Data Processing Agreement (DPA)

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

[OFFICIAL PUBLISHED · H-AI-H] Human-verified official EN primary master (H-AI-H Human–AI–Human governance).
Verification Role: LEGAL_COUNSEL_AND_RELEASE_OWNER | **Verified UTC:** 2026-11-25T08:36:41Z

Document ID	`edudata.dpa.en.v2.0.0-r01`	**Version**	**v2.0** (`v2.0.0-r01`)
Effective Date	2026-11-10	**Next Review Due**	2027-11-10
Language	English (en-GB)	**Security Certification**	ISO/IEC 27001:2022 (#123522, Prescient Security LLC)
Governance Model	**H-AI-H (Human–AI–Human)**	**Language Authority**	Primary Authoritative Master (EN)
Canonical Web URL	`https://www.edudata.io/trust-center#dpa`		
Canonical Body SHA-256 (UTF-8 NFC)	`191c2577b23dea879ab21745aebf83019c4975401ec6997e7b246d5063d483ba`		

The legally binding DPA governing personal data processing for the Edudata.io platform between the Data Processor and the Data Controller.

EDUDATA.IO DATA PROCESSING AGREEMENT

Version 2.0 | Effective: November 10, 2026

This Data Processing Agreement (DPA) is for EDUDATA ('Service'), which is run and provided by Cloudpoint Oy and is supplemental to, and forms an integral part of, the Main Agreement, including the Terms of Service ('ToS'), and is effective upon its acceptance. In case of any conflict or inconsistency with the terms of the entirety of the Agreements, this DPA will take precedence to the extent of such conflict or inconsistency.

Contracting Parties:

Data Processor: Cloudpoint Oy (2325703-6) / Edudata.io (3460068-8), part of Cloudpoint Oy (2325703-6, VAT ID FI23257036), Malminkaari 17-19B, 00700 Helsinki, Finland (Data Protection Officer / DPO: Jasse Tenko / ISM Leader: Hesham Abboud, tietosuoja@cloudpoint.fi, support: info@edudata.io, tel. +358 9 4257 9280)
Data Controller: Customer

1. Definitions

- **Data Controller:** Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; ("Controller").
- **Data Processor:** Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; ("Processor").
- **GDPR:** General Data Protection Regulation EU 2016/679.
- **Personal Data:** Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier

or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **Processing:** Means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Any other terms not defined in this DPA shall have the same meaning as in the GDPR.

2. Background and Purpose

The Controller has selected the service provider (Cloudpoint Oy) to act as a Processor in accordance with Article 28(3) of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, “GDPR”).

This DPA forms an integral part of the Main Agreement concluded between the Parties under which the Processor shall provide the Controller with the Edudata service, which consists of Edudata Compliance, Edudata Compliance Service, Edudata Privacy and Edudata Security, unless otherwise agreed in the Main Agreement.

The Processor will process information relating to an identified or identifiable natural person on behalf of the Controller. The detailed data processing practices are described in Annex 1 to this DPA.

The purpose of this DPA is to agree on the rights and obligations of the Parties involved in the processing activities as required by the GDPR and to safeguard the freedoms and rights of the data subject during processing.

3. Roles and Responsibilities

The Processor shall process personal data in accordance with this DPA and the documented instructions of the Controller. The Processor shall not use personal data for any purpose other than agreed in this DPA and in the instruction of the Controller. The instructions of the Controller must be compliant with the applicable data protection laws and consistent with this DPA.

If the Processor notices that any instruction given by the Controller is not compliant with the applicable laws or if they are insufficient, the Processor shall inform the Controller of such non-compliance.

The Controller is responsible for having a legal basis for the processing of personal data, for informing the data subjects of the processing of their personal data and for other data controller obligations set out in the GDPR.

The Controller is responsible for informing the Processor of the contact details of their Data Protection Officer and to ensure the contact details are up to date. Contact details are required in order for the Processor to comply with the notification obligations in case of a data breach incident.

