Data Processing Agreement — oec.sh Platform Service

OpenEducat Inc.

Version 1.0 — issued 2026-08-06

Data Processing Agreement

oec.sh Platform Service

Version: 1.0 — issued 2026-08-06

Parties

This Data Processing Agreement (“DPA”) is entered into by and between:

Processor: OpenEducat Inc. (“oec.sh”, “we”, “us”), a Delaware corporation with registered office at 2803 Philadelphia Pike, Suite B #1117, Claymont, DE 19703, USA (EIN 36-4981207).

Controller: [CUSTOMER LEGAL NAME], a [CUSTOMER JURISDICTION] [CUSTOMER COMPANY TYPE] with registered office at [CUSTOMER REGISTERED ADDRESS].

Each a “Party” and together the “Parties”.

This DPA forms part of, and is subject to, the Terms of Service between the Parties for use of the oec.sh Platform Service (the “Principal Agreement”). Where any conflict exists between this DPA and the Principal Agreement, this DPA governs in respect of the processing of Personal Data.

1. Definitions

Capitalised terms used but not defined herein have the meanings given in the Principal Agreement or in the UK GDPR / EU GDPR as applicable.

Term	Meaning
Applicable Data Protection Law	The UK GDPR, the EU GDPR (Regulation (EU) 2016/679), the UK Data Protection Act 2018, and any other applicable data protection or privacy laws of the jurisdictions in which the Parties operate.
Customer Personal Data	Personal Data that the Controller submits to or generates within the Platform Service, and that we process on the Controller’s behalf in our role as Processor.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data.
Restricted Transfer	A transfer of Customer Personal Data from the UK or the EEA to a country that has not been recognised as providing an adequate level of protection by the UK or the European Commission.

Term	Meaning
Standard Contractual Clauses (SCCs)	The standard contractual clauses for the transfer of personal data to third countries pursuant to the EU GDPR, approved by Commission Implementing Decision (EU) 2021/914, and the UK International Data Transfer Addendum as published by the ICO.
Sub-processor	Any third party engaged by us to process Customer Personal Data on our behalf in connection with the provision of the Platform Service.
TOMs	The technical and organisational measures set out in Schedule 2.

"Controller", "Processor", "Personal Data", "Data Subject", "Process / Processing", and "Supervisory Authority" have the meanings given in Applicable Data Protection Law.

---

2. Scope and Roles

2.1 The Parties acknowledge that for the purposes of Customer Personal Data processed under the Principal Agreement, the Controller is the data controller and we are the data processor.

2.2 The Platform Service is an **orchestration processor**: the Controller's Odoo environments and the data within them reside on infrastructure the Controller designates and engages directly (the Controller's chosen cloud provider, region, and storage destinations). OpenEducat manages the lifecycle of those environments via SSH and the platform admin console; under the default operating mode, Customer Personal Data held inside Controller environments does not transit OpenEducat-controlled infrastructure. The complete data-flow architecture, including the narrow exception paths where Customer Personal Data does transit our worker processes transiently, is set out at the head of **Schedule 1**.

2.3 The subject-matter, duration, nature, purpose, types of Personal Data and categories of Data Subjects of the processing are set out in **Schedule 1**.

2.4 Each Party shall comply with its respective obligations under Applicable Data Protection Law.

---

3. Instructions

3.1 We shall process Customer Personal Data only on documented instructions from the Controller, including with regard to Restricted Transfers, unless required to do so by law to which we are subject. In such a case, we shall inform the Controller of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

3.2 The Controller's instructions are set out in: - the Principal Agreement; - this DPA; - the Controller's use of the Platform Service via its admin console, API, and supported configuration interfaces; - any further written instructions provided by the Controller and acknowledged by us in writing.

For the purposes of this DPA, "documented instructions" means the sources listed above, and does not include oral instructions unless subsequently confirmed in writing.

3.3 We shall immediately inform the Controller if, in our opinion, an instruction infringes Applicable Data Protection Law.

---

4. Confidentiality

4.1 We shall ensure that personnel authorised to process Customer Personal Data are under appropriate obligations of confidentiality, whether contractual or statutory.

