av den personuppgiftsansvarige):** Biträdet genomför inga väsentliga ändringar i hur personuppgifter behandlas (såsom ändamål med behandlingen, kategorier av personuppgifter eller registrerade, lagringsregioner, lagringstider eller kärnförpliktelser enligt GDPR art. 28.3) utan den personuppgiftsansvariges godkännande. Sådana ändringar presenteras minst 30 kalenderdagar i förväg för elektroniskt godkännande av den personuppgiftsansvariges administratör eller beslutsfattare i **Edudata.io eller Cloudpoint Portal (`portal.cloudpoint.fi`) (med möjlighet att vidarebefordra begäran om godkännande direkt till organisationens behöriga firmatecknare)**.

Underskrifter

Parterna har godkänt och undertecknat detta DPA (Version 2.0) samt Användarvillkoren (Version 3.1) samtidigt antingen elektroniskt via **Cloudpoint Portal (`portal.cloudpoint.fi`)** (med stark e-legitimation `Bink.fi` / `Swedish BankID` och ett kryptografiskt `SHA-256` -kontrollvärde arkiverat i `GCS WORM` `europe-north1`) eller genom en extern elektronisk underskrift på Huvudavtalet / Beställningen registrerad i `portal.cloudpoint.fi` för centraliserad hantering av avtal, moduler och DPO-kontaktuppgifter.

Cloudpoint Oy / Edudata.io

Dataskyddsombud (DPO) och behörig företrädare, Cloudpoint Oy (Biträde)

Version 2.0 | Datum: 10 november 2026

[Kundens representant]

Behörig företrädare (Personuppgiftsansvarig)

Datum: [Datum för Huvudavtalets godkännande]

BILAGA 1: Beskrivning av behandlingen (Version 2.0 — 10.11.2026)

1. Ändamålet med behandlingen av personuppgifter

Biträdet behandlar personuppgifter på uppdrag av den personuppgiftsansvarige för att tillhandahålla Edudata-tjänsten, möjliggöra federerad enkel inloggning (SSO) och rollbaserad åtkomstkontroll (RBAC), administrera dataskydds- och riskbedömningar (DPIA) för digitala lärresurser och IT-system samt upprätthålla informationssäkerhet och revisionsspår i enlighet med Huvudavtalet, detta DPA och dokumenterade instruktioner från den personuppgiftsansvarige.

2. Kategorier av registrerade och modulavgränsning

Behandlingen av personuppgifter är uppdelad efter vilka moduler av Tjänsten som Kunden har beställt:

- **Kommunens personal och administratörer (*Edudata Compliance* & *Edudata Compliance Service* — kärnplattformen):** Kommunala tjänstepersoner, administratörer, rektorer, lärare, systemförvaltare, handläggare, beslutsfattare och dataskyddsombud (DPO) som använder plattformen för granskning och efterlevnadsbedömning av digitala tjänster.
- **Elever, studerande och vårdnadshavare (ENDAST vid tillvalsmodulerna *Edudata Privacy* och *Edudata Security*):** Personuppgifter om elever, studerande eller vårdnadshavare **behandlas inte** i kärnmodulen *Edudata Compliance*. Elev- eller vårdnadshavaruppgifter behandlas endast om den personuppgiftsansvarige uttryckligen har aktiverat de valfria elev- eller säkerhetsmodulerna (*Edudata Privacy* eller *Edudata Security*).
- **Skyddsregel för fritextfält (Free-Text Safeguard):** Om en användare hos den personuppgiftsansvarige av misstag skulle skriva in personuppgifter om en elev eller vårdnadshavare i ett fritextfält eller en bilaga under en bedömning, skyddas dessa uppgifter fullt ut av säkerhetsåtgärderna i detta DPA (AES-256-kryptering, TLS 1.2/1.3, logisk tenant-isolering och RBAC) och kan raderas omedelbart av kommunens administratör eller av Biträdet på begäran.

