

# Legentibus Data Security and Privacy Plan

Version 1.0 · 15 October 2026

---

## Scope and purpose

This plan sets out how Legentibus AB protects the personal data of students and teachers that it processes for schools and school districts, in the United States and in Europe. It forms part of the data protection agreement Legentibus signs with each school. It is the Data Security and Privacy Plan required by New York Education Law § 2-d and 8 NYCRR Part 121, and the description of security measures for agreements under the EU General Data Protection Regulation (GDPR).

Legentibus AB (org. no. 559432-8337, Nacka Strand, Sweden) makes Legentibus, an app for learning Latin, among other things by reading and listening to Latin texts, with tools such as synced audio, dictionaries, translations and courses. Teachers can create classes and student accounts, set reading assignments and follow their students' progress.

## Data collected and how it is used

Legentibus collects only the data needed to run the service, and uses it only to provide the service to the school, as set out in the school's agreement with Legentibus.

| Who      | Data                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Students | Name; email address (used as username); password, stored hashed; school and class membership; reading progress, reading and listening time, and assignment progress; word lookups and search queries; optional error reports on texts; app settings; diagnostic messages sent by the app; device data (device ID, device type and settings, app version, time zone, IP address, and country derived from it) |
| Teachers | Name; email address (used as username); password, stored hashed; school; the classes and assignments the teacher creates; for teachers who also read in the app, the same app and device data as students                                                                                                                                                                                                    |

Legentibus does not collect dates of birth, gender, ethnicity, addresses, phone numbers, grades, test scores, disability or health information, or teacher or principal evaluation data (APPR data). Teachers can create student accounts without an email address; the student then gets a generated username that does not identify them.

Legentibus never sells student or teacher data, never uses it for targeted advertising, and never builds profiles of students except for the educational purpose of the service. Students never receive marketing email, and student and teacher accounts are excluded from all advertising measurement. Legentibus may email teachers and school contacts about the service, such as new features and offers for the school; they can opt out of these emails at any time. For schools in Europe, offers go only to the school's contact person and to teachers who have asked for them.

## Legal framework

The school decides what data is processed and why; Legentibus processes it only on the school's instructions. Each school's agreement and the laws below set the rules, and this plan describes how Legentibus meets them.

|                                      | United States                                                                                                                        | European Union                                                                                                                           |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Main laws</b>                     | FERPA, COPPA, New York Education Law § 2-d and 8 NYCRR Part 121, and the state laws named in the school's DPA                        | GDPR, and national education rules such as the Dutch Privacy Covenant for Digital Educational Resources                                  |
| <b>Role of Legentibus</b>            | Treated as a "school official" under FERPA (34 CFR § 99.31), solely for access to student records; third-party contractor (New York) | Processor acting for the school, which is the controller (GDPR Article 28)                                                               |
| <b>Agreement</b>                     | Student Data Privacy Consortium National DPA, with state exhibits                                                                    | The school's data processing agreement, for example the Dutch Model Data Processing Agreement 4.0                                        |
| <b>Parents' and students' rights</b> | Through the school; the school's Parents Bill of Rights for Data Privacy and Security is part of this plan                           | Access, correction and deletion through the school; Legentibus helps the school answer requests                                          |
| <b>Where data is stored</b>          | In the United States (AWS)                                                                                                           | In the United States, under the EU standard contractual clauses in the AWS Data Processing Addendum and the EU-US Data Privacy Framework |

Legentibus helps the school answer a request from a parent, student or authority, and passes on any request it receives directly to the school. Parents, students and teachers can challenge the accuracy of their data through the school, and Legentibus makes any correction the school asks for.

## Security safeguards

Legentibus aligns its security practices with the NIST Cybersecurity Framework v1.1. The table groups the measures by the framework's five functions; the same measures answer the controls of the Dutch ROSA framework.

| NIST CSF function | Measures                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identify</b>   | A written inventory of the personal data held (see "Data collected") and of every system and subprocessor that touches it.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Protect</b>    | All data encrypted at rest with AES-256 (AWS KMS): the database, server disks, file storage and backups. All traffic encrypted in transit with TLS: between users and Cloudflare, between Cloudflare and the server, and between the server and the database. Passwords stored only as bcrypt hashes. The database sits in a private network with no public access. Personal sign-ins with two-factor authentication for every AWS user, and no shared accounts. Server access through AWS Systems Manager, with no SSH passwords. Automatic security updates for the operating system. Login attempts limited to 10 per account per minute. |

| NIST CSF function | Measures                                                                                                                                                                                                                                |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Detect</b>     | AWS CloudTrail records every administrative action, kept for at least one year. Application logs are kept for 14 days. Alarms on server and database health and on unusual costs go to both staff members.                              |
| <b>Respond</b>    | A documented incident procedure (see "Incidents and data breaches") with notice to affected schools within 72 hours.                                                                                                                    |
| <b>Recover</b>    | Automatic daily database backups with point-in-time restore, kept for at least 14 days, plus a copy in a second location. Restores are tested at least once a year and after any change to the backup setup, and each test is recorded. |

## Staff access and training

Two people can access personal data: Johan Winge (developer, and privacy and security contact) and Daniel Petterson (CEO). Legentibus uses no contractors with access to personal data. Staff work from Sweden, in the EU.