4. Technical and Organizational Measures

The Processor shall maintain appropriate technical and organizational security measures to protect against unauthorized or unlawful processing or access and against accidental loss, destruction or damage. When choosing the security measures, the Processor must take into account the state of the art, the costs of implementation and the nature, scope, context and purpose of the processing as well as the risk of varying likelihood and severity to the rights and freedoms of natural persons.

A detailed description of the employed measures is stipulated in Annex 2 to this DPA.

5. Obligation to Assist and DSAR Response SLA

The Processor processes personal data in accordance with this DPA and the instructions from the Data Controller and in compliance with the data protection legislation. The Processor must take the necessary measures to protect personal data from processing practices that are not in line with the terms of this DPA, the instructions or data protection legislation.

The Processor undertakes to ensure that those working for the Processor comply with the terms of this DPA and are informed of the relevant legislation. The Processor supports the Controller in ensuring the fulfillment of the obligations laid down in Articles 32–36 of the GDPR (including Data Protection Impact Assessments / DPIAs and prior consultations), when requested by the Controller.

The Processor undertakes to notify the Controller and forward any Data Subject Access Requests (DSARs) or other requests concerning the exercise of data subject rights under Chapter III of the GDPR **within no more than five (5) business days** of receipt. The Processor supports the Controller with appropriate technical and organizational measures so that the Controller is able to respond to such requests within statutory deadlines.

Standard assistance pursuant to GDPR Article 28 is included in the subscription fee at no additional cost. Only if the Controller requests bespoke software development or extensive manual extraction outside the standard functionality of the Service shall the Parties agree in writing in advance on reasonable compensation.

6. International Transfers, HubSpot `eu1` Governance, and Separation of Software Development

We process and store core platform personal data on servers located in the European Union / European Economic Area (Google Cloud region `europe-north1` in Finland and backup replication in `europe-west1` in Belgium). As a rule, there are no regular transfers of production databases outside the EU/EEA.

HubSpot `eu1` Governance & 5-Category Support Ticket Prohibition: For B2B customer relationship management and technical support ticketing concerning Customer-designated contact persons and administrators, **HubSpot Ireland Ltd** is pinned to the European regional data center `dataHostingLocation = eu1` (`app-eu1.hubspot.com`, AWS `eu-central-1` Frankfurt, Germany, with failover in Dublin, Ireland). The portal enforces HubSpot's GDPR Compliance Toolkit (including **GDPR Permanent Delete** within 90 days of contract termination or upon request) and Breeze AI locks (`customer_data_training_enabled = False` and `crm_sensitive_pii_access_enabled = False`). Any ancillary global support access by HubSpot, Inc. is safeguarded by the EU-U.S. Data Privacy Framework (DPF), European Commission Standard Contractual Clauses (SCCs 2021/914), and a Transfer Impact Assessment (TIA). Pursuant to Cloudpoint's `Data Management Policy v1.1.0`, an explicit **5-Category Support Ticket Prohibition** applies: (1) student data, (2) sensitive personal data (GDPR Art. 9 special categories), (3) security incident details, (4) authentication credentials or tokens, and (5) security logs must never be entered into or transferred to HubSpot support tickets.

GDPR Art. 25 & 32 Separation of Software Development in Egypt (`Aimpulse`): Aimpulse is Cloudpoint Oy's dedicated development unit / partner entity (Cairo, Egypt), operating exclusively under Cloudpoint Oy's operational control and ISO/IEC 27001:2022 certified ISMS. Egyptian developers actively participate in software development in isolated non-production environments (`edudata-compliance-staging`) using **100% synthetic/dummy data** (`CP-ISMS-DLP-001 v1.2`) and have **no access to operational customer data or personal data in the production environment (`edudata-compliance-prod`)**. Customer support and production personal data administration are performed exclusively within the EU/EEA (Finland). The relationship is governed by EU Standard Contractual Clauses (Decision (EU) 2021/914, Module 3: Processor-to-Processor), a documented Transfer Impact Assessment (TIA), and 400-day immutable Admin Activity audit logs.

