Accord de traitement des données (ATD)

Edudata.io (3460068-8) — Cloudpoint Oy (N° d'entreprise (FI) 2325703-6, TVA FI23257036) • Malminkaari 17–19 B, 00700 Helsinki, Finlande • DPO: tietosuoja@cloudpoint.fi

[OFFICIELLEMENT PUBLIÉ · H-AI-H] Édition localisée officielle vérifiée par un humain (gouvernance H-AI-H ; en cas de divergence, la version principale EN prévaut).
Verification Role: LEGAL_COUNSEL_AND_RELEASE_OWNER | **Verified UTC:** 2026-11-25T08:36:41Z

Identifiant	`edudata.dpa.fr.v2.0.0-r01`	**Version**	**v2.0** (v2.0.0-r01)
Date d'effet	2026-11-10	**Prochaine révision**	2027-11-10
Langue	Français (fr-FR)	**Certification sécurité**	ISO/IEC 27001:2022 (#123522, Prescient Security LLC)
Modèle de gouvernance	**H-AI-H (Human–AI–Human)**	**Autorité linguistique**	Traduction localisée (depuis la version principale EN)
URL canonique	`https://www.edudata.io/fr/trust-center#dpa`		
Empreinte SHA-256 du contenu (UTF-8 NFC)	`9c881a4eaacedebbef6612feff44bf966c6a29c4eee4114e503e5d95314b3dfd`		

L'Accord de traitement des données (ATD) juridiquement contraignant régissant le traitement des données à caractère personnel pour la plateforme Edudata.io entre le Sous-traitant et le Responsable du traitement.

ACCORD DE TRAITEMENT DES DONNÉES D'EDUDATA.IO

> Cette version localisée est une traduction assistée par IA de la
> version anglaise originale
> et est fournie à titre informatif et de référence uniquement. En cas de divergence, la version anglaise prévaudra.

Version 2.0 | Entrée en vigueur: 10.11.2026

Le présent Accord de traitement des données (« ATD ») concerne EDUDATA (« Service »), qui est géré et fourni par Cloudpoint Oy. Il complète et fait partie intégrante de l'accord principal, y compris les Conditions générales d'utilisation (« CGU »), et entre en vigueur dès son acceptation. En cas de conflit ou d'incohérence avec les termes de l'ensemble des Accords, cet ATD prévaudra dans la mesure de ce conflit ou de cette incohérence.

Parties contractantes:

Sous-traitant: Cloudpoint Oy (2325703-6) / Edudata.io (3460068-8), qui fait partie de Cloudpoint Oy (2325703-6, n° de TVA FI23257036), Malminkaari 17-19B, 00700 Helsinki, Finlande (Délégué à la protection des données / DPD: Jasse Tenko / Responsable ISM: Hesham Abboud, tietosuoja@cloudpoint.fi, service client: info@edudata.io, tél. +358 9 4257 9280)
Responsable du traitement: Le Client

1. Définitions

- **Responsable du traitement:** Désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou d'un État membre, le responsable du traitement ou les

critères spécifiques de sa désignation peuvent être prévus par le droit de l'Union ou d'un État membre (« Responsable du traitement »).

- **Sous-traitant:** Désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (« Sous-traitant »).
- **RGPD:** Règlement Général sur la Protection des Données (UE) 2016/679.
- **Données à caractère personnel:** Toute information se rapportant à une personne physique identifiée ou identifiable (personne concernée); est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
- **Traitement:** Désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'association, la limitation, l'effacement ou la destruction.

Tous les autres termes non définis dans le présent ATD ont la même signification que dans le RGPD.

2. Contexte et objet

Le Responsable du traitement a sélectionné le prestataire de services (Cloudpoint Oy) pour agir en tant que Sous-traitant conformément à l'Article 28(3) du Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement Général sur la Protection des Données, « RGPD »).

Le présent ATD fait partie intégrante de l'Accord principal conclu entre les Parties, en vertu duquel le Sous-traitant fournit au Responsable du traitement le service Edudata, composé des modules Edudata Compliance, Edudata Compliance Service, Edudata Privacy et Edudata Security, sauf convention contraire dans l'Accord principal.

Le Sous-traitant traitera des informations relatives à une personne physique identifiée ou identifiable pour le compte du Responsable du traitement. Les détails des pratiques de traitement des données sont décrits dans l'Annexe 1 du présent ATD.

L'objet de cet ATD est de convenir des droits et obligations des Parties impliquées dans les activités de traitement comme l'exige le RGPD, et de sauvegarder les libertés et les droits de la personne concernée au cours du traitement.

3. Rôles et responsabilités

Le Sous-traitant traitera les données à caractère personnel conformément au présent ATD et aux instructions documentées du Responsable du traitement. Le Sous-traitant n'utilisera pas les données à caractère personnel à d'autres fins que celles convenues dans le présent ATD et dans les instructions du Responsable du traitement. Les instructions du Responsable du traitement doivent être conformes aux lois applicables sur la protection des données et cohérentes avec cet ATD.

Si le Sous-traitant constate qu'une instruction donnée par le Responsable du traitement n'est pas conforme aux lois applicables ou s'avère insuffisante, le Sous-traitant informera le Responsable du traitement de cette non-conformité.