4.2 Access to Customer Personal Data within our organisation is limited to personnel who need it to perform their role in the provision of the Platform Service.

---

5. Security (Article 32)

5.1 We shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as described in **Schedule 2 (TOMs)**.

5.2 We shall review and, where appropriate, update the TOMs from time to time. Material reductions in protective effect will be communicated to the Controller in advance.

---

6. Sub-processors

6.1 The Controller provides general authorisation for us to engage Sub-processors to process Customer Personal Data, subject to this clause 6.

6.2 The current list of Sub-processors is set out in **Schedule 3**.

6.3 We shall notify the Controller of any intended additions or replacements of Sub-processors at least **fifteen (15) days** in advance, providing the new Sub-processor's name, location, and processing purpose. The Controller may object in writing within that period on reasonable data protection grounds. If the Parties cannot in good faith agree a resolution within thirty (30) days, the Controller may terminate the Principal Agreement and this DPA without penalty.

6.4 We shall impose data protection terms on each Sub-processor that are no less protective than this DPA. We remain liable to the Controller for any breach of this DPA caused by a Sub-processor.

7. Data Subject Rights

7.1 To the extent that the Controller is unable, in its use of the Platform Service, to address a request from a Data Subject seeking to exercise rights under Applicable Data Protection Law, we shall, on the Controller's documented request, provide reasonable assistance to the Controller in fulfilling that request, taking into account the nature of the processing.

7.2 We shall not respond to a Data Subject directly in relation to Customer Personal Data, except on the documented instructions of the Controller or as required by law. We shall inform the Controller promptly of any Data Subject request received that relates to Customer Personal Data.

---

8. Personal Data Breach

8.1 We shall notify the Controller of a Personal Data Breach without undue delay, and in any event within **seventy-two (72) hours** of becoming aware of the breach, providing such information as the Controller reasonably requires to fulfil its own breach notification obligations under Applicable Data Protection Law.

8.2 The initial notification shall include, to the extent then available: - the nature of the breach including the categories and approximate number of Data Subjects and records concerned; - the likely consequences; - the measures taken or proposed to address the breach and to mitigate possible adverse effects.

8.3 We shall provide updates and a final post-incident report as further information becomes available.

8.4 The notification address for breach reports is the Controller's billing email on file unless the Controller has provided a dedicated security contact in writing.

---

9. Data Protection Impact Assessment

9.1 On the Controller's reasonable request and taking into account the nature of the processing and the information available to us, we shall provide reasonable assistance to the Controller with any data protection impact assessment ("DPIA") or prior consultation with a Supervisory Authority that the Controller is required to conduct or perform under Applicable Data Protection Law.

---

10. Return or Deletion of Customer Personal Data

10.1 On termination or expiry of the Principal Agreement, the Controller may request return or deletion of all Customer Personal Data. We shall, at the Controller's choice: - return all Customer Personal Data in a structured, commonly-used, machine-readable format; or - delete all Customer Personal Data and existing copies,

within **thirty (30) days** of receipt of the Controller's instruction.

10.2 After the deletion or return period, we shall delete or anonymise any remaining Customer Personal Data and provide written confirmation of deletion within a further fifteen (15) days, except to the extent that (a) storage is required by applicable law (in which case we shall protect the confidentiality of such data and process it only for the purpose required by law), or (b) Customer Personal Data persists in routine backup rotations for the duration of the backup-retention cycle (not exceeding ninety (90) days from termination), during which it shall not be processed for any purpose and shall be securely destroyed at the end of that cycle.

---

11. Audit and Inspections

11.1 We shall make available to the Controller all information necessary to demonstrate compliance with this DPA and Article 28 of the UK GDPR / EU GDPR, and shall allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller, in accordance with this clause.