7. Duty of Confidentiality

The Processor and all natural persons working for the Processor shall observe both confidentiality and professional secrecy during the Processing. The Processor ensures that all natural persons working for the Processor are bound by a confidentiality agreement.

The Processor ensures that there is a non-disclosure agreement (NDA) with the subprocessors and a confidentiality agreement in place between the subprocessor and all natural persons working for the subprocessor participating in the processing. This duty of confidentiality shall remain in force after the termination of the Main Agreement and this DPA.

8. Right to Audit

The Controller shall have the right to reasonably audit the facilities and processing activities of the Processor to examine the level of protection and security provided for under this DPA, and to assess the Processor’s compliance with the provisions of this DPA.

The Controller shall bear all costs for undertaking an audit. The Controller shall inform the Processor in writing at least 30 working days (or at least 14–30 days in public-sector JIT agreements) in advance before conducting the audit.

The Controller's right to audit shall be exercisable no more than once every twelve (12) months, unless a specific data breach or substantiated concern necessitates an earlier audit.

Where an audit may lead to the disclosure of business or trade secrets of the Processor, or threaten the intellectual property rights of the Processor, an independent expert must be employed to carry out the audit, and such expert shall agree to be bound by a confidentiality agreement.

9. Subprocessors

The Processor shall have the right to involve subprocessors to process personal data in connection with the provision of the Service, to the extent such appointment does not lead to non-compliance with the Processor’s obligations under this DPA.

The Processor ensures that the involved subprocessors operate under a written data processing agreement with the Processor and comply with data protection obligations no less protective than those set out in this DPA (GDPR Article 28(4)).

The Processor shall provide the Controller with **direct written notification (via email to the Controller’s designated contact person) at least thirty (30) calendar days in advance** of adding or replacing any subprocessor. The Controller has **thirty (30) calendar days** from receipt of the notification to object in writing on reasonable data protection grounds. If the Parties cannot reach a mutually acceptable resolution within the 30-day notice period, the Controller shall have the right to terminate the affected Service without penalty.

10. Personal Data Breaches (Two-Stage NIS2 Art. 23 & GDPR Art. 33 Model)

In accordance with the Processor’s Incident Response Procedure (`CP-ISMS-IR-002 v1.0` ; VPM-38 4-tier incident response SLA: P1 < 1h, P2 < 4h, P3 < 24h, P4 < 72h), personal data breach detection and notification follow a two-stage model:

- **Stage 1 — Automated 24/7/365 Monitoring & Preliminary Early Warning (≤ 24 hours):** Production infrastructure is monitored 24/7/365 (including weekends and public holidays) by automated security and anomaly detection alerts (Google Cloud Security Command Center, Cloud Logging, and Datadog). Upon becoming aware of an actual or reasonably suspected personal data breach, the Processor sends an initial written or automated **Early Warning** to the Controller’s designated contact person **no later than 24 hours** after detection (stating the detection timestamp, affected service, active technical containment measures, and contact points).
- **Stage 2 — Formal DPO Assessment & Detailed 8-Point Report (Next Business Day / ≤ 72 hours):** Formal human-verified investigation, root-cause analysis (RCA), and impact evaluation by the Data Protection Officer (`tietosuoja@cloudpoint.fi` , DPO Jasse Tenko / ISM Leader Hesham Abboud) commence immediately and, for alerts triggered outside normal business hours, on the **next business day**, delivering a comprehensive GDPR Article 33(3) report within 24–48 hours of confirmation and always within the statutory **72-hour** ceiling.

The Processor’s detailed 8-point breach report to the Controller includes: (1) description of the nature of the breach, (2) categories and approximate number of affected data subjects, (3) categories and approximate number of affected personal data records, (4) name and contact details of the DPO / contact point, (5) likely consequences of the breach, (6) remedial and mitigating measures taken or proposed, (7) exact timestamps of detection, containment, and resolution along with technical root cause, and (8) audit trail documentation required for the Controller’s supervisory authority notifications.