Le Responsable du traitement est responsable de l'existence d'une base juridique pour le traitement des données à caractère personnel, de l'information des personnes concernées concernant le traitement de leurs données et de l'exécution des autres obligations incombant au responsable du traitement en vertu du RGPD.

Le Responsable du traitement est tenu d'informer le Sous-traitant des coordonnées de son Délégué à la protection des données (DPD) et de s'assurer que ces coordonnées sont tenues à jour. Ces coordonnées sont indispensables pour permettre au Sous-traitant de respecter ses obligations de notification en cas de

violation de données.

4. Mesures techniques et organisationnelles

Le Sous-traitant maintiendra des mesures techniques et organisationnelles de sécurité appropriées pour se prémunir contre tout traitement ou accès non autorisé ou illicite, ainsi que contre toute perte, destruction ou altération accidentelle. Lors du choix des mesures de sécurité, le Sous-traitant doit tenir compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques de probabilité et de gravité variables pour les droits et libertés des personnes physiques.

Une description détaillée des mesures appliquées est stipulée dans l'Annexe 2 du présent ATD.

5. Obligation d'assistance et SLA de réponse aux demandes des personnes concernées (DSAR)

Le Sous-traitant traite les données à caractère personnel conformément au présent ATD, aux instructions du Responsable du traitement et à la législation sur la protection des données. Le Sous-traitant doit prendre les mesures nécessaires pour protéger les données à caractère personnel contre des pratiques de traitement non conformes aux termes de cet ATD, aux instructions ou à la législation applicable.

Le Sous-traitant s'engage à veiller à ce que les personnes travaillant pour son compte respectent les termes du présent ATD et soient informées de la législation pertinente. Le Sous-traitant soutient le Responsable du traitement pour garantir le respect des obligations énoncées aux Articles 32 à 36 du RGPD (notamment les analyses d'impact relatives à la protection des données / AIPD et les consultations préalables), à la demande de ce dernier.

Le Sous-traitant s'engage à informer le Responsable du traitement et à lui transmettre toutes les demandes des personnes concernées relatives à l'exercice de leurs droits en vertu du RGPD (DSAR) **dans un délai maximal de cinq (5) jours ouvrés** à compter de la réception de la demande. Le Sous-traitant soutient le Responsable du traitement par des mesures techniques et organisationnelles appropriées afin que ce dernier puisse répondre aux demandes dans les délais légaux.

L'assistance standard au titre de l'Article 28 du RGPD est incluse dans les frais d'abonnement sans coût supplémentaire. Si le Responsable du traitement demande des travaux de développement sur mesure ou une intervention manuelle importante sortant du cadre des fonctionnalités standard du Service, les Parties conviendront par écrit au préalable d'une compensation raisonnable.

6. Transferts internationaux, gouvernance HubSpot `eu1` et séparation du développement logiciel

Nous traitons et stockons les données à caractère personnel de la plateforme principale sur des serveurs situés dans l'Union européenne / l'Espace Économique Européen (Google Cloud région `europe-north1` Finlande et sauvegardes `europe-west1` Belgique). En règle générale, il n'y a pas de transferts réguliers des bases de données de production en dehors de l'UE/EEE.

Gouvernance HubSpot `eu1` et interdiction des 5 catégories dans les tickets de support: Pour la gestion de la relation client B2B et le support technique concernant uniquement les personnes de contact et administrateurs désignés par le Client, **HubSpot Ireland Ltd** est épinglé au centre de données régional européen `dataHostingLocation = eu1` (`app-eu1.hubspot.com` , AWS `eu-central-1` Francfort, Allemagne, avec basculement à Dublin, Irlande). Le portail applique le GDPR Compliance Toolkit de HubSpot (incluant la **suppression définitive RGPD [GDPR Permanent Delete]** dans les 90 jours suivant la fin du contrat ou sur demande) ainsi que les verrous de sécurité Breeze AI (`customer_data_training_enabled = False` et `crm_sensitive_pii_access_enabled = False`). Les éventuels accès de support mondial de HubSpot, Inc. sont encadrés par le Data Privacy Framework UE–États-Unis (DPF), les Clauses Contractuelles Types de la Commission européenne (CCT 2021/914) et une Analyse d'impact des transferts (TIA). Conformément à la `Data Management Policy v1.1.0` , il est strictement interdit de saisir ou de transférer dans les tickets de support HubSpot les cinq (5) catégories suivantes: (1) données relatives aux élèves, (2) données sensibles / catégories particulières (art. 9 du RGPD), (3) détails d'incidents de sécurité, (4) identifiants ou jetons d'authentification, et (5) journaux de sécurité (logs).

Séparation du développement logiciel en Égypte (art. 25 et 32 du RGPD — `Aimpulse`): Aimpulse est l'unité de développement dédiée / entité partenaire de Cloudpoint Oy (Le Caire, Égypte), opérant exclusivement sous le contrôle opérationnel et le SMSI certifié ISO/IEC 27001:2022 de Cloudpoint Oy. Les ingénieurs en Égypte participent activement au développement logiciel exclusivement dans des environnements hors production isolés (`edudata-compliance-staging`) à l'aide de **données 100 % synthétiques / fictives** (`CP-ISMS-DLP-001 v1.2`) et n'ont **aucun accès aux données opérationnelles des clients ni aux données à caractère personnel dans l'environnement de production (`edudata-compliance-prod`)**. Le support client et l'administration des données à caractère personnel de production sont effectués exclusivement au sein de l'UE/EEE (Finlande). La relation contractuelle est encadrée par les Clauses Contractuelles Types de l'UE (CCT, décision (UE) 2021/914, Module 3: Sous-traitant à Sous-traitant), une Analyse d'impact des transferts (TIA) et des journaux d'audit Admin Activity immuables conservés pendant 400 jours.

