Renode LMS Platform Data Protection and Compliance Document

Effective date: 24 May 2026
Document owner: Renode Technologies (Pty) Ltd
Platform: Renode LMS Platform / OpenCampus LMS
Audience: Enterprise clients, government stakeholders, legal reviewers, security teams, developers and internal staff

Executive Summary

This document describes the data protection, cybersecurity and compliance posture for the Renode LMS Platform. It is intended to support enterprise due diligence, government procurement review, internal governance and legal compliance assessment.

The LMS processes education records, child learner data, user-generated content, support tickets, identity records, institutional branding, payment references and technical security logs. Because the platform is used in education environments, its governance model prioritises lawful processing, child protection, role-based access, tenant isolation, secure storage, auditability and resilience.

This document addresses POPIA, GDPR, CCPA/CPRA, the South African Consumer Protection Act, NIS2 and general cybersecurity governance.

Compliance Frameworks

POPIA

Scope

POPIA regulates the processing of personal information by public and private bodies in South Africa. The LMS processes personal information relating to learners, teachers, sponsors, admins and provider staff.

Applicability to the LMS

Institutions typically act as responsible parties for their education data. Renode Technologies acts as an operator where it processes institution data under instruction, and as a responsible party for its own website, support, provider portal, demo request and commercial records.

Compliance Obligations

Obligation LMS Application
--- ---
Accountability Assign privacy responsibilities and maintain governance controls.
Processing limitation Process data for lawful education and platform purposes.
Purpose specification Define why user and learner data is collected.
Further processing limitation Avoid incompatible secondary use.
Information quality Support correction of inaccurate records.
Openness Provide privacy notices and processing transparency.
Security safeguards Apply technical and organisational security controls.
Data subject participation Support access, correction and objection requests.

Organisational Responsibilities

Renode Technologies must maintain operator controls, security safeguards, incident

procedures and support for institution-led privacy requests. Institutions must ensure lawful learner onboarding, consent where required and appropriate user administration.

GDPR

Scope

The GDPR applies to personal data of individuals in the European Economic Area where the platform is used by EU-based institutions, EU learners, EU staff or where processing is otherwise subject to GDPR.

Applicability to the LMS

The LMS may be a processor for institution-controlled EU personal data and a controller for Renode-controlled commercial or support data.

Compliance Obligations

The platform governance model supports transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability. GDPR rights include access, rectification, erasure, restriction, objection, portability and rights relating to automated decision-making where applicable.

CCPA/CPRA

Scope

The CCPA/CPRA applies to certain businesses processing personal information of California residents when statutory thresholds are met.

Applicability to the LMS

The LMS is not designed to sell personal information. Where CCPA/CPRA applies, Renode Technologies must provide required notices and honour verified consumer requests in line with applicable thresholds.

Compliance Obligations

Right or Obligation LMS Response
--- ---
Right to know Provide categories and purposes of processing.
Right to delete Support deletion where lawful and technically possible.
Right to correct Support correction of inaccurate information.
Right to opt out The platform does not require sale of personal information for core operation.
Sensitive information Restrict sensitive information processing to necessary purposes.
Non-discrimination Do not penalise users for exercising privacy rights.

Consumer Protection Act South Africa

Scope

The Consumer Protection Act, 2008 regulates fair marketing, fair terms, service quality, disclosure and consumer rights in South Africa.

LMS Application

The platform’s commercial terms must be clear, fair and transparent. Subscription pricing, renewal terms, service limitations, cancellation processes and support obligations must be communicated accurately.

NIS2

Scope

NIS2 is an EU cybersecurity directive intended to strengthen cybersecurity risk management and incident reporting across essential and important entities and certain digital service providers.

LMS Application

NIS2 may be relevant where Renode Technologies or its customers operate in EU-regulated sectors or provide services to EU entities. The platform’s cybersecurity governance should align with NIS2 risk management principles even where NIS2 is not directly applicable.

Compliance Obligations

Relevant measures include risk management, incident response, supply chain security, vulnerability management, access control, encryption, business continuity, security monitoring and management accountability.

General Cybersecurity Governance

The platform should align with recognised security principles including least privilege, defence in depth, secure development, vulnerability management, incident readiness, auditability and resilience.

Security Controls

Identity and Access Management

Control Description
--- ---
Role-based access Admin, teacher, learner, sponsor and provider roles have defined permissions.
Tenant scoping Institution users may access only their institution’s records.
Provider access control Provider portal roles separate support, finance, sales, UI/UX, language editing and super admin functions.
Session timeout Users are logged out after inactivity.
SSO Institution-managed Google, Microsoft or generic OIDC SSO is supported.
Password handling Argon2id hashing and forced reset for imported users.

Incident Response

Renode Technologies should maintain an incident response plan covering:

1. Detection and triage.
2. Containment.
3. Evidence preservation.
4. Impact assessment.
5. Customer and regulator notification.
6. Remediation.