11. Return and Deletion of Personal Data

Prior to the termination or expiry of the Main Agreement, the Controller has the right to export its assessments, decisions, and compliance records in structured, machine-readable formats (CSV / JSON / PDF). After the Controller has permanently ceased to use the Service:

- **Primary Production Databases (within 30 calendar days):** The Processor permanently deletes all active Customer personal data from primary production databases within no more than **thirty (30) calendar days** of the effective termination date.
- **Encrypted Backups & Snapshots (within 90 calendar days):** Residual data in encrypted backups is automatically and irreversibly overwritten as backup cycles expire, and within no more than **ninety (90) calendar days**: Cloud SQL `edudata-comp-db` (21-day automated backups + 7-day PITR), Cloud SQL `edudata-ai-db` (7-day automated backups + 7-day PITR), Firestore managed exports (7 to max 90 days), and Cloud Storage buckets (7-day soft-delete window / `604800` seconds).
- **Cryptographic Safeguards & Deletion Confirmation on Request:** Throughout the deletion and backup expiry window, all data remains encrypted at rest using AES-256 and blocked from active processing. Upon request, the Processor provides a written confirmation of deletion (e.g., via email) once deletion has been completed.

Inactive user accounts are deleted from the user database automatically when 366 days have passed since the system's last processing of login information.

12. AI-Assisted Processing, No Automated Decision-Making, and Limitation of Liability

AI-Assisted Processing (Google Cloud Vertex AI & Document AI): To deliver automated document analysis and compliance assessment assistance within the Service, the Processor utilizes **Google Cloud Vertex AI (Gemini enterprise models)** and **Google Cloud Document AI** within EU regions (`europe-north1` Finland and `eu` multi-region), backed by the dedicated PostgreSQL database `edudata-ai-db` (30-day active deletion, 7-day backup expiry). In accordance with Google Cloud's enterprise data governance and Cloudpoint Oy's `Data Management Policy v1.1.0`:

- **Zero AI Model Training:** Customer personal data, uploaded documents, prompts, and generated outputs are **never** used to train, fine-tune, or improve Google's, Cloudpoint Oy's, or any third party's foundation AI models.
- **No Automated Decision-Making or Profiling (GDPR Art. 22):** AI features in Edudata.io act strictly as assistive drafting and structuring tools for authorized Customer personnel (*Human-in-the-Loop*). The Service performs zero student or staff profiling and makes no solely automated decisions producing legal or similarly significant effects under GDPR Article 22.

Limitation of Liability: The Processor shall not be liable for any indirect or consequential damages under this DPA. The aggregate maximum liability of the Processor to the Controller under this DPA shall be limited to a sum corresponding to 100% of the payments made by the Controller to the Processor for the Service during the previous 12 months, unless otherwise agreed in the Main Agreement or where such limitation would be unlawful.

13. Term

This DPA (Version 2.0, effective November 10, 2026) and the Edudata.io Terms of Service (Version 3.1) are executed and enter into force simultaneously either electronically via the **Cloudpoint Portal (`portal.cloudpoint.fi`)** (using strong electronic identification `Bink.fi` FTN / `Swedish BankID` with a cryptographic `SHA-256` hash archived in `GCS WORM` in `europe-north1`) or via an external electronic signature on the Main Agreement / Order registered in `portal.cloudpoint.fi` for centralized contract, module, and DPO contact governance. This DPA shall continue to be in force until the Processor has ceased to process the Controller's personal data and completed its deletion obligations under Section 11, or until replaced by another agreement between the Parties with regard to the data processing.

14. Dispute Resolution and Jurisdiction

This DPA shall be subject to the provisions regarding dispute resolution and jurisdiction set out in the Main Agreement (Helsinki District Court and Finnish law).