7. Obligation de confidentialité

Le Sous-traitant et toutes les personnes physiques travaillant pour lui doivent respecter la confidentialité et le secret professionnel au cours du traitement. Le Sous-traitant garantit que toutes les personnes physiques travaillant pour lui sont liées par un accord de confidentialité.

Le Sous-traitant s'assure de l'existence d'un accord de non-divulgation (NDA) avec ses sous-traitants ultérieurs et d'accords de confidentialité entre chaque sous-traitant ultérieur et toutes les personnes physiques travaillant pour lui participant au traitement. Cette obligation de confidentialité demeure en vigueur même après la résiliation ou l'expiration de l'Accord principal et du présent ATD.

8. Droit d'audit

Le Responsable du traitement a le droit d'effectuer des audits raisonnables des installations et des activités de traitement du Sous-traitant afin d'examiner le niveau de protection et de sécurité prévu par le présent ATD, et d'évaluer la conformité du Sous-traitant avec ses dispositions.

Le Responsable du traitement supportera l'intégralité des coûts liés à la réalisation de l'audit. Le Responsable du traitement en informera le Sous-traitant par écrit au moins 30 jours ouvrés (ou 14 à 30 jours dans les marchés publics) avant la tenue de l'audit.

Le droit d'audit du Responsable du traitement s'exerce au maximum une fois tous les douze (12) mois, sauf si une violation spécifique de données ou une préoccupation étayée nécessite un audit anticipé.

Lorsqu'un audit est susceptible d'entraîner la divulgation de secrets commerciaux ou d'affaires du Sous-traitant, ou de menacer les droits de propriété intellectuelle du Sous-traitant, un expert indépendant doit être mandaté pour mener l'audit, et cet expert devra s'engager par un accord de confidentialité.

9. Sous-traitants ultérieurs

Le Sous-traitant a le droit de faire appel à des sous-traitants ultérieurs pour traiter les données à caractère personnel dans le cadre de la fourniture du Service, sous réserve que cette désignation n'entraîne pas de manquement aux obligations du Sous-traitant en vertu du présent ATD.

Le Sous-traitant s'assure que les sous-traitants ultérieurs impliqués agissent en vertu d'un contrat écrit de sous-traitance avec le Sous-traitant et respectent des obligations de protection des données au moins équivalentes à celles contenues dans le présent ATD (art. 28(4) du RGPD).

Le Sous-traitant fournira au Responsable du traitement une **notification écrite directe (par e-mail à la personne de contact désignée du Responsable du traitement) au moins trente (30) jours calendaires à l'avance** avant d'ajouter ou de remplacer un sous-traitant ultérieur. Le Responsable du traitement dispose de **trente (30) jours calendaires** à compter de la notification pour s'y opposer par écrit pour des motifs raisonnables liés à la protection des données. Si les Parties ne parviennent pas à une solution mutuellement acceptable dans ce délai de 30 jours, le Responsable du traitement aura le droit de résilier le Service concerné sans pénalité.

10. Violations de données à caractère personnel (Modèle en deux étapes NIS2 art. 23 et RGPD art. 33)

Conformément à la procédure de réponse aux incidents du Sous-traitant (`CP-ISMS-IR-002 v1.0` , SLA VPM-38 à 4 niveaux: P1 < 1 h, P2 < 4 h, P3 < 24 h, P4 < 72 h), la détection et la notification des violations de données à caractère personnel suivent un modèle en deux étapes:

- **Étape 1 — Surveillance automatisée 24h/24, 7j/7 et 365j/an & Alerte précoce préliminaire (Early Warning ≤ 24 heures):** L'infrastructure de production est surveillée 24h/24, 7j/7 et 365j/an (y compris les week-ends et jours fériés) par des alertes automatisées de sécurité et de détection d'anomalies (Google Cloud Security Command Center, Cloud Logging et Datadog). Dès qu'il a connaissance d'une violation de données à caractère personnel avérée ou raisonnablement suspectée, le Sous-traitant envoie une **alerte précoce préliminaire (Early Warning)** écrite ou automatisée à la personne de contact désignée du Responsable du traitement **au plus tard dans les 24 heures** suivant la détection (indiquant l'horodatage de détection, le service concerné, les mesures techniques d'endiguement en cours et les points de contact).
- **Étape 2 — Évaluation formelle du DPD et rapport détaillé en 8 points (Jour ouvré suivant / ≤ 72 heures):** L'investigation approfondie vérifiée par un humain, l'analyse des causes profondes (RCA) et l'évaluation formelle d'impact par le Délégué à la protection des données (`tietosuoja@cloudpoint.fi` , DPD Jasse Tenko / Responsable ISM Hesham Abboud) débutent immédiatement et, pour les alertes survenant en dehors des heures ouvrées, dès le **jour ouvré suivant**, aboutissant à un rapport complet conforme à l'art. 33(3) du RGPD dans un délai de 24 à 48 heures après confirmation et toujours dans le plafond légal de **72 heures**.

