Rflect AG
Technical and Organisational Measures (TOM)

pursuant to Art. 32 GDPR and Art. 8 revFADP in conjunction with Art. 1-6 DSV
Version 16 June 2026

Provider	Rflect AG, Neunbrunnenstrasse 118, 8050 Zurich, Switzerland
Contact	Niels Rot, Co-Founder, info@rflect.ch
Hosting	AWS, Frankfurt region (eu-central-1). AI inference exclusively in EU regions via AWS Bedrock.

This document describes the technical and organisational measures that Rflect AG, acting as data processor (Art. 28 GDPR / Art. 9 revFADP), has implemented to ensure data security. The infrastructure used (AWS) is certified to ISO/IEC 27001, 27017, 27018, 27701, 42001, SOC 2 Type 2 and BSI C5 Type 2; AWS Bedrock falls within the scope of these certifications.

1. Confidentiality

Area	Measure
Physical access	Pure cloud architecture with no own data centres. Physical security of the AWS data centres in Frankfurt (24/7 monitoring, multi-level access control, biometrics) per AWS SOC 2.
Authentication	End users: email/password (scrypt hashing), LTI 1.3 with OIDC launch. Administrators: mandatory MFA for AWS, repository and deployment pipeline.
Authorisation (RBAC)	Differentiated roles for students, lecturers and institutional admins on a need-to-know basis. Direct access to production infrastructure is limited to a few IAM accounts and logged via CloudTrail.
Hardware isolation	AWS ECS on the Nitro System: no SSH access and no exec access at container level. Host access only via bastion, restricted to a clearly defined group of people. Independently assessed by NCC Group in 2023 (public report).
Pseudonymisation	Monitoring and research are carried out in aggregate by user type/programme; no routine personal-level analysis. Web analytics is cookieless.

2. Integrity

Area	Measure
Encryption in transit	TLS 1.2+ for all transmissions (web, API, LTI, mobile). Weak cipher suites disabled.
Encryption at rest	AES-256 for the database (RDS), file storage (S3) and backups.
Input and audit control	HTTP requests are logged in CloudWatch (timestamp, account ID, method, status). Security-relevant operations such as password resets, account and programme deletions are additionally recorded in the database with a timestamp and the executing account ID. CloudWatch logs are encrypted in the EU region; access only for authorised personnel.
Application security	Server-side input validation; established safeguards against SQL injection, XSS and CSRF. Database in a private VPC subnet, not publicly accessible.

3. Availability and resilience

Area	Measure
High availability	AWS operation across multiple Availability Zones (RDS Multi-AZ, ECS across multiple AZs); capacity is scaled on demand via Infrastructure as Code.
Protective measures	AWS Shield Standard (Layer 3/4 DDoS), AWS Web Application Firewall with rate limiting, technical alerts for defined error conditions.
Backup and recovery	Daily automated DB backups with point-in-time recovery; encrypted storage across multiple AZs in the EU region. Documented restore procedure in which deletions made between the backup date and the restore date are re-applied, so that data deleted at the request of the controller or users is not reintroduced into the production environment by a restore (cf. DPA §4.2). Infrastructure as Code enables reproducible rebuilds.

4. Procedures for regular review

Area	Measure
Data protection management	Responsibility with the management; operational implementation by Engineering and Operations. A DPA is in place with all institutional customers.
Vulnerability and patch management	Automated dependency and vulnerability scanning (Dependabot, govulncheck) in the CI pipeline; critical security updates can be rolled out at short notice.
Code quality	All changes undergo peer review in the pull-request process. Strict separation of staging and production environments.

5. Sub-processors

The database (PostgreSQL on AWS RDS) is located in eu-central-1 in a private VPC subnet. All primary data processing takes place within the EU.

Provider	Location	Purpose	Transfer safeguard
AWS	EU, primarily Frankfurt	Compute (ECS), database (RDS), storage (S3), AI inference for feedback (Bedrock, EU inference profile; transient, not persisted), email delivery (SES), push notifications (SNS), speech-to-text for voice memos (Transcribe)	Processing within the EU
Friendly Analytics	Switzerland	Web analytics, cookieless, no targeted tracking of personal data	CH provider, CH servers
Sentry	EU (de.sentry.io)	Error monitoring, personal data reduced via URL scrubbing	Processing within the EU
Pipedrive	EU Frankfurt	CRM, transmission of sign-up, programme and invitation events (lecturers/students) via webhook	Processing within the EU

6. Data breaches and incident response

Area	Measure
Past incidents	No known reportable data breaches since founding.
Process	Containment, assessment, notification of the controllers without undue delay and in any case within 24 hours of becoming aware, root-cause analysis, remediation. Controllers are informed in good time so that they can meet their notification obligations under Art. 33 GDPR / Art. 24 revFADP.

7. AI-specific measures

Area	Measure
Models	Anthropic Claude via AWS Bedrock, inference only, no fine-tuning, no training on customer data.
Contractual guarantees	AWS Bedrock stores neither prompts nor completions. Anthropic has no operational access to Bedrock prompts or responses; the models run on AWS-managed infrastructure. Under the Bedrock Commercial Terms, Anthropic may not train models on customer data.
EU inference	All AI inference runs via the EU inference profile of AWS Bedrock; data remains within the AWS network inside the EU. To reduce latency and cost, the prompt may be held in an ephemeral, encrypted prompt cache within the EU inference environment for up to one (1) hour, after which it is automatically deleted. No prompts or responses are stored permanently.
Student privacy	Rflect staff do not read private reflections in normal operations. AI processing of private reflections takes place only if students activate the feature. Research only with explicit consent. AI-supported features for lecturers on shared content (e.g. Rflect TA) are part of the lecturer toolset.

8. Retention and deletion

Area	Measure
Technical logs	90 days; encrypted in CloudWatch (EU region).
Contract / master data	10 years (statutory Swiss retention periods).
End of contract	At the end of the contract, productive institutional data is deleted. Backups are retired within their retention period (snapshots 14 to 30 days, weekly snapshots 365 days).
Right to erasure	Individual requests (Art. 17 GDPR / Art. 32 revFADP) are handled promptly. Private reflections are deleted at the end of the contract or, at the user's option, returned to the user, and never released to the institution.
Data portability and account migration	Users can export or migrate the content they have authored (reflections regardless of sharing status, as well as feedback addressed to them) without the institution's consent. If the institution removes or deactivates an account, deletion of the self-authored data is held for 30 days so that users can export or migrate it (cf. DPA §3.6).

9. Organisational measures

Area	Measure
Confidentiality	Employees are subject to the statutory duty of loyalty, including confidentiality (Art. 321a CO).

Area	Measure
Awareness	Regular staff awareness training on data protection and information security.
Departure	Immediate revocation of all access upon an employee's departure.
Supplier management	Sub-processors are selected according to data-protection and security criteria (EU hosting preferred, established providers with their own compliance programmes). Providers' data-processing agreements (including EU Standard Contractual Clauses where applicable) apply.

These measures are reviewed regularly and adapted to technology and the threat landscape. The current version is available at any time from info@rflect.ch.