7. Lessons learnt.

Incidents involving child data must be escalated with heightened urgency and sensitivity.

Risk Management

Risk management should include:

- Regular risk assessments.
- Security control reviews.
- Legal and regulatory impact assessments.
- Third-party risk scoring.
- Vulnerability tracking.
- Data protection impact assessments for high-risk processing.

Vendor Management

Critical vendors include hosting providers, payment providers, cloud storage providers, meeting providers, email services, SSO providers and monitoring tools. Vendor management must assess privacy terms, security controls, data locations, breach notification commitments and service continuity.

Vulnerability Management

The platform should operate:

- Secure coding practices.
- Dependency inventory.
- Vulnerability scanning.
- Patch management.
- Penetration testing before major production releases.
- Remediation tracking.
- Change control.

Data Governance

Data Classification

Classification Examples Controls
--- --- ---
Public Marketing website content. Standard web controls.
Internal Operational notes, staff procedures. Staff-only access.
Confidential Support tickets, institution configurations. Role-based access and audit logging.
Restricted Child learner data, grades, assessment answers, credentials. Strong access control, encryption, retention limits and breach escalation.

Data Retention

Data retention must be based on law, contract, education policy and operational necessity. Retention schedules should be approved by legal, compliance and institutional stakeholders.

Data Minimisation

The LMS should collect only information needed for learning delivery, administration, support, security, payment and compliance purposes.

Consent Management

Where consent is required, the institution must maintain records of consent or lawful authorisation. Consent should be specific, informed, voluntary and revocable where applicable.

Data Processing Registers

Renode Technologies should maintain processing registers that document:

- Categories of data subjects.
- Categories of personal information.
- Processing purposes.
- Recipients and operators.
- Cross-border transfers.
- Retention periods.
- Security measures.

Cross-Border Transfers

Cross-border transfers must use lawful mechanisms such as contractual safeguards, data processing agreements, transfer impact assessments and adequate technical controls.

Data Breach Procedures

The breach procedure must include:

1. Internal incident logging.
2. Technical containment.
3. Determination of affected data.
4. Risk assessment to data subjects.
5. Institution notification.
6. Regulator notification where required.
7. Data subject notification where required.
8. Corrective action and board-level reporting for material incidents.

Operational Policies

Staff Responsibilities

Staff must:

- Access only data needed for their role.
- Use approved systems and credentials.
- Report suspected incidents promptly.
- Protect child and learner data.
- Follow customer support and reset-link procedures.
- Avoid unauthorised exports of personal information.

Security Awareness

Security awareness should cover phishing, password safety, child data protection, POPIA responsibilities, incident reporting, secure file handling and acceptable system use.

Access Reviews

Access reviews should be conducted regularly for provider users, institution admins, support agents, privileged accounts and integration credentials.

Third-Party Risk Assessments

Third-party risk assessments should evaluate:

- Data processed.
- Sub-processors.
- Location of processing.
- Security certifications.
- Incident history.
- Contractual safeguards.
- Business continuity.

Audit Readiness

Renode Technologies should maintain:

- Current privacy policies.
- Terms of Use.
- Data processing agreements.
- Security policies.
- Access review evidence.
- Incident logs.
- Backup restore test records.
- Vendor assessments.
- Penetration test reports.
- Change management records.

Compliance Reporting

Compliance reporting should be provided to management and, where applicable, customers. Reports should include security incidents, access reviews, vendor risks, vulnerability status, audit findings, data subject requests and remediation progress.

Business Continuity and Disaster Recovery

The production architecture should define:

Area	Control
Database	Automated encrypted backups, restore testing and replication strategy.
Application	Versioned deployments and rollback capability.
Storage	Replicated object storage and access controls.
DNS/CDN	Akamai failover and load balancing.
Monitoring	Availability, error and performance alerting.
RPO/RTO	Contractually agreed recovery objectives.

User Generated Content Governance

User Generated Content includes course material, PDFs, videos, online class recordings, messages, forum posts, comments, assessment responses and uploaded SCORM packages.

Controls include:

- Upload validation and file type restrictions.
- Institution ownership and tenant scoping.
- Admin and teacher moderation rights.
- Removal rights for unlawful or harmful content.
- Copyright and intellectual property obligations.
- Child safeguarding review for learner-facing content.
- Retention controls for recordings and learning records.

Compliance Roadmap

Recommended next steps:

1. Formalise data processing agreements with institutional customers.
2. Implement centralised audit logging.
3. Complete Google Cloud Storage signed delivery integration.
4. Add MFA for provider users and institution admins.
5. Establish regular penetration testing.
6. Create a formal data retention schedule.
7. Maintain a vendor risk register.
8. Establish recurring compliance reporting.

References

- Protection of Personal Information Act, 2013.
- Consumer Protection Act, 2008.
- Children’s Act, 2005.
- European Commission GDPR guidance.
- California CCPA/CPRA guidance.
- European Commission and ENISA NIS2 guidance.