Le rapport détaillé en 8 points comprend: (1) la nature de la violation, (2) les catégories et le nombre approximatif de personnes concernées, (3) les catégories et le nombre approximatif d'enregistrements de données concernés, (4) le nom et les coordonnées du DPD / point de contact, (5) les conséquences probables de la violation, (6) les mesures correctives et d'atténuation prises ou proposées, (7) l'horodatage précis de détection, de confinement et de résolution ainsi que la cause technique profonde, et (8) la documentation d'audit nécessaire aux notifications réglementaires du Responsable du traitement.

11. Restitution et suppression des données à caractère personnel

Avant la résiliation ou l'expiration de l'Accord principal, le Responsable du traitement a le droit d'exporter ses évaluations, décisions et données de conformité dans des formats structurés et lisibles par machine (CSV / JSON / PDF). Après la cessation définitive du Service:

- **Bases de données actives de production (dans les 30 jours calendaires):** Le Sous-traitant supprime définitivement toutes les données à caractère personnel du Client des bases de données actives de production dans un délai maximal de **trente (30) jours calendaires** à compter de la date effective de fin du contrat.
- **Sauvegardes chiffrées et instantanés (dans les 90 jours calendaires):** Les données résiduelles figurant dans les sauvegardes chiffrées sont écrasées automatiquement et de manière irréversible au fur et à mesure de l'expiration des cycles de sauvegarde, et au plus tard dans les **quatre-vingt-dix (90) jours calendaires**: Cloud SQL `edudata-comp-db` (21 jours de sauvegardes automatisées + 7 jours PITR), Cloud SQL `edudata-ai-db` (7 jours de sauvegardes automatisées + 7 jours PITR), exports gérés Firestore (7 à 90 jours maximum) et compartiments Cloud Storage (fenêtre de suppression logique [soft-delete] de 7 jours / `604800` secondes).
- **Protection cryptographique et confirmation de suppression sur demande:** Pendant la période de transition et de purge des sauvegardes, toutes les données restent chiffrées au repos avec AES-256 et leur traitement actif est bloqué. Sur demande, le Sous-traitant fournit une confirmation écrite de suppression (par ex. par e-mail) une fois la suppression effectuée.

Les comptes utilisateurs inactifs sont automatiquement supprimés de la base de données utilisateurs lorsque 366 jours se sont écoulés depuis le dernier traitement des informations de connexion.

12. Traitement assisté par l'IA, absence de décision automatisée et limitation de responsabilité

Traitement assisté par l'IA (Google Cloud Vertex AI & Document AI): Pour fournir les fonctionnalités d'analyse automatisée des documents et d'aide à l'évaluation de conformité de la plateforme, le Sous-traitant utilise les services **Google Cloud Vertex AI (modèles Gemini enterprise)** et **Google Cloud Document AI** dans les régions de l'UE (`europe-north1` Finlande et multi-région `eu`), appuyés par la base de données PostgreSQL dédiée `edudata-ai-db` (suppression active sous 30 jours, expiration des sauvegardes sous 7 jours). Conformément à la gouvernance des données de Google Cloud et à la `Data Management Policy v1.1.0` de Cloudpoint Oy:

- **Aucun entraînement de modèles d'IA:** Les données à caractère personnel, documents, invites (prompts) et résultats du Client ne sont **jamais** utilisés pour entraîner, affiner ou améliorer les modèles d'IA de fondation de Google, de Cloudpoint Oy ou de tiers.
- **Absence de prise de décision automatisée ou de profilage (art. 22 du RGPD):** Les fonctionnalités d'IA d'Edudata.io servent exclusivement d'outils d'aide à la rédaction et à la structuration pour les professionnels habilités du Client (principe de supervision humaine / *Human-in-the-Loop*). Le Service n'effectue aucun profilage des élèves ou du personnel et ne prend aucune décision entièrement automatisée produisant des effets juridiques ou affectant de manière significative les personnes concernées au sens de l'Article 22 du RGPD.

Limitation de responsabilité: Le Sous-traitant ne sera pas responsable des dommages indirects ou consécutifs en vertu du présent ATD. La responsabilité cumulée maximale du Sous-traitant envers le Responsable du traitement en vertu du présent ATD sera limitée à une somme correspondant à 100 % des paiements effectués par le Responsable du traitement au Sous-traitant pour le Service au cours des 12 mois précédents, sauf disposition contraire dans l'Accord principal ou lorsque cette limitation serait illégale.

13. Durée

Le présent ATD (Version 2.0, en vigueur à compter du 10.11.2026) et les Conditions générales d'utilisation d'Edudata.io (Version 3.1) sont conclus et entrent en vigueur simultanément soit par voie électronique via le **Cloudpoint Portal (`portal.cloudpoint.fi`)** (à l'aide d'une identification électronique forte `Bink.fi` FTN / `Swedish BankID` et d'une empreinte cryptographique `SHA-256` archivée dans `GCS WORM` en `europe-north1`), soit par une signature électronique externe sur l'Accord principal / le Bon de commande enregistrée dans `portal.cloudpoint.fi` pour la gouvernance centralisée des contrats, des modules et des coordonnées du DPD. Le présent ATD reste applicable jusqu'à ce que le Sous-traitant ait cessé de traiter les données à caractère personnel du Responsable du traitement et exécuté ses obligations de suppression conformément à la section 11, ou jusqu'à son remplacement par un autre accord entre les Parties.