3. Typer av personuppgifter och autentisering (Inga lösenord — CP-ISMS-AUTH-001 v1.1)

Biträdet behandlar följande kategorier av personuppgifter för användarrollerna (*Lärare, Lärare+, Handläggare, Beslutsfattare, Kundadministratör* samt i tillvalsmoduler *Elev*):

- **Identitets- och organisationsuppgifter:** Unikt användar-ID (Edudata UID), för- och efternamn (visningsnamn), tjänste-e-postadress, kommun-/organisationstillhörighet och domän, tilldelad användarroll (RBAC), språkval samt valfri profilbild.
- **Federerade SSO-autentiseringsuppgifter (inga lösenord):** Tjänsten använder uteslutande federerad enkel inloggning (SSO via Microsoft Entra ID / M365 eller Google Workspace) genom Firebase Authentication i `edudata-compliance-prod`. Tekniska attribut omfattar IdP-identifierare, OAuth 2.0 / OIDC JWT-sessionstoken, datum för kontoskapande, senaste inloggningstidpunkt, sessions-ID, IP-adress samt grundläggande webbläsar-/enhetsinformation. **Edudata.io tar aldrig emot, behandlar eller lagrar användarlösenord eller autentiseringshemligheter** (*Authentication & Token Security Standard CP-ISMS-AUTH-001 v1.1*).
- **Valfri metadata för tredjepartsapplikationer (OAuth App Discovery):** Inloggnings- och behörighetsmetadata för tredjepartsapplikationer behandlas endast om Kunden har aktiverat tillvalsmodulen för OAuth-appinventering i Google Workspace / M365.

4. Ansvarsmatris för Google Cloud (7 punkter), logglagring (CP-ISMS-LOG-001 v1.2) och kommunal arkivering

7-punkters ansvarsmatris för Google Cloud: För att undanröja varje oklarhet gäller följande ansvarsfördelning för produktionsmiljön:

1. **Ägandeskap av produktionsprojektet: Cloudpoint Oy** äger och förvaltar det dedikerade Google Cloud-produktionsprojektet (`edudata-compliance-prod`).
2. **Google CDPA-avtal:** Cloudpoint Oy innehar Google Cloud Data Processing Addendum (CDPA) med **Google Cloud EMEA Limited / Google Ireland Ltd**.
3. **Regionslåsning och databaser (v1/v2-kompatibel lagringsarkitektur):** Alla baskonton, bedömningar och relationsdatabaser lagras inom EU/EES (`europe-north1` Finland och `eu` -multiregion) i Cloudpoint Oy:s centraliserade Cloud SQL-databaser (`edudata-comp-db` och `edudata-ai-db`) samt i en separat Firestore-databas. (För befintliga kunder på lagringsmodell v1 som använder den valfria modulen för SSO- och applikationsloggar kan dessa loggar lagras i kundspecifika Google Cloud Firestore-projekt, medan nya driftsättningar använder vår centraliserade, strikt isolerade EU-multitenantarkitektur v2; `TenantStorageRouter` stödjer båda modellerna sida vid sida med full bakåtkompatibilitet.)
4. **IAM-åtkomststyrning:** Cloudpoint Oy administrerar IAM-behörigheter i molnet med påtvingad hårdvarubaserad multifaktorautentisering (Yubico YubiKey 2SV) och lägsta möjliga behörighet (Least

Privilege).

5. **Kryptering och nyckelhantering:** Cloudpoint Oy ansvarar för AES-256-kryptering i vila (Google-Managed Encryption Keys, GMEK) och hantering av hemligheter i Google Cloud Secret Manager.
6. **Teknisk radering:** Cloudpoint Oy verkställer teknisk radering av primärdata och säkerhetskopior enligt avsnitt 11 (30 dagar primärdata / 90 dagar säkerhetskopior).
7. **Revisions- och säkerhetsloggning:** Cloudpoint Oy ansvarar för centraliserad ISO/IEC 27001-revisionsloggning i EU BigQuery (`edudata_compliance_logging`).