15. Amendments and 3-Tier Change Governance

Updates to this DPA and the Trust Center documentation are governed by a three-tier change governance model:

- **Tier 1 — Editorial, Documentation & Security Enhancements (0 days' notice):** Typographical clarifications, updated audit certificates, and technical security improvements take effect upon publication. The Processor warrants a strict **No Material Degradation Guarantee**: no Tier 1 update shall reduce the overall level of information security, data privacy, or contractual commitments.
- **Tier 2 — Subprocessor Updates & Operational Notices (30 calendar days' prior written notice & right to object):** Any addition or replacement of a subprocessor (pursuant to GDPR Art. 28(2) and Section 9) is communicated via direct written email notice at least **thirty (30) calendar days in advance**, accompanied by the Controller's right to object and terminate without penalty.
- **Tier 3 — Material Changes to How Personal Data Is Processed & Custom Main Agreement Amendments (30 calendar days' prior notice + Explicit Electronic Controller Approval):** The Processor never makes material changes to how personal data is processed (such as processing purposes, categories of personal data or data subjects, storage regions, data retention periods, or core GDPR Art. 28(3) obligations) without the Controller's approval. Any such change is presented at least 30 calendar days in advance for electronic approval by the Controller's designated administrator or decision-maker via **Edudata.io or the Cloudpoint Portal (`portal.cloudpoint.fi`) (including the capability to forward the approval request directly to the organization's authorized signatory)**.

Signatures

The Parties below have accepted and executed this DPA (Version 2.0) and the Terms of Service (Version 3.1) simultaneously either electronically via the **Cloudpoint Portal (`portal.cloudpoint.fi`)** (using strong e-ID `Bink.fi` / `Swedish BankID` with a cryptographic `SHA-256` hash archived in `GCS WORM` `europe-north1`) or via an external electronic signature on the Main Agreement / Order registered in `portal.cloudpoint.fi` for centralized contract, module, and DPO contact governance.

Cloudpoint Oy / Edudata.io

Data Protection Officer (DPO) & Authorized Corporate Signatory, Cloudpoint Oy (Processor)

Date: November 10, 2026

[Customer Representative Signature]

Authorized Signatory (Controller)

Date: [Date of Acceptance]

ANNEX 1: Description of the Data Processing (Version 2.0 — 10.11.2026)

1. Purpose of the processing of Personal Data

The Processor shall process personal data on behalf of the Controller for the purposes of providing the Service, to the extent such provision of the Service requires processing of personal data by the Processor. The processing shall be carried out in accordance with the Main Agreement, this DPA, and the documented instructions given by the Controller.

2. Categories of Data Subjects and Module Matrix

The categories of data subjects depend on the specific Edudata.io modules subscribed to and enabled by the Controller:

- **Core Module — *Edudata Compliance* & *Edudata Compliance Service* (digital service risk & compliance assessments):** Authenticated users and data subjects consist **exclusively of Teachers, Draftsmen, Decision Makers, Data Protection Officers, and Customer Administrators** (roles: *Teacher, Teacher+, Draftsman, Decision Maker, Customer Admin*). Students do not log in to or use the core *Edudata Compliance* module.
- **Optional Add-On Modules — *Edudata Privacy* & *Edudata Security*:** Only where the Customer has explicitly contracted for and enabled the optional third-party OAuth audit or account security modules

may authentication and authorization metadata also concern **Students / Learners** (role: *Student*) alongside staff members.

Free-Text Safeguard: Although *Edudata Compliance* is designed to evaluate software applications rather than individuals, if a Customer user inadvertently enters personal data into free-text assessment comment fields, the Processor protects all database content under the exact same production-grade technical and organizational safeguards (AES-256 encryption, TLS 1.3, strict RBAC, and deletion schedules).

3. Types of Personal Data and Federated Zero-Passwords Authentication

In accordance with the Edudata.io Authentication Policy (`CP-ISMS-AUTH-001 v1.1`), the platform enforces a strict **Zero Passwords** architecture: user authentication is performed exclusively via federated Single Sign-On (SSO) through the Customer's Identity Provider (**Microsoft Entra ID** or **Google Workspace**) using OAuth 2.0 / OpenID Connect. Edudata.io never collects, processes, or stores user passwords or password hashes.