11.2 Audits shall: - be performed no more than once per twelve (12) month period (more often if required by a Supervisory Authority or following a confirmed Personal Data Breach); - be carried out during normal business hours with at least thirty (30) days' prior written notice; - not unreasonably interfere with the operation of the Platform Service; - be subject to the auditor signing reasonable confidentiality undertakings; - bear the Controller's own costs, unless the audit reveals a material breach of this DPA by us, in which case we shall bear reasonable audit costs.

11.3 In the first instance, the Controller agrees that the information set out in our annual security report and the TOMs in Schedule 2 may be sufficient to demonstrate compliance. We will provide updated security documentation on reasonable request.

---

12. International Transfers

12.1 The Parties acknowledge that processing of Customer Personal Data may involve transfers to countries outside the UK and the EEA, including to the locations of Sub-processors listed in Schedule 3.

12.2 To the extent that a transfer of Customer Personal Data constitutes a Restricted Transfer, the Parties enter into the **SCCs**, incorporated by reference into this DPA, as follows: - The Controller is the data exporter; we are the data importer. - Module Two (controller to processor) applies, where the Parties' relationship is controller-to-processor. - Clause 7 (docking clause) is included. - Clause 9(a): general authorisation for Sub-processors as described in clause 6 above, with **fifteen (15) days'** notice. - Clause 11(a): the optional language is not used. - Clause 17 (governing law): the law of the Republic of Ireland applies, as a Member State of the European Union. - Clause 18 (jurisdiction): courts of the Republic of Ireland have jurisdiction. - Annex I.A (Parties) is populated from the Parties section above. - Annex I.B (Description of

transfer) is set out in Schedule 1. - Annex I.C (competent supervisory authority): the Irish Data Protection Commission, acting as competent supervisory authority for the SCCs concluded under this DPA. - Annex II (TOMs) is set out in Schedule 2. - Annex III (List of Sub-processors) is set out in Schedule 3.

12.3 For transfers from the United Kingdom, the **UK International Data Transfer Addendum** to the SCCs applies. The Addendum is hereby incorporated by reference, with Tables 1, 2 and 3 populated from the Parties section, this clause, and Schedules 1–3 respectively. Table 4 (alternative termination): “Importer”.

---

13. Liability

The liability provisions of the Principal Agreement apply to the performance of this DPA. Nothing in this DPA limits any liability that cannot be limited under Applicable Data Protection Law.

---

14. Term and Termination

This DPA shall remain in force for as long as we process Customer Personal Data on the Controller’s behalf under the Principal Agreement. Clauses 10 (Return or Deletion) and 11 (Audit) survive termination.

---

15. Order of Precedence

In the event of any conflict between this DPA and the Principal Agreement, this DPA governs in respect of the processing of Customer Personal Data. In the event of any conflict between this DPA and the SCCs, the SCCs govern.

---

16. Governing Law and Jurisdiction

This DPA is governed by the laws of the State of Delaware, United States, without reference to its conflict-of-laws principles. The state and federal courts located in the State of Delaware have exclusive jurisdiction over any disputes arising out of or in connection with this DPA, save that, for transfers from the United Kingdom or the European Economic Area, the Standard Contractual Clauses incorporated under clause 12 are governed by the law and courts identified there.

Signatures

For the Processor:

Signed: _____

Name: Parthiv Patel

Title: Director

Date: _____

For the Controller:

Signed: _____

Name: [CONTROLLER SIGNATORY NAME — FROM CUSTOMER]

Title: [CONTROLLER SIGNATORY TITLE — FROM CUSTOMER]

Date: _____

Schedule 1 — Description of Processing

How processing happens (data-flow architecture)

The oec.sh Platform Service is an **orchestration processor**. Customer Personal Data is stored and processed inside Controller-designated infrastructure (the cloud VMs, regions, and storage destinations the Controller chooses, configures, and owns the relationship with). The Platform Service control plane orchestrates that infrastructure via SSH; it does not, under any normal operating mode, ingest or persistently store the Personal Data held inside Controller environments.