3-nivåers ISO/IEC 27001-matris för logg- och datalagring (*Logging & Retention Standard CP-ISMS-LOG-001 v1.2*):

- **Nivå 1 — Administrations- och systemhändelseloggar (400 dagar):** Oföränderliga Google Cloud `_Required` Admin Activity- och System Event-revisionsloggar samt EU BigQuery-loggarkiv (`edudata_compliance_logging`) bevaras i **400 dagar**.
- **Nivå 2 — Applikations-, databas- och nätverkssäkerhetsloggar (365 dagar / APM 15–30 dagar):** Google Cloud `_Default` -loggar, Cloud Run-loggar, Cloud SQL-revisionsloggar (`cloudsql_mysql_audit`) och VPC-säkerhetsloggar bevaras i **365 dagar**. Datadog APM-prestanda- och felspårningsloggar (med maskerade personuppgifter) bevaras i **15–30 dagar**.
- **Nivå 3 — Applikationslivscykel:** Inaktiva användarkonton raderas automatiskt efter **366 dagar** sedan senaste inloggning; obesvarade eller avvisade rollförfrågningar raderas inom **30 dagar**; telemetri i den valfria OAuth-appinventeringen sparas i högst **18 månader**.

Bedömningar, beslut och förfrågningar (lagring under hela avtalsperioden + 30 dagars raderingstid efter avtalets upphörande): Bedömningar, DPIA-underlag, beslut och förfrågningar som skapas av den personuppgiftsansvarige i Tjänsten **raderas inte innan kundens avtal med Edudata.io-tjänsten upphör** (såvida inte den personuppgiftsansvarige själv raderar dem). Den personuppgiftsansvarige har full exportmöjlighet (inklusive metadata, versionshistorik och revisionslogg) under hela avtalstiden. Efter att avtalet har upphört tillämpar vi en **raderingsfrist på 30 kalenderdagar** för radering av uppgifterna ur primära datalager (och 90 kalenderdagar för krypterade säkerhetskopior).

5. Godkända underbiträden

Biträdet anlitar följande godkända underbiträden för tillhandahållandet av Tjänsten:

Underbiträdets namn	Behandlingens omfattning, lagringsplats och skyddsåtgärder
Google Ireland Ltd (Google Cloud EMEA Limited)	Produktionsinfrastruktur i molnet (`edudata-compliance-prod`), Cloud SQL, Firestore, Firebase Auth SSO samt valfri Vertex AI (Gemini) & Document AI. Plats: **EU/EES (`europe-north1` Finland & `eu` -multiregion)**. Gäller samtliga användare av Tjänsten (Google CDPA, EU SCC & DPF).
HubSpot Ireland Ltd	Supportärendehantering (ticketing) och utsedda kundkontaktpersoner (inga elevdata; förbud mot 5 datakategorier i supportärenden). Plats: **EU/EES (`dataHostingLocation = eu1` , AWS `eu-central-1` Frankfurt, Tyskland)** (EU SCC, DPF & TIA).
Datadog, Inc.	24/7-övervakning av infrastrukturprestanda, latens och fellarm (APM) med maskering av personuppgifter (ingen bedömningsdata). Lagringstid: **15–30 dagar** (EU SCC & DPF).
Aimpulse (Cloudpoint Oy:s dedikerade utvecklingsenhet / partnerbolag, Kairo, Egypten)	Mjukvaruutveckling uteslutande under Cloudpoint Oy:s operativa styrning och ISO/IEC 27001:2022-certifierade ISMS. Arbetar **uteslutande i isolerad icke-produktionsmiljö (`edudata-compliance-staging`) med 100 % syntetiska testdata** (`CP-ISMS-DLP-001 v1.2`); **ingen åtkomst till operativ kunddata eller personuppgifter i produktionsmiljön (`edudata-compliance-prod`)**. Plats: Egypten (EU SCC Module 3, TIA & 400-dagars revisionslogg).