Depending on the enabled modules, the Processor may process the following types of personal data:

- First name and last name
- Work / school email address
- Edudata ID and federated SSO subject identifier
- Role of the user and organizational unit
- Organization (Customer) name and domain
- Language preference and profile picture (if passed via SSO)
- IP address and login timestamps (security audit logs)
- Browser and device technical metadata
- User creation date and user last login
- 3rd party service OAuth login metadata (only in optional *Edudata Privacy / Security* modules)

4. Google Cloud Architecture, Log Retention, and Duration of Processing

7-Point Google Cloud Responsibility Matrix:

1. **Production Project Ownership:** The Edudata.io production environment is hosted in the Google Cloud project `edudata-compliance-prod` , which is **owned, managed, and secured by Cloudpoint Oy** in region `europe-north1` (Hamina, Finland) with backup replication in `europe-west1` (Belgium).
2. **Contractual Chain (Google CDPA):** Cloudpoint Oy has executed the *Google Cloud Data Processing Addendum (CDPA)* directly with **Google Cloud EMEA Limited / Google Ireland Ltd**. The Customer is not required to enter into a separate Google Cloud agreement to use Edudata.io.
3. **Platform Databases:** Application records, assessments, and user profiles are stored by Cloudpoint Oy in dedicated Cloud SQL for PostgreSQL instances (`edudata-comp-db` and `edudata-ai-db`) and a separate Firestore database within `edudata-compliance-prod` in `europe-north1` .
4. **Multi-Tenant Logical Isolation:** Each Customer's data is logically isolated via verified organization tenant identifiers and strict Role-Based Access Control (RBAC).
5. **Cryptographic Keys & Certificates:** Cloudpoint Oy manages AES-256 encryption at rest, TLS 1.3 in transit, and mandatory mutual TLS client certificate authentication (`TRUSTED_CLIENT_CERTIFICATE_REQUIRED`) for Cloud SQL database connections.
6. **Centralized Audit Logging:** Security and administrative audit logs are aggregated into Cloudpoint Oy's centralized logging project (EU BigQuery sink `edudata_compliance_logging`) in compliance with ISO/IEC 27001:2022.
7. **v1/v2 Storage Architecture Compatibility (`TenantStorageRouter`) & Optional Customer Log Sink:** For existing/legacy customers under the v1 storage model using the optional SSO & App Log telemetry module, those specific SSO/App logs may reside in customer-specific Google Cloud Firestore projects, whereas new deployments use the centralized, strictly isolated EU multi-tenant storage architecture (v2), with `TenantStorageRouter` supporting both models side-by-side with full backwards compatibility.

3-Tier ISO/IEC 27001:2022 Log Retention Matrix (`A.8.15` & `A.8.16` — `CP-ISMS-LOG-001 v1.2`):

- **Tier 1 — Admin Activity & Security Audit Logs (400 days):** Google Cloud Admin Activity (`_Required`) audit logs and security audit events routed to the EU BigQuery sink `edudata_compliance_logging` are retained immutably for **400 days**.
- **Tier 2 — Operational Application & Data Access Logs (365 days / 15–30 days APM):** System and application logs in Google Cloud Logging `_Default` buckets are retained for **365 days** to support forensic security investigations under ISO/IEC 27001 controls `A.8.15` and `A.8.16`. Masked performance and error telemetry in Datadog APM is retained for **15–30 days**.
- **Tier 3 — Application Data Lifecycle & Controller-Governed Municipal Archiving:**
- **Inactive User Accounts:** Automatically deleted from the user database when **366 days** have elapsed since the last login activity.
- **Role Request Timeout:** Denied or unresponded role requests are automatically deleted after **30 days**.
- **Third-Party OAuth Telemetry (optional *Edudata Privacy* module):** Retained for up to **18 months**.
- **Assessments, Decisions & Requests (Retained for the Entire Duration of the Agreement + 30-Day Deletion Period After Termination):** Assessments, DPIAs, decisions, and requests are **not deleted before the Customer's agreement with the Edudata.io service terminates** (unless deleted earlier by Customer Administrators), and can be exported at any time during the term of the Main Agreement. Following termination of the Customer's agreement, we apply a **30-calendar-day deletion period** for removal of the data from primary data stores (with encrypted backups overwritten within 90 calendar days).
- **Post-Termination Deletion:** Primary databases are deleted within **30 calendar days** and encrypted backups are irreversibly overwritten within **90 calendar days** (Section 11).