- Access is given only to staff who need it to run the service, and only to the extent they need it.
- Everyone with access signs a written confidentiality undertaking before getting access.
- Everyone with access completes privacy and security training before getting access and every year after: GDPR, FERPA and New York Education Law § 2-d, and this plan.
- When someone leaves, their access is removed the same day.

## Subprocessors

Legentibus uses seven subprocessors for school accounts. Each is bound by a written data processing agreement with obligations at least as strict as Legentibus's own.

| Subprocessor                                          | Purpose                                                                                                           | Personal data                                                                            | Location                                   |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|--------------------------------------------|
| <b>Amazon Web Services</b>                            | Hosting, database, file storage, backups                                                                          | All data listed in "Data collected"                                                      | United States                              |
| <b>Cloudflare</b>                                     | Network protection and encrypted connections                                                                      | All traffic in transit, including IP addresses                                           | Global network; Cloudflare is a US company |
| <b>Stripe</b>                                         | Invoicing and payment for school licences                                                                         | The school's billing contact: name, email address, billing address. No student data      | Ireland and United States                  |
| <b>Mailchimp and Mailchimp Transactional (Intuit)</b> | Sending account emails (login details for new accounts, password resets) and emails to teachers about the service | Email address and name of the student or teacher; the generated password in login emails | United States                              |
| <b>ipinfo.io</b>                                      | Finding the country from an IP address                                                                            | IP address                                                                               | United States                              |
| <b>Google</b>                                         | Optional sign-in with Google                                                                                      | Name and email address                                                                   | United States                              |

| Subprocessor | Purpose                         | Personal data                                  | Location      |
|--------------|---------------------------------|------------------------------------------------|---------------|
| ClickUp      | Tracking error reports on texts | Error report text, without the user's identity | United States |

School accounts are excluded from advertising measurement (Meta), and students from marketing email. App store payments (Apple, Google Play) are used only for individual subscriptions, never for school accounts.

Legentibus tells schools at least 30 days before a new subprocessor starts handling their personal data, or longer where the school's agreement requires it (six weeks under the Dutch Model Data Processing Agreement), so a school can object. This covers only services that receive personal data of school users, not the tools used to build the app. When a change is urgent for security or to keep the service running, Legentibus may make it sooner and tells schools at once.

## Incidents and data breaches

Legentibus notifies every affected school without undue delay, and at the latest within 72 hours of confirming a breach of personal data.

1. **Detect and contain:** whoever notices a possible incident tells the privacy and security contact at once. Access is cut off and evidence kept.
2. **Assess:** what happened, when, which data and which schools are affected, and how many people.
3. **Notify:** the school's named contact gets a written notice by email containing the date and nature of the breach, the categories and approximate number of people and records involved, the likely consequences, the measures taken, and a contact person. Information not yet known follows as it becomes available.
4. **Cooperate:** Legentibus helps the school inform parents, students, staff and authorities. It does not contact them itself unless the school asks or the law requires it.
5. **Learn:** every incident, including suspected ones, is logged with its cause and the fix, and this plan is updated where needed.

## Return and deletion of data

When a school's agreement ends, Legentibus asks the school by email whether it wants its data returned, kept for a period it sets in writing, or deleted. Unless the school asks to keep it, Legentibus deletes the data 90 days after that email. A school can also ask for deletion at any time; Legentibus then deletes the data within 90 days.

- **Return first, if asked:** before deletion the school can ask for an export of its students' and teachers' data, delivered as CSV files.
- **What is deleted:** the accounts of the school's students and teachers, with everything linked to them: reading progress, usage data, lookups, error reports, device data, classes and assignments.
- **Backups:** deleted data disappears from the rolling backups as they expire, within 35 days at most. Backups are encrypted and never restored except to recover the service.
- **Confirmation:** Legentibus confirms the deletion to the school in writing.
- **Retention without a request:** data is kept only while the school uses the service, and after that only as described above. A student who leaves the school is deleted on the school's request.

Storage media at AWS are destroyed using methods consistent with NIST SP 800-88, as set out in AWS's own security documentation.

## **Contact and review**

Questions about privacy or security, requests, and incident reports go to Johan Winge, privacy and security contact, at [johan@legentibus.com](mailto:johan@legentibus.com).

Legentibus AB, Cylandervägen 18, 131 52 Nacka Strand, Sweden. Org. no. 559432-8337.

This plan is version 1.0. It is reviewed at least once a year and after any significant change to the service, its hosting or its subprocessors.