Underbiträdets namn	Behandlingens omfattning, lagringsplats och skyddsåtgärder
Online Partner AB	**Villkorad partner (Sverige):** Tillämpligt **endast** där Kunden har tecknat avtal via Online Partner AB som lokal återförsäljare eller 1:a linjens supportpartner. Behandlar inga personuppgifter för kommuner med direktavtal med Cloudpoint Oy. Plats: Sverige (EU/EES).
Visma AB	**Endast Cloudpoints egen B2B-fakturering:** Används uteslutande för Cloudpoint Oy:s lagstadgade B2B-ekonomi och fakturering där Cloudpoint agerar självständig personuppgiftsansvarig. Visma AB behandlar aldrig plattforms- eller bedömningsdata i Edudata. Plats: EU/EES.

6. Internationella överföringar

Alla produktionsdatabaser och allt kundinnehåll i Tjänsten lagras inom EU/EES (`europe-north1` Finland och `eu` -multiregion). I de fall en överföring utanför EES aktualiseras via ett underbiträde enligt kapitel V i GDPR baseras överföringen på EU-kommissionens beslut om adekvat skyddsnivå (såsom EU–U.S. Data Privacy Framework) och/eller EU-kommissionens standardavtalsklausuler (SCC 2021/914), kompletterat med konsekvensbedömning (TIA) och tekniska skyddsåtgärder.

BILAGA 2: Tekniska och organisatoriska säkerhetsåtgärder (Version 2.0 — 10.11.2026)

Biträdet genomför och upprätthåller tekniska och organisatoriska säkerhetsåtgärder i enlighet med artikel 32 i GDPR och sitt ISO/IEC 27001:2022-certifierade ledningssystem för informationssäkerhet (ISMS).

Varje person som är auktoriserad av Biträdet att behandla personuppgifter omfattas av bindande sekretessåtaganden och genomgår regelbunden utbildning i dataskydd och informationssäkerhet.

- **Cloudpoint Oy:s ISO/IEC 27001:2022-certifierade ISMS (Prescient Security LLC, #123522) & kontinuerlig Vanta-övervakning:** Cloudpoint Oy (2325703-6) upprätthåller ett **ISO/IEC 27001:2022-certifierat** ledningssystem för informationssäkerhet (ISMS, *Statement of Applicability v1.2* 20.10.2026; certifikat `#123522` Issue 1, utfärdat 18.11.2026, giltigt till 17.11.2029; utfärdat av IAS-ackrediterade **Prescient Security LLC**, MSCB-267, IAF MLA; huvudkontor Malminkaari 17-19 B, Helsingfors). Omfattningen täcker molnekosystem för offentlig sektor, utbildning och företag, GCP- och Google Workspace-infrastruktur samt avdelningarna IT, mjukvaruutveckling, HR, informationssäkerhet, juridik och ekonomi. Efterlevnaden övervakas kontinuerligt i realtid via Vanta, inklusive kontrollerna VPM-38 (nätverkshärdning, patch- och incidenthantering), VPM-3 (sårbarhets- och riskhantering) samt AST-4 – AST-9 (livscykelhantering för tillgångar och ändpunkter).
- **Logisk multi-tenant-isolering och kryptografiskt skydd (AES-256 & TLS 1.3):** Varje kommuns data är strikt isolerad genom organisations-ID-baserad logisk fleranvändarseparation (multi-tenancy) på både applikations- och databasnivå. Alla kunddata, databaser och säkerhetskopior krypteras i vila med AES-256 (Google-Managed Encryption Keys, GMEK) och under överföring med TLS 1.3 (lägst TLS 1.2). Databasanslutningar till Cloud SQL kräver mTLS-klientcertifikat (`TRUSTED_CLIENT_CERTIFICATE_REQUIRED`).
- **Åtkomstkontroll (Access Control Policy v1.1.0) & hårdvarubaserad YubiKey (U2F/FIDO2) MFA:** All åtkomst till produktionsmiljöer styrs av rollbaserad IAM enligt principen om lägsta behörighet (Least Privilege) och loggas i oföränderliga revisionsloggar. Alla administratörsinloggningar kräver obligatorisk multifaktorautentisering med hårdvarunycklar av typen Yubico YubiKey (U2F/FIDO2) samt fullständig hårddiskkryptering (Full Disk Encryption, FDE) på arbetsstationer. Behörigheter granskas kvartalsvis och återkallas inom 24 timmar vid avslutat uppdrag.
- **Oberoende penetrationstestning (juni 2026) & sårbarhetshantering (7 dagar / 14 dagar SLA):** Ett oberoende externt penetrationstest av webbapplikationen och molninfrastrukturen genomfördes i juni 2026 (*CP-ISMS-VSR-002 v1.0*), där samtliga identifierade avvikelser åtgärdades och verifierades per **16 augusti 2026**. Enligt *Vulnerability Management Procedure v2.1* åtgärdas kritiska sårbarheter (Critical CVEs) inom **7 dagar** och högrisksårbarheter (High CVEs) inom **14 dagar** (med automatisk skanning i Bitbucket Pipelines och Google Artifact Registry).