5. Authorized Subprocessors

The Processor engages the following subprocessors in connection with the provision and security of the Service:

Subprocessor Name	Role & Scope of Processing	Processing Location & Transfer Safeguards
Google Ireland Ltd (Google Cloud EMEA Limited)	Core production cloud infrastructure (`edudata-compliance-prod`), Cloud SQL databases (`edudata-comp-db` , `edudata-ai-db`), Firestore database, Cloud Storage, Cloud Logging / BigQuery, and AI-assisted document/assessment processing via Vertex AI (Gemini) and Document AI with zero model training. Applies to all users of the Service.	**EU/EEA:** `europe-north1` (Finland), backups in `europe-west1` (Belgium), and `eu` multi-region. Google CDPA, EU-U.S. DPF & SCCs (2021/914).
HubSpot Ireland Ltd	B2B CRM portal and technical support ticketing for Customer-designated contact persons and administrators only (subject to the strict 5-category support ticket prohibition and Breeze AI locks).	**EU/EEA:** Regional data center `eu1` (AWS `eu-central-1` Frankfurt, Germany; failover in Dublin, Ireland). EU-U.S. DPF, SCCs (2021/914) & TIA.
Datadog, Inc.	Infrastructure security monitoring, anomaly detection, and masked APM telemetry (15–30 day retention).	**EU / USA:** EU-U.S. Data Privacy Framework (DPF), SCCs (2021/914) & TIA.

Subprocessor Name	Role & Scope of Processing	Processing Location & Transfer Safeguards
Aimpulse (Cloudpoint Oy's dedicated development unit / partner entity, Cairo, Egypt)	Software development operating exclusively under Cloudpoint Oy's operational control and ISO/IEC 27001:2022 certified ISMS in isolated non-production environments (`edudata-compliance-staging`) using 100% synthetic/dummy data (`CP-ISMS-DLP-001 v1.2`); **no access to operational customer data or personal data in the production environment (`edudata-compliance-prod`)**.	**Egypt:** Isolated non-production environment, EU SCCs (Module 3), TIA & 400-day Admin Activity audit logs.
Online Partner AB	Local first-line support and reseller partner in Sweden. **Applicable ONLY where contracted by the Customer as local partner/reseller**; does not process data for direct Cloudpoint Oy municipal customers.	**EU/EEA:** Sweden.
Visma AB	Used solely for Cloudpoint Oy's statutory B2B financial invoicing and accounting as an independent Controller; **does not process Edudata.io platform assessment or user data**.	**EU/EEA:** Finland / Sweden.

6. International transfers

All core Edudata.io production data is stored and processed within the European Union / European Economic Area (`europe-north1` Finland and `europe-west1` Belgium). Where subprocessors involve cross-border processing or ancillary engineering support outside the EU/EEA (as detailed in Section 6 of the DPA and Table 5 above), transfers are safeguarded in accordance with Chapter V of the GDPR via an European Commission adequacy decision (EU-U.S. Data Privacy Framework), Standard Contractual Clauses (SCCs 2021/914, Modules 2 and 3), documented Transfer Impact Assessments (TIAs), and supplementary technical measures (AES-256/TLS 1.3 encryption and synthetic data isolation).

ANNEX 2: Technical and Organizational Security Measures (Version 2.0 — 10.11.2026)

The Processor implements and maintains an ISO/IEC 27001:2022 certified Information Security Management System (ISMS) designed to protect the confidentiality, integrity, and availability of personal data in accordance with GDPR Article 32.