Data movement	Where bytes flow	Do bytes transit OpenEducat infrastructure?
Scheduled backups to S3-compatible / FTP / object-storage destinations	Controller's Odoo container → Controller's chosen storage destination, via a curl process executed on the Controller's VM	**No.** OpenEducat triggers the job via SSH and verifies completion by reading the destination object; the backup bytes never enter an OpenEducat process.
Restore from such destinations	Controller's storage destination → Controller's VM, via curl on the VM	**No.**
Migration from external Odoo platforms (Odoo.sh and similar)	Source platform → Controller's target VM, via a curl process executed on the target VM	**No.** OpenEducat monitors progress over SSH but does not buffer the dump.
Clone (within the same Controller VM)	Source container → target container via `docker cp` on the host	**No.**
Backup or restore via SFTP destinations	Storage destination ↔ OpenEducat worker (transient buffer) ↔ Controller's VM	**Yes, transiently** (seconds, in worker memory or temporary file, deleted on completion or failure). This path applies only when the Controller has chosen an SFTP destination.
Clone across different Controller VMs	Source VM → OpenEducat worker (transient buffer) → target VM	**Yes, for the duration of the transfer** (minutes, in a worker temporary file, deleted on completion or failure). This path applies only when source and target environments live on different customer-designated VMs.
Control-plane data (admin login records, audit logs, billing data, encrypted credentials	Stored on OpenEducat-controlled infrastructure	**Yes.** This is the data the Platform Service holds in its own right as a Processor, and is subject to Schedule 2.

Data movement	Where bytes flow	Do bytes transit OpenEducat infrastructure?
granting access to Controller-designated infrastructure)		

The exception paths (SFTP destinations, cross-VM clone) are documented in writing to Controllers who select them; the default paths (S3-compatible / FTP / object-storage destinations and same-VM clone) involve no data transit through OpenEducat infrastructure.

Item	Detail
Subject-matter	Provision of the oec.sh Platform Service, including environment lifecycle management, backup orchestration, monitoring, and related operations.
Duration	For the term of the Principal Agreement plus any post-termination data retention period set out in clause 10.
Nature and purpose	Processing of Customer Personal Data necessary for the Controller to use the Platform Service to deploy, operate, and back up its Odoo environments. Specifically: (a) deploying customer-supplied container images and configuration; (b) orchestrating periodic backups and restores on the Controller's behalf to the Controller's designated storage destination; (c) generating control-plane monitoring metrics and audit-log records (which describe administrative actions taken in the Platform Service, not data content from Controller environments); (d) sending platform notifications via email and other channels enabled by the Controller.
Types of Personal Data	**(a) Inside Controller environments** (resident on Controller-designated infrastructure; orchestrated but not ingested by OpenEducat per the data-flow architecture above): Personal Data the Controller chooses to store within its Odoo environments, which may include customer names, contact details, billing addresses, transaction records, employee records, and any other categories the Controller chooses to load. We do not directly access this data in our role as Processor except (i) on the exception paths described above (SFTP destinations and cross-VM clones, transient transit only), or (ii) during a Controller-initiated and time-limited support session with explicit written authorisation. **(b) Inside the Platform Service control plane** (stored on OpenEducat-controlled infrastructure): Controller administrator email addresses, login timestamps, IP addresses, audit-log entries for actions taken by Controller users within the Platform Service, billing data, and encrypted credentials granting access to Controller-designated infrastructure.

Item	Detail
Special Categories of Personal Data	The Controller represents and warrants that it shall not process Special Categories of Personal Data within the Platform Service without first having entered into appropriate supplementary controls in writing with us. Where the Controller intends to process Special Category data, the bilateral notification-and-confirmation procedure in Schedule 4 §S4.5 governs the activation of the supplementary terms in Schedule 4.
Categories of Data Subjects	The Controller's own customers, suppliers, employees, contractors, and other individuals whose Personal Data the Controller loads into the Platform Service; the Controller's users of the Platform Service admin console (administrators, developers).
Frequency	Orchestration and control-plane processing: continuous, for the duration of the Controller's use of the Platform Service. Transit of Customer Personal Data through OpenEducat infrastructure: only on the exception paths set out in the Schedule 1 preamble, and only for the duration of the relevant operation.
Retention	For the duration of the Principal Agreement plus the period set out in clause 10 of this DPA.