14. Règlement des litiges et compétence juridictionnelle

Le présent ATD est soumis aux dispositions relatives au règlement des litiges et à la juridiction compétente définies dans l'Accord principal (Tribunal de première instance d'Helsinki et droit finlandais).

15. Modifications et gouvernance des changements à 3 niveaux

Les mises à jour du présent ATD et de la documentation du Trust Center sont régies par un modèle de gouvernance des changements à trois (3) niveaux:

- **Niveau 1 — Améliorations documentaires, techniques et de sécurité (préavis de 0 jour):** Les clarifications typographiques, les mises à jour de certificats d'audit et les améliorations techniques de sécurité entrent en vigueur dès leur publication. Le Sous-traitant garantit une **absence de dégradation substantielle (No Material Degradation Guarantee)**: aucune mise à jour de Niveau 1 ne réduira le niveau global de sécurité de l'information, de confidentialité ou des engagements contractuels.
- **Niveau 2 — Changements de sous-traitants ultérieurs et notifications opérationnelles (préavis écrit de 30 jours calendaires et droit d'opposition):** Tout ajout ou remplacement de sous-traitant ultérieur (conformément au RGPD art. 28, par. 2 et à la section 9) fait l'objet d'une notification écrite par e-mail au moins **trente (30) jours calendaires à l'avance**, assortie d'un droit d'opposition et de résiliation sans pénalité.

- **Niveau 3 — Modifications substantielles des modalités de traitement des données personnelles et avenants à l'Accord principal (préavis de 30 jours calendaires + approbation électronique expresse du Responsable du traitement):** Le Sous-traitant n'apporte aucune modification substantielle à la manière dont les données personnelles sont traitées (finalités, catégories de données ou de personnes concernées, régions de stockage, durées de conservation ou engagements fondamentaux au titre de l'art. 28, par. 3 du RGPD) sans l'approbation du Responsable du traitement. Ces modifications sont soumises au moins 30 jours calendaires à l'avance à l'approbation électronique de l'administrateur ou du décideur du Responsable du traitement via **Edudata.io ou le Cloudpoint Portal (`portal.cloudpoint.fi`) (avec la possibilité de transmettre la demande d'approbation directement au signataire habilité de l'organisation)**.

Signatures

Les Parties ci-dessous ont accepté et signé simultanément le présent ATD (Version 2.0) et les CGU (Version 3.1) soit électroniquement via le **Cloudpoint Portal (`portal.cloudpoint.fi`)** (avec identification électronique forte `Bink.fi` / `Swedish BankID` et empreinte cryptographique `SHA-256` archivée dans `GCS WORM` `europe-north1`), soit par signature électronique externe sur l'Accord principal / le Bon de commande enregistrée dans `portal.cloudpoint.fi` pour la gouvernance centralisée des contrats, des modules et des coordonnées du DPD.

Cloudpoint Oy / Edudata.io

Délégué à la protection des données (DPD) et représentant habilité, Cloudpoint Oy (Sous-traitant)

Date: 10.11.2026

[Signature du représentant du Client]

Signataire autorisé (Responsable du traitement)

Date: [Date d'acceptation]

ANNEXE 1: Description du traitement des données (Version 2.0 — 10.11.2026)

1. Finalité du traitement des données à caractère personnel

Le Sous-traitant traitera les données à caractère personnel pour le compte du Responsable du traitement aux fins de la fourniture du Service, dans la mesure où cette fourniture nécessite le traitement de données par le Sous-traitant. Le traitement s'effectuera conformément à l'Accord principal, au présent ATD et aux instructions documentées fournies par le Responsable du traitement.

2. Catégories de personnes concernées et matrice des modules

Les catégories de personnes concernées dépendent des modules Edudata.io souscrits et activés par le Responsable du traitement:

- **Module principal — *Edudata Compliance* et *Edudata Compliance Service* (évaluation de la conformité et des risques des services numériques):** Les utilisateurs authentifiés et personnes concernées sont **exclusivement les enseignants, rédacteurs, décideurs, responsables de la protection des données et administrateurs du Client** (rôles: *Enseignant, Enseignant+, Rédacteur, Décideur, Administrateur Client*). Les élèves ne se connectent pas au module principal *Edudata Compliance*.
- **Modules complémentaires optionnels — *Edudata Privacy* et *Edudata Security*:** Uniquement lorsque le Client a explicitement souscrit et activé les modules optionnels d'audit OAuth tiers ou de sécurité des comptes, les métadonnées d'authentification et d'autorisation peuvent également concerner les **élèves / apprenants** (rôle: *Élève*) ainsi que le personnel enseignant.

Garantie relative aux champs de texte libre (Free-Text Safeguard): Bien qu'*Edudata Compliance* soit conçu pour évaluer des applications logicielles et non des individus, si un utilisateur du Client saisit accidentellement des données à caractère personnel dans des champs de commentaires en texte libre, le

Sous-traitant protège l'intégralité du contenu de la base de données selon les mêmes contrôles de sécurité de niveau production (chiffrement AES-256, TLS 1.3, contrôle d'accès strict et règles de suppression).