- **Cloudpoint Oy ISO/IEC 27001:2022 Certified ISMS (Prescient Security LLC, #123522) & Continuous GRC Monitoring (Vanta):** Cloudpoint Oy (2325703-6) operates an **ISO/IEC 27001:2022 certified ISMS** (*Statement of Applicability v1.2* dated 20 October 2026; Certificate `#123522` Issue 1, issued 18 November 2026, valid until 17 November 2029 by IAS-accredited certification body **Prescient Security LLC**, MSCB-267, IAF MLA; Head Office Malminkaari 17-19 B, Helsinki; certified scope covering cloud-based ecosystems for public sector, education & private enterprise, GCP & Google Workspace infrastructure, and all 6 corporate departments) and is continuously monitored via Vanta (including controls VPM-38, VPM-3, and AST-4 – AST-9).
- **Cryptographic Protection & Database mTLS (AES-256 & TLS 1.3):** All customer data, databases, and backups are encrypted at rest using AES-256 and in transit using TLS 1.3 (minimum TLS 1.2). Cloud SQL database instances enforce encrypted connections with mandatory mutual TLS client certificates (`TRUSTED_CLIENT_CERTIFICATE_REQUIRED`) and private network routing with no public internet exposure.
- **Access Control, Quarterly Reviews & Hardware YubiKey MFA (`Access Control Policy v1.1.0`):** Administrative access to production environments is restricted under least-privilege IAM, logged in

immutable 400-day audit trails, and protected by mandatory hardware **Yubico YubiKey (U2F/FIDO2)** multi-factor authentication (2FA/MFA) and workstation Full Disk Encryption (FDE). Access rights are reviewed quarterly, and access revocation upon termination or role change is executed within a strict **24-hour SLA**.

- **External Penetration Testing & Vulnerability Remediation SLAs (`CP-ISMS-VSR-002 v1.0` & `Vulnerability Management Procedure v2.1`):** Independent grey-box and black-box penetration testing of the Edudata.io platform was conducted in June 2026 (zero critical vulnerabilities identified; all high and medium findings were 100% remediated and verified closed by **August 16, 2026**). Vulnerabilities are remediated under strict SLAs: **≤ 7 calendar days for Critical CVEs** and **≤ 14 calendar days for High CVEs**.
- **Business Continuity, RTO / RPO Targets & Verified Restore Drills (`CP-ISMS-BIA-001 v1.1` & `CP-ISMS-BCDR-002 v1.1`):** The platform maintains a Recovery Time Objective (**RTO**) of **4 hours (maximum 8 hours)** and a Recovery Point Objective (**RPO**) of **≤ 15 minutes (maximum 24 hours)** backed by Point-in-Time Recovery (PITR) and cross-region backups. Live database restore drills were verified on **June 3, 2026** (full restoration completed in **26 minutes**, 0-minute RPO) and **October 18, 2026** (PITR restoration completed in **9 minutes 52 seconds**, 0-byte data loss).
- **Physical Security (Malminkaari 17-19B, 00700 Helsinki):** Access-controlled, guarded, and 24/7 camera-monitored office premises at Malminkaari 17-19B, 00700 Helsinki, Finland and ISO/IEC 27001, ISO/IEC 27701, and SOC 2 Type II certified Google Cloud EU data centers (`europe-north1` Finland / `europe-west1` Belgium).

Software Development Lifecycle (SDLC) Security Controls:

- Strict separation between development/staging environments (`edudata-compliance-staging` using 100% synthetic data under `CP-ISMS-DLP-001 v1.2`) and production (`edudata-compliance-prod`).
- Mandatory peer code review and senior developer approval prior to CI/CD deployment.
- Automated dependency scanning, secret detection, and continuous vulnerability monitoring (VPM-3 / VPM-38).
- Mandatory onboarding and recurring annual information security and GDPR training for all personnel.

Cloud Infrastructure Governance & Customer Responsibilities:

Cloudpoint Oy owns, manages, and secures the production Google Cloud project (`edudata-compliance-prod`) and its databases on behalf of the Customer. The Customer, as the Data Controller, is responsible for managing its federated user accounts and roles within its Identity Provider (Microsoft Entra ID or Google Workspace) and ensuring the lawful basis for processing. Further information on underlying cloud infrastructure security can be found in the Google Cloud Security Whitepapers.