Schedule 2 — Technical and Organisational Measures (TOMs)

The following measures apply across the Platform Service.

2.1 Access Control

- All access to the Platform Service control plane requires authenticated login with multi-factor authentication available to all users and enforced for personnel with elevated privileges.
- Role-based access control governs which Platform Service personnel may access Controller environments. The default posture is least-privilege; elevated access requires logged, time-limited approval.
- Customer environments (Odoo containers, databases, filestore) run isolated on the Controller's designated infrastructure. Platform Service personnel do not have routine access to data inside Controller environments; access is initiated only on Controller request, time-limited, and logged.

2.2 Network Security

- Public ingress to customer environments is routed via Traefik with enforced TLS 1.2+, modern cipher suites, and automatic certificate renewal via Let's Encrypt or via the Controller's wildcard certificate where supplied.
- Platform control-plane SSH egress originates from a single static IP address per environment. Customers can allowlist this IP at their firewall.
- Cloudflare WAF and DDoS protection sit in front of the platform admin console.
- All admin-console traffic served over HSTS-pinned TLS with strict transport headers.

2.3 Encryption

- **In transit**: TLS 1.2+ for all platform-to-customer, customer-to-platform, and platform-to-Sub-processor connections.
- **At rest (control plane)**: Encrypted database storage. Customer secrets (SSH private keys, cloud-provider API credentials, OAuth tokens, Stripe keys, backup-destination credentials) encrypted at rest using Fernet (AES-128-CBC + HMAC-SHA256) with a key managed by OpenEducat Inc. in production secret storage.
- **At rest (customer environment)**: Encrypted block storage on the customer-designated cloud provider (default: AWS EBS gp3, GCP Persistent Disk, Hetzner volume, etc. — depending on provider).
- **At rest (backups)**: Backup destination encryption is configured by the Controller (S3 SSE-S3 / SSE-KMS, GCS CMEK, R2 default encryption, etc.). We support customer-managed-key configurations where the destination supports them.

2.4 Backup and Disaster Recovery

- Automated backups run on a Controller-configured schedule per environment, written to the Controller's designated S3-compatible bucket or other supported destination.
- Backup integrity verified by a daily watchdog that checks the destination object for presence and reports drift.
- Each backup includes a database dump and the Odoo filestore; full restore is supported into a fresh environment.
- The Platform Service control plane itself is backed up daily by OpenEducat Inc. for our own operational recovery; Customer Personal Data inside customer environments is NOT in the control-plane backup.

2.5 Logging and Monitoring

- **Application logs** (errors, request traces, performance metrics, debug output) for the Platform Service control plane are centralised, retained for **ninety (90) days**, and accessible only to authorised platform personnel.
- **Audit log** records every administrative action taken through the platform admin console (login, environment create / destroy, configuration change, backup trigger, role change, member invite, billing change). Audit-log entries are retained for at least **twelve (12) months** on the control-plane database and are available to the Controller for actions taken within its organisation.
- Active platform-level incident detection runs continuously: backup failures, environment health, migration progress, cron health, queue backlog, and certificate distribution.
- Critical-severity platform incidents trigger paged response via Slack / email integrations.

2.6 Vulnerability and Patch Management

- Container base images rebuilt and patched on a scheduled cadence.
- Dependency scanning runs on every release build via standard Python and Node.js tooling.
- Security-relevant CVEs in our dependencies tracked and patched within timeframes commensurate with severity.

2.7 Change Management

- All control-plane changes deployed via reviewed pull requests with automated test suite and pre-deploy compile checks.
- Rolling deploys with health-check gates before traffic shifts.
- Pre-deploy migrations run as one-shot containers with PostgreSQL advisory-lock concurrency protection.
- Rollback images preserved at every deploy.

2.8 Sub-processor Management

- Each Sub-processor (Schedule 3) bound by terms no less protective than this DPA.
- Sub-processor list reviewed annually; additions communicated per clause 6.