3. Types de données à caractère personnel et authentification fédérée sans mot de passe (Zero Passwords)

Conformément à la politique d'authentification d'Edudata.io (`CP-ISMS-AUTH-001 v1.1`), la plateforme fonctionne selon un principe strict **Zero Passwords (zéro mot de passe stocké)**: l'authentification des utilisateurs s'effectue exclusivement par connexion unique fédérée (SSO) via le fournisseur d'identité du Client (**Microsoft Entra ID** ou **Google Workspace**) à l'aide des protocoles OAuth 2.0 / OpenID Connect. Edudata.io ne collecte, ne traite ni ne stocke jamais de mots de passe utilisateurs ou d'empreintes (hashes) de mots de passe.

Selon les modules activés, le Sous-traitant peut traiter les types de données à caractère personnel suivants:

- Prénom et nom
- Adresse e-mail professionnelle / scolaire
- Identifiant unique Edudata (Edudata ID) et identifiant de fédération SSO
- Rôle de l'utilisateur et unité organisationnelle
- Nom et domaine de l'organisation (Client)
- Langue de l'interface et photo de profil (si transmise par le SSO)
- Adresse IP et horodatages de connexion (journaux de sécurité)
- Métadonnées techniques du navigateur et de l'appareil
- Date de création du compte et de dernière connexion
- Métadonnées de jetons d'accès tiers (uniquement dans les modules optionnels *Edudata Privacy / Security*)

4. Architecture Google Cloud, conservation des journaux et durée du traitement

Matrice de responsabilité Google Cloud en 7 points:

1. **Propriété du projet de production:** L'environnement de production d'Edudata.io est hébergé dans le projet Google Cloud `edudata-compliance-prod` , qui est **détenu, administré et sécurisé par Cloudpoint Oy** dans la région `europe-north1` (Hamina, Finlande) avec réplication de sauvegarde dans `europe-west1` (Belgique).
2. **Chaîne contractuelle (Google CDPA):** Cloudpoint Oy a conclu le *Google Cloud Data Processing Addendum (CDPA)* directement avec **Google Cloud EMEA Limited / Google Ireland Ltd**. Le Client n'a pas besoin de conclure de contrat Google Cloud distinct pour utiliser Edudata.io.
3. **Bases de données de la plateforme:** Les données d'application, évaluations et profils utilisateurs sont stockés par Cloudpoint Oy dans des instances Cloud SQL for PostgreSQL dédiées (`edudata-comp-db` et `edudata-ai-db`) ainsi que dans une base de données Firestore distincte (`Firestore database`) au sein du projet `edudata-compliance-prod` en `europe-north1` .
4. **Isolation logique multi-locataire:** Les données de chaque Client sont logiquement isolées au moyen d'identifiants d'organisation vérifiés et de contrôles d'accès basés sur les rôles (RBAC).
5. **Clés de chiffrement et certificats:** Cloudpoint Oy gère le chiffrement AES-256 au repos, TLS 1.3 en transit et l'authentification mutuelle par certificat client (`TRUSTED_CLIENT_CERTIFICATE_REQUIRED`) vers les bases de données Cloud SQL.
6. **Journaux d'audit centralisés:** Les journaux d'audit et de sécurité sont collectés dans le projet centralisé de journalisation de Cloudpoint Oy (sink BigQuery UE `edudata_compliance_logging`) conformément à la norme ISO/IEC 27001:2022.
7. **Compatibilité d'architecture v1/v2 (`TenantStorageRouter`) et collecteur de journaux optionnel:** Pour les clients existants sous le modèle de stockage v1 utilisant le module optionnel de journaux SSO/applications, ces journaux spécifiques peuvent résider dans des projets Google Cloud Firestore propres au client, tandis que les nouveaux déploiements utilisent l'architecture centralisée multi-

locataire UE v2 strictement isolée (`TenantStorageRouter` prenant en charge les deux modèles côte à côte avec rétrocompatibilité complète).

Matrice de conservation des journaux à 3 niveaux (ISO/IEC 27001:2022 `A.8.15` & `A.8.16` — `CP-ISMS-LOG-001 v1.2`):

- **Niveau 1 — Journaux d'audit d'activité d'administration et de sécurité (400 jours):** Les journaux d'activité d'administration Google Cloud (`_Required`) et les événements d'audit de sécurité exportés vers le sink BigQuery UE `edudata_compliance_logging` sont conservés de manière immuable pendant **400 jours**.
- **Niveau 2 — Journaux opérationnels d'application et d'accès aux données (365 jours / 15–30 jours APM):** Les journaux système et d'application dans les compartiments Google Cloud Logging `_Default` sont conservés pendant **365 jours** pour permettre les investigations forensiques conformément aux contrôles ISO 27001 `A.8.15` et `A.8.16` . Les télémétries de performance et d'erreurs masquées dans Datadog APM sont conservées pendant **15 à 30 jours**.
- **Niveau 3 — Cycle de vie des données d'application et gouvernance d'archivage du Responsable du traitement:**
- **Comptes utilisateurs inactifs:** Supprimés automatiquement après **366 jours** sans activité de connexion.
- **Demandes de rôle:** Les demandes refusées ou sans réponse sous **30 jours** sont automatiquement supprimées.
- **Télémétrie OAuth tiers (module optionnel *Edudata Privacy*):** Conservée jusqu'à **18 mois**.
- **Évaluations, décisions et demandes (conservation pendant toute la durée du contrat + délai de suppression de 30 jours après la fin du contrat):** Les évaluations, DPIA, décisions et demandes **ne sont pas supprimées avant la fin du contrat du Client avec le service Edudata.io** (sauf suppression par les administrateurs du Client) et peuvent être exportées à tout moment pendant la durée de l'Accord principal. Après la fin du contrat, nous appliquons un **délai de suppression de 30 jours calendaires** pour l'effacement des données des bases de données primaires (et 90 jours calendaires pour les sauvegardes chiffrées).
- **Suppression en fin de contrat:** Suppression des bases de données actives sous **30 jours calendaires** et écrasement complet des sauvegardes chiffrées sous **90 jours calendaires** (section 11).