- **Återställningstid (RTO), återställningspunkt (RPO) och verifierade återställningstester (CP-ISMS-BIA-001 v1.1 & CP-ISMS-BCDR-002 v1.1):**
- Cloud Run API-tjänster och Firebase Auth SSO: **RTO < 15 minuter, RPO = 0** (multizons hög tillgänglighet).
- Cloud SQL-produktionsdatabaser (`edudata-comp-db`, `edudata-ai-db`): **RTO < 1 timme**, RPO = 24 timmar (dagliga automatiska säkerhetskopior) och **nära noll (near-zero RPO)** genom 7 dagars kontinuerlig Point-in-Time Recovery (PITR)-loggning; hela plattformens RTO < 4 timmar.
- **Verifierade återställningsövningar:** Fullständig återställningsövning av produktionsdatabasen genomfördes med 100 % dataintegritet den **3 juni 2026 (26 minuter total återställningstid)** och PITR-återställningsövning den **18 oktober 2026 (9 minuter och 52 sekunder)**.
- **3-nivåers dataklassificering och fysisk säkerhet (Malminkaari 17-19B, 00700 Helsinki):** Kunddata och personuppgifter klassificeras som Confidential / Restricted i Google Cloud (`europe-north1` Finland). Kontorslokalerna på Malminkaari 17-19B, 00700 Helsinki, Finland har passerkontroll, bevakning och 24/7 kameraövervakning, och Google Clouds EU-datacenter är certifierade enligt ISO 27001, ISO 27017, ISO 27018 och SOC 2/3.

Säkerhetskontroller vid programvaruutveckling (SDLC):

- Strikt separerade utvecklings-, test- (`edudata-compliance-staging`) och produktionsmiljöer (`edudata-compliance-prod`); utveckling sker uteslutande med 100 % syntetiska testdata (`CP-ISMS-DLP-001 v1.2`).
- Obligatorisk kollegial kodgranskning (4-eyes peer review) och godkännande av senior utvecklare före varje produktionssättning.
- Automatiserad CI/CD-sårbarhets- och beroendeskanning (Bitbucket Pipelines & Google Artifact Registry).
- Lokal utveckling sker endast på centralt hanterade (MDM) bärbara datorer med fullständig diskkryptering (FDE).
- Regelbunden OWASP- och Google Cloud-säkerhetsutbildning för utvecklare samt löpande bevakning av cyberhot och sårbarheter.

Ansvarsfördelning för molninfrastruktur och Kundens ansvar:

Cloudpoint Oy äger och förvaltar produktionsmiljön i Google Cloud (`edudata-compliance-prod`) och ansvarar för dess säkerhet enligt denna Bilaga 2. Kunden ansvarar i egenskap av personuppgiftsansvarig för att administrera sina användares behörigheter i sin egen identitetsmiljö (Microsoft Entra ID / Google Workspace) samt för den lagliga grunden för de uppgifter som registreras i Tjänsten.

Tjänsten driftas i Google Cloud (`europe-north1` Finland). Ytterligare information om Googles fysiska och tekniska molnsäkerhet finns i Google Cloud Security Whitepapers.