2.9 Personnel

- Background checks on personnel with access to Customer Personal Data.
- Confidentiality obligations cover all personnel under contract or employment.
- Security training on onboarding and annually thereafter.
- Off-boarding revokes all access within one business day of departure.

2.10 Incident Response

- Incident-response practice with documented severity tiers and an accountable owner for each open incident. Founder-led on-call coverage today; expansion to a multi-person rotation alongside the 2026 H2 SOC 2 readiness programme.
- Personal Data Breach notification to Controller within seventy-two (72) hours of awareness (clause 8).
- Post-incident review (PIR) on Severity 1 incidents; PIR shared with Controller on request. A standardised written PIR template is being formalised as part of the SOC 2 readiness programme.

2.11 Physical Security

- All control-plane infrastructure hosted at Sub-processor data centres meeting ISO 27001 or equivalent. We do not operate any owned physical data centre.

2.12 Testing

- Application security testing on every release (linting, type checking, automated test suite).
- Regular review of the TOMs against ISO 27002 / SOC 2 control families.
- Independent third-party penetration testing scoped, with target window 2026 H2 alongside SOC 2 Type II observation. On completion, an executive summary will be made available on request under NDA, with at least annual cadence thereafter.

2.13 Data Minimisation

- The Platform Service collects only the operational data required to provide the service (admin email, login timestamps, audit log entries, billing data, support ticket data).
- We do not request, scrape, or retain Personal Data stored inside Controller environments outside of the Controller’s explicit backup configuration.

Schedule 3 — Approved Sub-processors

Effective as of the date of this DPA.

A Sub-processor is a third party we engage to process Customer Personal Data on our behalf in connection with the Platform Service. The list below covers entities that act on our instruction. Identity providers used for Controller user authentication (Google, Microsoft, Apple, etc.), source-code hosts the Controller connects (GitHub, GitLab, Bitbucket), and infrastructure providers the Controller chooses for its own environments (AWS, Google Cloud, Hetzner, DigitalOcean, Linode, OVH, etc.) are NOT our Sub-processors: they act on the Controller's own instruction or on the Data Subject's instruction, and the Controller maintains its own data processing relationship with them.

Sub-processor	Purpose	Location of processing	Transfer mechanism
Hetzner Online GmbH	Compute and storage for the platform control plane	Germany (Falkenstein / Nuremberg / Helsinki)	GDPR-internal — EU controller-processor
DigitalOcean, LLC	Compute and storage for platform supporting infrastructure (where applicable; not for Controller-designated customer environments)	US, with EU regions where used	SCCs
Cloudflare, Inc.	DNS, WAF, CDN, DDoS mitigation, TLS termination for the platform admin console and customer subdomain routing	US, with global edge	SCCs
Stripe, Inc.	Billing and payment processing for the Platform Service subscription	US, with EU entities for European customers	SCCs
Mailgun Technologies, Inc.	Transactional email delivery (account, billing, system notifications)	US, with EU region for European customers	SCCs
Functional Software, Inc. (Sentry)	Application error monitoring of the Platform Service control plane, with PII scrubbing applied before transmission	US	SCCs

Sub-processor	Purpose	Location of processing	Transfer mechanism
	(the scrubbing scheme is described in the Internal Controls Description, §6.6)		
PostHog Inc.	Product analytics on the Platform Service admin console (Controller user actions; no Customer Personal Data inside Controller environments)	US, with EU instance available	SCCs
Let’s Encrypt (Internet Security Research Group)	Automated SSL certificate issuance for platform domains and customer subdomains using public-key infrastructure	US	N/A — no Personal Data transferred

Not in scope (these are not our Sub-processors under this DPA):

- **Controller-designated cloud providers** for Controller environments (e.g., AWS for an environment the Controller chose to provision on AWS). The Controller engages these providers directly and maintains the data processing relationship with them. We orchestrate, but do not process on the Controller’s behalf at the storage layer for the Controller’s own infrastructure.
- **Identity providers** used by Controller users to sign in to the admin console (Google, Microsoft, Apple, passkey providers). These authenticate the user on the user’s own behalf, not on our instruction.
- **Source-code hosts** the Controller chooses to connect for environment deployments (GitHub, GitLab, Bitbucket). The Controller’s git connection is a direct relationship between the Controller and the host.