5. Sous-traitants ultérieurs autorisés

Le Sous-traitant fait appel aux sous-traitants ultérieurs suivants pour la fourniture et la sécurisation du Service:

Nom du sous-traitant ultérieur	Rôle et portée du traitement	Localisation du traitement et garanties de transfert
Google Ireland Ltd (Google Cloud EMEA Limited)	Infrastructure cloud de production (`edudata-compliance-prod`), bases de données Cloud SQL (`edudata-comp-db` , `edudata-ai-db`), base de données Firestore, Cloud Storage, Cloud Logging / BigQuery ainsi que traitement assisté par l'IA via Vertex AI (Gemini) et Document AI sans entraînement de modèles. S'applique à tous les utilisateurs du Service.	**UE/EEE:** `europe-north1` (Finlande), sauvegardes `europe-west1` (Belgique) et multi-région `eu` . Google CDPA, EU-U.S. DPF & CCT (2021/914).
HubSpot Ireland Ltd	Portail CRM B2B et gestion des tickets de support technique concernant uniquement les personnes de contact et administrateurs désignés par le Client (soumis à l'interdiction stricte des 5 catégories de données et aux verrous Breeze AI).	**UE/EEE:** Centre de données régional `eu1` (AWS `eu-central-1` Francfort, Allemagne; basculement à Dublin, Irlande). EU-U.S. DPF, CCT (2021/914) & TIA.

Nom du sous-traitant ultérieur	Rôle et portée du traitement	Localisation du traitement et garanties de transfert
Datadog, Inc.	Surveillance de la sécurité de l'infrastructure, détection d'anomalies et télémétrie APM masquée (conservation de 15 à 30 jours).	**UE / États-Unis:** EU-U.S. Data Privacy Framework (DPF), CCT (2021/914) & TIA.
Aimpulse (unité de développement dédiée / entité partenaire de Cloudpoint Oy, Le Caire, Égypte)	Développement logiciel opérant exclusivement sous le contrôle opérationnel et le SMSI certifié ISO/IEC 27001:2022 de Cloudpoint Oy. Travaille exclusivement dans des environnements hors production isolés (`edudata-compliance-staging`) avec des données 100 % synthétiques (`CP-ISMS-DLP-001 v1.2`); **aucun accès aux données opérationnelles des clients ni aux données à caractère personnel dans l'environnement de production (`edudata-compliance-prod`)**.	**Égypte:** Environnement hors production isolé, CCT de l'UE (Module 3), TIA et journaux d'audit Admin Activity de 400 jours.
Online Partner AB	Partenaire local de support de première ligne et revendeur en Suède. **S'applique UNIQUEMENT lorsque le Client a conclu un contrat via Online Partner AB**; ne traite aucune donnée pour les clients municipaux directs de Cloudpoint Oy.	**UE/EEE:** Suède.
Visma AB	Utilisé exclusivement pour la facturation financière B2B légale et la comptabilité de Cloudpoint Oy en qualité de Responsable du traitement indépendant; **ne traite aucune donnée d'évaluation ou d'utilisateur de la plateforme Edudata.io**.	**UE/EEE:** Finlande / Suède.

6. Transferts internationaux

Toutes les données de production de la plateforme Edudata.io sont stockées et traitées au sein de l'Union européenne / de l'Espace Économique Européen (`europe-north1` Finlande et `europe-west1` Belgique). Lorsque des sous-traitants ultérieurs impliquent un traitement transfrontalier ou un support d'ingénierie en dehors de l'UE/EEE (comme décrit à la section 6 de l'ATD et au tableau 5 ci-dessus), le transfert est encadré par le Chapitre V du RGPD au moyen d'une décision d'adéquation de la Commission européenne (EU-U.S. Data Privacy Framework), des Clauses Contractuelles Types (CCT 2021/914, Modules 2 et 3), d'Analyses d'impact des transferts (TIA) et de mesures techniques supplémentaires (chiffrement AES-256/TLS 1.3 et isolation des données synthétiques).

ANNEXE 2: Mesures de sécurité techniques et organisationnelles (Version 2.0 — 10.11.2026)

Le Sous-traitant met en œuvre et maintient un Système de gestion de la sécurité de l'information (SGSI / ISMS) certifié ISO/IEC 27001:2022 afin de protéger la confidentialité, l'intégrité et la disponibilité des données à caractère personnel conformément à l'Article 32 du RGPD.

- **SMSI de Cloudpoint Oy certifié ISO/IEC 27001:2022 (Prescient Security LLC, n° 123522) et surveillance GRC continue (Vanta):** Cloudpoint Oy (2325703-6) exploite un SMSI **certifié ISO/IEC 27001:2022** (*Statement of Applicability v1.2* du 20.10.2026; certificat `#123522` Issue 1, délivré le 18.11.2026, valide jusqu'au 17.11.2029 par **Prescient Security LLC**, accrédité IAS MSCB-267, IAF MLA; siège social Malminkaari 17-19 B, Helsinki; périmètre couvrant les écosystèmes cloud pour le secteur public, l'éducation et les entreprises, l'infrastructure GCP et Google Workspace ainsi que les 6

départements) et surveillé en continu via Vanta (incluant les contrôles VPM-38, VPM-3 et AST-4 – AST-9).

- **Protection cryptographique et mTLS sur les bases de données (AES-256 & TLS 1.3):** Toutes les données clients, bases de données et sauvegardes sont chiffrées au repos avec AES-256 et en transit avec TLS 1.3 (minimum TLS 1.2). Les instances Cloud SQL imposent des connexions chiffrées avec authentification mutuelle par certificat client obligatoire (`TRUSTED_CLIENT_CERTIFICATE_REQUIRED`) et adressage réseau privé sans exposition directe à Internet.
- **Contrôle d'accès, revues trimestrielles et MFA matérielle YubiKey (`Access Control Policy v1.1.0`):** L'accès administratif à l'infrastructure de production est restreint selon le principe du moindre privilège (IAM), protégé par une authentification multifacteur matérielle obligatoire **Yubico YubiKey (U2F/FIDO2)** et le chiffrement intégral du disque (FDE) sur les postes de travail. Les droits d'accès font l'objet d'une revue formelle trimestrielle et toute révocation d'accès est exécutée dans un délai maximal de **24 heures** suivant un départ ou un changement de rôle.
- **Tests d'intrusion externes et SLA de correction des vulnérabilités (`CP-ISMS-VSR-002 v1.0` & `Vulnerability Management Procedure v2.1`):** Des tests d'intrusion externes indépendants en boîte grise et boîte noire sur la plateforme Edudata.io ont été réalisés en juin 2026 (aucune vulnérabilité critique identifiée; l'ensemble des constats de niveau élevé et moyen a été intégralement corrigé et vérifié le **16 août 2026**). Les vulnérabilités sont corrigées selon des délais stricts: **≤ 7 jours calendaires pour les vulnérabilités critiques (Critical CVEs)** et **≤ 14 jours calendaires pour les vulnérabilités élevées (High CVEs)**.
- **Continuité d'activité, objectifs RTO / RPO et exercices de restauration vérifiés (`CP-ISMS-BIA-001 v1.1` & `CP-ISMS-BCDR-002 v1.1`):** La plateforme garantit un objectif de délai de reprise (**RTO**) de **4 heures (maximum 8 heures)** et un objectif de point de reprise (**RPO**) de **≤ 15 minutes (maximum 24 heures)** grâce à la récupération ponctuelle (PITR) et aux sauvegardes multi-régions. Les tests réels de restauration de base de données ont été vérifiés le **3 juin 2026** (restauration complète en **26 minutes**, RPO de 0 minute) et le **18 octobre 2026** (récupération PITR en **9 minutes et 52 secondes**, perte de données de 0 octet).
- **Sécurité physique (Malminkaari 17-19B, 00700 Helsinki):** Locaux professionnels sécurisés avec contrôle d'accès et vidéosurveillance 24h/24 et 7j/7 situés à Malminkaari 17-19B, 00700 Helsinki, Finlande, ainsi que des centres de données Google Cloud UE (`europe-north1` Finlande / `europe-west1` Belgique) certifiés ISO/IEC 27001, ISO/IEC 27701 et SOC 2 Type II.

Contrôles de sécurité du cycle de développement logiciel (SDLC):

- Séparation stricte entre les environnements de développement/test (`edudata-compliance-staging` avec données 100 % synthétiques selon `CP-ISMS-DLP-001 v1.2`) et l'environnement de production (`edudata-compliance-prod`).
- Revue de code obligatoire par les pairs (peer review) et approbation par un ingénieur senior avant tout déploiement CI/CD.
- Analyse automatisée des dépendances, détection des secrets et surveillance continue des vulnérabilités (VPM-3 / VPM-38).
- Formation obligatoire et régulière du personnel à la sécurité de l'information et au RGPD.

Gouvernance de l'infrastructure cloud et responsabilités du Client:

Cloudpoint Oy détient, administre et sécurise le projet Google Cloud de production (`edudata-compliance-prod`) et ses bases de données pour le compte du Client. Le Client, en sa qualité de Responsable du traitement, est responsable de la gestion des comptes et des rôles de ses utilisateurs au sein de son fournisseur d'identité fédéré (Microsoft Entra ID ou Google Workspace) ainsi que de la licéité des instructions de traitement. De plus amples informations sur la sécurité de l'infrastructure sous-jacente sont disponibles dans les Livres blancs sur la sécurité de Google Cloud.