Updates to this list are governed by clause 6 of this DPA.

Schedule 4 — Special Conditions for Healthcare and Other Sensitive Data

Where the Controller intends to process healthcare data, special-category data under Article 9 of the GDPR, or other regulated data (collectively, “Sensitive Data”) within the Platform Service, the following supplementary terms apply:

S4.1 The Controller represents that it has a lawful basis under Article 9 GDPR and any applicable sector-specific regulation (UK NHS DSPT, HIPAA where US data is involved, etc.) for the intended processing.

S4.2 For US healthcare data subject to HIPAA, the Parties will enter into a separate Business Associate Agreement meeting the requirements of 45 C.F.R. § 164.504(e). For UK / EEA healthcare data, the UK GDPR / EU GDPR together with this DPA constitute the data protection framework.

S4.3 The Controller is solely responsible for: (a) configuring its environments and backup destinations to meet its regulatory obligations; (b) restricting Platform Service users (administrators, developers) to those who are authorised under the applicable healthcare regulations to access Sensitive Data.

S4.4 We will not access Sensitive Data inside a Controller environment without an explicit, time-limited, written request from a Controller representative. Each such access is logged in the platform audit log and surfaced to the Controller.

S4.5 This Schedule 4 applies to Sensitive Data processing once (a) the Controller has notified us in writing of the intended processing, the categories of Sensitive Data involved, and the lawful basis under Applicable Data Protection Law; and (b) we have confirmed in writing that the Platform Service is suitable to support the intended processing. Either Party may propose further supplementary terms specific to the Sensitive Data category before that confirmation is given.

Schedule 5 — Policy Acceptance Audit Log

Added 2026-06-03.

When the Controller upgrades to or renews a paid plan on the Platform Service, the Platform records an audit log entry documenting the Controller's acceptance of the No Refund Policy at the moment of payment. The entry preserves the policy version in force at the time, together with a forensic copy of the request (IP address, user agent, checkbox state) where the moment is customer-initiated. This Schedule sets out the categories of data collected, the retention period, and the treatment of those records under data subject rights requests.

5.1 Categories of Data Collected

- The Platform Service user account and email address that confirmed the acceptance interstitial.
- The Controller organisation for which the acceptance was given.
- The policy version in force at the time of acceptance (e.g., `2026-05-18`).
- For the customer-initiated interstitial moment: the source IP address and user-agent string of the request.
- For Stripe-side moments (checkout session completion, subscription creation, subscription renewal): no IP address or user-agent string, because the recording is triggered by a server-to-server webhook from Stripe to the Platform Service and no Data Subject browser is in the request path.
- A copy of the Stripe webhook payload that triggered the recording.

5.2 Retention Period

The Platform Service retains policy acceptance audit log entries indefinitely. The entries are the legal evidence that the No Refund Policy was enforceable at the moment of payment and are required for chargeback defence. The Platform Service retains each entry for as long as the Controller account exists and for the longest applicable statute of limitations after account closure (typically up to seven (7) years), regardless of any earlier deletion of the underlying Controller account.

5.3 Data Subject Rights

On a verified data subject access request from a Data Subject identified in a policy acceptance audit log entry, we shall:

- Disclose the user-facing fields (timestamp, policy version, acknowledgments confirmed, policy URL).
- Redact the forensic webhook payload field (`raw_payload`) before disclosure, in order to avoid re-disclosing any third-party data that Stripe may have included in the payload.

- Retain the underlying row after the request is closed, because the row remains load-bearing for chargeback defence under clause 5.2 above.

5.4 Withdrawal of Acceptance

A recorded acceptance cannot be retroactively withdrawn: it was given at the moment of payment and reflects a contractual position at that time. The Controller may cancel its subscription at any time from the Platform Service admin console (Settings → Billing). Cancellation stops future renewals but does not modify or remove the historical audit log entry.

End of DPA.